TLP: WHITE

APCERT Annual Report 2018

APCERT Secretariat
E-mail: apcert-sec@apcert.org URL: http://www.apcert.org

CONTENTS

Chair's Message 2018

The Australian Cyber Security Centre (ACSC), (formerly CERT Australia) was honoured to be re-elected Chair of the APCERT Steering Committee (SC) for a fourth and final term at the APCERT Annual General Meeting in Shanghai, China in October 2018.

The commitment and dedication of APCERT Members and Partners to a safe, clean and reliable cyber space in the Asia Pacific Region is something we should all be proud of. I would also like to recognise and thank my fellow APCERT SC Members—Cyber Security Malaysia (Deputy Chair), JPCERT (Secretariat), CNCERT/CC, CERT-In, KrCERT and TWNCERT—for their tireless efforts and enthusiasm in making APCERT a dedicated community of cooperation and collaboration.

Our community was committed to our collective ability to detect, prevent and mitigate malicious cyber activity. We shared threat information, conducted training and workshops and cooperated through our numerous Working Groups, two of which were established in 2018—the IoT Security WG and the Secure Digital Payment WG.

I would like to thank all participants for your contributions, but wish to particularly thank our Working Group Conveners for all your efforts and achievements.

The APCERT AGM and Conference, held in October last year in Shanghai, was a resounding success.

I would particularly like to thank CNCERT/CC for organising and hosting this event. There were many interesting presentations and talks at the conference and some great outcomes; we agreed to amend the Operational Framework to better define a quorum and voting procedures at AGMs; and for the first time we partnered with the Forum of Incident Response Security Teams to deliver a FIRST Regional Symposium, directly after the Conference.

APCERT Members and Partners participated in a number of collaborative face-to-face events throughout the year, including at APRICOT, the FIRST Conference, and a number of Member's national conferences and events.

These face-to-face meetings are important in building trust within our community and I thank Microsoft for its ongoing support in providing fellowship grants to enable these engagements.

On behalf of all APCERT Members I would like to express my gratitude to ThaiCERT and the DRILL WG for planning and running the 2018 APCERT Cyber Drill, which was

themed 'Data Breach via Malware on IoT'. The scenario simulated an attack on the medical sector where the initial compromise was followed with exfiltration of data and infection of IoT devices.

The drill theme demonstrates APCERT's mature approach to addressing contemporary cyber security issues within the region.

APCERT also welcomed The Organisation of Islamic Cooperation CERT (OIC-CERT) again to the Cyber Drill and I thank them for their continued participation in our activities.

Finally, I would like to recognise and thank JPCERT for continued dedication as the Secretariat. JPCERT has fulfilled this role since becoming a founding member of in 2003, and they have maintained outstanding commitment and support to our community throughout their tenure.

In 2019 the ACSC looks forward to working with APCERT Steering Committee Members, the new APCERT Steering Committee Chair when they are elected at the 2019 AGM in Singapore, and with all APCERT Members and Partners.

It has been a privilege to serve as Steering Committee Chair for four years, and we are excited about our continued active participation in the APCERT community in 2019 and beyond!

Andrea Wood
Chair, APCERT SC
Australian Cyber Security Centre

I. About APCERT

1. Objectives and Scope of Activities

The Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) within the Asia Pacific region. The organisation was established in February 2003 with the objective of encouraging and supporting the activities of CERTs/CSIRTs in the region.

APCERT maintains a trusted network of cyber security experts in the Asia Pacific region to improve the region's awareness of malicious cyber activity and its collective ability to detect, prevent and mitigate such activity through:

1. Enhancing the Asia Pacific's regional and international cooperation on cyber security;
2. Jointly developing measures to deal with large-scale or regional network security incidents;
3. Facilitating information sharing and technology exchange on cyber security among its members;
4. Promoting collaborative research and development on subjects of interest to its members;
5. Assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response; and
6. Providing inputs and/or recommendations to help address legal issues related to cyber security and incident response across regional boundaries.

APCERT approved its vision statement in March 2011 – "APCERT will work to help create a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration." Cooperating with our partner organisations, we are now working towards its actualisation.

The formation of CERTs/CSIRTs at the organisational, national and regional levels is essential to the effective and efficient response to malicious cyber activity, widespread security vulnerabilities and incident coordination throughout the region. One important

role of CERTs/CSIRTs is building cyber security capabilities and capacity in the region, including through education and training to raise awareness and encourage best practices in cyber security. APCERT coordinates activities with other regional and global organisations, such as:

- Asia Pacific Network Information Centre (APNIC: www.apnic.net);
- Forum of Incident Response and Security Teams (FIRST: www.first.org);
- Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT: www.oic-cert.net);
- STOP. THINK. CONNECT program (www.stopthinkconnect.org/).

The geographical boundary of APCERT activities is the same as that of the Asia Pacific Network Information Centre (APNIC). The region covers the entire Asia Pacific, comprising of 56 economies. The list of those economies is available at: www.apnic.net/about-APNIC/organization/apnics-region

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia Pacific region, and its membership has continued to increase since then. For further information on the APCERT membership structure and criteria, please refer to the APCERT Operational Framework: https://www.apcert.org/documents/pdf/APCERT%20Operational%20Framework%20-%20Oct%202018.pdf

As of December 2018, APCERT consists of 30 Operational Members from 21 economies across the Asia Pacific region and 3 Corporate Partners.

Operational Members (30 Teams / 21 Economies)

Team	Official Team Name	Economy
ACSC	Australian Cyber Security Centre	Australia
AusCERT	Australian Computer Emergency Response Team	Australia
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team	Bangladesh

BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
BtCIRT	Bhutan Computer Incident Response Team	Bhutan
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CERT-In	Indian Computer Emergency Response Team	India
CERT NZ	CERT NZ	New Zealand
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
EC-CERT	Taiwan E-Commerce Computer Emergency Response Team	Chinese Taipei
GovCERT.HK	Government Computer Emergency Response Team Hong Kong	Hong Kong, China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
ID-SIRTII/CC	Indonesia Security Incident Response Team of Internet Infrastructure/Coordination Center	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
LaoCERT	Lao Computer Emergency Response Team	Lao People's Democratic Republic
mmCERT/CC	Myanmar Computer Emergency Response Team	Myanmar
MNCERT/CC	Mongolia Cyber Emergency Response Team / Coordination Center	Mongolia
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macao
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
MyCERT	Malaysian Computer Emergency Response Team (CyberSecurity Malaysia)	Malaysia
SingCERT	Singapore Computer Emergency Response Team	Singapore

Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
TechCERT	TechCERT	Sri Lanka
ThaiCERT	Thailand Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

Corporate Partners (3 Teams) *formerly referred to as Supporting Members

- Bkav Corporation
- Microsoft Corporation
- SecureWorks

Chair, Deputy Chair, Steering Committee (SC) and Secretariat

At the APCERT AGM 2018, ACSC was re-elected as Chair of APCERT, and Malaysian Computer Emergency Response Team (MyCERT, CyberSecurity Malaysia) as Deputy Chair.

Terms of each Steering Committee (SC) member are as follows:

Team	Term	Other positions
ACSC	2018 - 2020	Chair
CERT-In	2017 - 2019	
CNCERT/CC	2018 - 2020	
JPCERT/CC	2017 - 2019	Secretariat
KrCERT/CC	2018 - 2020	
MyCERT (CyberSecurity Malaysia)	2017 - 2019	Deputy Chair
TWNCERT	2018 - 2020	

3. Working Groups (WG)

There are currently nine (9) Working Groups (WGs) in APCERT.

1) TSUBAME WG (formed in 2009)

- Objectives:

- Establish a common platform for Internet threat monitoring, information sharing and analyses for the Asia Pacific region and others
- Promote collaboration among the CSIRTs in the Asia Pacific region and others using the platform, and
- Enhance the capability of global threat analyses by incorporating 3D Visualization features to the platform.

- Secretariat (1): JPCERT/CC
- Members (24): AusCERT, bdCERT, BruCERT, CamCERT, CCERT, CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, ID-SIRTII/CC, KrCERT/CC, LaoCERT, maCERT, mmCERT, MNCERT, MOCERT, MonCIRT, MyCERT (CyberSecurity Malaysia), NCA-CERT, PHCERT, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

2) Information Sharing WG (formed in 2011)

- Objectives:
  - Improve information and data sharing within APCERT, including by improving members' understanding of the value of data sharing and motivating APCERT members to exchange information and data
  - Organize members to establish and enhance the necessary mechanisms, protocols and infrastructures to provide a better environment for members to share information and data
  - Help members to better understand the threat environment and share data to improve each team's capability as well as the cyber security of their constituent networks, and
  - Work as the Point of Contact (PoC) for APCERT to other organizations on information sharing.
- Convener (1): CNCERT/CC
- Members (15): AusCERT, Bkav, CERT-In, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, Microsoft, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC. TWNCERT, VNCERT

3) Membership WG (formed in 2011)

- Objectives:
  - Promote collaboration and participation by all APCERT members

- Establish the organizational basis to enhance the partnership with cross-regional partners and supporters
- Guide activities such as checking and monitoring for sustaining the health of the membership structure, and
- Promote harmony and cooperation among APCERT members.

- Convener (1): KrCERT/CC
- Members (12): AusCERT, BruCERT, CNCERT/CC, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, MOCERT, MyCERT (CyberSecurity Malaysia), Sri Lanka CERT|CC, TechCERT, VNCERT

4) Policy, Procedure and Governance WG (formed in 2013)

- Objectives:
  - Promote the Vision and Mission of APCERT through the development and coordination of policies and procedures for APCERT and provision of advice on governance issues
  - In consultation with the SC, periodically review the Operational Framework to ensure it continues to meet its intended effect, and provide advice to the SC
  - Review associated policies and procedures as they relate to the Operational Framework (also known as sub-documents), and supplement these with guidelines or other documents as needed
  - Identify and resolve issues relating to APCERT policies, procedures and governance, including through referring them to the SC or APCERT membership where appropriate, and
  - Undertake other activities related to policy, procedures and governance for APCERT as directed by the SC.
- Convener (1): ACSC
- Members (6): HKCERT, JPCERT/CC, KrCERT/CC, MOCERT, MyCERT (CyberSecurity Malaysia), Sri Lanka CERT|CC

5) Training WG (formed in 2015)

- Objectives
  - Establish an overall training program to assist members to develop, operate, and improve their incident management capabilities
  - Provide a channel for members to share and exchange valuable experiences

with other member teams at regular intervals, and

- Nurture cooperation and collaboration among members, providing training activities such as conducting online and face to face technical workshops to enhance fellow members' cyber security capabilities and capacities in mitigating cyber incidents more efficiently and effectively.

- Convener (1): TWNCERT
- Members (11): CERT-In, CNCERT/CC, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, MOCERT, MonCIRT, Sri Lanka CERT|CC, ThaiCERT, TWCERT/CC

6) Malware Mitigation WG (formed in 2016)

- Objectives
  - Share information on the malware infections of each participating economies to analyse type of malware infecting the economies as the character and motive of each infection may differ from one to another;
  - Share the resources for the initiatives taken in reducing the number of malware infections, including potential funding, cost, personnel and time; and
  - Increase collaborative efforts in mitigating malware infections affecting APCERT economies – as a group, collaboration among economies is easier as trust has been created for information sharing in mitigating malware infection.
- Convener (1): MyCERT (CyberSecurity Malaysia)
- Members (11): BruCERT, GovCERT.HK, HKCERT, ID-CERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TWCERT/CC, Bkav Corporation, SecureWorks

7) Drill WG (formed in 2017)

- Objectives
  - To serve as a permanent Organizing Committee for the annual cyber drills and assist the Lead Organizing CERT
  - To maintain centralized documentation for the drills, their working documents, procedures, handbooks and feedback.
  - To allow continuous improvements.
- Convener (1): ThaiCERT

- Members (12): ACSC, AusCERT, CERT-In, HKCERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

8) IoT Security WG (formed in 2017)

- Objectives
  - Propose steps to address the security issues including vulnerabilities tailored for some of the priority sectors.
  - Incident response mechanisms/measures for responding to cyber physical security incidents impacting human life.
  - Discussions on existing Security Standards and gaps for IoT Ecosystem and considerations for adoption in specific sector.
- Convener (1): CERT-In
- Members (7): BGD e-GOV CIRT, CERT-In, CERT NZ, HKCERT, IDSIRTII/CC, JPCERT/CC, VNCERT

9) Secure Digital Payment WG (formed in 2017)

- Objectives
  - Understand the products and services as well as the infrastructure and platforms in the digital payments space.
  - Understand the digital payment ecosystem / supply chain
  - Incident response mechanisms/measures for responding to cyber security incidents impacting digital payments.
- Convener (1): CERT-In
- Members (5): BGD e-GOV CIRT, CNCERT/CC, HKCERT, JPCERT/CC, Sri Lanka CERT|CC

4. APCERT Website

In its role as the APCERT Secretariat, JPCERT/CC manages and updates the APCERT website: https://www.apcert.org/.

II. APCERT Activity Report 2018

1. International Activities and Engagements

APCERT has been dedicated to represent and promote APCERT activities in various international conferences and events. From January to December 2018, APCERT Teams have hosted, participated and/or contributed in the following events:

- AP* Retreat Meeting (24 February – Kathmandu, Nepal)
  APCERT Chair and Secretariat attended the AP* Retreat Meeting which was held in conjunction with APRICOT 2018 and presented activities of APCERT to the community.

- APCERT Drill 2018 (7 March)
  https://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf
  APCERT Drill 2018, the 14th APCERT Cyber Exercise Drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. Pursuant to the Memorandum of Understanding on collaboration between APCERT and the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) in September 2011, APCERT invited the participation from OIC-CERT Teams for the third time. 27 teams from 20 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam), and 5 teams from 5 economies of OIC-CERT (Egypt, Morocco, Nigeria, Oman and Pakistan) participated in the Drill. The theme of the drill was "Data Breach via Malware on IoT".

- APEC-TEL 57 (3 – 8 June – Port Moresby, Papua New Guinea)
  APCERT participated APEC TEL 57 and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- 30th Annual FIRST Conference (24 - 29 June – Kuala Lumpur, Malaysia)
  https://www.first.org/conference/2018/

APCERT Teams attended the Annual FIRST Conference in Kuala Lumpur, Malaysia, and shared valuable experience and expertise through various presentations.

- National CSIRT Meeting (29 - 30 June – Kuala Lumpur, Malaysia)
  APCERT teams attended the National CSIRT Meeting, hosted by CERT/CC and exchanged various activity updates as well as recent projects and research.

- ASEAN CERT Incident Drill (ACID) 2017 (5 September)
  ACID 2018, led and coordinated by SingCERT, entered its 13th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing an opportunity for teams to improve their skills on investigating and responding to ransomware incident, including malware analysis to uncover its characteristics and subsequently escalating to the necessary parties for mitigation.

- APCERT Annual General Meeting (AGM) & Conference 2018 (21 – 24 October - Shanghai, China)
  http://apcert2018.cert.org.cn/
  The APCERT Annual General Meeting (AGM) & Conference 2018 was held on 21 – 24 October, 2018 at The Westin Bund Center Shanghai, China.

  Programme Overview:

21 October (Sun)	AM:	Working Group Meetings
	PM:	APCERT Team Building, Welcome Cocktail
22 October (Mon)	AM:	Training (Microsoft)
	PM:	Steering Committee Meeting
23 October (Tue)	AM:	APCERT Closed Conference
	PM:	APCERT Annual General Meeting
24 October (Fri)	AM:	Open Conference

- APEC-TEL 58 (28 September – 5 October – Taipei, Chinese Taipei)
  APCERT participated at APEC TEL 58 and presented the APCERT's overview and latest activities including the coming APCERT 2018 AGM and new APCERT Working Groups.

Other International Activities and Engagements

- **DotAsia**

  APCERT serves as a member of the Advisory Council of DotAsia to assist in policy development and relevant community projects. HKCERT represented APCERT in attending the meetings of the Advisory Council.

- **Forum of Incident Response and Security Teams (FIRST)**

  Koichiro Komiyama of JPCERT/CC has served as a member of FIRST.org Board of Directors since June 2014 to June 2018.

- **STOP. THINK. CONNECT (STC)**

  APCERT has collaborated with STOP. THINK. CONNECT (STC) under a Memorandum of Understanding since June 2012 in order to promote awareness towards cyber security and more secure network environment.

- **Asia Pacific Network Information Security Centre (APNIC)**

  APCERT and Asia Pacific Network Information Centre (APNIC) signed a Memorandum of Understanding in 2015.

2. APCERT SC Meetings

From January to December 2018, SC members held 5 teleconferences and 2 face-to-face meeting to discuss APCERT operations and activities.

16 January	Teleconference
23 February	Face-to-face meeting concurrently held at APRICOT 2018 in Kathmandu, Nepal
18 April	Teleconference
12 July	Teleconference
6 August	Teleconference
20 September	Teleconference
22 October	Face-to-face meeting at APCERT AGM 2018 in Shanghai, China
17 December	Teleconference

3. APCERT Training

APCERT held five (5) training calls and one (1) training workshop in 2018 to exchange technical expertise, information and ideas.

Date	Title	Presenter
6 February	Malware Information Sharing Platform (MISP) in a CERT	AusCERT
3 April	Analyses of A Compromised Linux Server	APNIC
5 June	Performing Forensics on and Azure Virtual Machine	Microsoft
7 August	Shaoye Botnet – Android Malware & DNS Hijacking	TWNCERT
21 October	Digital Forensics with a Focus on the Cloud (Workshop)	Microsoft
4 December	Inside the APCERT Drill: Player, Observers, EXCON and OC Confirmation	AusCERT

For further information on APCERT, please visit the APCERT website or contact the APCERT Secretariat as below.

URL: https://www.apcert.org/

Email: apcert-sec@apcert.org.

III. Activity Reports from APCERT Members

ACSC

Australian Cyber Security Centre – Australia

1. Highlights of 2018

1.1 Summary of major activities

In 2018 CERT Australia transitioned from Australia's Attorney-General's Department to become part of the Australian Cyber Security Centre (ACSC). The ACSC now provides Australia's national Computer Emergency Response Team (CERT) and has replaced CERT Australia within the APCERT community. A high point for the ACSC was working with the APCERT community as Chair of the APCERT Steering Committee. In October 2018, the ACSC was re-elected to the APCERT Steering Committee and subsequently as Chair of the Committee for a fourth and final term.

1.2 Achievements & milestones

The Australian Government announced that from 1 July 2018, the ACSC would become a part of the Australian Signals Directorate (ASD), incorporating the functions of both CERT Australia and the Digital Transformation Agency's cyber security responsibilities. The ACSC has been established as the credible and authoritative voice on cyber security in Australia and is the main Australian contact focusing on cyber security risks for:

- the community;
- businesses, small, medium and large; and
- federal, state and territory governments.

The ACSC has established a 24/7 Global Watch to implement and strengthen constant monitoring and early warning capability around emerging cyber threats and incidents. In February 2018, the ACSC stood up the 24/7 Global Watch to work with partners across domestic and international governments and industry to undertake projects related to real-time integration of multi-source information and shared situational awareness. The key outcome of this collaboration is the establishment of a real-time cyber threat detection and notification capability that will underpin a National Cyber Security Situational Awareness Program.

The Prime Minister formally launched the new ACSC on 16 August 2018, at its

purpose-built headquarters in Canberra, to support cooperation, coordination and collaboration between cyber security experts across the private sector, government and research community.

A key initiative of Australia's 2016 *Cyber Security Strategy* was the establishment of Joint Cyber Security Centres (JCSCs) in Brisbane, Sydney, Melbourne, Perth and Adelaide. The Perth and Adelaide JCSCs were launched in 2018, two years ahead of schedule.

The Centres bring together people from business, the research community and government agencies in collaborative and trusted environments, to support information-sharing and network-hardening activities.

- JCSCs build and run regular capture the flag (CTF) activities with critical infrastructure and industry partners. Based on real-world incidents, the CTF activities put the participants in the role of an incident responder and let them test their skills as if they were facing an Advanced Persistent Threat (APT) actor. CTFs also feed into other uplift activities including training courses and 'how to' workshops where both technical and non-technical participants walk through the exercises, learning vital incident response skills. CTFs are run at many JCSC events including centre openings, industry events, conferences and competitions.

The ACSC continues its work in support of Australia's International Cyber Engagement Strategy with the goal of achieving a strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community.

2. About ACSC

2.1 Introduction

The ACSC brings cyber security capabilities from across the Australian Government together into a single location. It is the hub for private and public sector collaboration and information-sharing to combat cyber security threats.

The ACSC's vision is to make Australia the safest place to connect online, by:

- **Leading Cyber Security**. The ACSC is a trusted national asset that positively affects cyber security awareness and behaviours.

- **Countering Cyber Enabled Threats**. The ACSC aims to improve understanding of malicious cyber actors operating within Australia to better thwart the threat.
- **Providing Trusted Advice & Expertise**. The ACSC engages consistently and professionally with stakeholders across the Australian economy to boost national cyber security and resilience.

The ACSC is Australia's national CERT and will continue to work with traditional and international CERT partners. The ACSC will continue CERT Australia's support for critical infrastructure and systems of national interest, and the new ACSC structure will enable access to cyber security expertise from government and industry.

2.2 Establishment

The ACSC began operating in November 2014, bringing together staff from ASD, CERT Australia, DTA, Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), Australian Security Intelligence Organisation (ASIO) and Defence Intelligence Organisation (DIO).

Following the 2017 Independent Intelligence Review, the Government identified a need to provide enhanced cyber security capabilities and a single point of advice and support on cyber security.

On 1 July 2018, ASD became a Statutory Agency and the ACSC transformed, merging together with CERT Australia and the DTA Cyber Security Office under Machinery of Government changes. As part of this change, the JCSC program transitioned to the ACSC. During 2018, as a key deliverable under the 2016 Australian *Cyber Security Strategy*, the ACSC moved into a new, purpose-built facility, bringing together for the first time the operational and policy cyber capabilities from across Australian Government.

2.3 Resources

There are several hundred staff, including partner agencies and cyber policy staff from the Department of Home Affairs housed in the ACSC and JCSCs.

2.4 Constituency

The ACSC's remit has grown to encompass improving cyber resilience across the

whole-of-economy including critical infrastructure and systems of national interest, federal, state, territory and local governments, small and medium business, academia, the not-for-profit sector and the Australian community. Former CERT Australia and ASD services and advice were consolidated during the latter half of 2018 and are now delivered by the ACSC.

3. Activities & Operations

3.1 Scope and definitions

The ACSC's key activities include:

- response to cyber security threats and incidents;
- collaboration with the private and public sector, as well as international partners, to share information on threats and increase resilience;
- working with governments, industry and the community to increase awareness of cyber security; and
- providing information, advice and assistance to all Australians.

3.2 Incident handling

In 2018 the ACSC triaged a large number of incidents ranging from low-level malicious attacks on individuals and small businesses to more sophisticated incidents affecting large business.

Not all organisations need the ACSC's help in addressing these cyber security issues, however services such as the Australian Internet Security Initiative (AISI) and the ACSC 24/7 hotline are helping Australians identify when they may be exposed to risk online.

3.3 Publications

The ACSC publishes cyber security alerts and advisories. These alerts and advisories contain up-to-date information on cyber threats and software vulnerabilities and steps that can be taken to improve computer network and system security.

3.4 New services

24/7 Global Watch

In February 2018, a 24/7 cyber incident monitoring and response capability was established. This team takes a whole-of-economy approach and includes outreach to

industry and government partners through provision of near real time alerts and 24/7 media and crisis communications support. The initial operating capability was delivered in advance of the 2018 Commonwealth Games on the Gold Coast.

ACSC Cyber Newsroom

The ACSC 24/7 Cyber Newsroom provides media relations, content development and publishing services. The Newsroom's mission is to position the ACSC as the Australian Government's authoritative source of information on cyber security awareness, prevention and response. The Newsroom uses the ACSC's communication channels including the cyber.gov.au website and social media, to build relationships with thought leaders, researchers, and national and international media.

This work program is shaping the public narrative on cyber, providing advice and information to Australian individuals, governments and businesses to help make Australia the safest place to connect online. A number of significant national and international cyber security incidents and events saw the ACSC's media profile surge between its launch in August 2018 and the end of the calendar year.

The Managed Service Provider Partner Program (MSP³)

MSP³ is an ACSC initiative that assists Australian businesses to protect themselves from cyber threats. MSP³ was announced in response to the global compromise of managed service providers (MSPs). The program is designed to improve the cyber security practices of MSPs in Australia and grow a new culture of continual improvement through a 12-month engagement program. Underpinning the MSP³ framework are the eight *Managed Service Provider Better Practice Principles*, which provide the guiding rules of action to enable businesses to improve their cyber resilience. MSP³ also includes periodic evaluation activities that assess the cyber security posture and resilience of the participating MSPs and their customer base.

4. Events organized / hosted

4.1 Training

The ACSC developed and delivered a range of cyber security exercise training courses nationally in 2018. Participants included government and industry partners.

4.2 Drills and exercises

The ACSC developed, facilitated and participated in a range of cyber security exercises

nationally in 2018, including government and industry partners.

4.3 Conferences and seminars

The ACSC hosted its annual ACSC Conference in Canberra in March 2018, bringing together more than 1,000 cyber security experts from Australia and overseas to discuss the latest trends, mitigations and advances in cyber security.

5. International Collaboration

5.1 International partnerships and agreements

The ACSC remains committed to being a valued and active contributor to the APCERT community.

The Australian International Cyber Engagement Strategy (ICES), released in 2017, outlined ways in which Australia would enhance international partnerships. Under the Strategy, the ACSC is strengthening and expanding its network of international relationships, especially in the Asia-Pacific region.

- Announced under the ICES, Australia has been working with regional partners in the Pacific as a member of the Pacific Cyber Security Operational Network (PaCSON). PaCSON had its inaugural meeting in Brisbane in May 2018, which included an annual general meeting (AGM), information exchange and cyber security workshops. PaCSON Member countries are Australia, Fiji, Tonga, Samoa, Solomon Islands, Papua New Guinea, Palau, Kiribati, Niue, Vanuatu, Tokelau, Cook Islands, Tuvalu, Marshall Islands and New Zealand.

5.2 Capacity building

ICES outlines a commitment to assist partners in the Asia-Pacific develop their capacity to address cyber threats, strengthen cyber security and combat cybercrime through the Cyber Cooperation Program (CCP). The CCP was designed to boost the resources behind Australia's cyber capacity building efforts. Please refer:
https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html

5.2.1 Drills & exercises

The ACSC participated in and observed six international cyber security exercises in 2018, including the APCERT Drill.

5.2.2 Seminars & presentations

The ACSC attended the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Nepal in February and chaired the APCERT Conference in Shanghai in October 2018.

5.3 Other international activities

Throughout 2018, the ACSC also presented at and/or participated in several other international forums including:

- RSA Security Conference – USA
- FIRST Conference; National CSIRTs Meeting ('Second Conference') and Global Forum for Cyber Expertise – Malaysia
- Blackhat & DefCon – USA
- Other closed events organised by international government organisations and CERTs.

6. Future Plans

6.1 Future projects

The ACSC's 24/7 Situational Awareness capability uses global all-source monitoring tools to detect and validate potential, imminent or emerging cyber threats and trends to provide early warning at speed to stakeholders.

This activity seeks to identify and communicate the means, motives and technologies behind malicious cyber threats.

The ACSC is developing a new critical infrastructure, sector-based product series that provides relevant and consumable information for C-suite executives, enabling timely and informed decisions about cybersecurity requirements based on their sector's risk profile.

The product will provide a high-level overview of the cyber security environment, case studies, cyber crime and cyber security incident statistics.

6.2 Future Operation

The ACSC will continue to expand and focus on taking a whole-of-economy approach to cyber security and ensuring Australia is a safe place to connect online. The ACSC's focus on international partnerships and collaboration will remain a priority.

7. Conclusion

The ACSC is expanding its capacity, significantly increasing operations and its ability to engage internationally. APCERT continues to be a major focus for the ACSC.

The ACSC values its ongoing engagement with the APCERT community and remains an active and collaborative member.

AusCERT

Australian Computer Emergency Response Team – Australia

1. Highlights of 2018

1.1 Summary of major activities

AusCERT continues to deliver sought after computer security incident handling and early warning information, whilst engaging members in cyber security.

1.2 Achievements & milestones

1.2.1 Production run of the Education Sector MISP Implementation

The AusCERT instance of Malware Information Sharing Platform (MISP), for the Education Sector proved itself in 2017 and was placed in full production in 2018.

1.2.2 Constituency growth

AusCERT, with a membership-based constituency, has increased the breadth of organisations that it serves.

1.2.3 Increased Capacity.

AusCERT has expanded its operational capacity providing more information and allowing to work on capability improvement projects of which will be able to be rolled out in 2019 that will improve the value of AusCERT to its constituency.

2. About AusCERT

2.1 Introduction

AusCERT is a leading Cyber Emergency Response Team for Australia and provides information security advice to its members, including the higher education sector. As a not-for-profit security group based at the University of Queensland's (UQ) Information Technology Services (ITS), AusCERT is the single point of contact for dealing with cyber security incidents affecting or involving member networks. AusCERT helps members prevent, detect, respond to and mitigate cyber and Internet based attacks.

2.2 Establishment

AusCERT was officially established on 8 March 1993 through the collaboration of three Brisbane based universities, including the University of Queensland.

Formed in 1993, AusCERT is one of the oldest CERTs in the world and was the first CERT in Australia to operate as the national CERT, which it did until 2010.
Over time, as the Internet grew, and government, business and ordinary users began to use the Internet for daily communications and business, AusCERT's focus changed from being university centric to include the interests of all sectors.

2.3 Resources

AusCERT is self-funded and covers its operating costs through a variety of sources including member subscriptions, the annual AusCERT conference and service contracts.
As an active member of the Forum for Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), AusCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis.

2.4 Constituency

AusCERT is a member-based organization and its constituents consist of private, government and education businesses.
AusCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT).

3. Activities & Operations

3.1 Scope and definitions

AusCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.
Services provided are listed as:

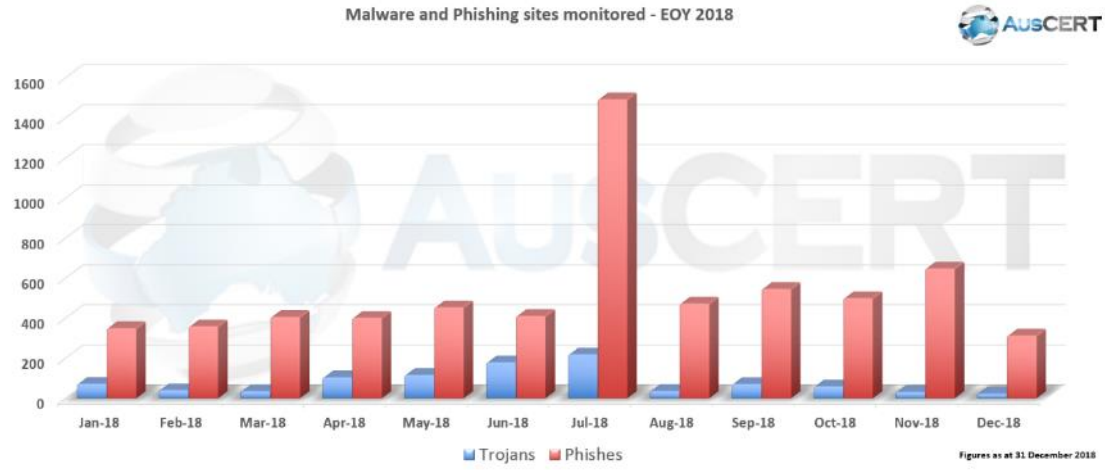
- Incident Management [3.2], https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service [3.3]

https://www.auscert.org.au/services/early-warning-service/

- Malicious URL Feed [3.4]
  https://www.auscert.org.au/services/malicious-url-feed/
- Member security incident notification's (MSINs)[3.5.1]
  https://www.auscert.org.au/services/security-incident-notifications/
- Phishing take-down [3.6]
  https://www.auscert.org.au/services/phishing-take-down-service/
- Security Bulletin Service [3.7]
  https://www.auscert.org.au/bulletins/
- Leaked Credential Service [3.8]
- AusCERT's member only IRC channel
- AusCERT Conference [4.1]
  https://conference.auscert.org.au/
- AusCERT Certificate Service
  https://cs.auscert.org.au/

3.2 Incident Management Service

AusCERT's Incident Management Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AusCERT's subscription services.



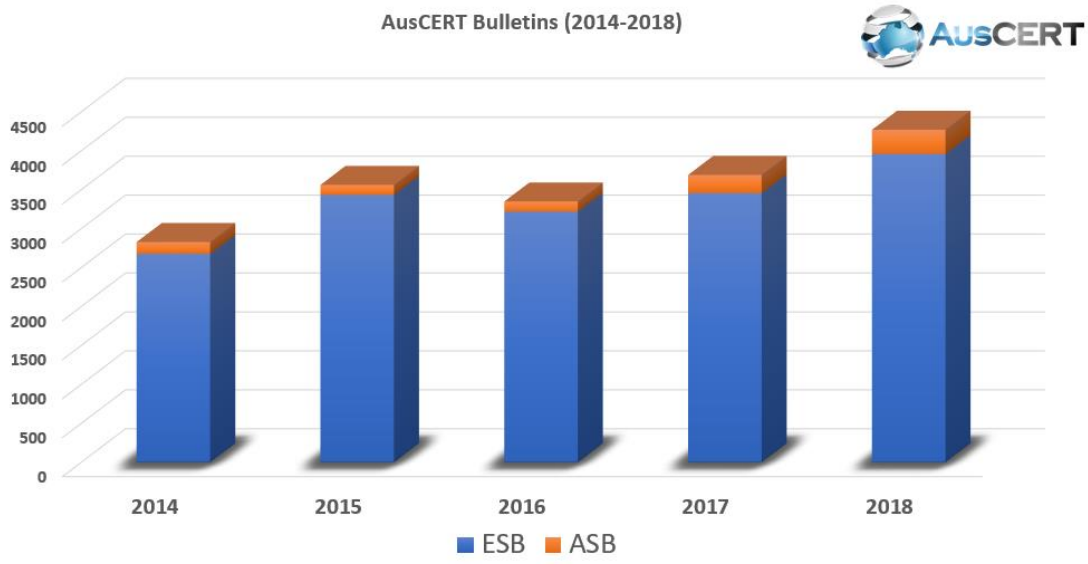
The above diagram is the statistics of incidents that required handling either of phish site or that of malware, for the calendar year of 2018. These tallies are sites that are located around the world that, when interacted with, affects the security of the constituency that AusCERT is serving.

3.3 Early Warning System

Members can subscribe to receive urgent SMS notifications, when AusCERT's Security Bulletin Service identifies a vulnerability that has reached critical stages. In most circumstances this occurs when AusCERT is aware of active, in-the-wild exploitation of a vulnerability.

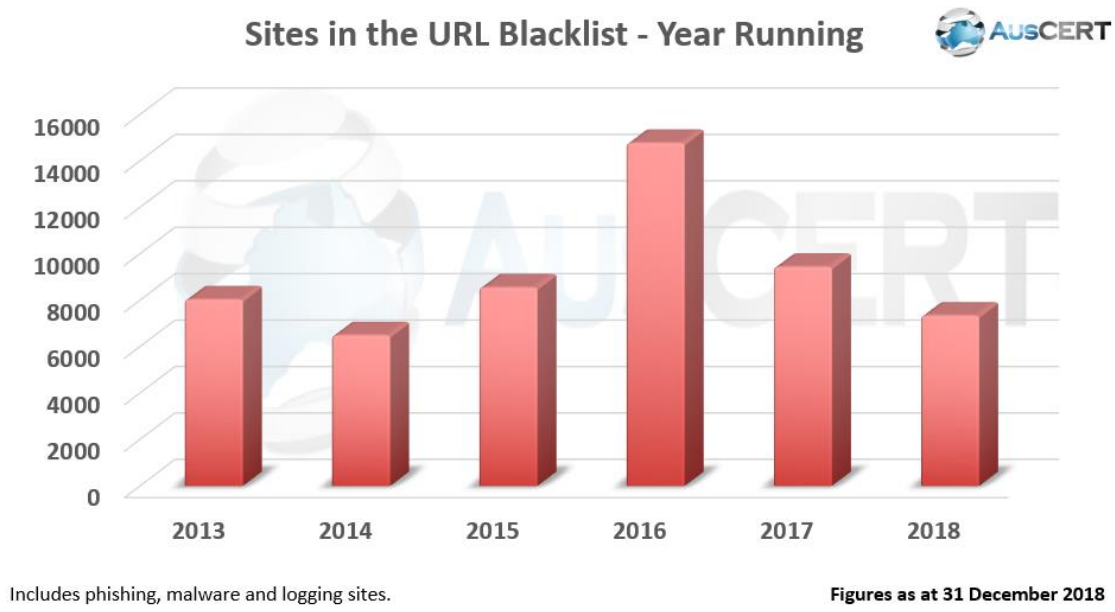
Alerts are sent along with Bulletins, with additional flagging of the Bulletins. These Bulletins are given special importance with respect to the nature of the issue. Throughout the year of 2018 sixty (60) bulletins had merits to be elevated to "ALERTS" where the constituency was advised to take special attention to the information contained in the bulletin released. Of the sixty alerts, only a subset was of an importance that required to send an accompanying SMS.

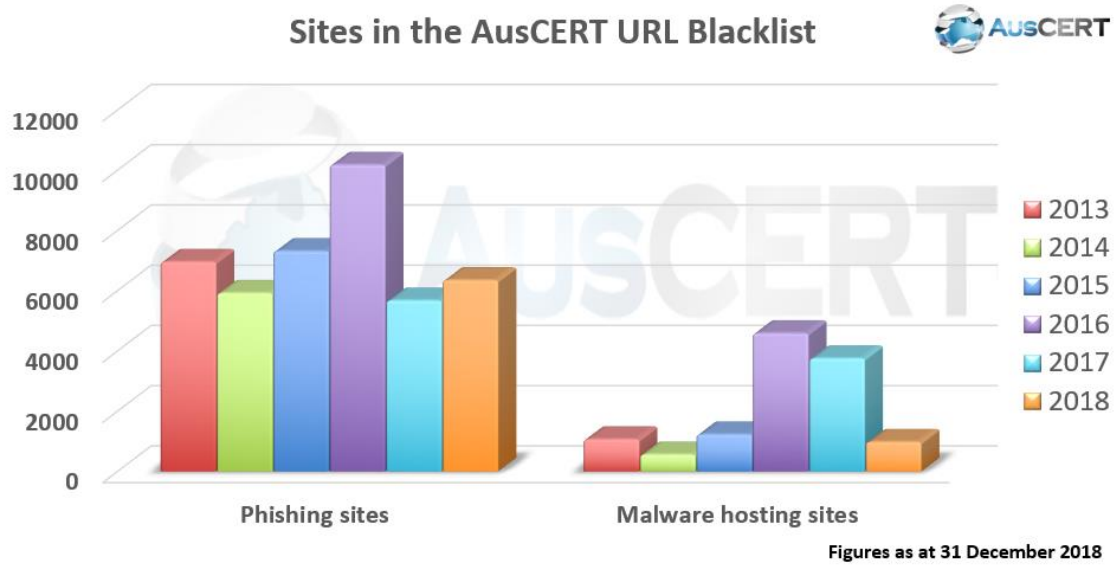
Of note is the growing number of bulletins that are being handled, this is in line with the increased capacity at AusCERT to process additional streams of advisories.



3.4 Malicious URL Feed.

On a daily basis, AusCERT encounters numerous phishing, malware, malware logging or mule recruitment web sites, including those directed at Australian Internet users. AusCERT collects this information and provides a feed that can be added to a firewall blacklist to prevent inadvertent compromise of client computers on the protected network; or that list can be used to check web log files to see if any client computers on the protected network may have already connected to these web sites. The Malicious URL feed is an effective resource to assist in detecting potential compromises as well as protecting client computers.



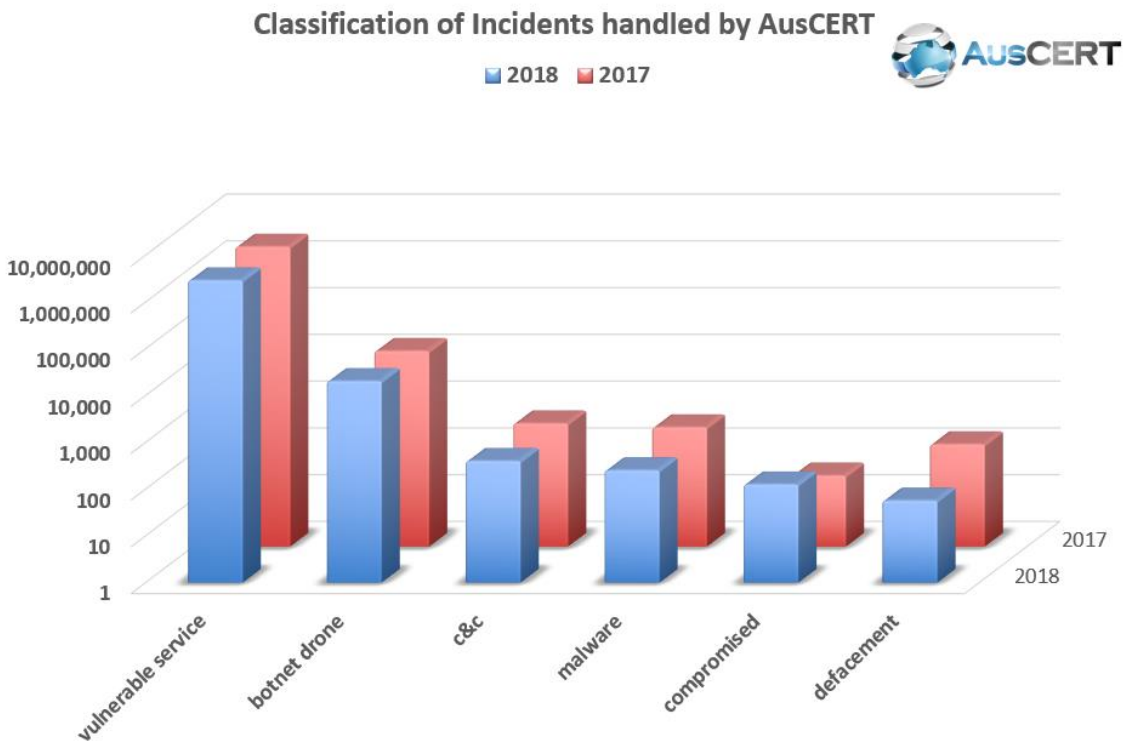


3.5 Notifications

3.5.1 Member Security Incident Notifications.

AusCERT Members benefits from AusCERT's considerably large overseas and local threat intelligence feeds with respect to incidents that have been detected by other parties but concern the members. There are several categories of incidents and this service has been running for members for several years. In 2018, as compared with 2017, follows the same distribution of incidents, except for numbers of compromised host and defaced sites.

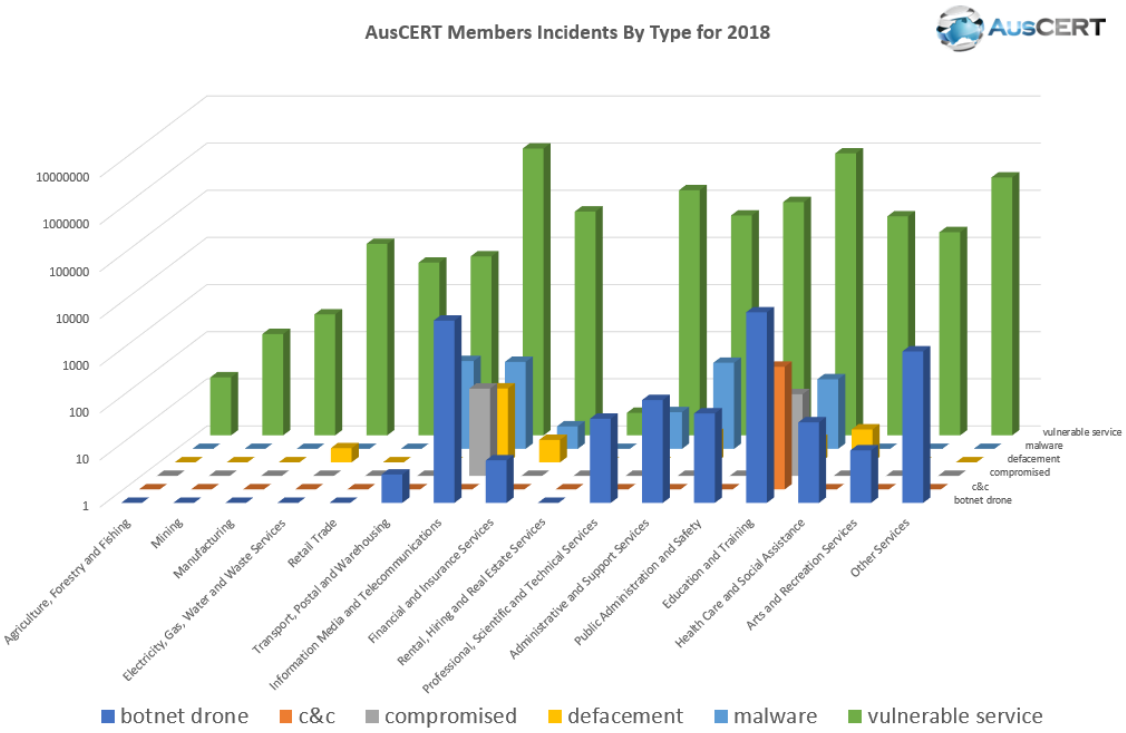
These notifications are a mix of Indicators of Vulnerabilities (IoV) and Indicators of Compromise (IoC). The numbers of IoV far outweigh other categories and hence to be able to better display all the categories of the graph of the notifications are done on a logarithmic scale.



Indicators of Vulnerabilities, such as the notification of internet-exposed vulnerable services run by members, were tallied at a staggering two million, nine hundred and eleven thousand, four hundred and sixty-one (2,911,461) events.

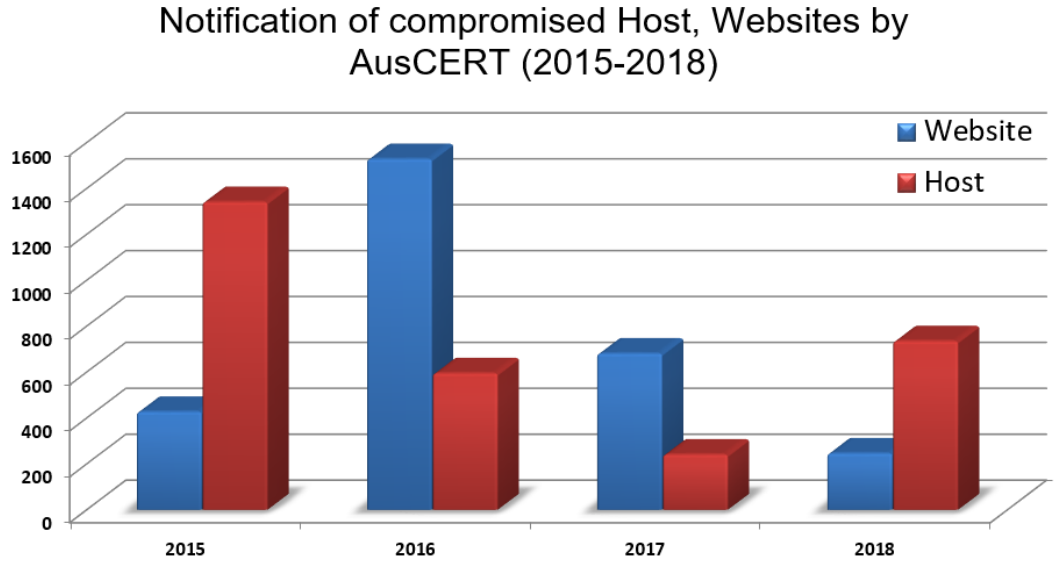
The numbers of other types of notifications are not as many but are just as important. Botnet drones tallied up from last year at twenty thousand four hundred and sixteen (20,416), Command and Control were down from last year at three hundred and ninety-nine (399) unique events, Defacement down at fifty-seven (57) and compromised hosts up at one hundred and twenty-six (126) events.

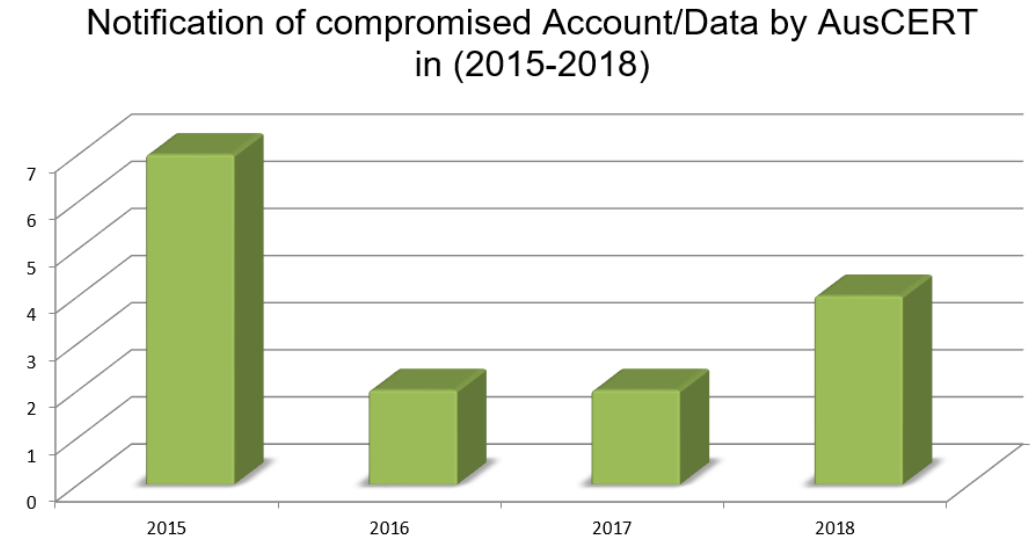
In the year 2018, further in-depth reporting is provided where the types of incidents are spanned out to show the different industry classifications of AusCERT members affected.

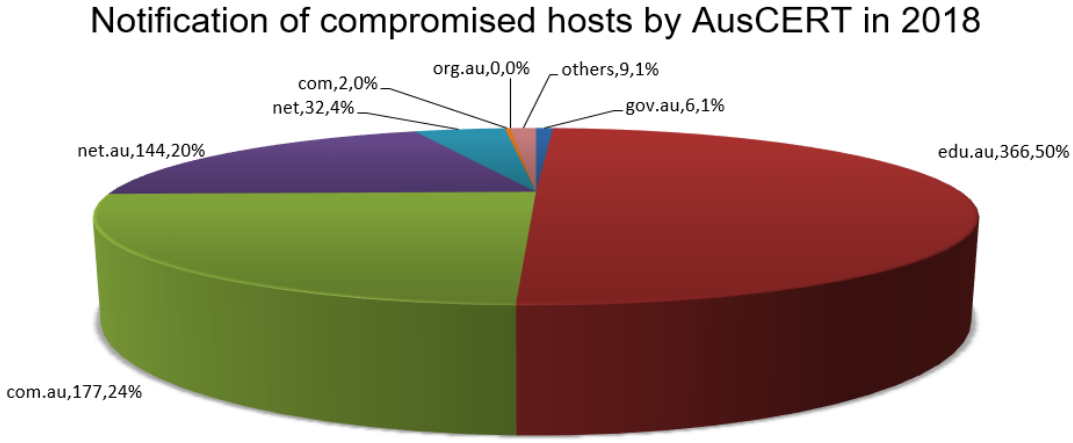


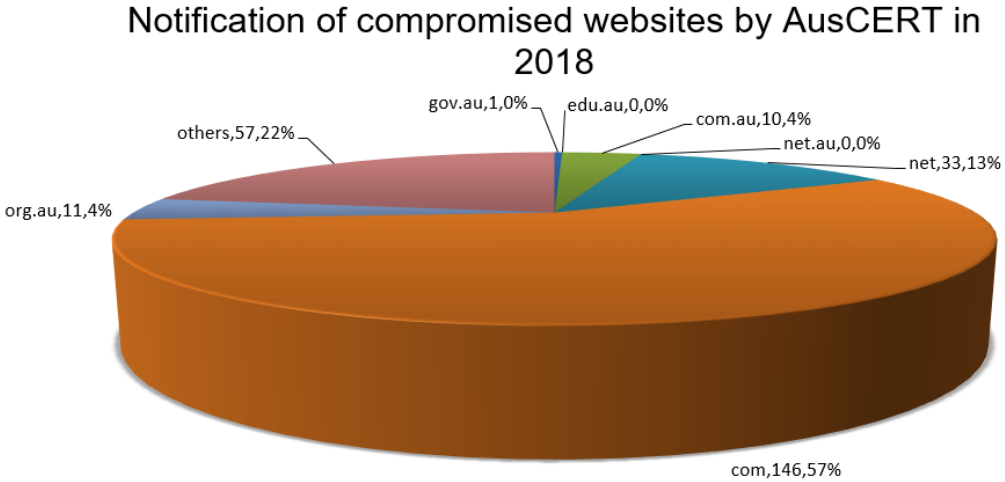
3.5.2 Legacy notification and reporting system.

To be able to compare notes of the continued notification of compromised host and websites, the following graphs are still provided for reference. These numbers are and graphs are provided this year as a bridge to the new system and its reporting capability.



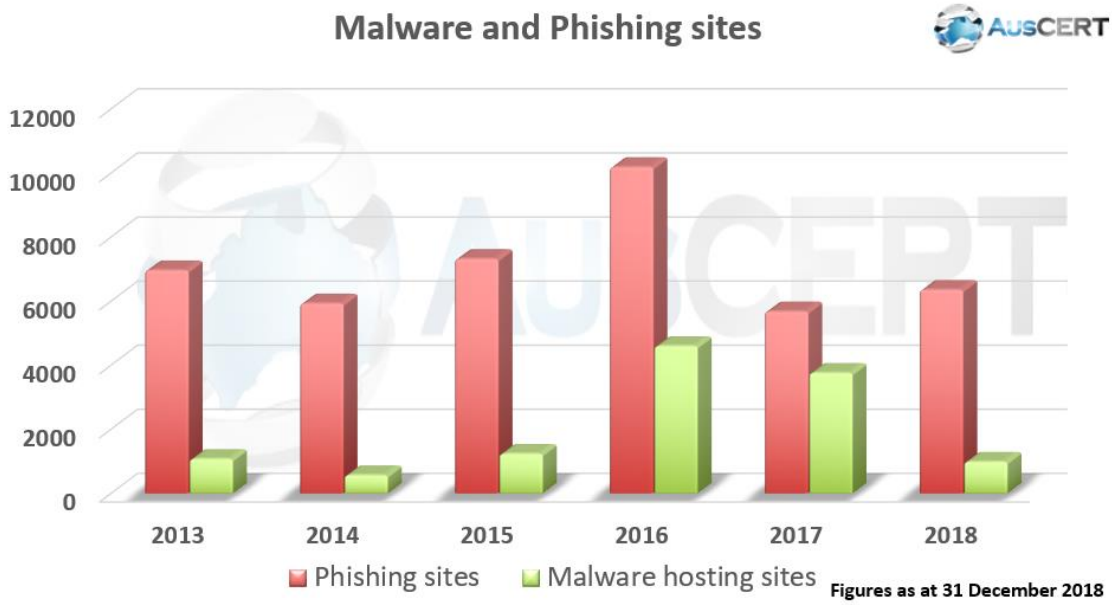

Notification of compromised Account/Data by AusCERT in (2015-2018)
7
6
5
4
3
2
1
0
2015
2016
2017
2018


Notification of compromised hosts by AusCERT in 2018
org.au,0,0%
others,9,1%
com,2,0%
net,32,4%
gov.au,6,1%
net.au,144,20%
edu.au,366,50%
com.au,177,24%


Notification of compromised websites by AusCERT in 2018
gov.au,1,0%
edu.au,0,0%
com.au,10,4%
others,57,22%
net.au,0,0%
net,33,13%
org.au,11,4%
com,146,57%

3.6 Phishing Takedown

AusCERT Members can utilise AusCERT's considerably large overseas and local contact network for removal of phishing and malware sites. The number of sites that were handled in the year 2018 has already been graphed in the section Malware URL. Specifically, for Phish site, the tally is six thousand three hundred and fifty-five (6,355). This service is not limited to taking down phishing sites but also of takedowns of sites that are serving malware. Of those malware sites, nine hundred and eighty-five (985) sites have been reported in the calendar year of 2018. This can be seen from the diagram below.

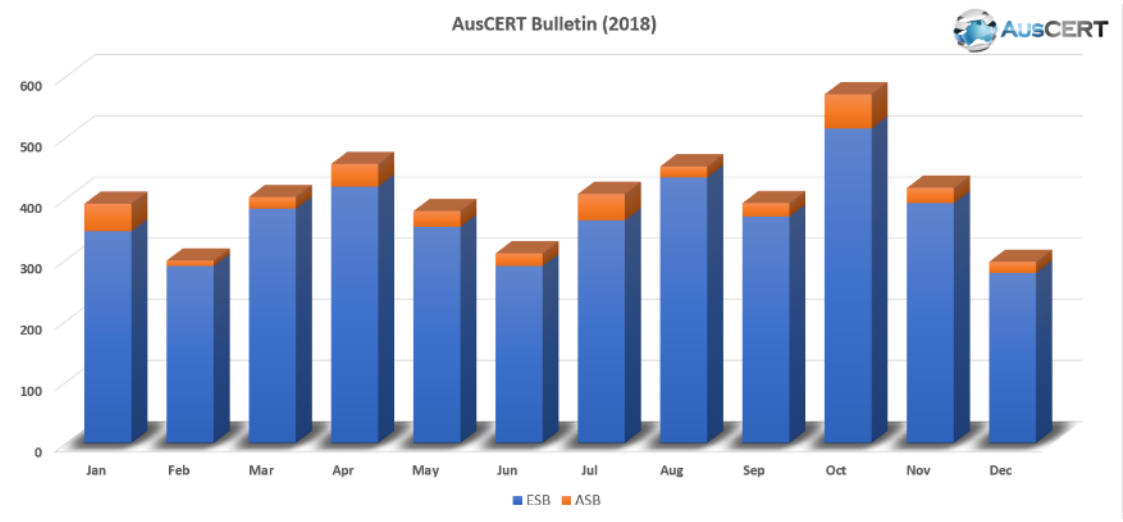


3.7 Security Bulletins

AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website. Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.

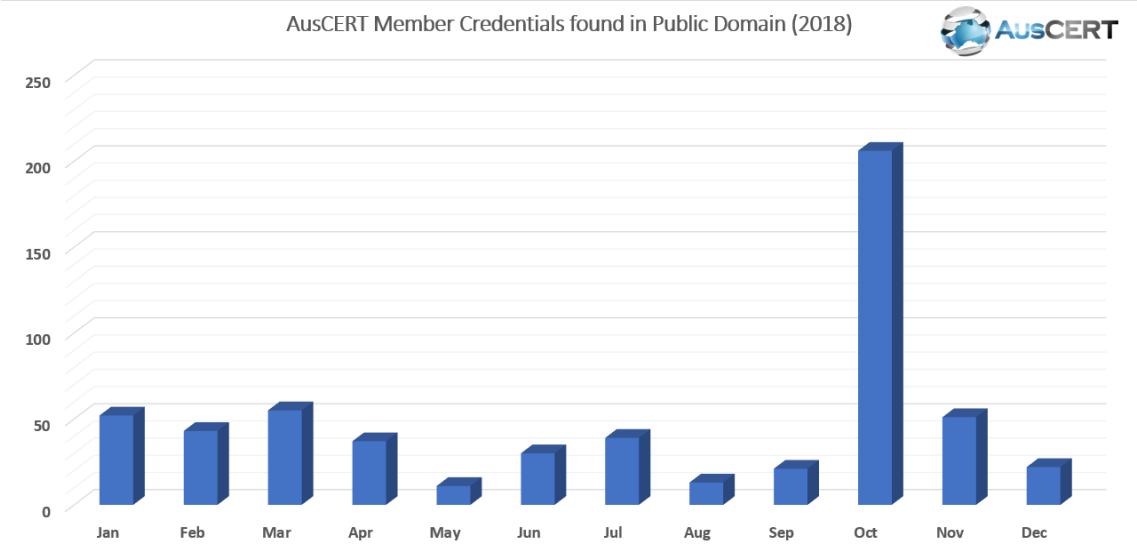
During 2018, three thousand four hundred and fifty-three (3,453) External Security Bulletins (ESBs) and two hundred and thirty-four (234) AusCERT Security Bulletins (ASBs) were published.

The ESBs are made publicly available immediately however the ASBs are available only to members for a period of one month after which they become available for public consumption.



3.8 Leaked Credential Service

A service that AusCERT has been offering since 2016 has been leaked credential reports. On occasion, AusCERT finds credentials of members that have been leaked on the internet. As soon as these credentials are found, a report is sent to the owner organisation so that they may invoke their security processes that deal with leaked credentials. The following graph shows the tally of unique credentials that have been reported back to members.



3.9 Publications

3.9.1 Week-In-Review

Every week the highlights of the week's Incident handling and bulletin publications are listed in the Week-In-Review.

3.9.2 Social Media

Publishing is great but getting the word out of a publication or an event is best done using the current social media platforms. AusCERT supports heralding news and events through the platforms, Twitter, LinkedIn and Facebook.

3.9.3 Newsletters

Newsletters are also supported in getting the word out about what AusCERT is doing. Member newsletters come out every two (2) months to keep members engaged in AusCERT activities.

3.9.4 Blog Posts

Depending upon the gravity of news, articles are published for the public of ongoing issues. This is placed in the AusCERT website in the Blog section.

4. Events organized / hosted

4.1 AusCERT Conference

The AusCERT Conference 2018, took place from 29th May -1st June 2018 in Surfers Paradise Gold Coast, Australia with the theme of "Building Resilience". The AusCERT Conference is the biggest annual member event, which is open to public attendance. Against a backdrop of evolving technologies and emerging threats, AusCERT2018 encouraged the information security community to deliberate new ways of building cyber security resilience. The conference highlighted emerging new technological solutions, case studies, frameworks, the psychology of the workforce handling cyber security incidents as well as issues faced with training cyber professionals and management methodologies. AusCERT2018 explored these aspects and more through world-class speakers, presentations and tutorials.

5. International Collaboration

5.1 International partnerships and agreements

AusCERT maintains relationship and membership with Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Information Response Security Teams (FIRST).

5.2 Capacity building

5.2.1 APCERT Drill 2018

Every year, AusCERT participates in an exercise that tests its operational readiness to the full. The Asia Pacific Computer Emergency Response Team (APCERT), of which AusCERT is a member, conducts an annual drill among its constituents. This year, the theme was "Data Breach via Malware on IoT". The drill fosters communication between the CERTs in the region and beyond. In all, 27 CERT/CSIRT teams from APCERT participated, along with five (5) teams from the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT). AusCERT operations staff members were kept busy throughout the exercise with tasks that included email analysis, malware analysis and log file analysis.

5.3 ACID Drill 2018

AusCERT was also invited in participating the ASEAN Cyber Incident Drill hosted by Singapore Cyber Security Agency. This well composed drill allowed further interaction with the CERT/CSIRT community and validate internal processes and skill sets.

6. Conclusion

This year of 2018, for AusCERT, was marked by further growth in capacity. This was immediately reflected in the number of bulletins that were able to be processed in the year. Also, something that was not immediately apparent was the efforts placed in increasing capability, of which will become evident in the report for the year 2019. AusCERT has been committed in providing back its constituency, quality services from the support that the membership provides AusCERT. This direct feedback allows AusCERT to improve in doing its part in keeping the internet a safe and reliable resource.

BGD e-Gov CIRT

Bangladesh e-Government Computer Incident Response Team - Bangladesh

1. Highlights of 2018

1.1 Summary of major activities

- 870 cyber security incidents registered in our tracking system.
- Arranged 1 international cyber security conference.
- Arranged 8 cyber security trainings.
- 10 Cyber Sensor units have been deployed to Critical Information Infrastructures.
- "Cyber Range" the cyber defense training center is operational.
- "Digital Forensic Lab" is operational and successfully solving government cases.
- Developed Cyber Risk Assessment framework for Critical Information Infrastructures (CIIs)

1.2 Achievements & milestones

- Become "Accredited" Member of TF-CSIRT.

2. About CSIRT

2.1 Introduction

BGD e-GOV CIRT mission is to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh, which will make these programs more efficient and reliable.

2.2 Establishment

The process to establish BGD e-GOV CIRT was started on November 2014 and team starts operation on February 2016.

2.3 Resources

Currently 9 people are working in BGD e-GOV CIRT and more people will join soon.

2.4 Constituency

Constituency of BGD e-GOV CIRT are all governmental ministry & institutions of Bangladesh.

3. Activities & Operations

3.1 Scope and definitions

Main objectives of the BGD e-GOV CIRT are:

- Manage cyber security in Bangladesh government's e-Government network and related infrastructure;
- Serve as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders.
- Make efforts to establish national cyber security incident management capabilities in Bangladesh.

It serves the following pro-active services to its constituents:

- Security Assessment
- Intrusion Detection
- Security Consulting
- Awareness Building

In order to accomplish its mission, BGD e-GOV CIRT will provide the following reactive services to its constituents:

- Incident response support
- Coordination
- Reporting

3.2 Incident handling reports

- We have registered 870 cyber security incidents in our tracking system.
- Successfully solved 4 Digital Forensic cases.

3.3 Publications

- Government of Bangladesh Information Security Manual (GoBISM) has been published.
  https://www.cirt.gov.bd/wp-content/uploads/2017/06/GOBISM2.pdf
- Data Loss Prevention (DLP) Policy.
  https://www.cirt.gov.bd/wp-content/uploads/2019/01/Data-Loss-Prevention-Policy.pdf

3.4 New services

- Cyber Sensor

  Detecting intrusion, suspicious activity & development of methodology of assessing maturity level of Critical Information Infrastructure in Bangladesh government IP network, thus sensor network is being implemented.

- Digital Forensic

  The purpose is forensic investigation of digital evidence. It helps the incident handling unit as reactive service after an incident occurs by providing forensic support on evidence included in the incident. Digital Forensic team is also capable of recovery and investigation of material found in digital device including mobile, PC, Drone or any IOT's or computational devices. CIRT Lab Capabilities: Computer Forensic, Mobile Forensic, Network Forensic.

- Cyber Security Strategy & Risk Assessment Framework Development

  Enhance national cyber security strategy to address cyber security as a country wide risk and a foundation for economic viability and develop CIIP strategy. Provide a basic cyber security package for the owners of CIIs by establishing common taxonomy of standards, guidelines and practices to strengthen Bangladesh critical infrastructure's resilience to cyber threats.

- Cyber Range

  Cyber Range Service helps security-staff to build the skills and necessary experience to combat modern cyber threats. Cyber Range Service provides a synthetic war-gaming environment that allows staff to play the role of both attacker and defender to learn the latest methods of vulnerability exploitation and the use of advanced tools and techniques to mitigate and defend threats.

4. Events organized / hosted

4.1 Training

- Workshop on Cyber Security Capacity Maturity by University of Oxford.
- Workshop on Bangladesh Cyber Security Threat Landscape.
- Training on "Cyber Sensor Operations".
- Workshop on "Cyber Range Operation".

4.2 Drills & exercises

- Arranged Cyber Drill exercise from Cyber Range Lab

4.3 Conferences and seminars

- Arranged International Cyber Security Conference 2018

5. International Collaboration

5.1 International partnerships and agreements

- Forum of Incident Response and Security Teams (FIRST.Org)
- Asia Pacific Computer Emergency Response Team (APCERT)
- The Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT)
- Indian - Computer Emergency Response Team
- Anti-Phishing Working Group (APWG)
- EC-Council
- Norway Registers Development (NRD)
- Team Cymru

5.2 Capacity building

5.2.1 Training

- Attend on ”MTCP Scholarship on Cyber Security by CyberSecurity Malaysia”.

5.2.2 Drills & exercises

- We have participated APCERT Drill 2018.
- Achieved 75% score in OIC Drill 2018.

5.3 Other international activities

- Attend on “55th TF-CSIRT Meeting”.
- Attend on “30th Annual FIRST Conference in Malaysia".
- Attend on “APCERT Annual General Meeting & Conference 2018 in China”.
- Attend “Regional Cyberdrill for CIS” at Baku, Azerbaijan in 2018.
- Attend “Fintech Indonesia 2018” at Jakarta, Indonesia in 2018.
- Attend “Security Scape Bangalore” India in 2018.
- Attend “Annual Conference 2018 of Meridian Process” in South Korea in 2018.

6. Future Plans

6.1 Future projects

- In Cyber senor project additional five more sensor units will be installed into the Critical Information Infrastructures.
- In CIRT Enhancement project there will be some new service like vulnerability advisory management, penetration testing service etc.

6.2 Future Operation

- Continue the security incident handling services.
- Arrange Cyber security awareness programme (Seminar, workshop)
- Development of self-assessment tool kit for cyber risk assessment that will be used by CIIs.
- "Cyber Sensor Operations" training will be provided to appointed technical persons from Critical Information Infrastructures, for actively participate on Cyber Threat hunting & remediation.
- Provide cyber range operational training to Govt. officials to enhance the capacity about cyber security.

7. Conclusion

Cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines. In Bangladesh, need for cybersecurity workers is likely to continue to be high, it is difficult to find the skilled cybersecurity workforce. More attention to both the capacity and capability of the Bangladesh cybersecurity workforce is needed. BGD e-GOV CIRT goals for 2019 include improving and expanding communication as well as incident response capacity of its technical team and associated new tools, which will provide greater value during incident response and assessment activities. The team will continue to refine and update its training offerings that will allow government organizations to better meet the demands of challenging and evolving technical issues in cyber security.

8. Attachment (Photos)

Figure 1: BGD e-GOV CIRT Forensic LAB inauguration

Figure 2: Training on "Cyber Sensor Operations"

Figure 3: Workshop on "Cyber Security Capacity Maturity" with team from Oxford University

Figure 4: Workshop on "Cyber Security Capacity Maturity" with team from Oxford University

BruCERT

Brunei Computer Emergency Response Team – Negara Brunei Darussalam

1. About BruCERT

1.1 Introduction

Brunei Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

1.1.1 BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet.

1.2 BruCERT Establishment

BruCERT coordinates with local and international Computer Security Incident Response Team (CSIRTs), Network Service Providers, Security Vendors, Law Enforcement Agencies as well as other related organizations to facilitate the detection, analysis and prevention of security incidents on the Internet.

1.3 BruCERT Workforce

BruCERT currently has a strength of 66 staff (100% local) of which a majority is

specialized in IT and the rest is administration and technical support. Its staff has undergone training on various IT and security modules, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP, BS7799 Implementer and SANS trainings such as GREM, GCIA, GCIH, GCFA, GPEN, where most of BruCERT workforce has gained certifications in.

1.4 BruCERT Constituents

BruCERT has close relationship with Government agencies, 2 major ISPs and various numbers of vendors.

Government Ministries and Departments

BruCERT provide Security incident response, Managed Security Services and Consultancy services to the government agencies. Security Trainings such as forensic and awareness trainings were provided by BruCERT in collaboration with some Government Agencies.

E-Government National Centre (EGNC)

E-Government National Centre provides IT Services to all Government Departments and Ministries in Brunei Darussalam. Services such as IT Central procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), Co-hosting are provided by EGNC. BruCERT work closely with EGNC in providing Incident Response and Security Monitoring since most of the government equipment resided at EGNC.

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force (RBPF) and other Law-Enforcement Agencies (LEAs)

BruCERT has been collaborating with RBPF and other LEAs to resolve computer-related incidents through our Digital and Mobile Forensic services.

TelBru – BruNet

TELBru, the main Internet service provider. and BruCERT have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

DST –

The second largest internet service provider in Brunei.

1.5 BruCERT Contact

The *Brunei Computer Emergency Response Team Coordination Centre (BruCERT)* welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn
website: www.brucert.org.bn
www.secureverifyconnect.info

2. BruCERT Operation in 2018

2.1 Incidents response

In 2018, BruCERT had deployed security threat intelligence sensors in strategic network infrastructure to detect any malicious activities in network. Most of the High severity threats are due to malware related activity such as generic malware, malware infection, malicious bot and IRC Bot. There were some cases involving unauthorized user access to files and shares. The statistic of the security incident is shown as ***Figure 1***.

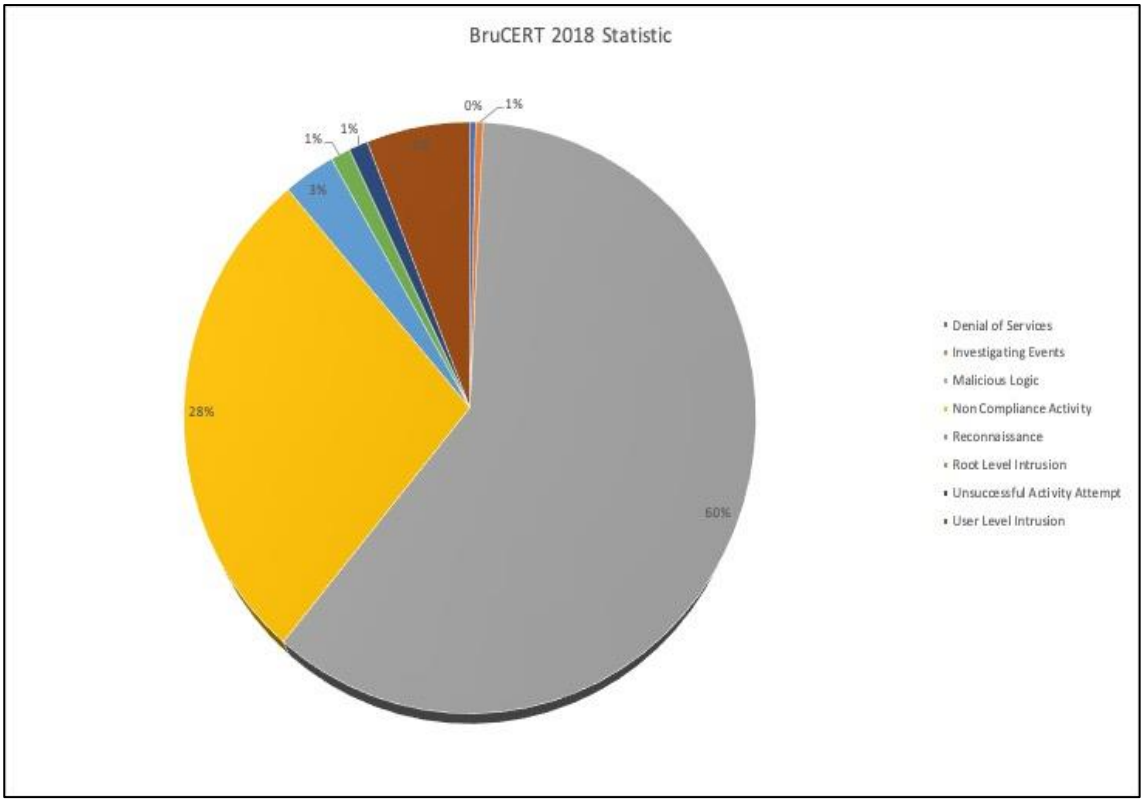


Figure 1

Types of Attack	Count
Denial of Services	10
Investigating Events	13
Malicious Logic	1791
Non Compliance Activity	825
Reconnaissance	90
Root Level Intrusion	34
Unsuccessful Activity Attempt	33
User Level Intrusion	180

Table 1

2.2 BruCERT Honey Pot

There were around 790045 events were captured, where a total of 641 data payload had been downloaded of varying type as shown at Figure 2.

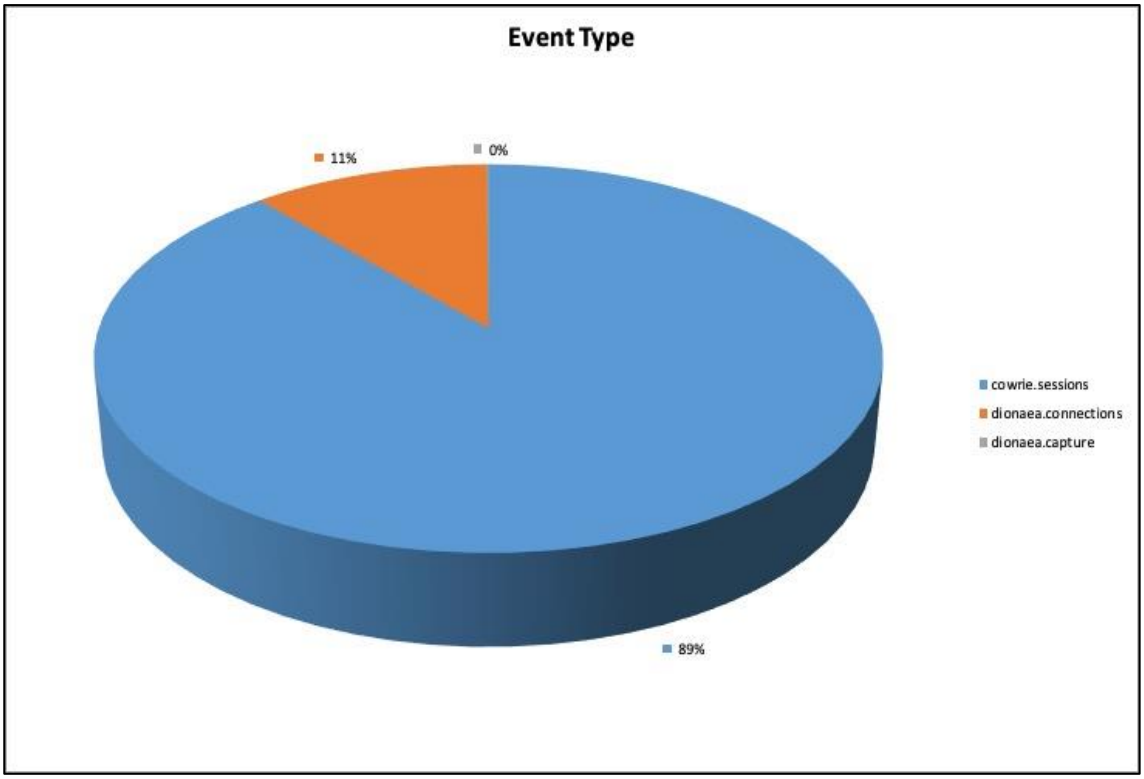


Figure 2

Cowrie.sessions is connections made by using SSH and Telnet connections. Connections to the system are usually not legitimate and allow a network defender to detect the attacker through detailed logging. The logging can reveal not only normal connection information but also session information revealing the techniques, tactics and procedures (TTP) used by the attacker. From CWC honeypots which is connected to the Internet, it can monitor the tools, scripts and hosts in use by password guessing attackers. Most of cowrie.sessions attempted to use port 22 and port 23 to establish their connections. It is assume that most of the sessions were coming from self-replicating scripts or bots. The script or bots spreads by finding open ports and guessing passwords, once it gets a shell it copies itself over and continues to spread using the same method.Dionaea.connections is connections establish by malicious software, trying to exploit vulnerable services exposed by the network. Out of 89574 malicious software connections, CWC Honeypot had captured a number 641 hashes type of malicious software (dionaea.capture).

Event Type	*Count*
cowrie.sessions	700471
dionaea.connections	89574
dionaea.capture	641
Total	*790686*

Table 2

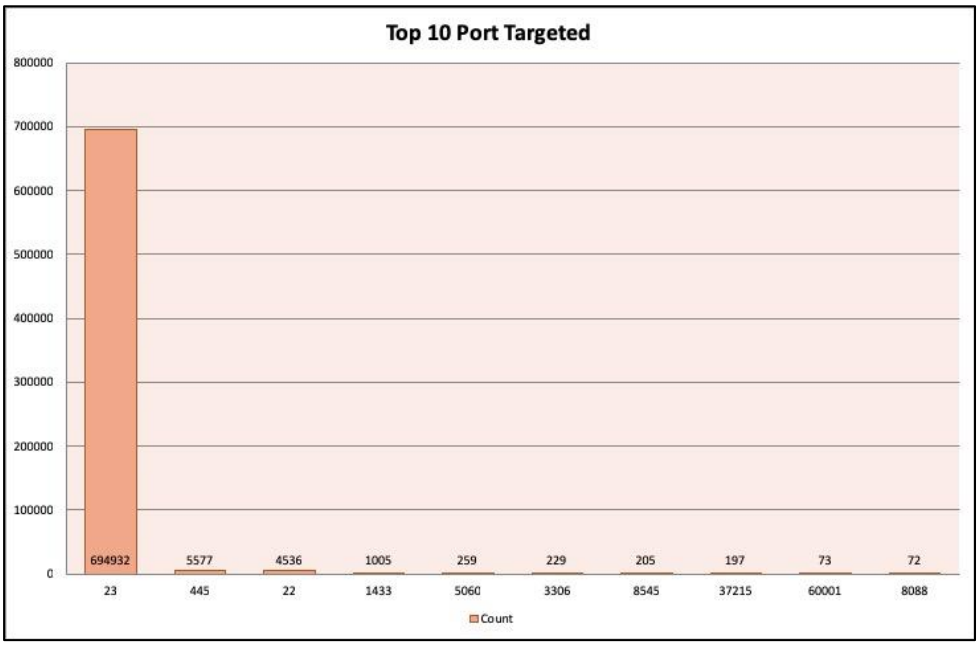


Figure 3

Port	Count
23	694932
445	5577
22	4536
1433	1005
5060	259
3306	229
8545	205
37215	197
60001	73
8088	72

Table 3

3. BruCERT Activities in 2018

3.1 Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security.

- On 26th November 2018 until 29th November 2018 - Two BruCERT delegates attended the OIC-CERT AGM and Annual Conference 2018 which takes place at Shiraz, Iran, hosted by Shiraz University CERT.
- On 25th October 2018 until 26th October 2018 - Three BruCERT delegates attended the APCERT AGM and Annual Conference 2018 which takes place at Royal Park Hotel, Shanghai, China, hosted by CNCERT/CC.

3.2 Awareness Activities

Cyber Battle: Capture The Flag 2018 and Awareness Talk

August, 4 2018

This was the fourth time ITPSS organized the annual competition. The qualifying round was held online on 29th July 2018, while the final round was hosted at Annajat Complex on August 4 2018. The winners of the competition were *Team /x00.* Permanent Secretary (Security and Enforcement) at the Prime Minister's Office Lieutenant Colonel (Rtd) Pengiran Haji Muhamad Sazali bin Pengiran Haji Yakob, as the guest of honour, handed over the prizes and certificates.

BtCIRT

Bhutan Computer Incident Response Team – Bhutan

1. Highlights of 2018

1.1 Summary of major activities

In 2018, BtCIRT conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted vulnerability assessment, post-incident analysis, and awareness programs targeting end users.

1.2 Achievements & milestones:

- The number of compromises to government websites reduced substantially from 21 in 2017 to 5.
- Implemented OS hardening template at GDC (Government Data Centre).
- Cybersecurity simulation exercise conducted for high officials to create awareness amongst the decision makers.
- Workshop on Information and Network Security conducted.
- Workshop on Incident Resolution conducted.

2. About BtCIRT

2.1 Introduction

Bhutan Computer Incident Response Team (BtCIRT) is a part of Department of Information Technology and Telecom, Ministry of Information and Communications. The overall mission of BtCIRT is to enhance cyber security in the country by coordinating cybersecurity information and establishing computer security incident handling capabilities in the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

2.2 Establishment

The BtCIRT's mandate was approved by the *Lhengye Zhungtshog*/Cabinet on 20 May 2016 formally identifying the team as the national focal point for cybersecurity activities and initiatives.

2.3 Resources

Currently, BtCIRT consist of 5 working team members.

2.4 Constituency

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. While BtCIRT services like awareness and reactive services is extended to all users within the country.

3. Activities & Operations

3.1 Scope and definitions:

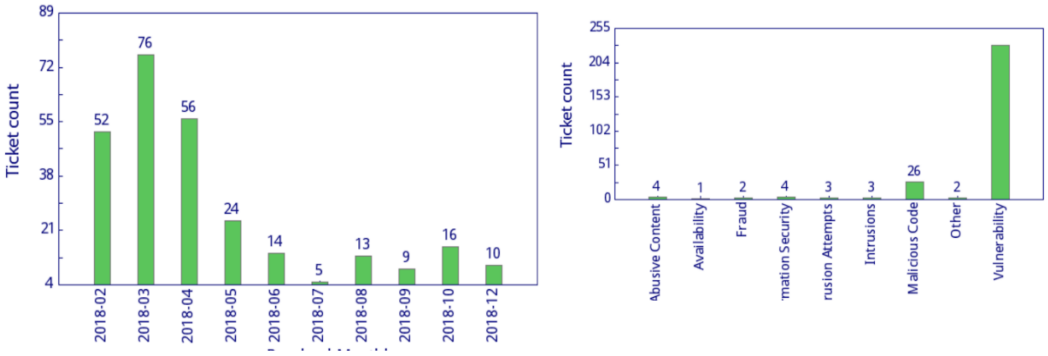
- BtCIRT is a national contact in relation to cyber security issues.
- BtCIRT conducts end-user awareness at national level and disseminates information on threats and vulnerabilities, and conducts security workshops related to various cyber security domains.
- BtCIRT actively monitors system hosted in Government Data Centre (GDC) for attacks and vulnerabilities, and provides timely report to GDC operating team along with system administrators.
- BtCIRT also conducts periodic security assessment of government systems while for non-government organisations it provides services on request basis.
- Represents the country in international forums.
- BtCIRT also develops strategies, policies, standards, guidelines and baseline documents.

3.2 Incident Handling Report

The year saw 8% increase in the incidents reported to BtCIRT as compared to 2017 taking the total of resolved incidents to 275. This is attributed to awareness programs being conducted in the dzongkhags in the beginning of the year hence encouraging constituents to report incidents leading to increase in the incidents reported in BtCIRT. There were 50 incidents reported by constituents.

Most of the government websites were assessed for security vulnerabilities and system hardened accordingly. These websites were monitored on daily basis and that has reduced number of attacks on the government websites substantially to 5 from 21 in 2017.

The following graphs provide number of incidents resolved on a monthly basis. It also depicts the types of incidents resolved by the team during the year.



March saw 76 incidents, highest number of incidents handled in the year.

3.3 Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website (www.btcirt.gov.bt) and facebook page (BtCIRT).

In addition, the team also publishes advisories to assist constituents in resolving the most common threats and vulnerabilities observed. Besides, email advisory are also sent out to government and critical sector ICT official to notify possible attacks as and when it is detected.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

- ***A workshop on incident resolution*** was conducted on May 2018 to educate the system owners on the latest vulnerabilities existing in the systems and to address the capacity gaps faced by the system owners in resolving and patching the detected vulnerabilities

- ***A workshop on Information and Network Security*** was conducted from 12th to 16th November, 2018 with financial and technical support from APT (Asia Pacific Telecommunity) and APNIC (the Asia-Pacific Network Information Centre). The week long program was aimed to train system administrators in securing their information systems and network infrastructure and, responding to potential threats and attacks with practical sessions on identifying and defending threats and vulnerabilities. Participants from government agencies, corporations, financial institutions, telecom service providers and other relevant private sector

organisations participated.

- A day long ***security mock drill*** was also conducted to assess the readiness of response capabilities of system and network administrators. The drill was based on plausible cyber security cases and commonly occurred incidents.
- On November 27, 2018 ***Cyber Incident Simulation*** was conducted with support from the International Telecommunication Union (ITU). The exercise was designed exclusively for heads of government, policy makers and other high ranking figures to increase awareness on cyber security and preparedness to make critical decisions in response to cyber attacks.
- ***Configured hardened OS template*** and enforced its use as minimal security requirement for deployment of any systems at GDC.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT is a member of two international organisations, Asia Pacific Computer Emergency Response Team (**APCERT**) and Forum of Incident Response and Security Teams (**FIRST**) as of now.

5.2 Capacity building

5.2.1 Seminars & presentations

BtCIRT has attended following conference/seminars/workshops:

- 30th Annual Conference on Computer Security organised by FIRST (Forum of Incident Response and Security Teams).
- APT Training Course on Policy on Cyber Security for Safeguarding Public Safety
- APAN45 CSIRT Capacity Building
- APCERT online training: Performing Forensics on and Azure Virtual Machine

6. Future Plans

- Deploy SSL/TLS certificates for systems.
- Conduct workshop on Secure coding in collaboration with APNIC and TEIN.
- Conduct awareness programs at schools and colleges.
- Develop Child Online protection guidelines and programs
- Develop National Information Security Management Policy.
- BtCIRT also looks forward to collaborate with more organisations internally and

internationally to strengthen its cooperation.

7. Conclusion:

As we step into 2019, the team is positive to build on gaps identified in 2018 and further improve the services and strengthen national and international collaboration and cooperation.

CCERT

CERNET Computer Emergency Response Team - People's Republic of China

1. About CSIRT

1.1 Introduction

The China Education and Research Computer Network Emergency Response Team (CCERT) is referred to CERNET network security emergency response architecture. The main tasks of CCERT include:

- Network security incidents co-ordination and handling (mainly for CERNET users)
- Network security situation monitoring and information publication
- Technical consultation and security service
- Network security training and activities
- Research in network security technologies

1.2 Establishment

China Education and Research Computer Network Emergency Response Team (CCERT) was founded in May 1999 and is the earliest CERT in China.

1.3 Resources

CCERT sends both security early-warning and notice to users via website(https://www.ccert.edu.cn) and mailing lists, and in the meanwhile, utilize instant messaging technology (such as Wechat and QQ) to communicate with users for fast handling of security events.

1.4 Constituency

CCERT provides quick response and technical support services for network security incidents to China Education and Research Computer Network and its members, as well as other network users.

2. Activities & Operations

2.1 Scope and definitions

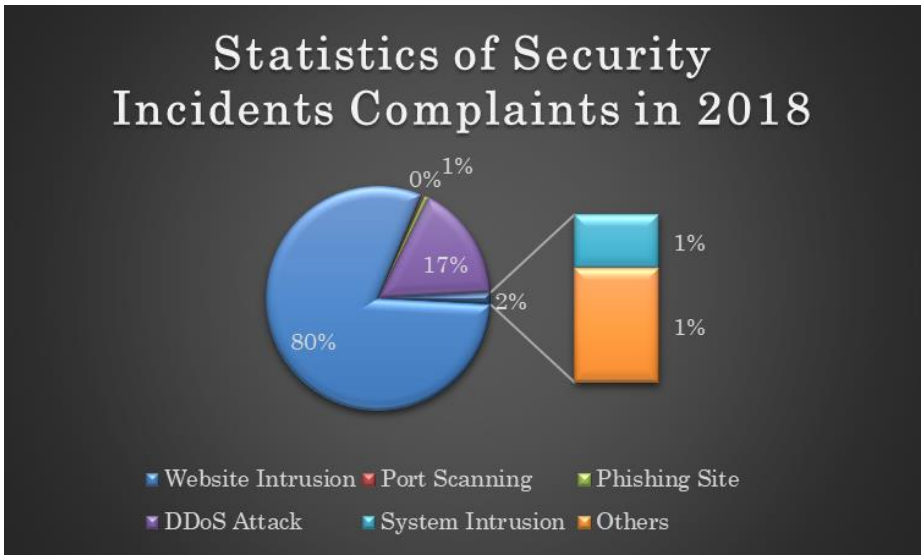
Currently, CCERT mainly deal with security events for CERNET users, which include:

- CERNET Network Monitoring
- Complaint from Other CERT Organizations

- Information Sharing with Other Security Manufacturers

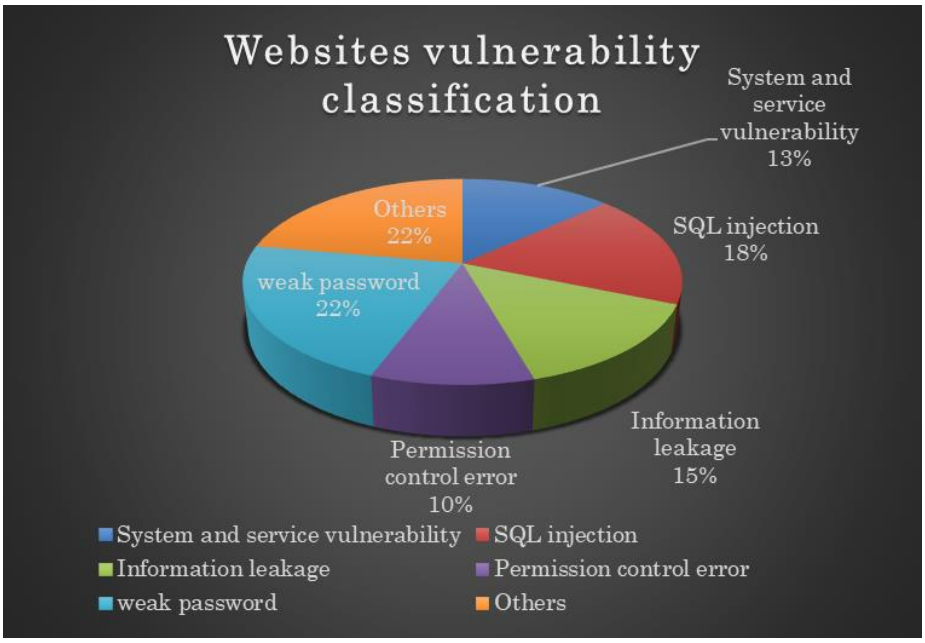
2.2 Incident handling reports

In 2018, CCERT handled 2827 security incident complaints, which include 2276 for Website Intrusion, 8 for Port Scanning, 22 for Phishing Site Complaints, 474 for DDoS Attack, 15 for System Intrusion and 32 for other network security complaints.



2.3 Abuse statistics

After analyzing the 2276 security events of website attacking, we found all the security vulnerabilities which are used to attack the websites, for more detail please see the following figure:

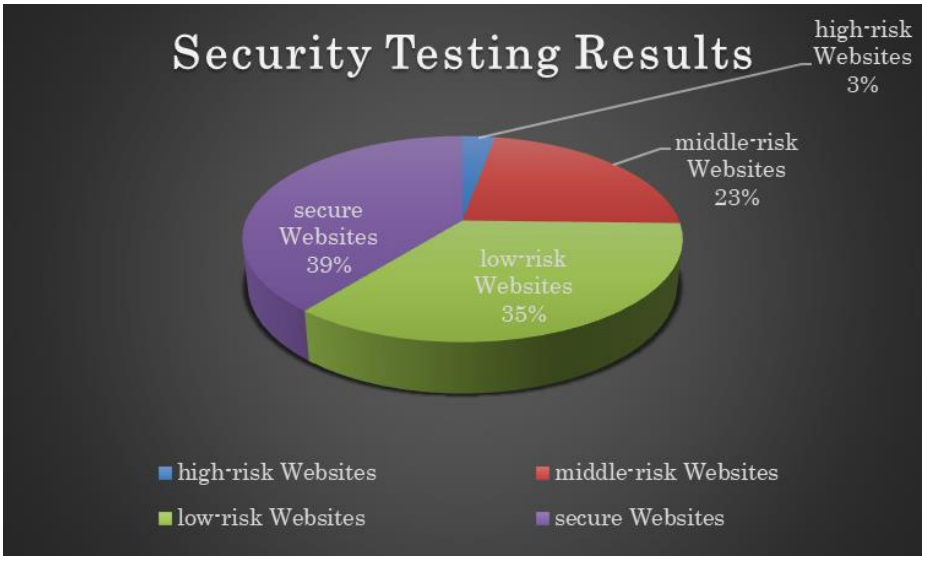


2.4 Publications

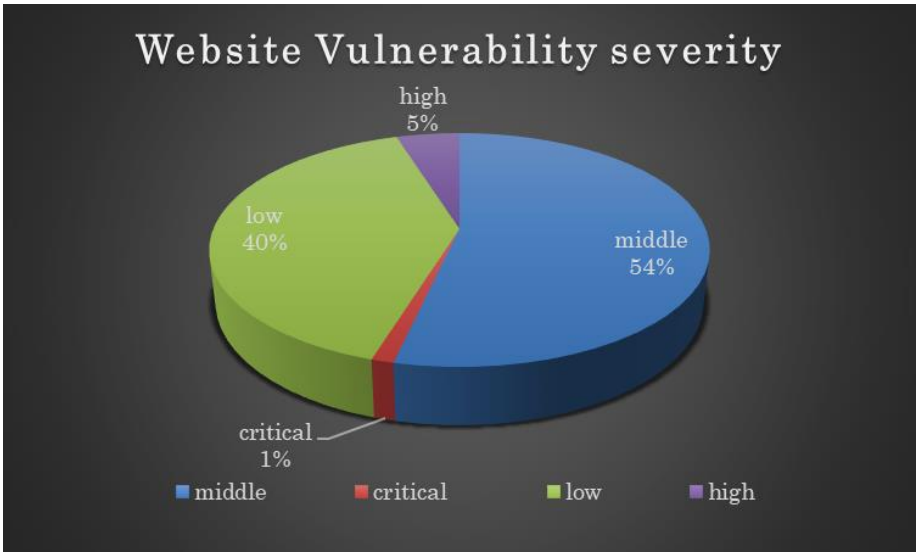
For security bulletins and vulnerability articles published by CCERT, please visit our website https://www.ccert.edu.cn

2.5 Security services

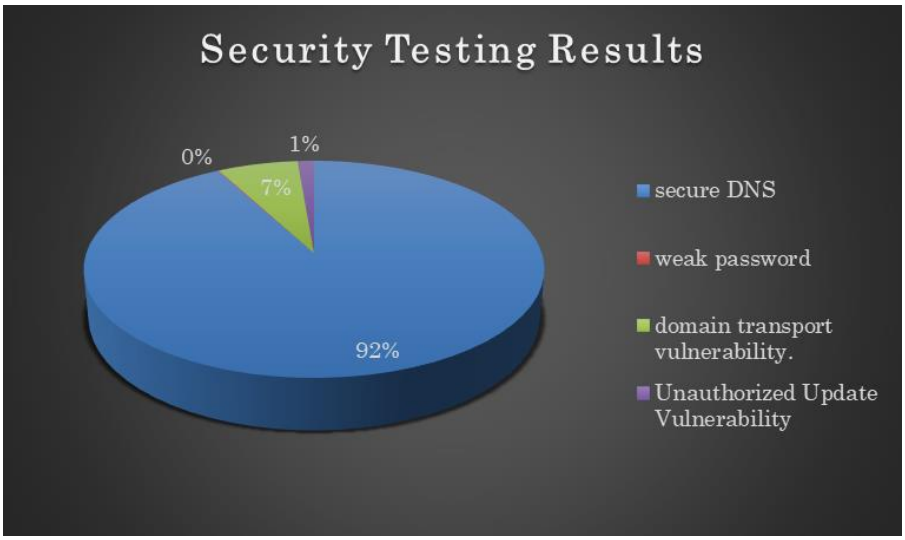
In 2018, CCERT provided security scanning service (free of charge) to 4361 websites. and found that there are about 124 websites with high-risk vulnerabilities (3%), 984 websites with middle-risk vulnerabilities (23%), and 1542 websites with low-risk vulnerabilities (35%). No security problems was detected on 1711 websites (39%).



Provided special security checks for 2100 Colleges and Universities admission websites. 13966 vulnerabilities were found in these websites.



The security test of more than 2000 authoritative parsing services in the CERNET find 2 weak password, 27 DNS Unauthorized Update Vulnerability and 132 DNS domain transport vulnerability.



3. Events organized / hosted

3.1 Training

Organized 4 trainings, which includes:

- Information Security Construction of Colleges and Universities
- Governance of Campus Network Security
- Personal Privacy Data Protection
- Discussion on IPV6 Security

3.2 Conferences and seminars

- Attend the 25th annual meeting of CERNET Users, 22 October, 2018, XiNing
- CNVD Annual Working Conference 2018, 26 November, 2018, BeiJing
- Attend the Informationization Security Annual Meeting of Colleges and Universities, 6 December 2018, HangZhou

4. Future Plans

4.1 Future projects

- Strengthen team building for ccert
- Enhancing the Construction of CERNET Security System

4.2 Future Operation

In 2018, CCERT will keep devoting to network security emergency response work and strengthen the cooperation with other security organizations, so as to make more contribution to Internet security.

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2018

1.1 Summary of major activities

a) CERT-In is in a strategic position as a Steering Committee Member in APCERT and also convening two working groups namely IoT Security and Secure Digital Payments.

b) In the year 2018, CERT-In handled **208456** incidents. The types of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and vulnerable service. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

c) CERT-In is keeping track on latest cyber threats and vulnerabilities. **193** security alerts, **36** advisories and **222** Vulnerability Notes were issued during the year 2018.

d) CERT-In conducted **24** cyber security training and awareness programs to Government, Public and Critical Sector organisations and communication & Information infrastructure providers to educate them in the area of Information Security with the latest security threats, needs and developments & deployment of techniques and tools in order to minimize security risk.

e) CERT-In participated as a player in **3** International cyber security drills and in **1** exercise participated as observer country.

1.2 Achievements & milestones

- Botnet Cleaning and Malware Analysis Centre ("Cyber Swachhta Kendra") was awarded as one of 51 "Gems of Digital India 2018" in June 2018. "Cyber Swachhta Kendra" also awarded "SKOCH Order-of-Merit and Gold Award" for Cost Effective Cyber Security Model in the month of December 2018. The centre is providing detection of malicious programs and free tools to remove the same for common users.
- Indian Computer Emergency Response Team is carrying out cyber security exercises comprising of table top exercises, crisis management plan mock drills and

joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Total of 11 such exercises have been conducted in 2018.

- In 2018, CERT-In has signed Memorandum of Understandings (MoUs) on cyber security cooperation with two countries namely The Department of Information Communications Technology, The Republic of Seychelles and The Moroccan Computer Emergency Response Team (ma-CERT), National Defence Administration, The Kingdom of Morocco to enable information sharing and collaboration for incident resolution.
- CERT-In has set up its own automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) among some select stake holders.
- CERT-In has launched its Threat and Situational Awareness Project (TSAP) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2. About CERT-In

2.1 Introduction

CERT-In is a functional organisation of Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

The Information Technology Act, 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

2.2 Establishment

CERT-In has been operational since January, 2004.

2.3 Resources

CERT-In has a team of 95 technical members.

2.4 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Government, Public and Private sectors. In addition, CERT-In provides services to the individuals and home users also.

3. Activities & Operations

3.1 Scope and definitions

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks
- Reactive services when security incidents occur so as to minimize damage
- Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills

3.2 Incident handling reports

The summary of activities carried out by CERT-In during the year 2018 is given in the following table:

Activities	Year 2018
Security Incidents handled	208456
Security Alerts issued	193
Advisories Published	36
Vulnerability Notes Published	222
Trainings Organized	24
Indian Website Defacements tracked	16655

Table 1: CERT-In Activities during year 2018

3.3 Abuse statistics

In the year 2018, CERT-In handled **208456** incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and Vulnerable Services.

The summary of various types of incidents handled is given below:

Security Incidents	2018
Phishing	454
Network Scanning / Probing/Vulnerable Services	127481
Virus/ Malicious Code	61055
Website Defacements	16655
Website Intrusion & Malware Propagation	905
Others	1906
Total	208456

Table 2: Breakup of Security Incidents handled

Various types of incidents handled by CERT-In are given in Figure 1.

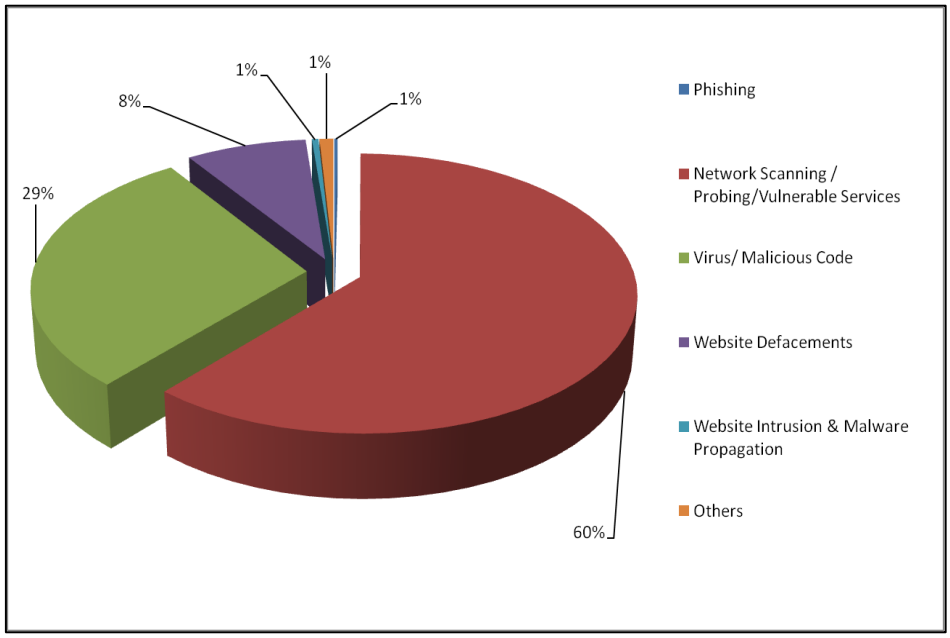


Figure 1: Summary of incidents handled by CERT-In during 2018

3.3.1 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. A total of **16655** numbers of defacements have been tracked.

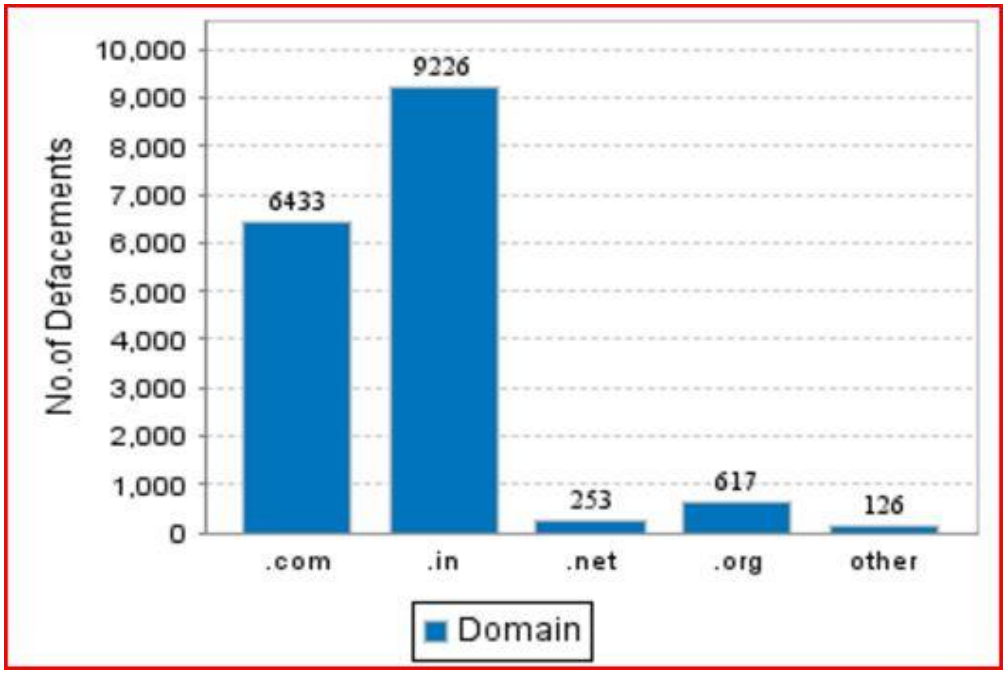


Figure 2: Indian Website Defacements tracked by CERT-In during 2018

3.3.2 Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.gov.in) has been established by CERT-In for detection of compromised devices in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers academia and Industry.

Botnet Cleaning and Malware Analysis Centre ("Cyber Swachhta Kendra") was awarded as one of 51 "Gems of Digital India 2018" in June 2018. "Cyber Swachhta Kendra" also awarded "SKOCH Order-of-Merit and Gold Award" for Cost Effective Cyber Security Model in the month of December 2018.

Botnets events processed by Botnet Cleaning and Malware Analysis centre (Cyber Swachhta Kentra) during 2018.

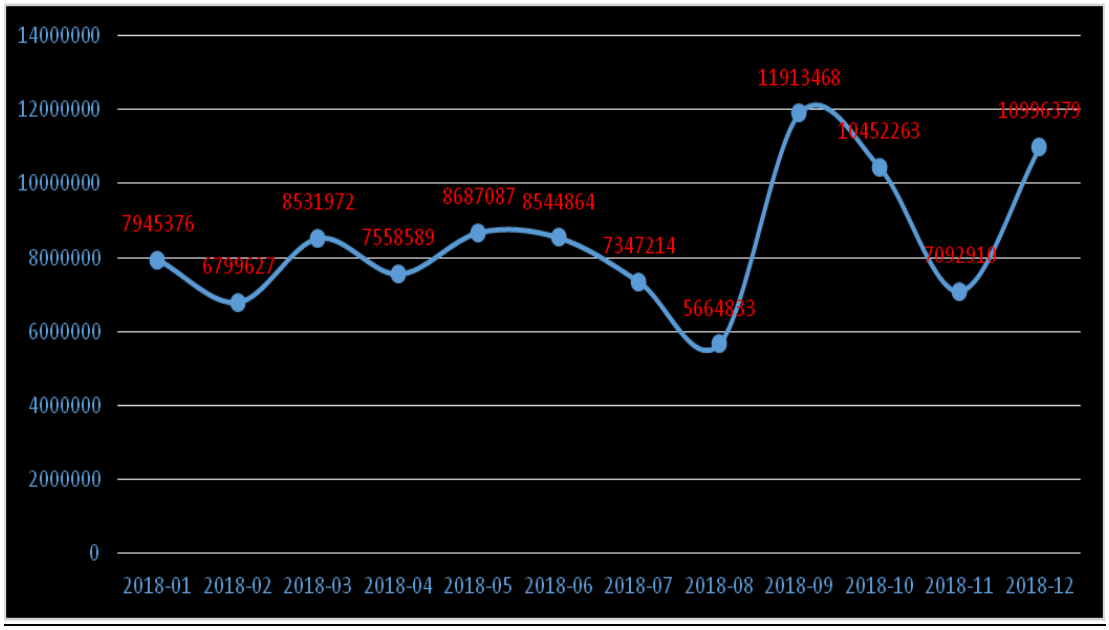


Figure 3: Botnet events tracked by Botnet Cleaning and Malware Analysis Centre

3.3.3 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, CERT-In has empanelled **76** technical IT security auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Implementation enabling workshops/interactions have been conducted. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

4. Events organized / hosted

4.1 Security awareness, skill development and training

In order to create security awareness within the Government, Public and Critical Sector organisations, CERT-In regularly conducts trainings / workshops to train officials of

Government, critical sector, public sector industry, financial & banking sector on various contemporary and focused topics of Cyber Security. In 2018, CERT-In has conducted 24 trainings on various specialized topics of cyber security. A total of 746 officers including system/Network Administrators, Database Administrators, Application Developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained. CERT-In carried out a specific training session only for women IT professionals.

CERT-In has conducted the following training programmes in 2018:

- Workshop on " Protection Against Social Media Misuse & Cyber Frauds " in January 2018
- Joint Workshop with JPCERT/CC on “Android Security & Secure Coding" at New Delhi in February 2018
- Joint Workshop with JPCERT/CC on "Android Security & Secure Coding” at Bengaluru in February 2018
- Workshop on " Redefining Cyber Security " in February 2018
- Workshop on "Cyber Security Threats & Mitigations" in February 2018
- Workshop on " Darknet and Importance of Cyber Intelligence For Next Gen SoC" in March 2018
- Workshop on "Workshop on Cyber Threats & Countermeasures" in March 2018
- Workshop on "Cyber Crisis Management Plan" in May 2018
- Workshop on " Cyber Threat Hunting with Analytics " in June 2018
- Workshop on " Cyber Crisis Management Plan" in June 2018
- Workshop on “"Combating Advanced Cyber Security Threats using Artificial Intelligence " in July 2018
- Workshop on " Cyber Crisis Management Plan " in August 2018
- Workshop on " SDWAN Security & Next Generation Firewall " in August 2018
- Workshop on "Advanced Cyber Security Threats Detection & Mitigation" in September 2018
- Workshop on "Cyber Threats & Countermeasures" in September 2018
- Workshop on " Cyber Threat Landscape & Role of CERT-In" in September 2018
- Workshop on " Automated Security Configuration Management" in September 2018
- Workshop on " Cyber Threats & Role of CERT-In " in October 2018
- Workshop on " Cyber Threats and Countermeasures exclusively" in October 2018

- Workshop on " Network Security, Visibility & Monitoring " in October 2018
- Workshop on " Workshop on Vigilance Awareness " in October 2018
- Workshop on "Cyber Crisis Management Plan" in November 2018
- Workshop on " Cyber Threat Landscape & Role of CERT-In" in December 2018
- Workshop on " Workshop on Cloud Security" in December 2018

4.2 Cyber Security Exercises

Cyber security exercises are being conducted by the Government to help the organizations to assess their preparedness to withstand cyber attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 11 exercises in 2018.

4.3 Cyber Forensics

CERT-In is equipped with the tools and equipment to carry out retrieval and analysis of the data extracted from the digital data storage devices using computer forensics and mobile device forensic techniques. CERT-In's facility for Digital Forensics data extraction and analysis is being utilised in investigation of the cases of cyber security incidents, submitted by central and state government ministries, departments, public sector organizations, law enforcement agencies, etc. CERT-In imparts training through workshops organised by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices. CERT-In also provides support to the other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

5. International Collaboration

5.1 International partnerships and agreements

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understandings (MoUs) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information

in a timely manner for preventing cyber incidents and cyber attacks as well as collaborating for providing swift response to such incidents. In 2018 CERT-In signed MoUs on cyber security cooperation with two countries namely The Department of Information Communications Technology, The Republic of Seychelles and The Moroccan Computer Emergency Response Team (ma-CERT), National Defence Administration, The Kingdom of Morocco to enable information sharing and collaboration for incident resolution. CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.

5.2 Drills & exercises

CERT-In played the role of EXCON and also participated as a player in APCERT Drill 2018 conducted in March 2018 based on the theme "Data breach via malware on IoT" to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. The objective was to enables CERTs to review, practice and strengthen computer security incident handling mechanism and exercise coordination with multiple parties (internal and external) when handling computer security incidents.

CERT-In participated in the ASEAN CERTs Incident Response Drill (ACID) in September 2018 wherein the objective was strengthening cyber security preparedness of ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination to test incident response capabilities. The theme of the drill was handling System Vulnerabilities and Crypto currency Mining.

CERT-In participated in The Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) drill in September 2018. The theme of the drill was handling Crypto-currencies Risks and Emerging Threats.

5.3 Other international activities

- CERT-In participated in Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) Conference and APCERT SC Meeting from 24 to 28 February 2018 at Kathmandu, Nepal.
- CERT-In participated in the Asia Pacific Computer Emergency Response Teams

(APCERT) Annual General Meeting (AGM), Steering Committee (SC) Meeting and Conference 2018 from 21 to 26 October 2018 at Shanghai, China.

- CERT-In participated in the FIRST AGM & Conference and National CSIRT Meetings from 25 to 30 June 2018 at Kuala Lumpur, Malaysia.
- CERT-In participated in 3rd Singapore International Cyber Week (SICW), Annual Meeting of the Global forum for Cyber Expertise (GFCE) and 6th Europol-INTERPOL Cybercrime Meetings from 18th to 20th September 2018 at Singapore.
- CERT-In was an observer at the NATO "Cooperative Cyber Defense Centre of Excellence" organised Cyber Defense Exercise "Locked Shields 2018". Locked shields is the world's largest and most complex international technical cyber defense exercise.
- CERT-In is a contributing member of review group of the Second Security, Stability, and Resiliency (SSR2) of the Domain Name System(DNS) Review is mandated by Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws Section 4.6(c) to examine how effectively ICANN is meeting its commitment to enhance the operational stability, reliability, resiliency, security and global interoperability of the systems/processes internal/external) that affect the Internet's unique identifiers. The SSRReview Team is reviewing the extent to which ICANN has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability, and resiliency of the DNS, consistent with ICANN's Mission.
- CERT-In has participated in meetings of Internet Governance Forum (IGF) and the discussions under the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations in 2018.
- CERT-In is a participating and contributing task force member in the Cyber Incident Management and Critical Information Protection working group of the Global Forum for Cyber Expertise (GFCE), a global platform for countries, international organisation and private companies to exchange best practices and

expertise on cyber capacity building by identifying successful policies, practices and ideas so as to multiply these on a global level.

6. Future Plans

6.1 Future projects

CERT-In has evolved as the most trusted referral agency in the area of information security in the country. The future plans envisaged are:

- Setting up of Internet of Things (IoT) device Security Testing lab to enable IoT integrators, developers and manufacturers to enhance the security of smart technologies.
- A full pledged automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) across stake holders will come up in the coming year.
- A full pledged version of Threat and Situational Awareness Project (TSAP) named National Cyber Coordination Centre (NCCC) will be implemented by CERT-In in the coming years.

6.2 APCERT Working Groups

- IoT Security Working Group
  - To ensure the secure usage of IoT devices in priority sectors and build trust in secure usage of IoT Ecosystem
- Secure Digital Payments Working Group
  - Build trust in secure usage of digital payments so as to ensure economic stability.

Contact Information

Postal Address:

Indian Computer Emergency Response Team (CERT-In)
Department of Electronics & information Technology
Ministry of Communication & information technology
Government of India
Electronic Niketan
6, CGO Complex, Lodhi Road
New Delhi – 110003, India

Incident Response Help Desk:

Phone: +91-11-24368572

+91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546

+91-1800-11-6969 (Toll Free)

PGP Key Details:

User ID: incident@cert-in.org.in

Key ID: 0x643B5C9F

Key Type: RSA

Expires: 2019-05-23

Key Size: 4096/4096

Finger Print: 4604 0698 6802 80E4 13E0 091D 4C31 F91E 643B 5C9F

User ID:

info@cert-in.org.in

advisory@cert-in.org.in

subscribe@cert-in.org.in

Key ID: 0xCCA20F32

Key Type: RSA

Expires: 2019-05-23

Key Size: 4096/4096

Finger Print: 9486 28E6 0268 8DD2 47AF DE72 579D 0C18 CCA2 0F32

*****

CERT NZ

CERT NZ – New Zealand

1. Highlights of 2018

1.1 Summary of major activities

CERT NZ was launched in April 2017, joining New Zealand to the international network of over 100 other CERT-like partner agencies worldwide to get a picture of the cyber threat landscape, both in New Zealand and across the globe. Since establishment, CERT NZ has quickly become an active member of the international CERT network, in addition to playing an important role in its domestic cyber security ecosystem.

1.2 Achievements & milestones

- CERT NZ has run two Cyber Smart Awareness Weeks, published regular quarterly reports, advice and guidance on its website, and built a network of private sector partners to help share information and messaging to achieve greater reach than it could alone.
- CERT NZ's Coordinated Vulnerability Disclosure service allows a process for coordinated disclosures to be made via the CERT NZ website.
- Worked with the international CERT network on a number of incidents, issuing advisories and sharing information.
- Supported the establishment of the Pacific Cyber Security Operational Network (PACSON, a group set up to help build cyber security operational engagement in the Pacific.

2. About CERT NZ

2.1 Introduction

CERT NZ is New Zealand's national computer emergency response team. CERT NZ was set up to improve cyber security in New Zealand, using our broad access to people, information and data to help New Zealand better understand and stay resilient to the threat landscape. It is designed to meet the needs of the whole New Zealand economy. CERT NZ is for all New Zealanders and supports everyday New Zealanders, and all types of businesses and organisations, from small and medium-sized enterprises through to government agencies and large corporates.

2.2 Establishment

CERT NZ was launched in April 2017 following an announcement in May 2016 that the New Zealand Government would invest in a new organisation to combat cyber security threats.

2.3 Resources

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has 20 FTE, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

2.4 Constituency

CERT NZ serves all New Zealanders: from individuals and small businesses, all the way through to multi-national organisations and government departments.

3. Activities & Operations

3.1 Scope and definitions

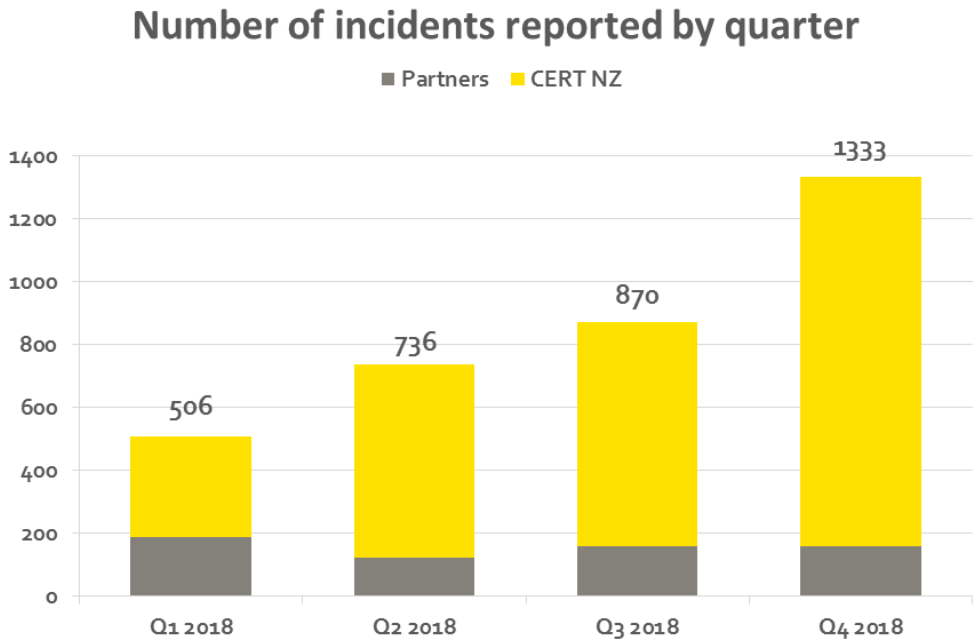
CERT NZ's key services are:

- **Threat identification**: We analyse the international landscape and report on threats.
- **Vulnerability identification**: We analyse data and report on vulnerabilities in New Zealand.
- **Incident reporting**: We triage reported incidents and make referrals.
- **Response coordination**: We lead the response to some incidents, coordinate the response to others and we support the national emergency response process.
- **Readiness support**: We help to define the best protections, and raise awareness of cyber security risks, mitigations and impacts.

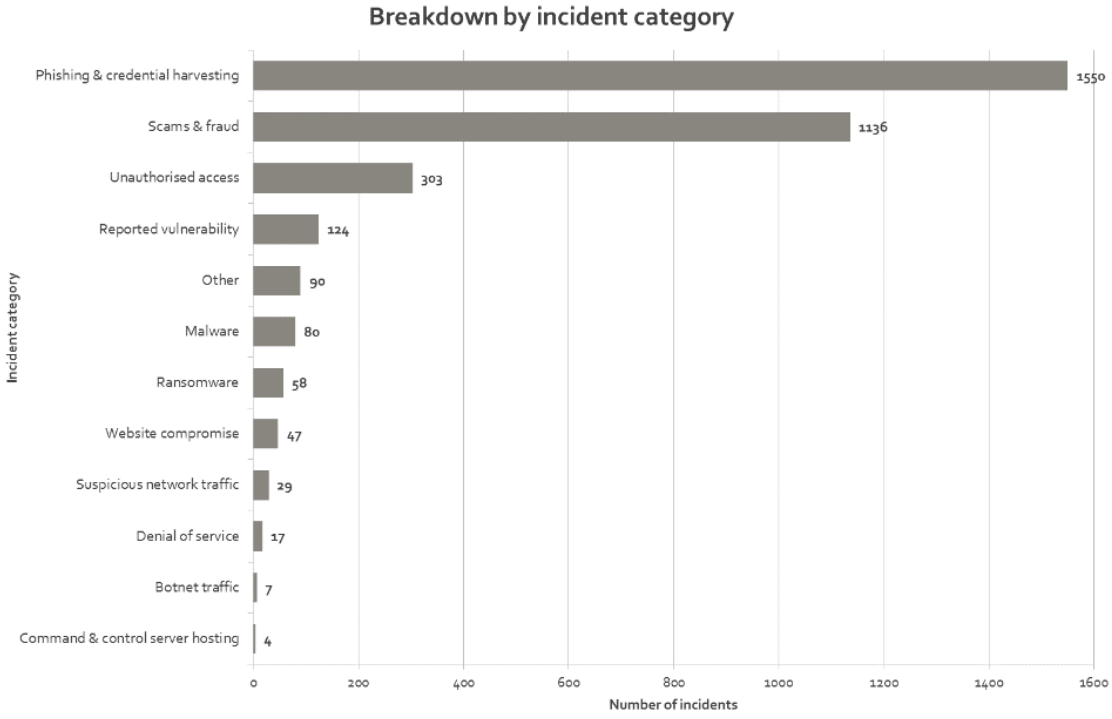
3.2 Incident handling reports

In 2018, CERT NZ received 3445 incident reports through its website reporting tool. Of these incident reports, 2818 were responded to directly by CERT NZ and 627 were referred to partner agencies. Referrals occur if it's more appropriate that a partner agency investigate it. CERT NZ's partner agencies for referrals are: Department of Internal Affairs, National Cyber Security Centre (NCSC), Netsafe and NZ Police. The graph below shows the breakdown of incident reports, including referrals, by quarter in

2018.

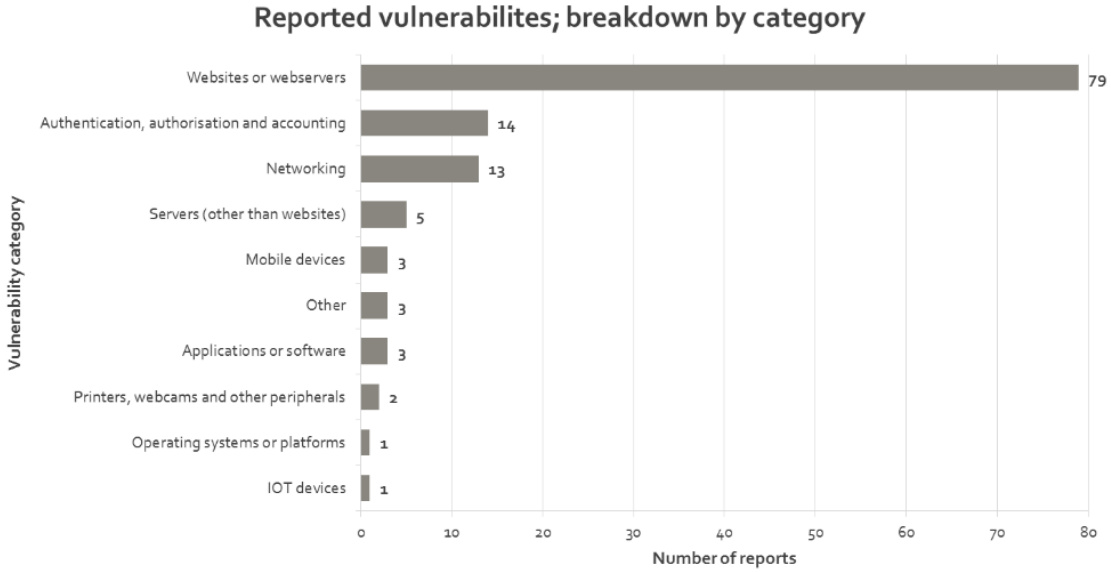


CERT NZ uses categories to record the types of incident reports it receives. The 2018 breakdown by category, including referrals, is presented in the graph below.



Reported vulnerabilities are further broken down under sub-categories below. 22 (18%)

of the reported vulnerabilities received, were handled under CERT NZ's Co-ordinated Vulnerability Disclosure (CVD) policy.



For further information on the incidents handled in 2018, see CERT NZ publications[1].

4. Publications

4.1 Advisories and alerts

CERT NZ publishes two types of public advisories – one for everyday New Zealanders and one for a more technical audience. The former is often used by media and organisations to communicate with their customers or staff. The latter has more technical detail and readers are assumed to understand industry specific jargon. CERT NZ determines what type of advisory to publish depending on the type of threat, and who the information is targeted at.

Advisories are shared on our website, emailed to subscribers, and shared via social media (Twitter):

- Technical advisories: https://www.cert.govt.nz/it-specialists/advisories/
- Non-technical advisories:

https://www.cert.govt.nz/businesses-and-individuals/recent-threats/

[1] https://www.cert.govt.nz/about/quarterly-report/

4.2 Quarterly reporting

For 2018 a new format was trialed, splitting quarterly reports into two documents:

- **Quarterly Report: Highlights** document which summarises key observations and focus areas that our data is demonstrating
- **Quarterly Report: Data Landscape** document which provides graphs and information about the reports we receive and the impact this has on New Zealand

These reports include high level analysis, deep dives into trending issues, case studies and details of the numbers of cases being referred to its partner agencies. This allows others to learn from the incidents reported to CERT NZ, and the information we received from the international CERT community.

By producing high quality & regular content, CERT NZ meets its commitment to produce information in an open and transparent way. Quarterly reports have been well received by the technical community, government agencies and media, as well as lending greater credibility to CERT NZ as we become more established in the New Zealand landscape.

4.3 Quarterly news updates

CERT NZ produces a subscription-based e-newsletter that is sent out quarterly, it

includes first access to the CERT NZ Quarterly reports, information on recent threats, and updates on new content available from CERT NZ.

4.4 CERT NZ social media

CERT NZ runs a Twitter account @CERTNZ, and is one of our main channels to share information with New Zealanders.

4.5 CERT NZ Critical Controls

CERT NZ's ten critical controls would mitigate, or better contain, the majority of attacks we've seen, and will be reviewed on an annual basis based on the reports we've received.

4.6 Other publications

CERT NZ has produced a range of resources help keep New Zealanders safe online, such as how to create strong passwords.

5. Events organised / hosted

5.1 Conferences and seminars

CERT NZ ran its second cyber security awareness campaign, Cyber Smart Week, in October 2018. CERT NZ engaged with partners from across government and the private sector to share cyber security safety messages that gave people the tools to stay safe online. CERT NZ worked with 78 partner organisations with a combined reach of over 4 million people. CERT NZ created resources that were easily shared, and came with the backing of New Zealand's national authority on cyber security. 98% of participants in the 2018 campaign said they would be likely to participate in future campaign activities.

A mini "protect it!" campaign aimed at small to medium businesses protecting their websites ran from 30 July to 3 August 2018. Forty organisations signed up to be involved in the mini campaign. A campaign page was created on the CERT NZ website for more detailed information and links to relevant content to contain campaign costs whilst still providing key material and messages for participants.

6. International Collaboration

6.1 International partnerships and agreements

CERT NZ is a member of the Asia Pacific CERT forum (APCERT), the Forum of Incident Response Teams (FIRST), the International Watch and Warning Network (IWWN) and the Pacific Cyber Security Operational Network (PACSON).

7. Capacity building

7.1 Training

No formal international training activities were undertaken in 2018.

7.2 Drills & exercises

CERT NZ's focus remained on participation in domestic drills & exercises in 2018, and will engage in international exercises in 2019.

7.3 Seminars & presentations

Key presentations in 2018 by CERT NZ are listed below:

- ACSC, April 2018
- NatCSIRT, June 2018
- CHCON Christchurch, October 2018
- Netsafe, October 2018
- PACSON, November 2018
- NZITF, November 2018

8. Future Plans

8.1 CERT NZ will continue to build and expand the delivery of its core services over the next 12 months, and align its work with the updated New Zealand cyber security strategy. Central to its focus is active participation in the international CERT community, to ensure CERT NZ supports the global efforts to improve cyber security.

9. Conclusion

CERT NZ is still very new, but it's growing fast and will continue to deliver and mature in 2019.

Contact Information

Website:

www.cert.govt.nz

Twitter:

@CERTNZ

By post:

CERT NZ

PO Box 1473

Wellington 6140

By phone (to report an incident):

- In New Zealand, call us on 0800 CERT NZ (0800 2378 69).
- From overseas, call +64 3 966 6295

PGP Key details:

Send PGP encrypted email to: ir@ops.cert.govt.nz

Our PGP fingerprint is: D26F 509F 510D 5618 761D 83FF E2CD 67C3 9AE4 71F2

CNCERT/CC

National Computer network Emergency Response technical Team / Coordination Center of China - People's Republic of China

1. About CNCERT

1.1 Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) is a non-governmental non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community.

1.2 Establishment

CNCERT was founded in 2002, and became a member of FIRST in Aug the same year. It also took an active part in the establishment of APCERT as a founding member.

1.3 Workforce power

CNCERT, which is based in Beijing, the capital of China, has spread branch offices in 31 provinces, autonomous regions and municipalities in mainland China.

1.4 Constituency

As a national CERT, CNCERT strives to improve the nation's cybersecurity posture and protect critical infrastructure cybersecurity. CNCERT leads efforts to prevent, detect, warn and coordinate cybersecurity threats and incidents, pursuant to the guideline of "proactive prevention, timely detection, prompt response and maximized recovery".

1.5 Contact

E-mail : cncert@cert.org.cn

Hotline : +8610 82990999（Chinese）, 82991000（English）

Fax : +8610 82990375

PGP Key : http://www.cert.org.cn/cncert.asc

2. Activities & Operations

2.1 Incident handling

In 2018, CNCERT received a total of about 106.7 thousand incident complaints, a 3.2%

increase from the previous year. And among these incident complaints, 677 were reported by overseas organizations, making a 40.7% rise from the year of 2017. As shown in Figure 2-1, most of the victims were plagued by phishing (33.3%), vulnerabilities (27.0%) and malware (21.5%). Phishing overtook vulnerabilities to be the most complained about category.

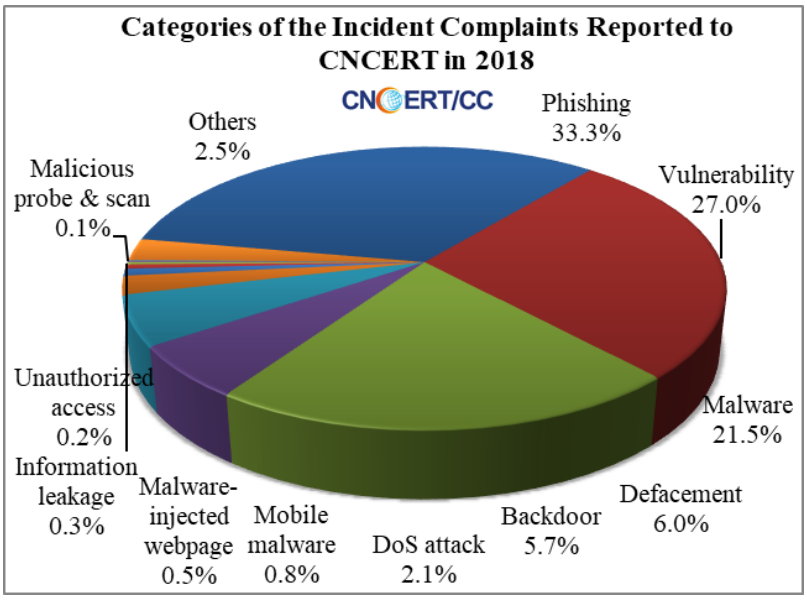


Figure 2-1 Categories of the Incident Complaints Reported to CNCERT in 2018

In 2018, CNCERT handled almost 105.7 thousand incidents, a rise of 2.0% compared with that in 2017. As illustrated in Figure 2-2, phishing (33.5%) dominated the chart about categories of the incidents handled by CNCERT in 2018, followed by vulnerability (27.0%) and malware (21.4%).

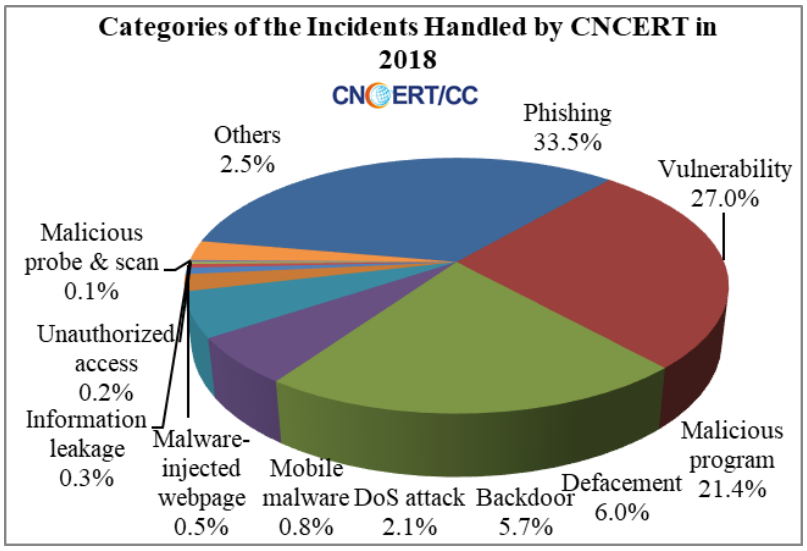


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2018

2.2 Internet Threats

2.2.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 6.56 million, which decreased by 47.8% compared with that in 2017. We saw more than 49.5 thousand overseas C&C servers which increased by 4.5% from 2017. As shown in Figure 2-3, the U.S. hosted the largest number of overseas C&C servers' IPs of Trojan or Botnet, followed by Hong Kong, China and France.

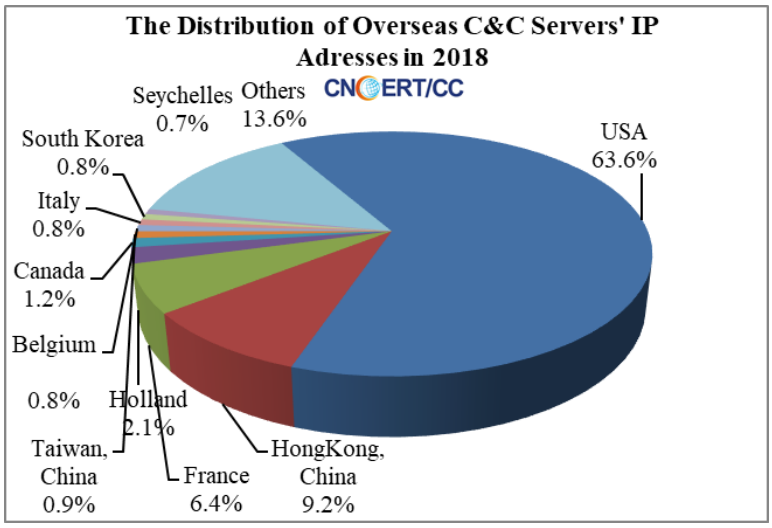


Figure 2-3 Distribution of overseas C&C servers' IP addresses in 2018

By CNCERT's Conficker Sinkhole, over 15.0 million hosts were suspected to be compromised all over the world, among which 2.4 million were located in mainland China. As shown in Figure 2-4, mainland China (16.8%) had the most infection, followed by India (8.2%), and Indonesia (5.2%).

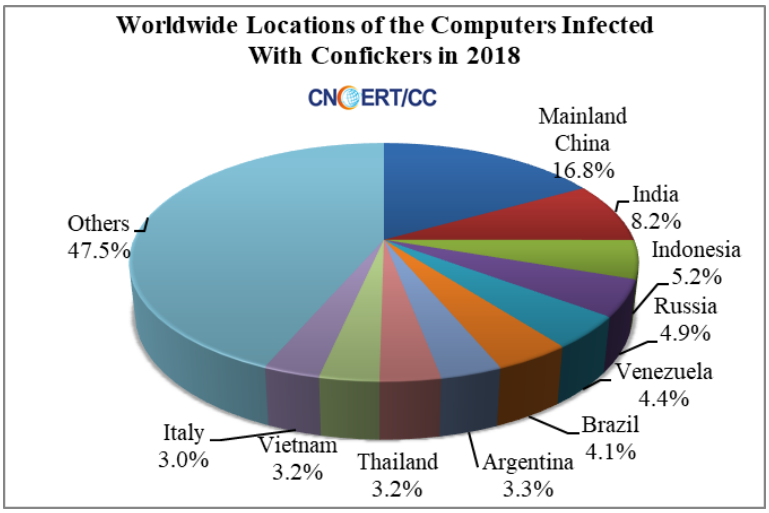


Figure 2-4 Worldwide Locations of the Computers Infected with Conficker in 2018

Malware-hosting websites are the jumping-off places for malware propagation. The malware-hosting websites monitored by CNCERT in 2018 involved about 308 thousand domains, 1.4 million addresses and 1.2 million malware download links. Among the 308 thousand malicious domains, 71.4% of their TLDs fell into the category of .com. Among the 1.4 million malicious IPs, 36.0% were located overseas.

2.3 Website Security

About 7.0 thousand websites in mainland China were defaced, a decrease of 64.9% compared with that in 2017, including 216 government sites. Besides, about 23.6 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, out of which 674 were government sites.

In 2018, CNCERT found about 5.3 thousand phishing sites targeting the websites in mainland China. About 10.4 thousand IPs were used to host those fake pages, and 99.5% were out of mainland China. Most of the phishing servers (17.5%) were located in Russia.

CNCERT found almost 14.3 thousand overseas IPs conducting remote control on over 16.5 thousand websites in mainland China. As shown in Figure 2-5, 3,325 (23.2%) were located in the U.S., followed with 1,565 (10.9%) in Russia and 584 (4.1%) in Hong Kong, China.

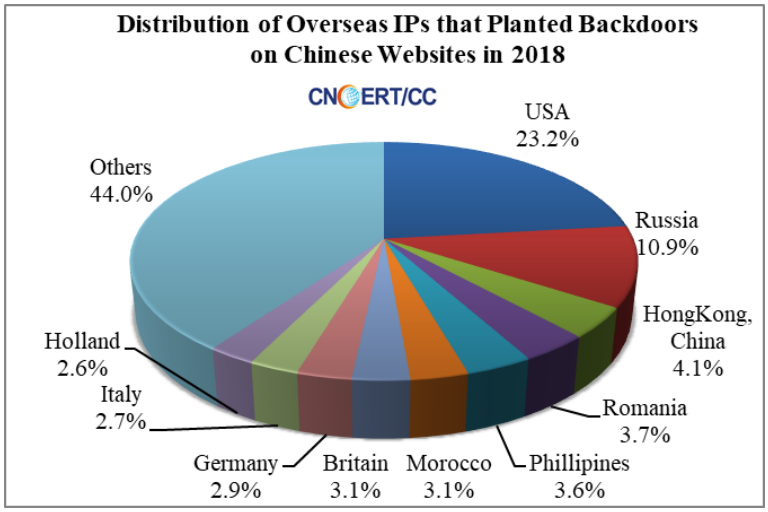


Figure 2-5 Distribution of Overseas IPs that Planted Backdoors on Chinese Websites in 2018

2.4 Mobile threats

In 2018, CNCERT collected about 2.83 million mobile malware samples in total. In

terms of the intentions of these mobile malware, rogue behavior took the first place (45.8%), fee consumption (24.3%) secured the second rank, and the next two were those intended for stealing privacy and malicious fee deduction for 14.8% and 11.6% respectively.

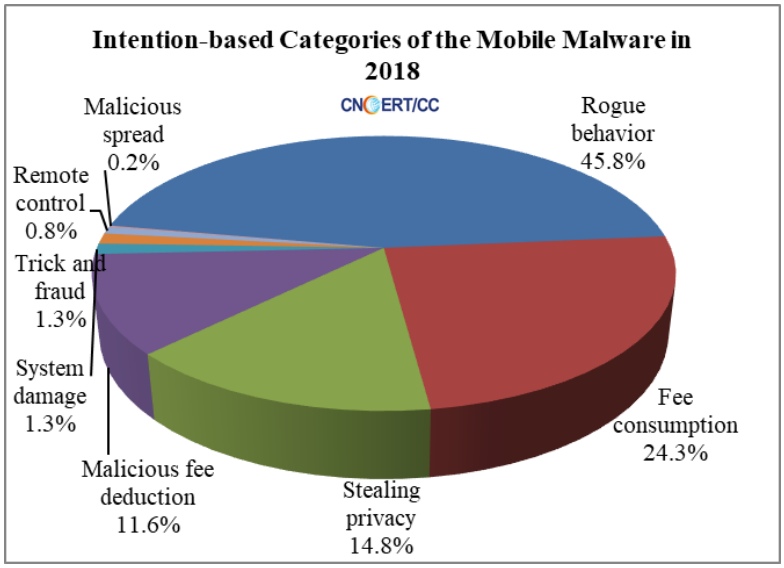


Figure 2-6 Intention-based Categories of the Mobile Malware in 2018

All of these mobile malware identified by CNCERT ran on Android system, recording about 0.12 million (100.0%).

3. Events organized/co-organized

3.1 Conferences

The 2018 CNCERT Annual Conference in Beijing

On August 15th, 2018, CNCERT held the 2018 Annual Chinese Conference on Computer and Network Security in Beijing. Focusing on the theme "Escort Intelligence Ecology with the Intelligent Brain", the conference invited representatives from government departments, important information system units, universities, research institutes and network security industries to discuss and exchange new trends, problems and ideas of network security, so as to build a bridge for communication between network security and all sectors of society.

The FIRST Regional Symposium in Shanghai

The 2018 FIRST Regional Symposium, co-sponsored by CNCERT and the International FIRST Forum, was successfully held from 25th to 26th, October in

Shanghai. The seminar attracted more than 70 delegates from governments, industries, research and academic institutions. The seminar not only covered the latest development trend of network security, but also enabled participants in the Asia-Pacific region to have a deeper understanding of FIRST.

The China-ASEAN Network Security Emergency Response Capacity Building Seminar in Shanghai

On October 22nd, 2018, CNCERT organized the China-ASEAN Network Security Emergency Response Capacity Building Seminar in Shanghai. Delegates from the government departments for telecom affairs and CERTs of Cambodia, Indonesia, Laos, Malaysia, Singapore, Myanmar, Thailand and Vietnam attended the Seminar. The participants exchanged technological development experience in the field of network security and discussed ways to conduct cooperation on network security emergency response between China and ASEAN.

The 2018 APCERT Annual General Meeting in Shanghai

The 2018 APCERT Annual Conference sponsored by CNCERT was successfully held in Shanghai from October 21st to 24th. More than 150 delegates from 50 organizations of 30 countries and regions participated in the meeting. The theme of APCERT Annual General Meeting is "Promoting Information Sharing and Developing Effective Collaborative Emergency Response". 27 members of APCERT (30 members in APCERT) attended the meeting, exchanging views on APCERT policy, operation, membership rules and working group progress.

4. Drill attended

APCERT Incident Drill 2018

CNCERT participated in the APCERT 2018 Drill on 7th, March, 2018 and completed it successfully. The theme of the APCERT Drill 2018 was "Data Leakage Caused by Malware on the Internet of Things". This drill was based on the real events and situations on the Internet, simulated the scene of the attacked medical institutions, analyzed and coordinated the handling of data infiltration and Internet of Things equipment infection incidents caused by malicious software.

China-ASEAN Network Security online Training 2018

CNCERT participated in China-ASEAN Network Security Field Training from 11th

to 17th, November in Naypyidaw, Myanmar and Jakarta, Indonesia. The training was carried out to implement specific measures for the construction of China-ASEAN information ports and the "Initiative for the field training on China-ASEAN network security" adopted by China and ASEAN. Participants from CERT organizations, local governments and partners from both countries attended the training.

5. Achievements

CNCERT's weekly, monthly and annual reports, as well as other released information, were reprinted and cited by massive authoritative media and thesis at home and abroad.

Table 5-1 Lists of CNCERT's publications throughout 2018

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (http://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Reports (Chinese)	12	Issued to over 400 organizations and individuals on a regular basis and published on CNCERT's website (http://www.cert.org.cn/)
CNCERT Annual Reports (Chinese)	2	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	302	Published on journals and magazines

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. Highlights of 2018

EC-CERT is committed to supporting and strengthening E-commerce companies' ability to respond to and handle security incidents, and is working with E-commerce Alliances to promote PII and information security activities. EC-CERT has established a basic checklist for E-commerce information security, promoting E-commerce companies to check the completion of security protection and encouraging this industry to strengthen security management.

EC-CERT organizes a seminar inviting hackers to exchange views with CEOs of E-commerce companies face to face. In the past, due to lack of IT professionals and budget, many small scale E-commerce companies couldn't find out security-related loopholes by themselves, by this way, they discussed security breach issue and work out a resolution of the security as well as strengthen transaction security protection.

2. About EC-CERT

2.1 Introduction

EC-CERT stands for "Electronic Commerce - Computer Emergency Response Team", which is supported by Ministry of Economic Affairs of ROC. EC-CERT regularly task composed of information security consulting service and website vulnerability scanning with penetration testing, incident response, issue security information alert, etc., EC-CERT offers services confirmed favor on prevent E-commerce finance fraud in case of monetary loss and smoothly developing of Taiwan's E-commerce market.

2.2 Establishment

EC-CERT was established in 2010. The main role of EC-CERT is to assistance E-commerce industry enhanced information security, to help deal with information security incidents, avoid being hacked as well as including take promotion of information security and PII protect activities.

2.3 Constituency

EC-CERT aims to enhance E-commerce Company's ability to respond and deal with

security incidents and relative issues. EC-CERT provides security counseling, respectively as E-commerce platforms, logistics providers and service providers, counseling by E-commerce to enhance information security protection in case of external attacks.

3. Activities & Operations

3.1 Scope and definitions

In 2018, EC-CERT planned to come out many E-commerce industry information security reports including web site security online consulting records and step-by-step practical case-solving procedures and recommendations.

3.2 Incident handling reports

EC-CERT provides 29 event visits, handling 24 security incidents, providing 23 security advices, and received 33 computer security incident reports from E-commerce companies

3.3 Publications

- Online retail industry information security protection practice case selection
- Online retail industry information security basic checklist

4. Events organized / hosted

4.1 Conferences and seminars

- Information security promotion activities * 3
- Participation Asia PKI Union Conference * 2

5. International Collaboration

5.1 Capacity building

5.1.1 Training

EC-CERT participated and benefited from the following APCERT Training topics:

- Malware Information Sharing Platform MISP in a CERT
- Analyses of A Compromised Linux Server
- Performing Forensics on and Azure Virtual Machine
- Shaoye Botnet - Android Malware & DNS Hijacking
- Inside the APCERT Drill

5.1.2 Drills & exercises

EC-CERT participated in the APCERT Drill in March 2018. The topic of APCERT online drill is ”Data Breach via Malware on IOT”.

5.2 Other international activities

EC-CERT attended APCERT AGM and Conference 2018 (October, Shanghai, China)

6. Future Plans

EC-CERT aims to create an E-commerce response centre that can help optimize the capability of security incidents, coordination, response and handling in the face of security incident.

The E-commerce industry's security incidents will easily cause increases in consumer fraud cases, how to help E-commerce industry conduct prevention with other detective controls and follow up improvement is the key point of EC-CERT in 2019.

7. Conclusion

As long as information technology in progresses, there will always be scams but the key to point is the user awareness and the security management. EC-CERT will continue to work on E-commerce information security in Taiwan.

GovCERT.HK

Government Computer Emergency Response Team Hong Kong – Hong Kong, China

1. Highlights of 2018

1.1 Summary of Major Activities

To enhance the city's overall defensive capability and resilience against cyber attacks, we officially launched a Partnership Programme for Cyber Security Information Sharing named "Cybersec Infohub" and the first cross-sector cyber security information sharing and collaborative platform (Cybersechub.hk) in September 2018. Since then, we have organised numbers of seminars and workshops to promote trusted partnership of local cyber security stakeholders across prominent sectors for sharing cyber security information and providing actionable insights to the community.

Within the Government of the Hong Kong Special Administrative Region (HKSAR Government), we continued to co-organise with the Hong Kong Police Force (HKPF) to run the annual inter-departmental cyber security drill for government departments. The drill of this year not only walked through the procedures of incident response, but also provided a hands-on workshop simulating a cyber attack scenario for participants to get familiar with hands-on investigation and analysis techniques.

A keen appreciation of the threat landscape could help organisations and individuals to understand better the cyber threat environment so as to adopt early and appropriate mitigation measures. In 2018, we continued publishing threat trends, security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public. We further tailored specific threat awareness updates for government departments.

We are also committed to promoting information security awareness to various sectors of the community by collaborating with different organisations to regularly hold various cyber security publicity events to raise public awareness and capability development.

1.2 Achievements and Milestones

Cyber Security Information Sharing

With the objective to facilitate cross-sector collaboration for a better visibility of cyber

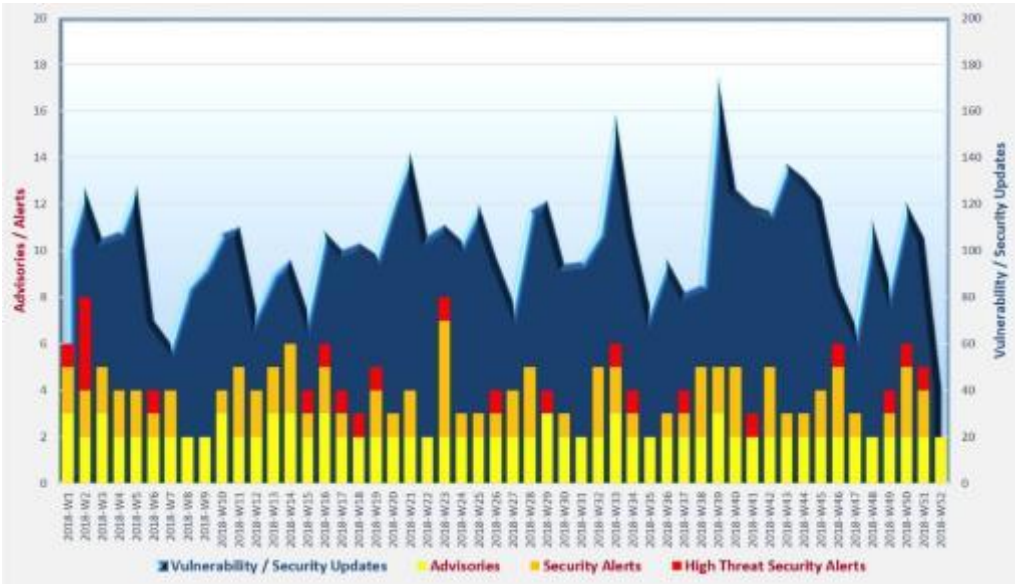
threats globally and locally, Cybersec Infohub serves well as an enabler to nurture culture in sharing cyber security information.

We are grateful to see active participation since the launch of Cybersec Infohub. As of 2018, over 100 organisations with more than 300 representatives across various sectors have joined the Programme. Many of them have taken the lead to share information on the platform. The Programme has become an essential reference for organisations in gathering security intelligence and meeting with peers to share experiences and successes.

Cyber Threat Intelligence Management

GovCERT.HK has been monitoring cyber security threat trends and sharing relevant information with our constituents and the community for taking early precautions and together reinforcing Hong Kong's cyber security. We publish monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight the observations of latest cyber security threat landscape for reference by the public to enhance their situational awareness.

Cyber Security Threat Landscape



Liaison and Collaboration

We proactively participate in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and work closely with the Computer Emergency Response Team (CERT) community in handling threat information. In 2018, we delivered a

presentation at the APCERT Annual General Meeting and Conference to promote partnership and collaboration in cyber security information sharing.

Capability Development

To facilitate the HKSAR Government in developing staff capabilities to tackle evolving cyber threats, we established the GovCERT.HK Technology Centre in 2018. The centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning and security testing for potential security issues of their web applications.

Awareness Building and Public Education

User awareness of information security plays a vital role in coping with cyber threats. In view of the rising trend of phishing attacks, GovCERT.HK created a series of promotional materials including educational videos and smart tips for the public to protect themselves from and defend against phishing attacks.

GovCERT.HK also devotes much attention to public education and capacity building in different business sectors and age groups. In 2018, we organised 36 school visits to reach out to some 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams of the HKSAR Government.

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling; and empowered close collaboration with the industry, critical Internet infrastructures, and the CERT community for timely exchange of cyber threat information and coordinated responses. GovCERT.HK also works closely with Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and local industry on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security and resilience through social and mass media.

GovCERT.HK also collaborates with the CERT community globally in sharing threat

intelligence and incident information; participating in training events, workshops, forums and drills; and organising public awareness promotion activities and capability development initiatives.

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

GovCERT.HK is an establishment under OGCIO and funded by the HKSAR Government.

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident responses within the HKSAR Government and develop CERT-related services to assist government departments in understanding the associated risks of information and cyber security, implementing appropriate security measures, monitoring potential threats and responding to security events with a view to ensuring government's information infrastructure would be well protected.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team for the HKSAR Government, providing centrally managed incident response services and timely security advice; coordinating cyber security drills; promoting public awareness and capabilities; and engaging global CERT community with a view to enhancing information and cyber security locally and in the region.

3.2 Security News Bulletins

In 2018, GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public.

- "Security Vulnerabilities and Patches" information was consolidated on every working day and disseminated to registered subscribers through emails;

- "Security Industry News" was gathered on every working day and top news with wide impact was compiled and disseminated to registered subscribers through emails; and
- "Weekly IT Security News Bulletins" was published on the first working day of each week to highlight top two to three hot security news and summarise vulnerabilities by products for easy reference by security practitioners. These Bulletins were distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information. (www.govcert.gov.hk/en/reports.html#weekly-reports)

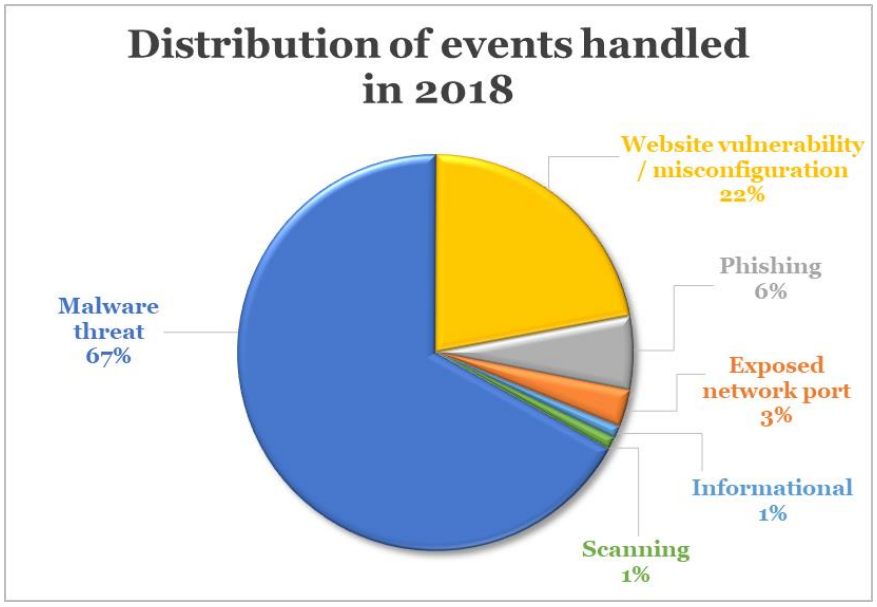
3.3 Alerts and Advisories

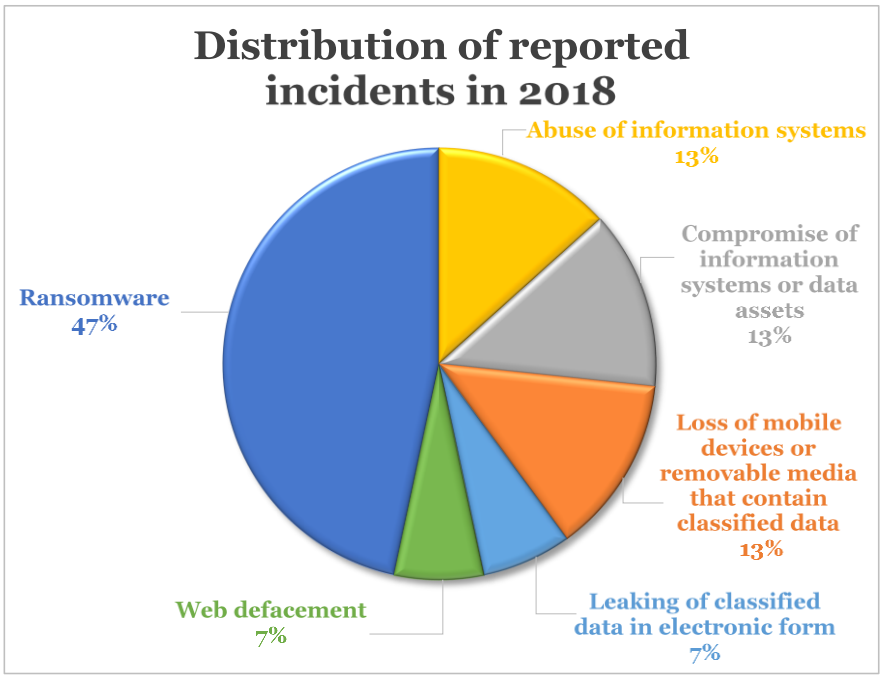
In 2018, we published 103 product security alerts associated with computing products widely deployed in government installations. We also released a security advisory for public reference highlighting the risk of the VPNFilter malware attack and recommending appropriate measures to protect their network equipment. (www.govcert.gov.hk/en/advisories.html)

In 2018, we conducted threat analysis on over 300 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents for appropriate follow-ups.

3.4 Security Events and Incident Handling

Security events indicate possible breaches of information security or failure of security controls. Security incidents, however, are in relation to one or multiple events that can harm information systems and/or data assets or compromise their operations. In 2018, GovCERT.HK dealt with various cyber security events and reported incidents that were related to government installations. The following chart shows the distribution of events and reported incidents handled in 2018.



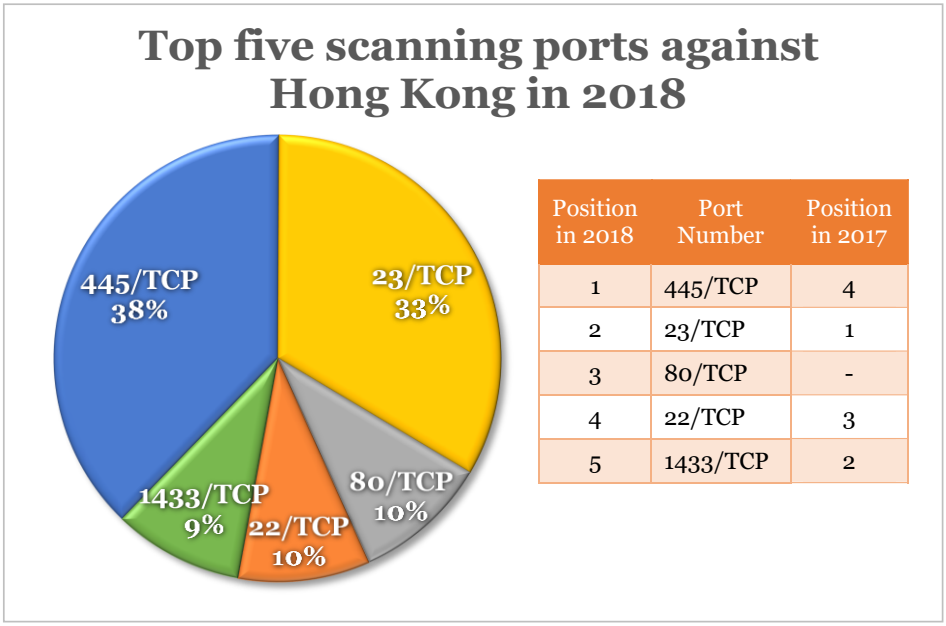


To facilitate the public to access the statistics on information security incidents in the Government, relevant data has been released to the Government's Public Sector Information Portal.
(www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident)

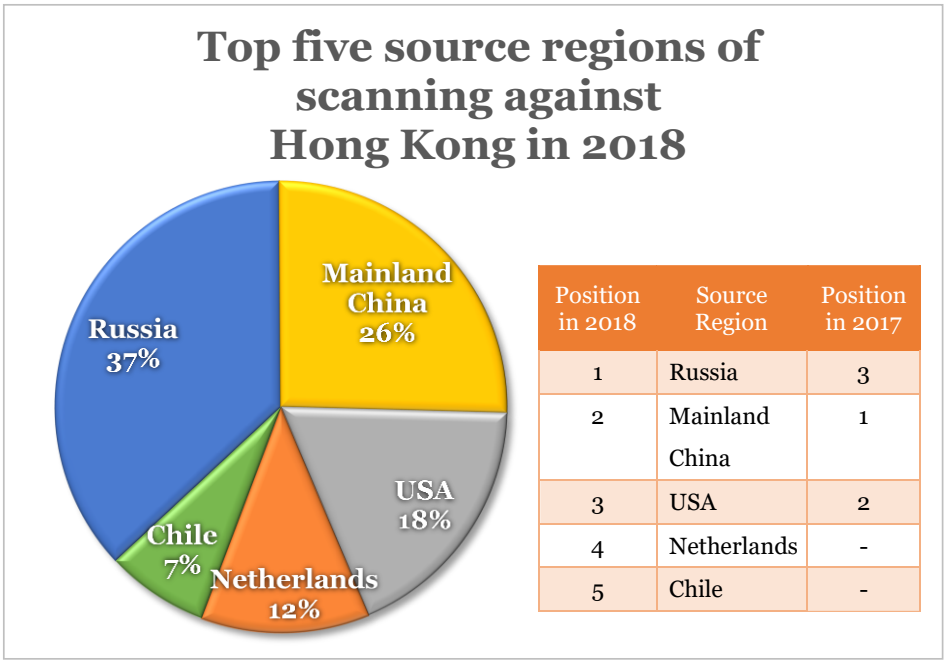
3.5 Abuse Statistics

As a member of the TSUBAME project, GovCERT.HK has set up sensors to collect and

analyse network scanning activities targeting Hong Kong. The following charts show the top five scanning ports and the top five source regions of scanning activities detected by the TSUBAME sensors installed in Hong Kong.



Position in 2018	Port Number	Position in 2017
1	445/TCP	4
2	23/TCP	1
3	80/TCP	-
4	22/TCP	3
5	1433/TCP	2



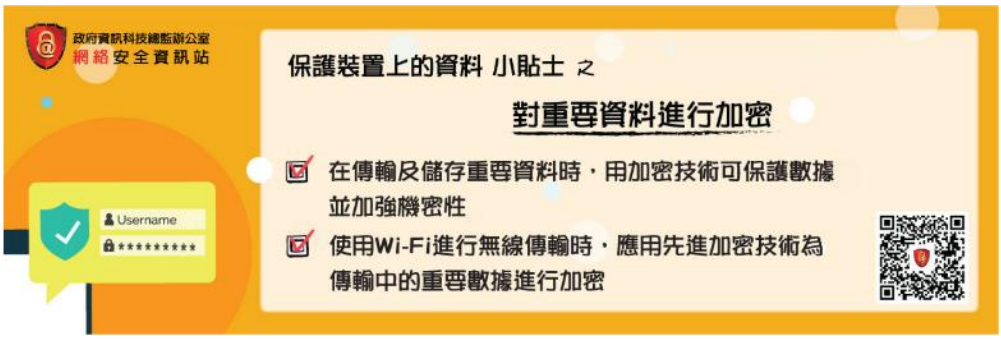
Position in 2018	Source Region	Position in 2017
1	Russia	3
2	Mainland China	1
3	USA	2
4	Netherlands	-
5	Chile	-

3.6 Publications and Mass Media

As cyber attacks continue to increase in number and sophistication, members of the public face cyber security risks when using different technologies, such as mobile devices, cloud services and social networking applications. We have made use of

different promotion channels to reach out to our target audience and collaborated with industry players during the process.

- We broadcasted radio episodes entitled "e-World Smart Tips" to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each month featured a specific theme and offered associated tips on mitigating the risks of cyber threats through daily life examples and in a lively and interesting way. In 2018, we covered a wide range of topics including Wi-Fi security, data security, social networking security, endpoint security, etc.
  (www.cybersecurity.hk/en/media.php#Radio)



- To provide practical tips and advice for Small and Medium Enterprise (SMEs) to defend against cyber attacks, a series of "Information Security Guide for Small Businesses" were developed to help them to secure their business.
  (www.cybersecurity.hk/en/resources.php#leaflets)

- To raise public awareness on the threats of cyber scams, we organised the "Stay Smart, Keep Cyber Scams Away" video ad contest in 2018. Participants fully demonstrated their creativity to compile short video ad on how to guard against cyber security threats and promote smart tips to keep cyber scams away. The winning entries were uploaded to the InfoSec YouTube Channel for public reference as well.
  (www.cybersecurity.hk/en/contest-2018-prize.php)

InfoSec YouTube Channel (www.youtube.com/user/infosecgovhk)

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share latest knowledge on security measures, best practices, skills and security solutions with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2018, we organised a total of 18 seminars, trainings and solution showcases for government IT staff and users to enhance their awareness of latest security vulnerabilities and update their knowledge in information security technologies.

- Seminars, trainings and showcases were conducted for government IT staff and users to raise their security awareness and introduce latest IT security technologies and solutions. The topics included industry best practices, phishing, DNSSEC, and security of Internet-connected devices.
- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest requirements and approaches in dealing with cyber security threats and adopting mitigation measures.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the HKSAR Government

GovCERT.HK has coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis and test their incident response procedures with a view to enhancing the overall incident response capability.

With the ever-changing cyber threat landscape, it is imperative to enhance the competencies in mitigating cyber threats. We collaborated with the HKPF to conduct the inter-departmental cyber security drill with over 40 departments participated to enhance the overall information security incident response capability of the Government. The drill included a tabletop exercise and a hands-on workshop. Participants discussed how to respond to a simulated malicious attack against a website and handle media enquiries in the tabletop exercise. They also conducted incident response and investigation and applied their cyber security skills in a controlled and simulated environment during the hands-on workshop.

APCERT Drill

As the Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Data Breach via Malware in Internet of Things" in March 2018. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

In view of the emerging threats of cyber scams in 2018, GovCERT.HK adopted the slogan "Stay Smart, Keep Cyber Scams Away" as the theme. A series of promotional activities were organised for businesses, organisations, schools and the public to raise their awareness against cyber scams such as phishing.

- Two seminars were organised under the "Build a Secure Cyberspace" promotional campaign in May and September 2018, aiming to promote public awareness of information security and adoption of security best practices, in particular the risks of cyber scams.

- Thirty-six school visits were conducted at primary and secondary schools in 2018, reaching out to some 10 000 students, parents and teachers for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.

- To promote the development of cyber security technologies and industry in Hong Kong and the Mainland, the third Hong Kong-Mainland Cyber Security Forum with the theme of "Challenges and Opportunities of Secure, Smart Connectivity" was held in April 2018. The forum attracted some 180 information security professionals from the Government, research institutions, academia, professional organisations and the information security industry to exchange views and observations on cyber security landscape and advise how to meet the challenges to be brought by smart connectivities.

5. Local and International Collaboration

GovCERT.HK has been working closely with HKCERT and other regional and global CERTs for coordinating threat information sharing and incident response.

5.1 Local collaboration

GovCERT.HK is keen on fostering exchanges and experience sharing among the local information security industry. In 2018, we launched Cybersec Infohub, a partnership programme to promote closer collaboration among local information security stakeholders of different sectors. Under the Programme, we have provided a community-driven collaborative platform (Cybersechub.hk) and organised various industry events to facilitate exchange of cyber security information. As of 2018, over 100 organisations with more than 300 representatives across various sectors have joined the Programme.
(www.cybersechub.hk)

The Internet is critical to communications, conduct of e-business and access to e-services. GovCERT.HK has been acting as a supportive role in the Internet Infrastructure Liaison Group (IILG) established and led by OGCIO. The key roles of the IILG are to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders for the healthy operation of the Internet infrastructure of Hong Kong. In 2018, the IILG collaboration mechanism was activated six times to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks.

5.2 International Collaboration

To foster closer collaboration with international security experts for sharing experience in information security and strengthening the knowledge of emerging cyber threats, vulnerabilities and appropriate mitigation solutions, GovCERT.HK strives to learn from the CERT community on global trends in international standards development, global information security and data privacy policies, cyber crime initiatives and technological researches.

GovCERT.HK participated in the following events in 2018:

- Hong Kong – Mainland Cyber Security Forum
- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- 2018 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- Five APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

The accelerated development of emerging technologies is spurring continuous innovation, however, it could also bring along different cyber security threats. GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. In the coming year, we will launch a new round of review of the Government IT Security Policy and Guidelines by making reference to the latest international standards and industry best practices. In addition, a penetration testing platform will be set up to provide simulated network and system environments for testing web applications against potential cyber attacks.

To enhance the capability of cyber threat intelligence management, GovCERT.HK plans to operate a Malware Information Sharing Platform (MISP) instance in 2019 to enable sharing, storing and correlation of Indicators of Compromise.

6.2 Future Operations

Artificial intelligence elements will be introduced to the collaborative platform of

Cybersec Infohub by making use of machine learning to build and operate the text analytics model in the first half of 2019. This move will assist members in the integration and analysis of cyber security information and facilitate easier and faster acquisition of required information by experts for timely dissemination of the information to the public.

7. Conclusion

Cyber security attacks are increasingly sophisticated, with the forms they take becoming more diversified. GovCERT.HK has been proactively collaborating with local and global CERTs, making timely response and enhancing appropriate defensive measures to the inevitable cyber security threats. GovCERT.HK will continue to foster all stakeholders to take forward communication and exchange of cyber security information so as to keep abreast of the fast-evolving cyber security landscape and enhance the cyber security resilience capability of the community.

Contact: cert@govcert.gov.hk

Websites: www.govcert.gov.hk
www.cybersecurity.hk
www.cybersechub.hk

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre - Hong Kong, China

1. About HKCERT

1.1 Establishment

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong Special Administrative Region (HKSAR) Government. The Hong Kong Productivity Council (HKPC), which is a government subvented organisation in Hong Kong, has operated the centre since then.

1.2 Organisation and Workforce power

The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care by the Centre Manager, two Consultants and six Security Analysts and one Assistant Project Manager.

1.3 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for the constituency (local enterprises and Internet users) in Hong Kong.

The mission of HKCERT is to be the cyber threats response and defense coordinator in Hong Kong to protect the Internet environment and the economic and social interests of Hong Kong.

The objectives of HKCERT are to serve as a focal point in Hong Kong for information security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams (CERTs), and relevant bodies outside Hong Kong; to promote awareness of the community on computer security issues and the latest international best practices and standards; and to provide assistance to the community in the protection against computer security threats and the prevention of security attacks and in recovery actions for computer security incidents

2. Activities and Operations

2.1 Incident Handling

During the period from January to December of 2018, HKCERT had handled 10,081 security incidents which was 55% increase of the previous year (see Figure 1).

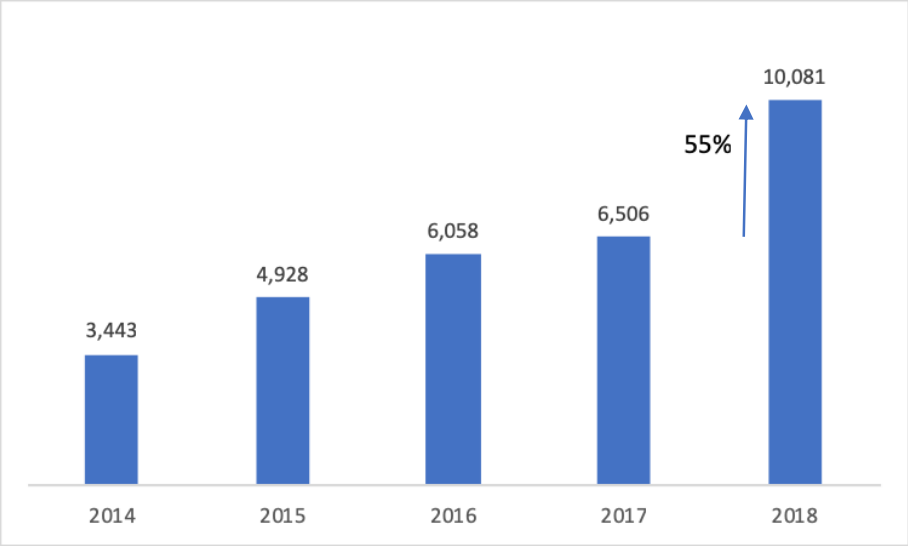


Figure 1. Incident Reports Handled by HKCERT

The increase of the number of incidents was due to the increase of referral cases as a result of closer collaboration with global security researchers and organisations. Referral cases accounted for 95% of the total number of security incidents.

Two major categories of security incidents, Botnet (3,783 cases) and Phishing (2,101 cases) remained at similar level as in the previous year (see Figure 2).

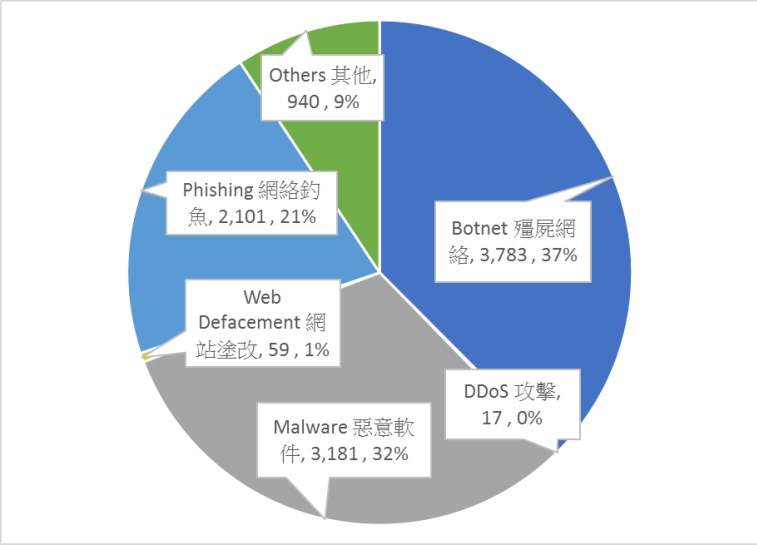


Figure 2. Distribution of Incident Reports in 2018

The number of malware infection incident reports rose sharply by 56% in 2018 (see Figure 3.) These cases were mainly due to WannaCry sinkhole detections (bot-Wannacry) and XcodeGhost contaminated mobile apps. Among all malware reports, despite fewer ransomware incident reports (114 cases) were made to HKCERT last year, there were 2,426 bot-Wannacry cases, which doubled the number 1,210 of 2017.

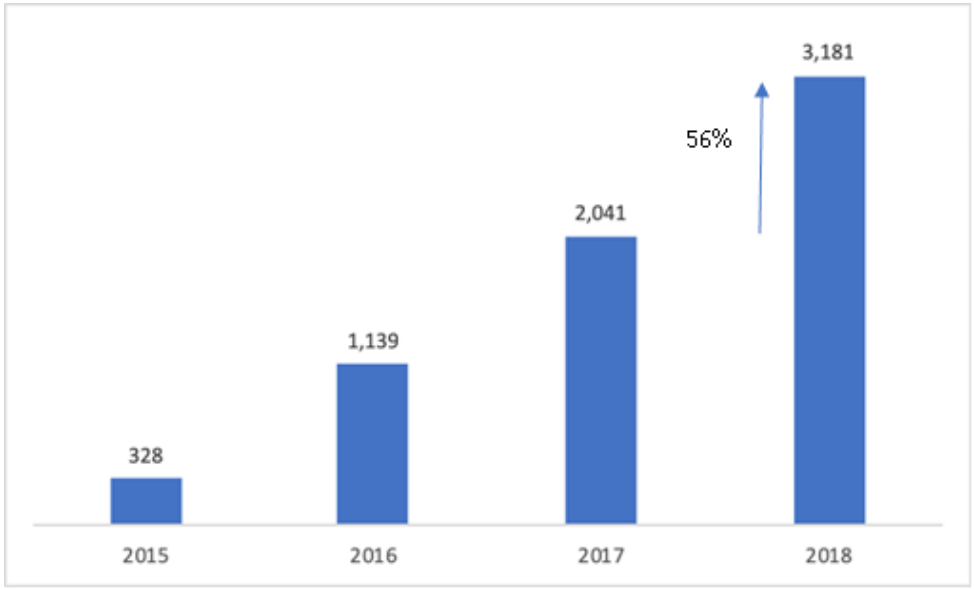


Figure 3. Number of Malware Incident Reports in the past 4 years

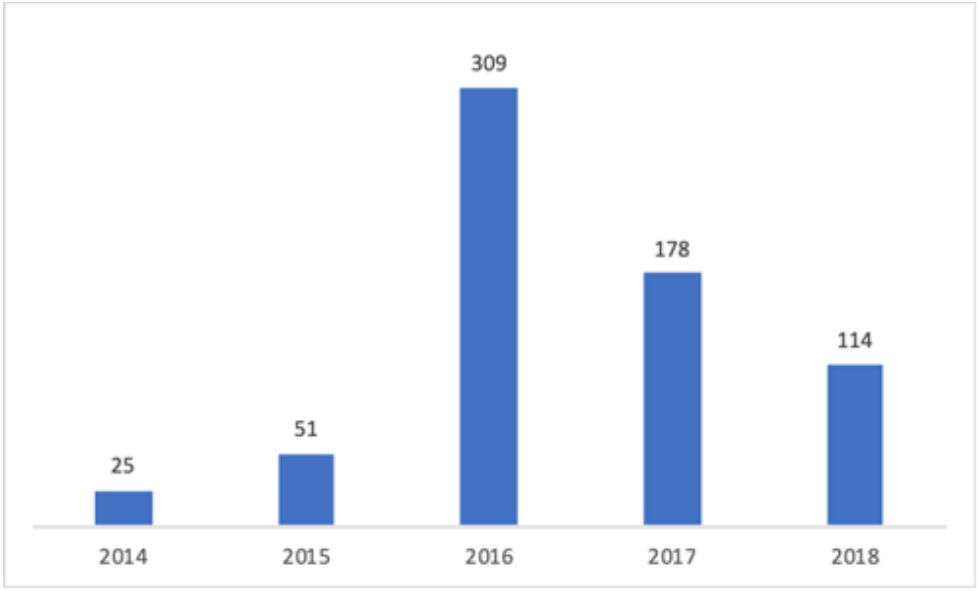


Figure 4. Number of Ransomware Incident Reports in the past 5 years

2.2 Watch and Warning

During the period from January to December of 2018, HKCERT published 240 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 99 blogs, including security advisories on DDoS extortion, marketing adware, smart device installation, ransomware, IoT Botnet, remote desktop service risk, third party plugins, etc. HKCERT also published the "best security reads of the week" every fortnight to inform the public of good security articles.

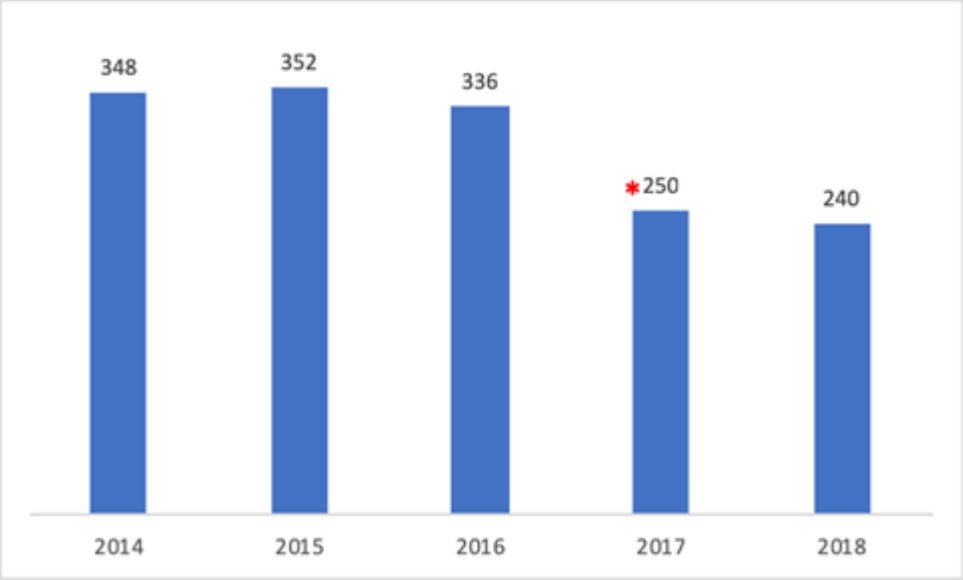


Figure 5. HKCERT Published Security Bulletins

*The drop of Security Bulletins was mainly due to consolidation of MS & Adobe security bulletins

HKCERT used the centre website (www.hkcert.org), RSS, HKCERT mobile app, and Hong Kong Government Notification mobile app to publish security bulletins, blogs and news. HKCERT also used email and SMS to publish selected security bulletins to subscribers. The subscriptions are free of charge.

2.2.1 Embrace global cyber threat intelligence

HKCERT used the Information Feed Analysis System (IFAS) to collect intelligence of compromised machines in Hong Kong from global security researchers. The system provided a better picture of security status of Hong Kong and a way to verify the effectiveness of the security incident response. For example, Figure 6 showed the trend of bot-related security events was on the rise in the past year (from 4,690 in Q4 2017 to

7,307 in Q4 2018), largely attributed to the significant rise of Mirai events as depicted in Figure 7.

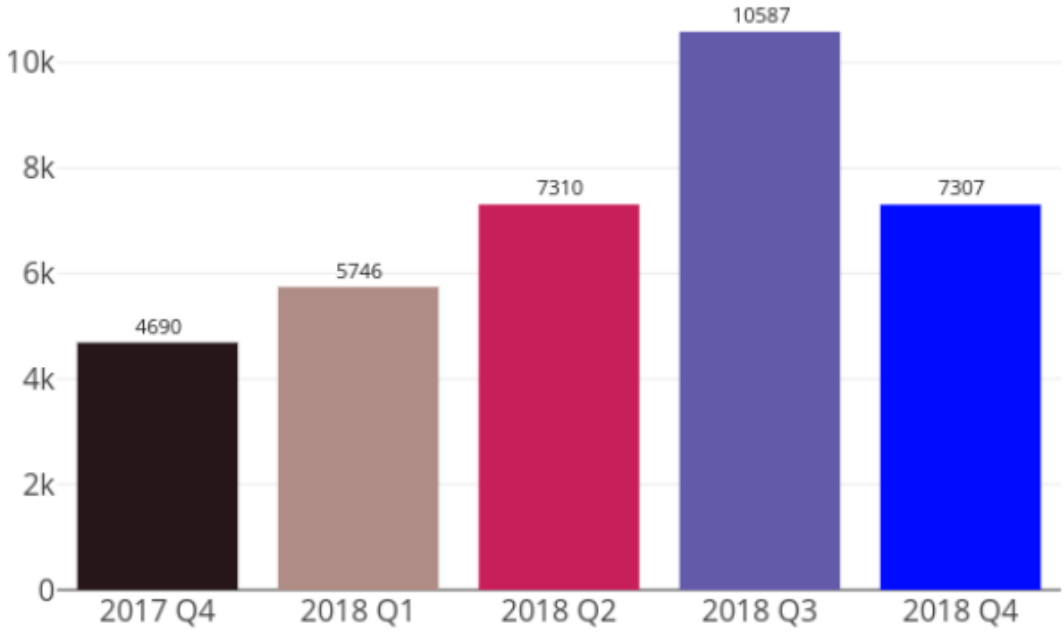


Figure 6. Trend of Bot related security events in the past year

(Source: data feeds from overseas security researchers, not from incident reports)

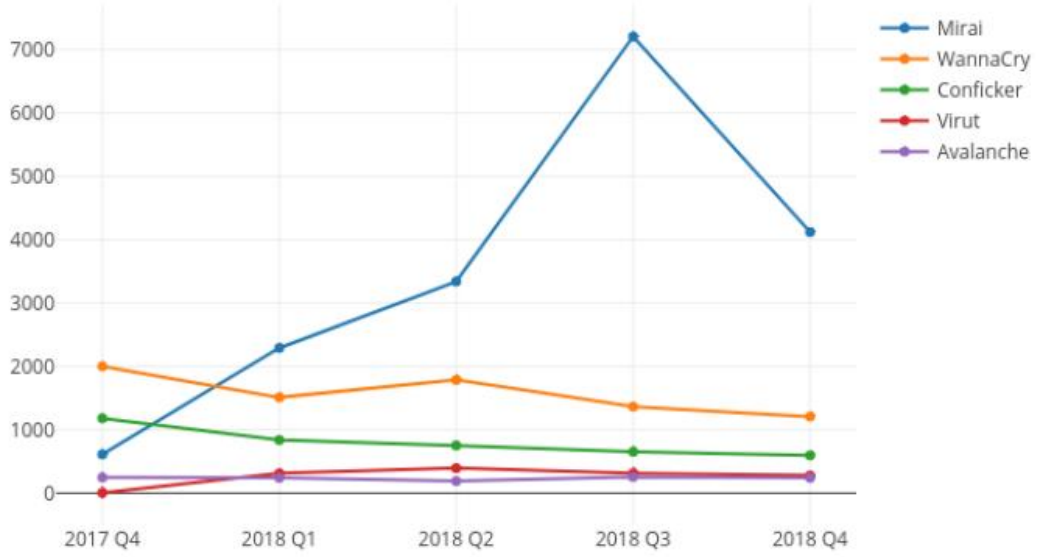


Figure 7. Trend of Top 5 Botnet Families in the past year

(Source: data feeds from overseas security researchers, not from incident reports)

2.3 Publications

- HKCERT had published 4 quarterly issues of Hong Kong Security Watch Report showing the status of compromised computers in Hong Kong from the data collected from overseas security researchers (see https://www.hkcert.org/hkswr).

- HKCERT had published 12 issues of Hong Kong Google Play Store's Apps Security Risk Report. The Report is a co-operation with CNCERT/CC. (see https://www.hkcert.org/play-store-srr).

- HKCERT had published 12 issues of monthly e-Newsletter in the period (see https://www.hkcert.org/newsletters).
- HKCERT had published the statistics of incident reports and security bulletins every quarter (see https://www.hkcert.org/statistics).

  HKCERT had published 50 weekly column articles in a local Chinese newspaper (Hong Kong Economic Times) to raise the cyber security awareness of business executives. (see https://hkpc.org/en/corporate-info/media-centre/media-focus#1).

3. Events organised and co-organised

3.1 Seminars, Conference and Meetings

HKCERT jointly organised the "Build a Secure Cyberspace 2018" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a 1-Minute Video Ad Contest. Two public seminars were organised in April and September 2018.

For the 1-Minute Video Ad Contest, HKCERT had received about 55 applications from Open Category, Family Category, Secondary School and Primary School Category. A professional judge panel selected winners with most innovative and impressive videos (See Figure 8).

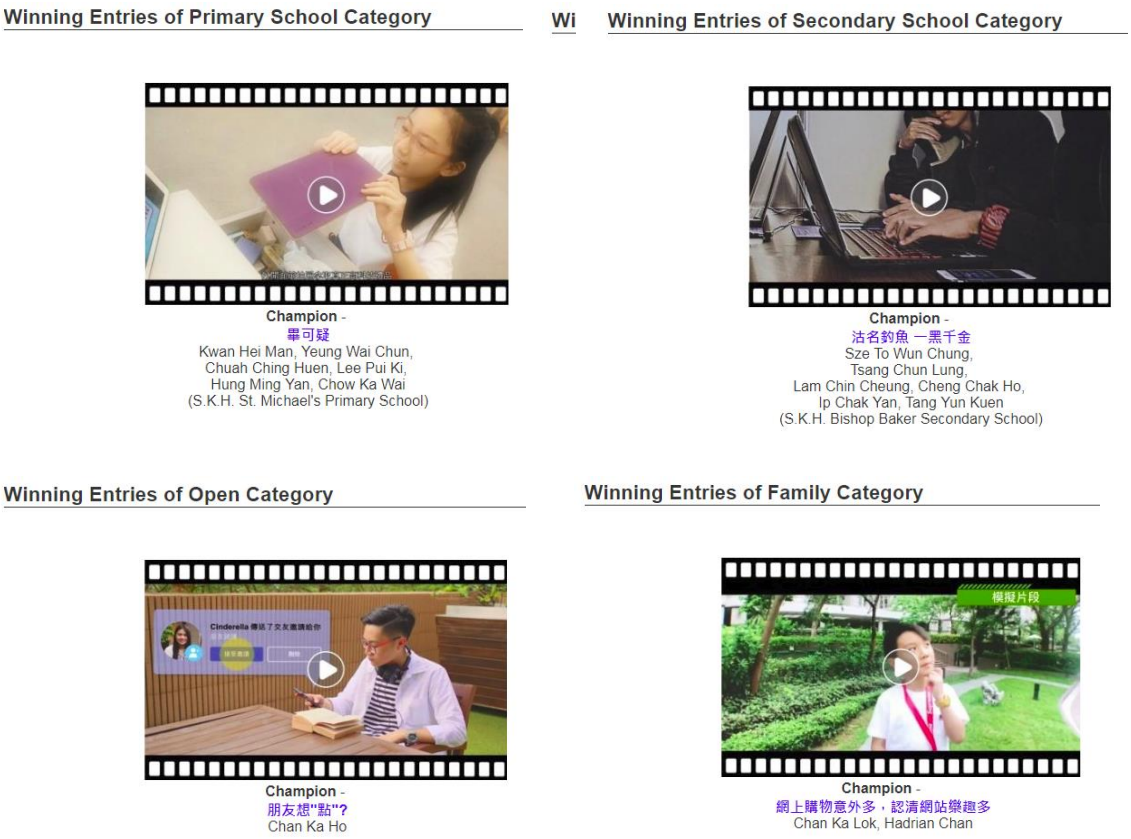


Figure 8. Champion entries of Primary School, Secondary School, Open and Family Category

See this link to view those winning entries online:
https://www.cybersecurity.hk/en/contest-2018-prize.php

We co-organised the 2-day Information Security Summit 2018 with other information security organisations and associations in September 2018, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Speeches and Presentations

HKCERT was invited to deliver speeches and presentations on various occasions for the Government, associations and schools.

3.3 Proactive approach to promote awareness for different sectors in HK

HKCERT proactively approached several sectors in HK to promote cyber security awareness, e.g. travel industry, retail and securities, etc.

3.4 Media promotion, briefings and responses

- HKCERT published an advertorial in September 2018 to promote the public seminar and the 1-Minute Video Ad Contest.
- HKCERT was interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

4. Collaboration

4.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events:

- Participated in the APCERT AGM and Conference in Shanghai
- Participated in the FIRST Meeting and National CSIRT Meeting in Kuala Lumpur
- Participated in the CNCERT Conference in Beijing
- Participated in the AusCERT Conference in Gold Coast
- Participated in the HITCON Community in Taipei
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- Participated in (ISC)2 APAC Security Congress

HKCERT collaborated with APNIC closely in taking down bad reputation ASNs whose owners were suspicious and may not provide proper contact information.

4.2 Local Collaboration

HKCERT worked with a number of local organisations in different areas. Some examples:

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held meetings to exchange information and to organise joint events regularly.
- To promote cyber security information sharing among industries in Hong Kong, the Hong Kong SAR Government launched the Cyber Security Information Sharing platform called 'Cybersec Infohub". Over 100 Information Security companies and critical infrastructure organisations were invited to join the platform. Cyber security information and intelligence were shared among the members. HKCERT joined as a member of the Programme. HKPC, the parent organisation of HKCERT,

is the programme manager of the Programme.

- HKCERT continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong.
- HKCERT was a judge panel member of the Cyber Security Professionals Awards organised by the Hong Kong Police.
- HKCERT continued to maintain the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet infrastructure organisations, and advised on latest information security issues through the list.
- HKCERT also liaised with critical infrastructure sector and had delivered awareness briefings to these organisations for better protecting the security environment of Hong Kong; created the Information Security Advisory and Collaboration (ISAC-CI) Mailing list with the critical infrastructure organisations, and advised on latest information security issues through the list.

5. Other Achievements

5.1 Advisory Group Meeting

HKCERT had held the Advisory Meeting in November of 2018. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

5.2 Three Year Strategic Plan

HKCERT prepared its rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report, the previous CERT Study Tour and discussion with the government. The plan would be updated annually. HKCERT based on this plan to prepare the annual plan and budget to solicit funding support from the government.

5.3 Embrace global intelligence and build security health metrics

HKCERT had implemented the IFAS to collect intelligence of compromised machines in Hong Kong. The system provided a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong. HKCERT publicised the information to the public quarterly and used the information in decision making. HKCERT joined the Cyber Green project initiated by JPCERT/CC to explore development of useful metrics for measuring cyber health.

5.4 Year Ender press briefing

HKCERT organised a year ender press briefing to media in January 2019 to review cyber security 2018 and provided outlook to 2019 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 9. HKCERT at the Year Ender press briefing.

6. Future Plans

6.1 Strategy

"Proactivity", "Share to Win" and "Security is not an Island" are the strategic directions of HKCERT which would work closer with other CERTs and security organisations to build a more secure Hong Kong and Internet.

6.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2019/2020. We shall work closely with the government to plan for the future services of HKCERT. We shall continue to propose new initiatives to the government and seek support from the government.

6.3 Enhancement Areas

HKCERT is working on enhancing the infrastructure to increase the efficiency of information search and sharing. HKCERT was developing automation tools to enhance the incident response process.

7. Conclusion

In 2018, there were data breach cases in airlines and telecommunication companies in Hong Kong. Process flaws were also exploited by fraudsters in registration of third-party wallets in mobile payment. Besides promoting public information security awareness, HKCERT also urged enterprises to adopt “Security by Design” and enhance risk management process.

The cross-border collaboration and intelligence driven response continued to improve the proactiveness and effectiveness of incident response. HKCERT has seen the immense power of collaboration and would invest more to further this success.

With the Internet security facing more crises from financially motivated cyber crimes, Internet of Thing (IoT) attacks, more use of mobile payment apps, more regulation for security and privacy and supply chain attacks, HKCERT expects 2019 would be continuously a challenging year.

ID-CERT

Indonesia Computer Emergency Response Team

1. ABOUT ID-CERT

1.1 INTRODUCTION

ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by Budi Rahardjo, MSc., PhD. in 1998. ID-CERT together with JP-CERT (Japan), AusCERT (Australia), is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum.

1.1.1 ESTABLISHMENT

In 1998 there was no CERT in Indonesia. Based on that Budi Rahardjo, MSc., PhD., an internet security expert, encouraged himself to establish ID-CERT. At the same time, countries around Indonesia began to establish their own CERTs and this continued into Asia-Pacific forum which later became the APCERT.

ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers, either locally and internationally. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.

In 2013 ID-CERT has been officially incorporated.

1.1.2 WORKFORCE POWER

Chairman	:Budi Rahardjo, MSc., PhD.
Vice Chairman	:Andika Triwidada
Manager	:Ahmad K. Alkazimy
Incident Response HelpDesk	:Rahmadian L. Arbianita
Technical Editor :	-Emil Yakhya
	-Bainul

Volunteers	- Setia Juli Irzal (Malware Analyst) - Ikhlasul Amal - Maman Sutarman - Oryzandi - Other volunteers

1.1.3 CONSTITUENCY & ETC

Constituent

ID-CERT Membership is open to all Indonesia Internet community who are concerned in the internet security, either from the ISP or non-ISP, such as government organizations (ministries, local goverments, state enterprises, enterprises, etc.) as well as private citizens.

Respondent

ID-CERT has 40 respondents participating in Incident Monitoring Report. ID-CERT still welcome to new respondents who wish to join in the various researches/studies conducted by ID-CERT.

Volunteer

From the beginning, ID-CERT are supported by many volunteers who work selflessly to contribute and concern for internet security in Indonesia. Generally, ID-CERT volunteers are individual one.

2. ACTIVITY AND OPERATION

2.1 INCIDENT HANDLING REPORT

Total incident reports	:	144.620
Incident handling	:	748

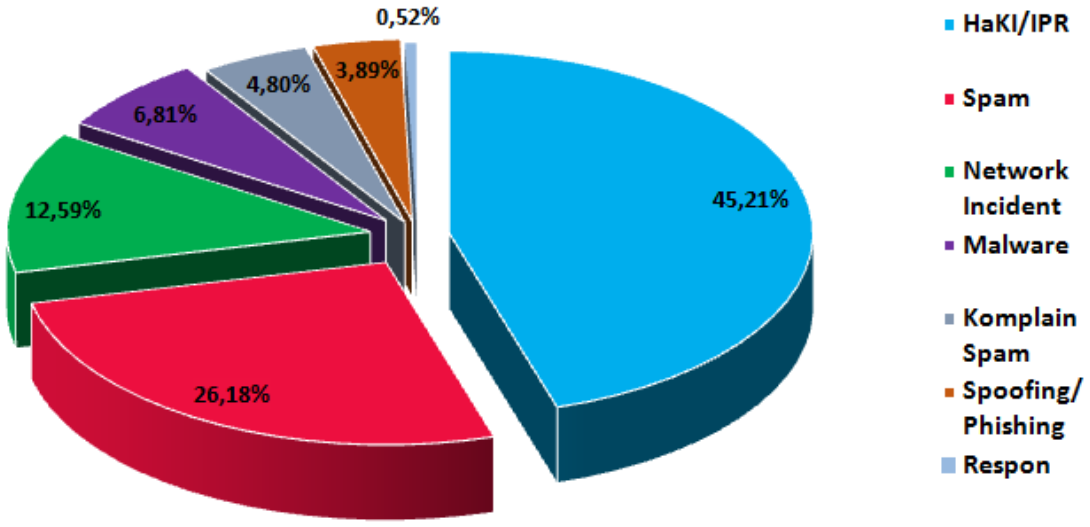
2.2 ABUSE STATISTIC

Percentage

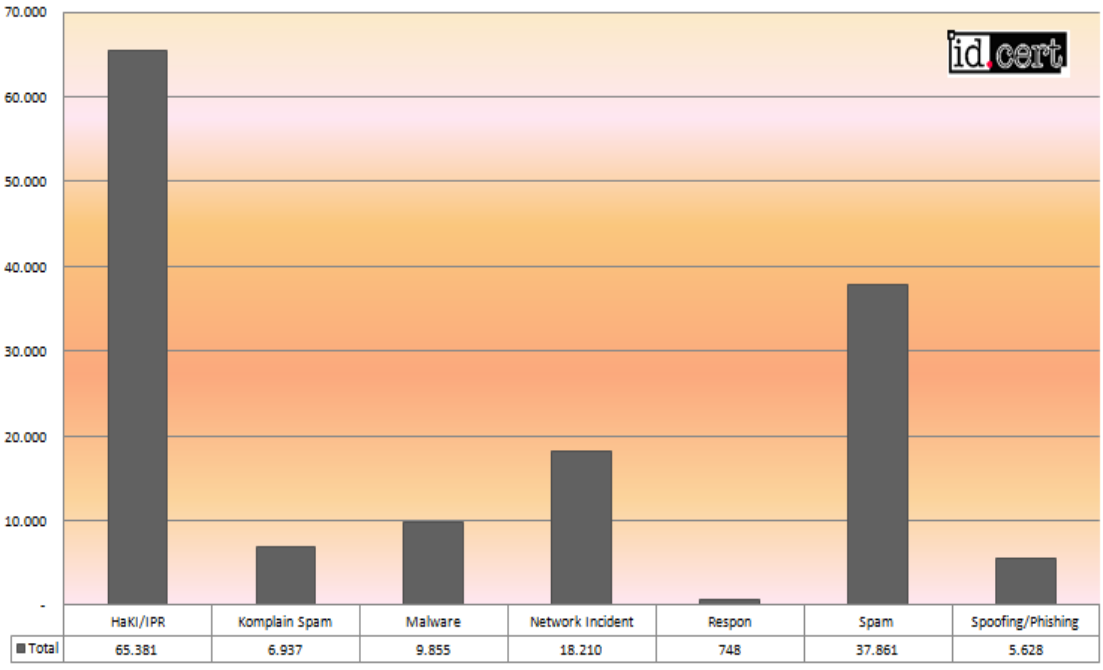
HaKI/IPR (Intellectual Property Rights)	:	45,21%
Spam	:	26,18%
Network Incident	:	12,59%
Malware	:	6,81%
Complaint Spam	:	4,80%

Spoofing/Phishing	:	3,89%
Response	:	0,52%

Incident Monitoring Report
Persentase Pengaduan per Kategori
Januari-Desember 2018



Incident Monitoring Report
Jumlah Pengaduan Total per Kategori
Januari-Desember 2018



Total number

HaKI/IPR (Intellectual Property Rights)	:	65.381
Spam	:	37.861
Network Incident	:	18.210
Malware	:	9.855
Complaint Spam	:	6.937
Spoofing/Phishing	:	5.628
Response	:	748

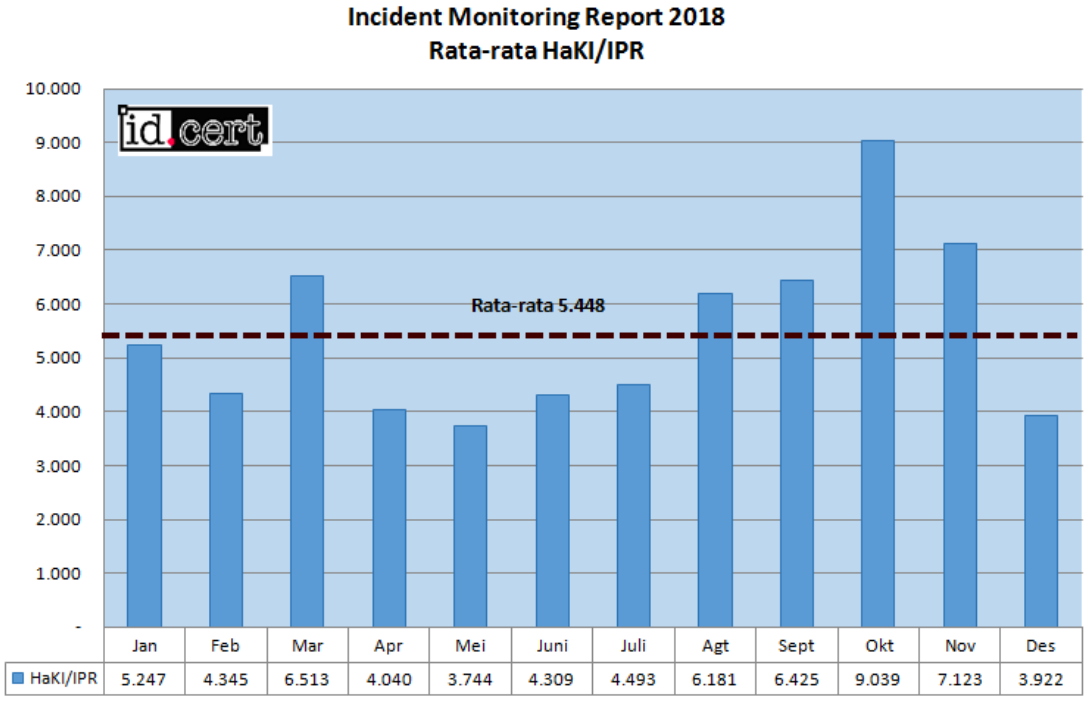
2018	HaKI/IPR	Spam	Network Incident	Malware	Komplain Spam	Spoofing/ Phishing	Respon
Januari	5.247	3.789	1.877	520	562	991	82
Februari	4.345	2.810	583	416	130	533	65
Maret	6.513	2.880	1.435	517	212	366	81
April	4.040	2.376	1.066	632	250	310	83
Mei	3.744	2.221	1.421	754	388	491	74
Juni	4.309	2.012	1.279	1.007	374	572	70
Juli	4.493	2.846	1.199	1.088	561	358	53
Agustus	6.181	2.547	2.006	1.153	848	335	50
September	6.425	4.458	2.305	1.163	978	505	64
Oktober	9.039	4.205	2.357	1.387	492	489	55
November	7.123	3.667	1.354	562	1.274	368	36
Desember	3.922	4.050	1.328	656	868	310	35
Total	**65.381**	**37.861**	**18.210**	**9.855**	**6.937**	**5.628**	**748**
Rata-rata	**5.448**	**3.155**	**1.518**	**821**	**578**	**469**	**62**
%	**45,21%**	**26,18%**	**12,59%**	**6,81%**	**4,80%**	**3,89%**	**0,52%**

Average number

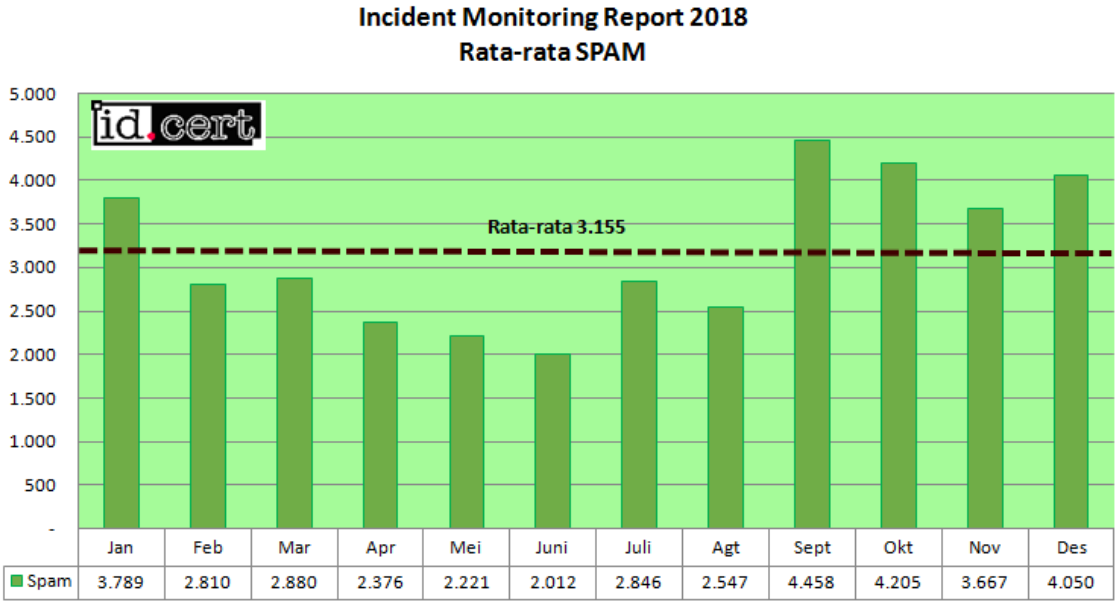
HaKI/IPR (Intellectual Property Rights)	:	5.448
Spam	:	3.155
Network Incident	:	1.518
Malware	:	821
Complaint Spam	:	578
Spoofing/Phishing	:	469
Response	:	62

HaKI/IPR (Intellectual Property Rights)

- 100% reports from abroad
- Movies and music sharing P2P at Indonesia IPs
- Request to take down the files



Spam

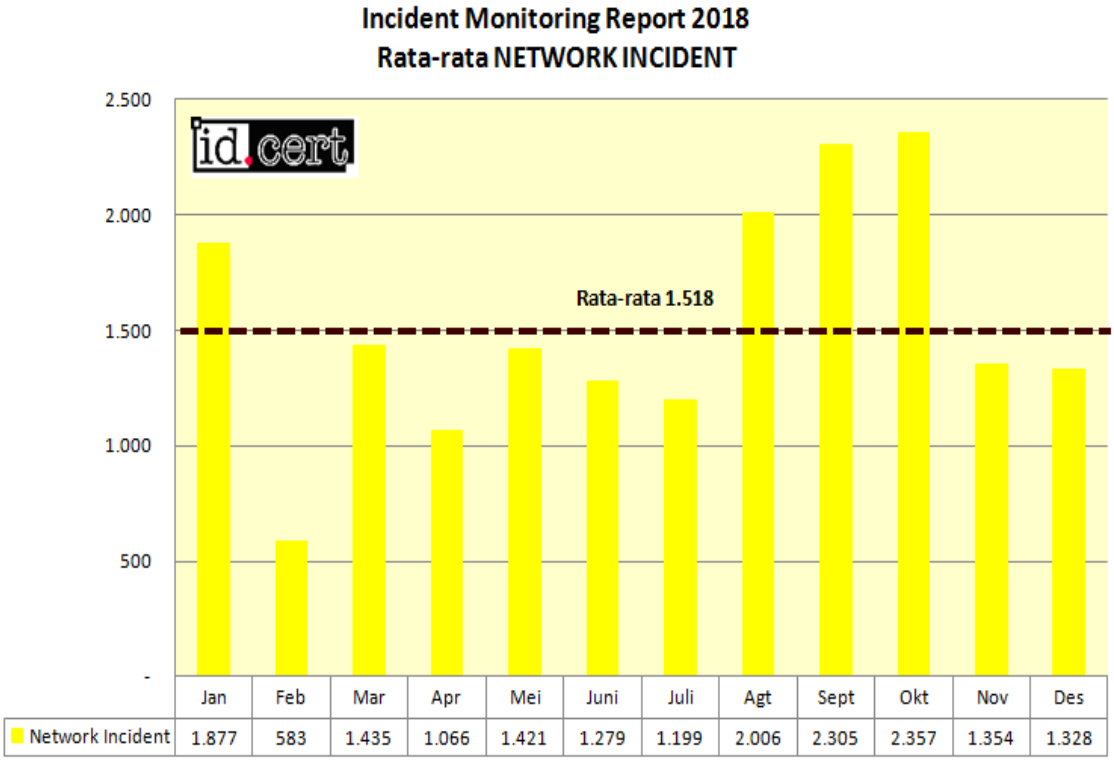


Network Incident

- Mostly brute force
- Logged in succeed then:
  - Web/IP is infiltrated by malware
  - Web/IP is infiltrated by hacking tools
  - Web/IP is made into C&C
  - Stealing data

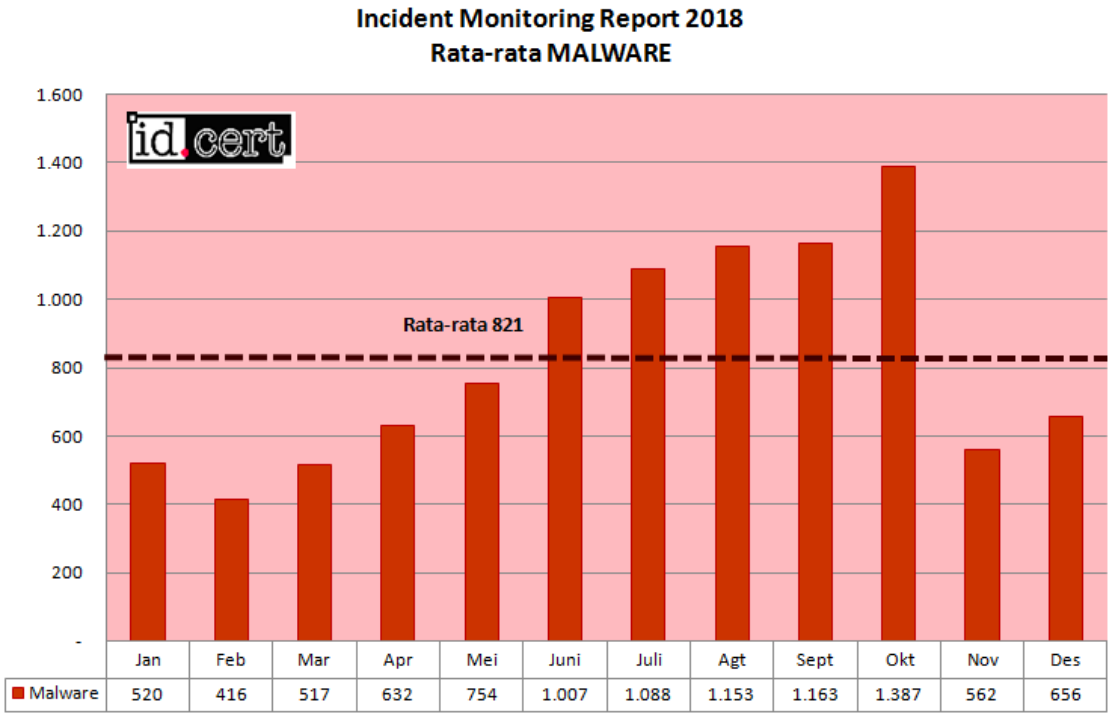
- Hacking/deface

- Mostly targeted: government websites

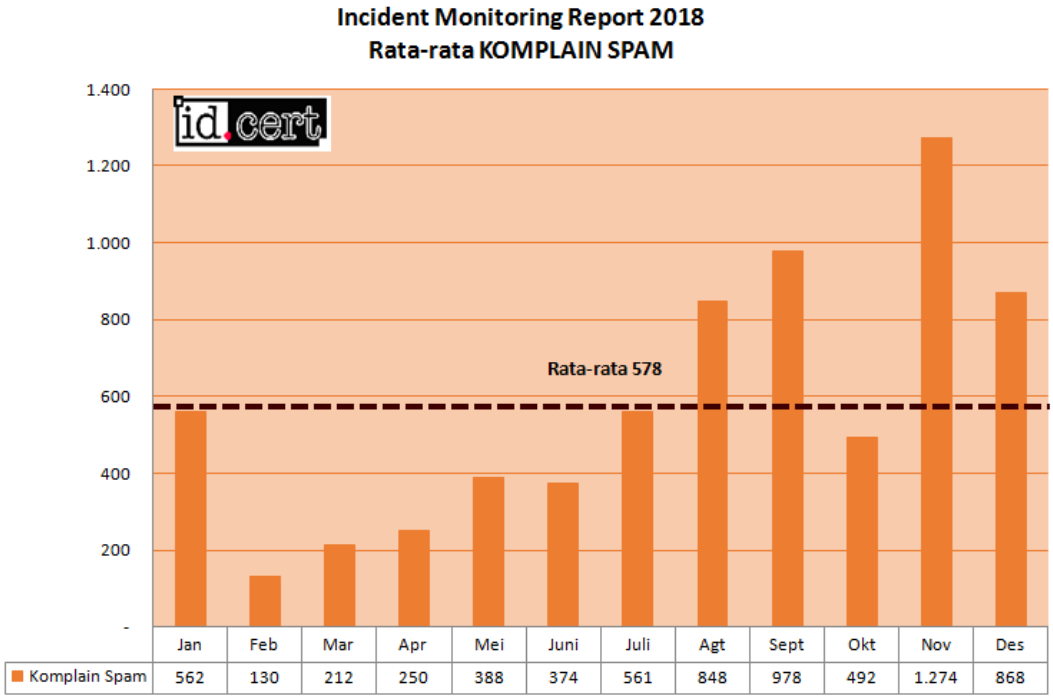


Malware

Some cases a malware was attached to a phishing email.



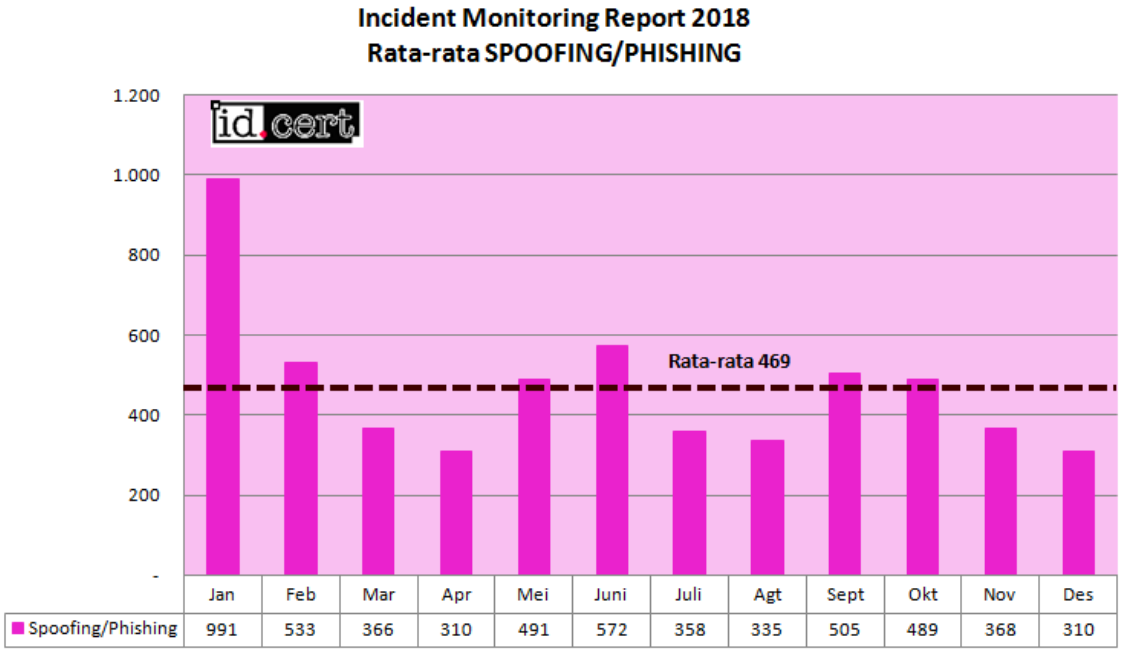
Complaint Spam



	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Komplain Spam	562	130	212	250	388	374	561	848	978	492	1.274	868

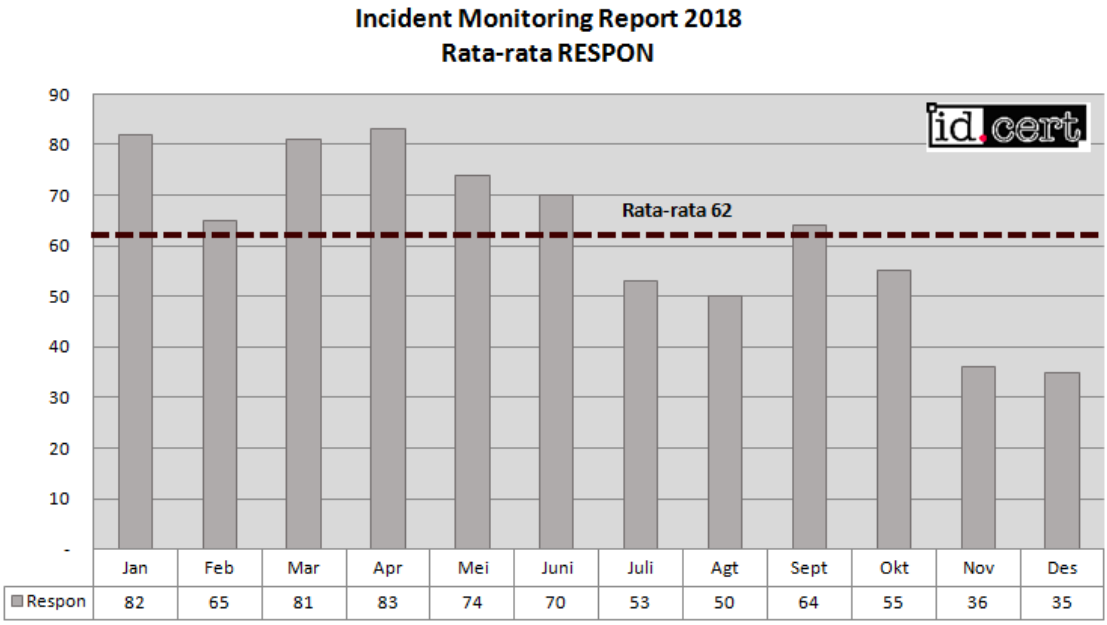
Spoofing/Phishing

- Phishing at Indonesia .ac.id or sch.id to fake log in at abroad universities or schools
- Phishing abroad banking at Indonesia IP
- Phishing Indonesia banking at Indonesia/abroad IPs
- Phishing at Indonesia government websites



	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Spoofing/Phishing	991	533	366	310	491	572	358	335	505	489	368	310

Response



2.3 NEW SERVICE

Event Report Tools

Tools to process feed log data.

3. EVENT

3.1 DRILL

ID-CERT participated in APCERT Drill, held on March 7, 2018.

ID-CERT held a Drill for ASIAN Games 2018 IT Division in preparing ASIAN Games 2018 on August 9, 2018 at Jakarta.

3.2 SEMINAR & ETC

ID-CERT Annual Gathering/Meeting IX, held on April 13, 2017 at Bandung.

ID-CERT Annual Gathering/Meeting X, held on December 6, 2017 at Jakarta.

ID-CERT Chairman, Budi Rahardjo MSc., PhD., attended Cyber Intelligence Asia V held on March 20-22, 2018 at Singapore as keynote speaker.

ID-CERT Vice Chairman, Andika Triwidada, attended APCERT Annual General Meeting 2018 held on October 21-24, 2018 at Shanghai.

4. ACHIEVEMENT

4.1 PRESENTATION

Andika Triwidada had a presentation at APCERT AGM 2018 about ASIAN Games 2018 IT Division.

5. FUTURE PLAN

5.1 FUTURE PROJECT

- Malware Survey
- Android Anti Malware Scanner (AndroScan Project)
- Malware Wiki
- Malware Advisory

5.2 FRAMEWORK

5.2.1 FUTURE OPERATION

- Incident Handling
- IMR respondent addition
- Internal infrastructure improvement/development
- Antispam RBL
- ID-CERT Annual Gathering XI
- Training

6. CONCLUSION

ID-CERT wants to focus on Malware Research and hopes that other CERTs could help and give some input/suggestion/advice about it.

ID-SIRTII/CC

Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center – Indonesia

1. Highlight of 2018

1.1 Summary of major activities

5 January 2018 : Meeting with Head of the new established National Cyber and Crypto Agency (NCCA) regarding the merge preparation of Id-SIRTII/CC to this agency

25 January 2018 : Participated and Speaker in 6th ASEAN CIO FORUM in Laos.

19-20 March 2018 : Participated and Speaker in Malaysia Cyber Security Summit in Kuala Lumpur, Malaysia

29-30 March 2018 : Participated and Speaker in KEIO UNIV International Cyber Security Symposium at Tokyo, Japan

26 March 2018 : Id-SIRTI/CC moved from Ministry of Communication and Information Technology to National Cyber and Crypto Agency and operating under National Cyber Security Operation Center of NCCA as its technostructure body

17 April 2018 : Speaker in PUTRA JAYA FORUM and DEFENSE SERVICE ASIA in Kuala Lumpur , Malaysia.

24-29 June 2018 : Participated in FIRST 2018 at Kuala Lumpur, Malaysia

29-30 June 2018 : Participated and Speaker in NatCSIRT meeting 2018 at Kuala Lumpur

10-12 July 2018 : Participated and Speaker in OWASP Appsec Conference in Taipeh, Taiwan.

22-23 July 2018 : Participated in ASEAN JAPAN Information Security Working Group in Manila, Philippines.

16 August 2018 : Speaker in ASEAN Cyber Security Summit in Singapore

18 August to 2 September 2018 : Participated in Cyber Security Team for ASIAN GAMES

25 September 2018 : Speaker in Cyber Security Malaysia - Awards Conference and Exhibitions (CSM-ACE) in Kuala Lumpur, Malaysia

9-12 October 2018 : Hosted Codebali Cyber Security Conference and Exhibitions in Conjuction with FIRST TC, OIC CERT-Workshop, and National Cyber Security Contest (Cyber Jawara) in Denpasar, Bali

16-17 October 2018 : Participated in ASEAN-JAPAN Information Security Policy meeting in Tokyo

21-24 October 2018 : Participated in APCERT AGM in Shanghai, China

13 November 2018 : Organized National Internet Security Days event in Indonesia.

26-29 November 2018 : Participated in OIC-CERT AGM in Shiraz, Iran.

7 December 2018 : Speaker in Cyber Security Indonesia in Jakarta, Indonesia and Organized Jakarta Hacking Competition

1.2 Achievements and milestones

As one of its activities for capacity building and building networking for young generation who has talent and concern in information security, Id-SIRTII conduct National Cyber Security and Hacking Contest (CYBER JAWARA) every year. The winner become Indonesia representative to participate in ASEAN cyber security contest (Cyber Seagame) and later on may join Japan Security Contest. This year Indonesia became the Winner of Cyber Seagame. And also took rank 8th in Japan Security Contest.

Indonesia is elected as Deputy Chair of OIC-CERT in OIC-CERT Annual General Meeting at 26 November 2018 in Shiraz, Iran

2. About Id-SIRTII/CC

2.1 Introduction

Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) is the national csirt of Indonesia and has the main duty to socialize with stake holders related to Internet Security, to do an early monitoring and detection, give an early warning against threats to telecommunication networks from both inside and outside country, particularly in the security measures of network utilization, creating/performing/developing log files and statistics of Indonesian's internet security.

2.2 Establishment

Id-SIRTII/CC is established at 4 May 2007 by Minister of Communication and Information Decree no 26 in 2007. Id-SIRTII/CC has a function as National CSIRT and Coordination Center for national incident handling and work under Directorate of Telecommunication of the Ministry. Based on Presidential Decree no 53 in 2017, Id-SIRTII/CC merged and moved to National Cyber and Crypto Agency and works under its National Cyber Security Operation Center since April 2018.

3. Activities and Operations

3.1 Monitoring Reports

In 2018, Id-SIRTII/CC security monitoring system collected important informations as below:

- Received 2,885 security incident reports from local and overseas.
- Found 4,499 phishing site
- Found 16,939 website defacement incidents
- Found 232,447,977 indication of cyber attacks, which dominantly targeted port 53 and the use of trojan

3.2 Abuse Statistics

Incident reports to Id-SIRTII/CC in 2018 were categorised as in Figure 1. About 61,2% of the reports were on malware, followed by fraud (29,7%) and vulnerability (4,7%).

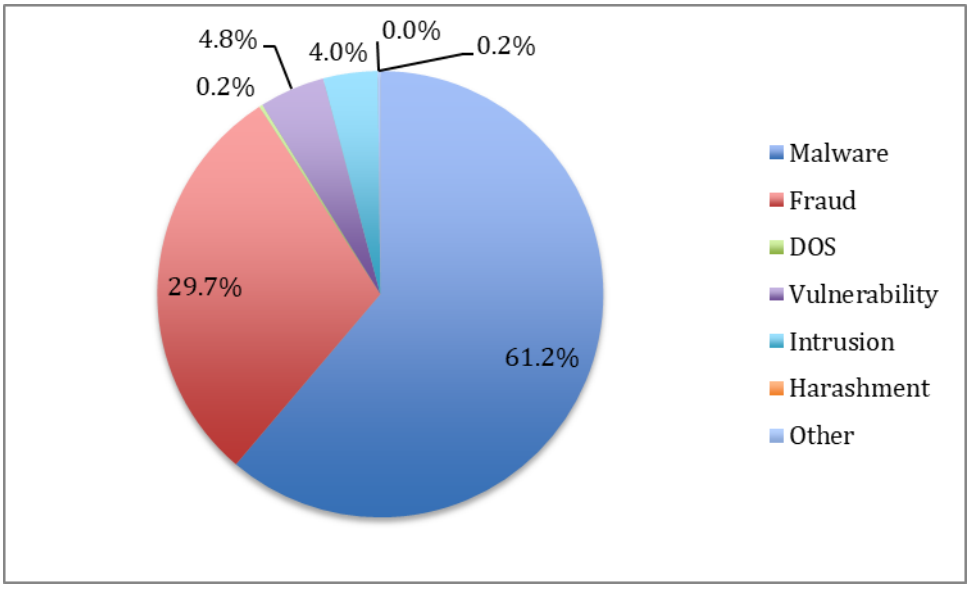


Figure 1. Incident reports in 2018

In 2018 Id-SIRTII/CC found 4,499 phishing sites targeting Indonesian user, 37% of them used .id domain while 63% used other international domain as shown in Figure 2.

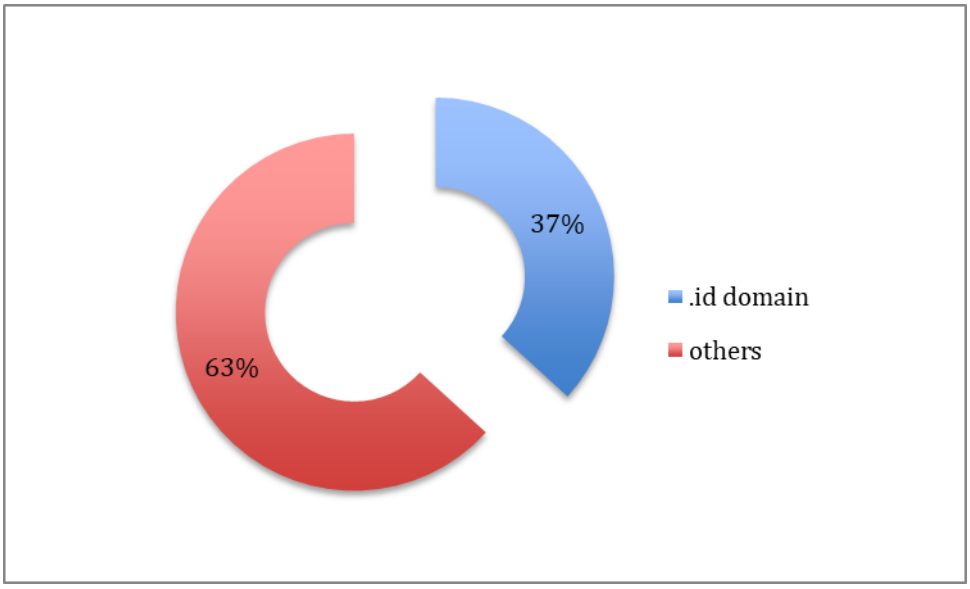


Figure 2. Phishing Site targeting Indonesia User

In 2018 Id-SIRTII/CC found also 16,939 website defacement incidents, 37% of them used .id domain while 63% used other international domain as shown in Figure 3.

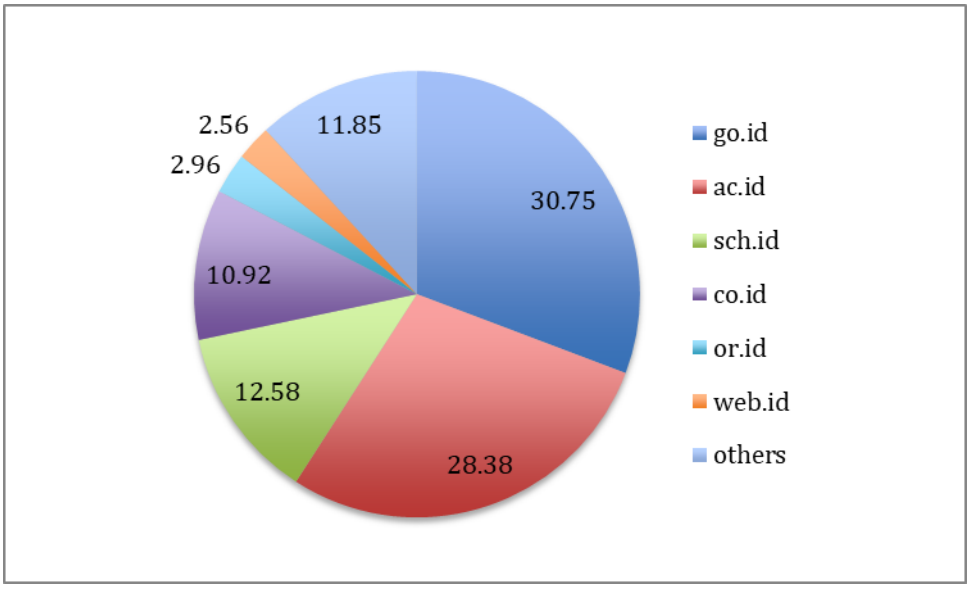
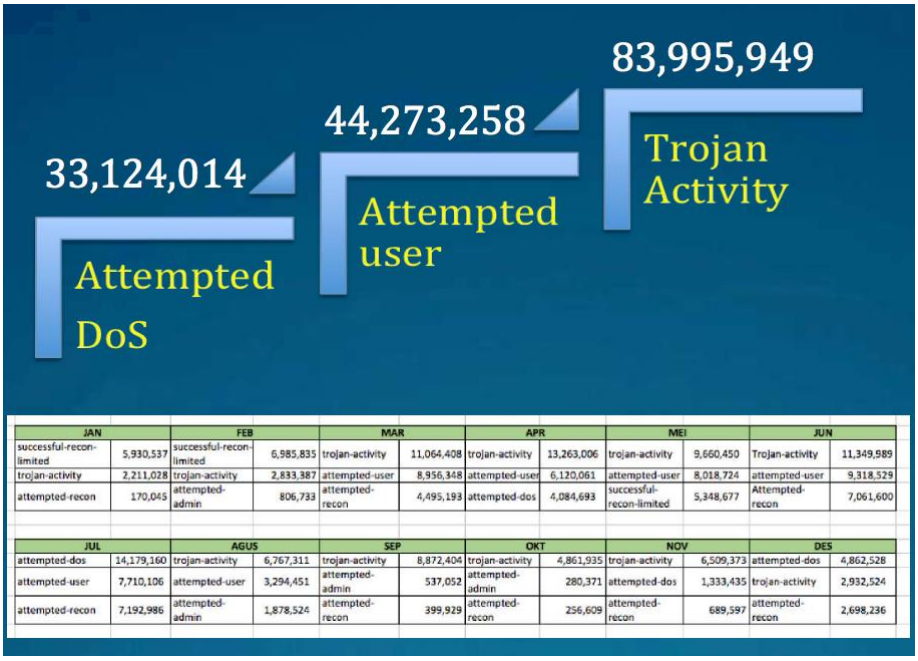


Figure 3. Web Defacement

From National Monitoring System, Id-SIRTII/CC found 232,447,977 indication of cyber attacks, which dominantly targeted port 53 and the use of trojan as top first of attack type as shown in Figure 4.



JAN		FEB		MAR		APR		MEI		JUN	
successful-recon-limited	5,930,537	successful-recon-limited	6,985,835	trojan-activity	11,064,408	trojan-activity	13,263,006	trojan-activity	9,660,450	Trojan-activity	11,349,989
trojan-activity	2,211,028	trojan-activity	2,833,387	attempted-user	8,956,348	attempted-user	6,120,061	attempted-user	8,018,724	attempted-user	9,318,529
attempted-recon	170,045	attempted-admin	806,733	attempted-recon	4,495,193	attempted-dos	4,084,693	successful-recon-limited	5,348,677	Attempted-recon	7,061,600

JUL		AGUS		SEP		OKT		NOV		DES	
attempted-dos	14,179,160	trojan-activity	6,767,311	trojan-activity	8,872,404	trojan-activity	4,861,935	trojan-activity	6,509,373	attempted-dos	4,862,528
attempted-user	7,710,106	attempted-user	3,294,451	attempted-admin	537,052	attempted-admin	280,371	attempted-dos	1,333,435	trojan-activity	2,932,524
attempted-recon	7,192,986	attempted-admin	1,878,524	attempted-recon	399,929	attempted-recon	256,609	attempted-recon	689,597	attempted-recon	2,698,236

Figure 4. Top three of cyber attacks

3.3 Publications

Id-SIRTII/CC publish periodically especially three publications. Every month Id-SIRTII/CC publish its National Monitoring Monthly Report and Every year

Id-SIRTII/CC publish Proceeding of Information Security Focus conferences (included FIRST TC) and Indonesia Cyber Security Report.

Figure 5. National Monitoring Monthly Report

Figure 6. Proceeding of Information Security

Figure 7. Id-SIRTII/CC Annual Report

4. Events Organized / Hosted

4.1 Cyber Drills

- Amazing Trace , an extraordinary cyber drill
- Cyber drill test for government institution with BSSN

4.2 HandsOn Workshop and Training

- Web Application Security Assessment
- Creating and Managing ISAC for Enhancing National Cyber Security : Financial and Critical Information Infrastructure Sector)
- IoT Pentest
- DNS Security
- Practical Packet Analysis for Incident Response
- Open-Source Intelegent (OSINT)
- Chief Information Security Officer

4.3 Conferences and Seminars

- Codebali
- FIRST TC
- OIC-CERT Workshop
- NISD

5. International Collaboration

5.1 International Partnerships and Agreements

Id-SIRTII/CC maintains its partnerships and agreements with other CERT organizations such as JP-CERT/CC , CNCERT, CSM/Mycert, and any other cyber security related entities such as

5.2 Capacity Building

Id-SIRTII/CC dispatched experts to the following trainings/ projects/ events in 2018.

- Timor Leste

Id-SIRTII/CC receive a experts visit to the following trainings/join research projects/events in 2018.

- CMU Creating and Managing CSIRT training
- CMU Creating and Managing CSIRT for ToT

- NTT East Speaker in NISD
- CNCERT workshop in NISD
- NTT East Research in Malware Analysis

5.3 Conferences and Presentation

In 2018, Id-SIRTII/CC participated and dispatched speakers to the following international cyber security events:

- 6th ASEAN CIO FORUM (25 January, Laos)
- Malaysia Cyber Security Summit (20 March, Kuala Lumpur - Malaysia)
- Keio Univ International Cyber Security Symposium (30 March, Tokyo - Japan)
- Putra Jaya Forum and Defense Service Asia (17 April, Kuala Lumpur - Malaysia)
- NatCSIRT Annual Meeting (29 June, Kuala Lumpur - Malaysia)
- OWASP Appsec Conference (10 July, Taipei - Taiwan)
- ASEAN Cyber Security Summit (16 August, Singapore)
- CSM-ACE (25 September, Kuala Lumpur - Malaysia)

6. Future Plans

Since April 2018, Id-SIRTII/CC moved to the New established National Cyber and Crypto Agency (NCCA) and works under the National Cyber Security Operation Center as its technostructure unit.

Based on this NCCA vision , mission and its function , Id-SIRTII/cc has to changes and consolidate its function to match with its main organization.

7. Id-SIRTII/CC Contact Information

Office address:
Menara Ravindo Lt. 17
Jl. Kebon Sirih No. 75
Jakarta Pusat, 10340
Indonesia

URL: https://www.idsirtii.or.id/
E-mail: info@idsirtii.or.id

Telp. +62 21 3192 5551
Fax. +62 21 3193 5556

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. Highlights of 2018

1.1 Summary of major activities

- New Board Chairman

  On 21 June, JPCERT/CC Board of Directors appointed Dr. Hiroaki Kikuchi as Board Chairman of JPCERT/CC. The predecessor Kazumasa Utashiro will continue in the management as Executive Director.

- Office relocation

  JPCERT/CC office was relocated to the following with effect from 26 November 2018.

  New address:

  8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 1030023 JAPAN

  New telephone number:

  Tel: +81-3-6271-8901

  Fax: +81-3-6271-8908

1.2 Achievements & milestones

- Organised Japan Security Analyst Conference 2018 for the first time

  On 25 January, JPCERT/CC organised the first edition of "Japan Security Analyst Conference 2018" in Tokyo with an aim to share information to deal with ever-evolving cyber attacks among technical experts. Presentations were selected from proposals submitted from experts in Japanese enterprises and security researchers. JPCERT/CC received positive feedback from the participants and will continue this event for the next years.

2. About JPCERT/CC

2.1 Introduction & Establishment

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. It is an independent, non-profit organisation, serving as a national point of contact in the technical layer for CSIRTs in Japan and worldwide.

After its inception in 1992, JPCERT/CC was officially established in 1996 and has been conducting incident handling operations, vulnerability handling operations, engaging in malware and threat analysis, working on control system security, publishing security alerts and advisories to the wide public, organizing forums and seminars to raise awareness of security issues, and supporting the establishment and operations of CSIRTs in Japan and overseas.

2.2 Constituency

JPCERT/CC's constituencies cover overall Internet users in Japan with a focus on technical staff of enterprises. JPCERT/CC also coordinates with network service providers, security vendors, government agencies, as well as industry associations in Japan.

3. Activities & Operations

3.1 Incident Handling Reports

In 2018, JPCERT/CC received 15,751 computer security incident reports from Japan and overseas.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	3,786	3,815	3,908	4,242	15,751

Figure 1. Incident reports to JPCERT/CC (2018)

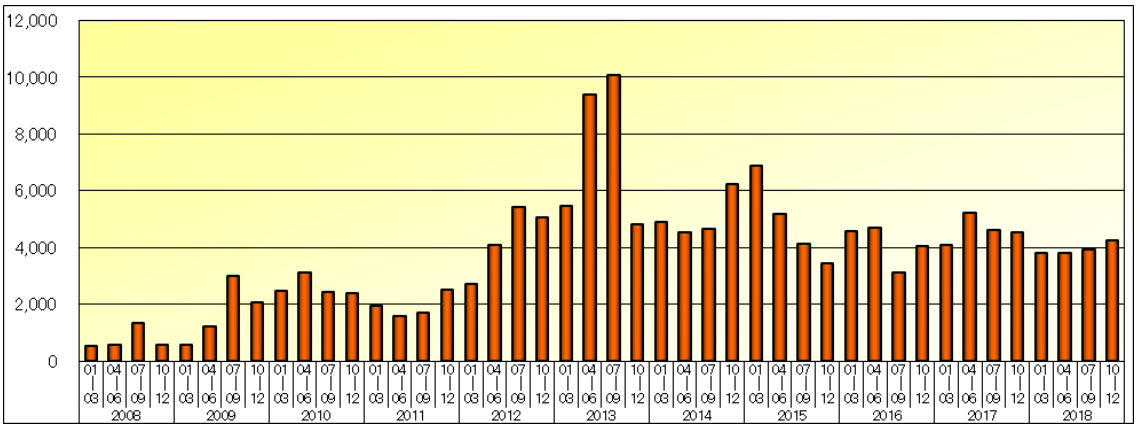


Figure 2. Incident reports to JPCERT/CC (2008-2018)

3.2 Abuse statistics

Incident reports to JPCERT/CC in 2018 were categorised as in Figure 3. About 38.7% of

the reports were on scan, followed by phishing and website defacement.

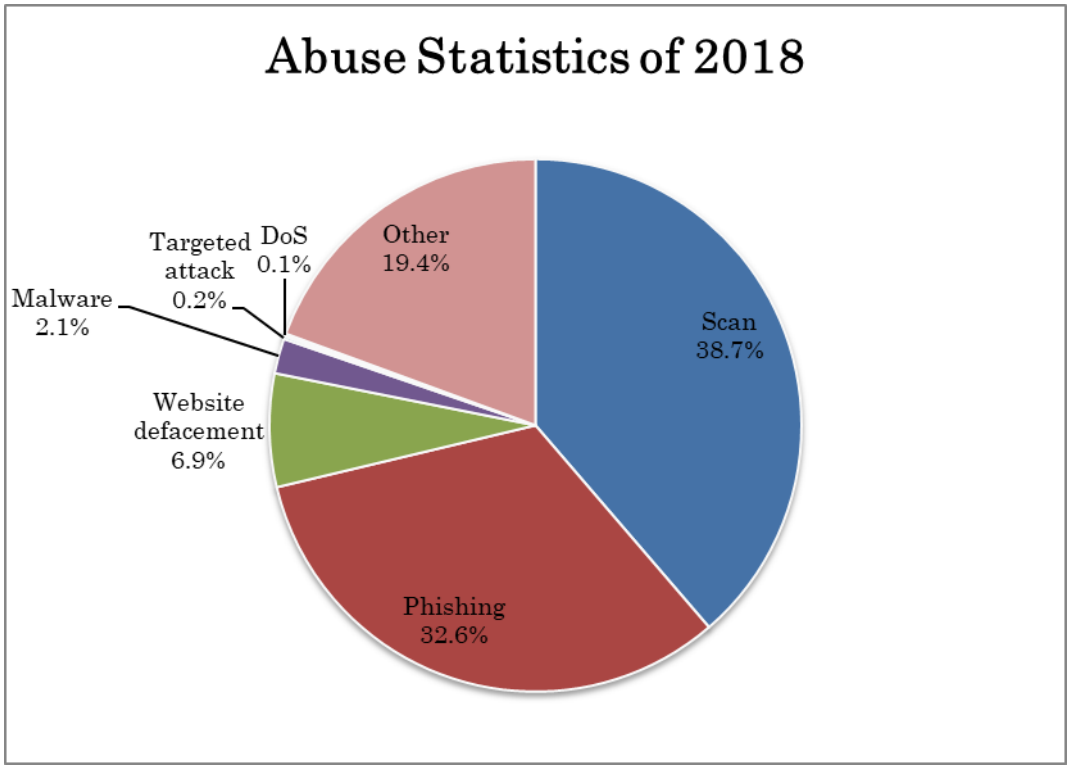


Figure 3. Abuse Statistics of 2018

3.3 Security Alerts, Advisories and Publications

- Security Alerts

https://www.jpcert.or.jp/english/at/ (English)

https://www.jpcert.or.jp/at/ (Japanese)

JPCERT/CC publishes security alerts on widespread, emerging information security threats and their solutions. In 2018, 52 security alerts were published.

- Early Warning Information

JPCERT/CC publishes early warning information to the Japanese government and organisations providing national critical infrastructure services and products through a dedicated portal site called "CISTA: Collective Intelligence Station for Trusted Advocates". Early warning information contains reports on threats, threat analysis and their solutions.

- Japan Vulnerability Notes (JVN)

https://jvn.jp/en/ (English)

https://jvn.jp/ (Japanese)
JVN is a portal site that provides vulnerability information and countermeasures for software products. JVN is jointly operated by JPCERT/CC and the Information-technology Promotion Agency (IPA) to provide descriptions, solutions, and developers' statements on vulnerabilities (including information on affected products, workarounds and solutions, such as updates/patches).
For products that affect a wide range of developers, JPCERT/CC coordinates with CERT/CC (https://www.cert.org/), ICS-CERT (https://ics-cert.us-cert.gov/), CPNI (https://www.cpni.gov.uk/), NCSC-FI (https://www.ncsc.fi/) and NCSC-NL (https://www.ncsc.nl/). JPCERT/CC also directly receives vulnerability reports from overseas researchers and coordinates with the researchers and developers with vulnerable products. Once solutions become publicly available, JPCERT/CC publishes advisories for the reported issues on JVN.
In 2018, 213 vulnerabilities coordinated by JPCERT/CC were published on JVN. 142 were cases published with IPA through the Information Security Early Warning Partnership, and 71 were published through partnerships with overseas coordination centers, developers, researchers, etc.
Of the 142 published through the Information Security Early Warning Partnership, 121 were reported to IPA by researchers, security vendors, etc. 21 were reported by developers on software developed by themselves. Of the 71 published through global partnerships, 36 were reported and published by CERT/CC, 1 by NCSC-FI, 3 by ICS-CERT, 19 were reported by developers on software they developed, 2 were reported by Japanese researcher, and 10 were published originally by JPCERT/CC through public monitoring activities and based on the information collected via the channels that JPCERT/CC has established privately.
In June 2010, JPCERT/CC became a CVE Numbering Authority (CNA). Since then, JPCERT/CC has been releasing Japan Vulnerability Notes (JVN) and JVN iPedia entries that contain reserved CVE Identifier numbers.

JPCERT/CC's Vulnerability Handling and Disclosure Policy is available here (English):
https://www.jpcert.or.jp/english/vh/2018/20180330-vulpolicy.pdf

- JPCERT/CC Weekly Report

JPCERT/CC publishes weekly reports on selected security information of the preceding week, including a useful tip which is relevant to current issues. (Japanese only)

- JPCERT/CC Official Blog

https://blogs.jpcert.or.jp/en/ (English)

Since September 2010, JPCERT/CC has been providing security news and technical observations related to Japan, as well as international activities that JPCERT/CC engages in on the blog. The blog platform was renewed in October 2018.

- Quarterly Activity Reports

https://www.jpcert.or.jp/english/menu_documents.html (English)

https://www.jpcert.or.jp/report/ (Japanese)

JPCERT/CC publishes quarterly activity reports and study/research reports both in Japanese and English.

- JPCERT/CC on Twitter

https://twitter.com/jpcert_en (English)

https://twitter.com/jpcert (Japanese)

Since January 2009, JPCERT/CC has been providing Security Alerts, Blog updates, etc. via Twitter.

3.4 Services

- Industrial Control System Security

Since 2008, JPCERT/CC has been working on awareness raising of industrial control system (ICS) security in Japan, and since January 2013, JPCERT/CC's incident handling service was extended to cover the ICS area. JPCERT/CC has provided presentations at seminars and has supported cyber incident exercises for engineers of Japanese asset owners. Furthermore, JPCERT/CC released an ICS security assessment tool "J-CLICS", developed in collaboration with experts from ICS vendors and asset owners. The tool has been translated into English and published on JPCERT/CC's website.

https://www.jpcert.or.jp/english/cs/jclics.html

- TSUBAME (Internet Threat Monitoring Data Sharing Project)

https://www.apcert.org/about/structure/tsubame-wg/index.html

The TSUBAME project is designed to collect, share and analyze Internet traffic data, in order to better understand the Internet threats mainly in the Asia Pacific region. It deploys sensors widely in the region, collecting and sharing the data with all

participating teams. The TSUBAME project aims to establish a common platform to promote collaboration among CSIRTs mainly in the Asia Pacific region. TSUBAME Working Group is active in APCERT and observation results are exchanged among the teams.

- Demonstration Test: Internet Risk Visualisation – Mejiro

https://www.jpcert.or.jp/english/mejiro/

JPCERT/CC has launched a demonstration test to visualise risks on cyber space based on data provided by multiple sources in comparison to the number of IP addresses assigned to each economy. Users can select a region and specify a period to perform analyses from various angles and obtain a more accurate picture of the situation. In January 2018, JPCERT/CC released this service on the website in Japanese, followed by the English version in August.

3.5 Projects

- CyberGreen Initiative

http://www.cybergreen.net/

CyberGreen is a global initiative designed to efficiently create a "healthy" cyberspace through cooperation with technical partners such as CSIRTs, ISPs and security vendors across the globe. The initiative provides metrics-based measurement and statistical analysis that can be compared across nations and regions. JPCERT/CC is working with Cyber Green Institute to improve upon the metrics, statistical analysis methods and visualisation.

3.6 Associations and Communities

- Nippon CSIRT Association

https://www.nca.gr.jp/en/index.html (English)

https://www.nca.gr.jp/index.html (Japanese)

The Association is a community for CSIRTs in Japan. JPCERT/CC serves as a member of the Steering Committee and Secretariat for the Association.

- Council of Anti-Phishing Japan

https://www.antiphishing.jp/ (Japanese)

JPCERT/CC serves as the Secretariat for the Council of Anti-Phishing Japan.

4. Events

4.1 Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staff, system administrators, network managers, etc. JPCERT/CC hosted the Control System Security Conference in February (held annually since 2009).

5. International Collaboration

5.1 International partnerships and agreements

- MoU

To further strengthen the cooperation, JPCERT/CC exchanges a Memorandum of Understanding (MoU) with various security organisations. In 2018, JPCERT/CC renewed the MoU with aeCERT and HKCERT, and newly signed an MoU with CERT-GOV-MD.

- FIRST (Forum of Incident Response and Security Teams)

https://www.first.org

JPCERT/CC contributes to the international CSIRT community and served as a member of the Board of Directors of FIRST. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST.

- APCERT (Asia Pacific Computer Response Team)

https://www.apcert.org/

Since its establishment, JPCERT/CC has been serving as a Steering Committee member and Secretariat. JPCERT/CC is also the convener of the TSUBAME Working Group, which aims to establish a common platform for Internet threat monitoring, information sharing & analysis within the region.

5.2 Capacity building

5.2.1 Training

JPCERT/CC dispatched experts to the following trainings/projects/events in 2018.

- Web defacement and Open Source Intelligence (OSINT) training at Africa Internet Summit (May, Dakar)
- OSINT training at CODE BALI (September, Bali)
- OSINT training at AfriNIC29 (November, Hammamet)

5.2.2 Drills & Exercises

JPCERT/CC participated in the following drills in 2018 to test our incident response capability:

- APCERT Drill 2018 (14 March)
- ASEAN CERTs Incident Drill (ACID) 2018 (5 September)

5.2.3 Seminars & presentations

In 2018, JPCERT/CC dispatched speakers to the following international events:

- 2018 APISC Security Training Course (April, Seoul)
- AusCERT Conference 2018 (May, Gold Coast)
- 30th Annual FIRST Conference (June, Kuala Lumpur)
- National CSIRT Meeting (June, Kuala Lumpur)
- Blackhat USA, Bsides LV (August, Las Vegas)
- Asia Pacific Telecommunity Symposium on Cybersecurity (September, Seoul)
- Global Conference on Cyber Stability (September, Singapore)
- FIRST Regional Symposium Asia-Pacific (October, Shanghai)
- CODEBLUE 2018 (November, Tokyo)
- HITCON Pacific (December, Taipei)

...and many more

5.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2018:

- USENIX Enigma 2018 (January, Santa Clara)
- S4x2018 ICS Security Conference (January, Miami)
- CanSecWest 2018 (March, Vancouver)
- RSA Conference US 2018 (April, San Francisco)
- ISO/IEC JTC 1/SC 27 Working Group Meeting (April, Wuhan) (September, Gjøvik)
- APWG eCrime (May, San Diego)
- DEFCON 26 Hacking Conference (July, Las Vegas)
- HITCON 2018 (July, Taipei)
- HITB GSEC (August, Singapore)
- The 6th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (August, Tokyo)
- BlueHat v18 (September, Seattle)

- Singapore International Cyber Week (September, Singapore)
- ACM Conference on Computer and Communications Security (October, Toronto)
- Virus Bulletin Conference 2018 (October, Montreal)
- FIRST TC Kiev (October, Kiev)
- APCERT AGM and Conference 2018 (October, Shanghai)
- Objective by the Sea (November, Hawaii)
- Botconf 2018 (December, Toulouse)

…and many more

- International Standard

(ISO/IEC JTC 1/SC 27 Information technology – Security techniques)

JPCERT/CC contributes to the following International Standards being developed under ISO/IEC JTC 1/SC 27 WG3:

ISO/IEC 29147: Vulnerability Disclosure

ISO/IEC 30111: Vulnerability Handling Processes

and WG4:

ISO/IEC 27035-1: Principles of incident management

ISO/IEC 27035-2: Guidelines to plan and prepare for incident response

ISO/IEC 27035-3: Guidelines for incident response operations

6. Future Plans

6.1 Future projects/operation

- Enhance English publications

JPCERT/CC has upgraded its blog platform in October 2018 to offer contents about technical observation, cyber security trends and event information etc. In 2019 and onwards, JPCERT/CC aims to publish more contents that can be useful for local and international cyber security communities.

7. JPCERT/CC Contact Information

URL: https://www.jpcert.or.jp/english/
E-mail: global-cc@jpcert.or.jp
Phone: +81-3-6271-8901
Fax: +81-3-6271-8908

KrCERT/CC

Korea Internet Security Center – Korea

1. Highlights of 2018

1.1 Summary of major activities

In 2018, KrCERT/CC prepared to face newly emerging cyber threat as attacks are evolving with new technology such as AI and machine learning and with new trends like spreading of IoT devices. KrCERT/CC has expanded and deepened its cooperation with domestic and international partners. It also improved its systems by applying machine learning technology to handle the emerging cyber threat efficiently. Furthermore, it held several seminars and trainings to raise awareness and share information.

1.2 Achievements & milestones

As the number and size of ransomware damages is growing, KrCERT/CC published "Guideline for preventing and responding ransomware" in order for users and companies to prevent and minimize cyber threat. It contains how ransomware works, what major symptoms are, how to prevent and respond including the way of reporting to KrCERT/CC.

KrCERT/CC also tries to proactively respond to the newly emerging cyber threat. Cyber threat is increasing and getting complex, which needs CERT's active attitude to the threat. For effective response, KrCERT/CC made an effort to apply AI and Bigdata technology to detect, prevent and respond the evolving cyber threat. It established "Cyber Security Bigdata Center" in December, 2018. It collects data from the KrCERT/CC's detection and analysis, including cooperation with both its domestic and international partners. KrCERT/CC provides the processed data including malicious IPs, malware, C&C servers, distribution sites and etc.

KrCERT/CC also operating two kinds of alliance with domestic and international concerning organizations under the name of "Cyber Threat Intelligence" and "Global Cyber Threat Intelligence". It hosts meetings with the members on a regular basis for exchanging knowledge about recent threat and technology. One of the results of the knowledge exchange, KrCERT/CC announced "the Cyber Attack Forecast" with the 7 points to take note in 2019. Based on the analysis of the trend in 2018, it predicts cyber threat trends in 2019 for people and information security-related entities to prepare

and prevents their assets.

2. About CSIRT

2.1 Introduction

The Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC) is Korea's national CSIRT which is responsible for the private sector. Formed under the Korea Internet & Security Agency (KISA), KrCERT/CC is composed of three divisions, one center with fourteen teams.

KrCERT/CC carries out various responsive and preventive programs designed to minimize damage by enabling a promptly response to incidents and to increase awareness in order to prevent incident.

2.2 Establishment

KrCERT/CC was established in 1996 as a small team responsible for hacking incidents under the Korea Information Security Agency (former KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet Crisis caused by so-called 'slammer worm' in 2003. At that time, KrCERT/CC had difficulties in communication efficiently with a telecommunication carrier, which marked the turning point for the Korean Government to recognize the importance of cooperation with security incident response teams and businesses such as ISP. As a result, the Security Incident Response Team was established under KISA (former KISA) in December 2003, and has evolved into its current form by responding to major national security incidents that occurred in 2007, 2009 and 2013.

The multiple names of KrCERT/CC occasionally give cause for confusion. In South Korea, it is called KISC, or the Korea Internet Security Center.

2.3 Resources

As of Dec. in 2018, around 160 employees from 3 divisions and 1 center, work for KrCERT/CC.

2.4 Constituency

KrCERT/CC serves as the focal point to coordinate security incidents in all Korean constituencies. According to the national cybersecurity framework and the related legislation, KrCERT/CC is responsible for handling incidents and ensuring the security

of information systems and networks in the private sector, such as the telecommunication sector and home users. At the international level, KrCERT/CC cooperates with many leading national CERTs/CSIRTs, international organizations and security vendors.

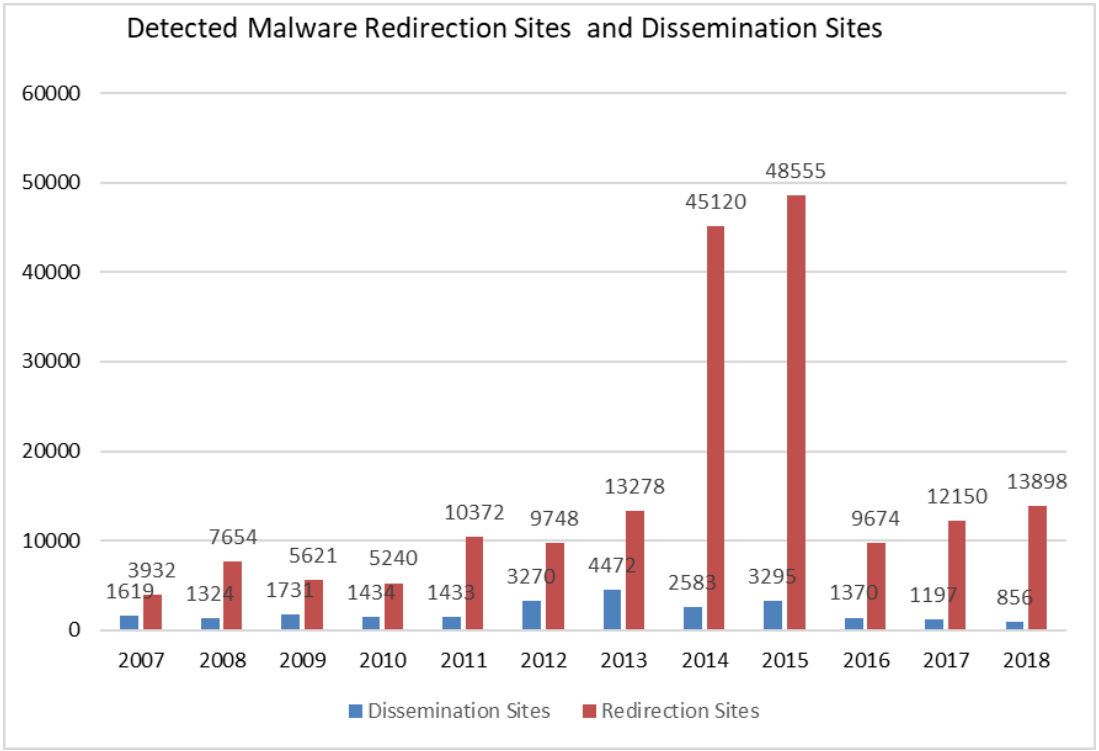
3. Activities & Operations

3.1 Scope and definitions

KrCERT/CC works for the safe and reliable cyber space by preventing cyberattacks and enhancing countermeasures. The mission of it is 1) to guarantee a rapid response to major nationwide Internet incidents to prevent and minimize damages, 2) To cooperate closely with domestic (ISPs, anti-Virus Companies) and foreign partners (FIRST, APCERT, etc.), 3) 7 days/24 hours Monitoring, Early Detection/Response on cyberattacks in the private sector.

3.2 Abuse statistics

Compared with the number of last year, the number of compromised website distributing hidden malware decreased in 2018 by 28% from 1197 to 856. Meanwhile, the number of redirection sites increased by 10% from 12,150 to 13,898 after a plunge in 2016.



3.3 Publications

KrCERT/CC semiannually publishes a malware detection report and issues advisory on its websites whenever a major security issue occurs. Also, on a quarterly basis, it uploads a cyber threat trend report on the website. Furthermore, an annual white paper in both Korean and English is uploaded on the website.

4. Events organized / hosted

4.1 Training

KrCERT/CC held the 2018 APISC Training Course, which is an annual invitation-based security training course on CSIRT establishment and operation that KrCERT/CC has been hosted since 2005. The course opens a door for the participants from different countries mainly in the Asia-Pacific region to build a human network at the working-level which is one of the most important elements in cybersecurity incident response. 16 participants from 16 countries including the Australia, Serbia, Malaysia participated in the 2018 training course and shared their expertise on cybersecurity structure and CERT operation.

KrCERT/CC also runs GCCD, the Global Cybersecurity Center for Development (GCCD) which was established in June 2015. In 2018, GCCD, in collaboration with the World Bank and the University of Oxford, held seminars in the Eastern Europe – Macedonia, Bosnia and Herzegovina, and Albania. At the seminars, experts provided knowledge about CERT/CSIRT operation, Cyber threat landscape, information sharing system, or C-TAS and etc.

4.2 Drills & exercises

KrCERT/CC hosted domestic cyber threat drill in November 2018 with the Ministry of Science and ICT(MSIT) to check readiness of rapid cyber threat response and an organic cooperative system. 35 companies, including ISPs, security vendors, portal service providers, financial institutions, and cryptocurrency exchanges, participated in the drill. It enabled participants to check an entire response process from threat detection to incident investigation through these drills. Aside from this, 2 more cyber drills were conducted with relevant agencies.

4.3 Conferences and seminars

In collaboration with the Ministry of Science and ICT, KISA hosts the 6th "Day of Information Security" celebration and "International Conference on Information

Security (ICIS)" on July 12. Speakers share their view and experiences about cyber security on Infrastructures, recent cyber threat with technological innovation and so on. Furthermore, KrCERT/CC holds a meeting on a regular basis with domestic organizations and entities for sharing expertise and knowhow under the name of "Cyber Threat Intelligence".

4.4 Competition

KrCERT/CC hosted the 15th Hacking Defence Contest (HDCON) with the MSIT in December 2018. HDCON is a time-honored domestic contest that started in 2004. This year, HDCON tried new format of contest while it held competition for competing participants' skills on incident analysis and forensics. In 2018, participants applied with the idea about handling and preventing current cyber security issues that companies actually have difficulty in dealing with. At the final stage, 6 teams presented their ideas about three topics, supply chain attack, internal network security and account stealing. KrCERT/CC the new format help to inspire companies to come up with solution that they can actually apply in their cyber security environments.

5. International Collaboration

5.1 International partnerships and agreements

In response to a need for stronger and more effective collaboration at the global level to maintain a safe cyberspace, KrCERT/CC established the Cybersecurity Alliance for Mutual Progress (CAMP) serving as a platform where members take collective actions to keep cyberspace secured. In this regards, CAMP annual meeting was held in September 2018 in Seoul, where all members gather to discuss the direction of operations, and exchange best practices that advance mutual interests. Along with the closed member meeting, open conference and exhibitions are also held. Regional Forums held in Serbia and Korea intend to intensify cross-border co-operation and discover potential future tasks for CAMP. Member countries and potential members had in-depth discussions on the current state of cybersecurity within the region.

5.2 Capacity building

5.2.1 Training

KrCERT/CC participates in APCERT online training on a regular basis. In 2018, two experts participated in the US-Japan joint training for ICS cybersecurity. KrCERT/CC provides chance for various trainings and conferences for improving the techniques and

knowhow and broaden views for cyber security such as FIRST Regional Symposium, RSA, Blackhat and etc.

5.2.2 Drills & exercises

KrCERT/CC joined in the APCERT Drill in March, 2018. The drill required the participants to solve virtual incident with 9 injects.

5.2.3 Seminars & presentations

KrCERT/CC took part in the following seminars and conferences:

- FIRST TC at APROCOT 2018 in February 2018, Nepal
- FIRST AGM and conference in June, Malaysia
- 2018 APCERT AGM in October, Shanghai, China
- NIST conference in November, the United States

6. Conclusion

Technology in cyber space is getting evolving and devices are getting more connected. The changes give challenges and require more developed skills for cyber security. KrCERT/CC will improve its capability by embracing new technology and face proactively with challenges. Establishment of Bigdata center and hosting a new format of contest are part of it endeavor. KrCERT/CC will try diverse attempt to safer and securer cyber space and contribute to cyber security in the world.

LaoCERT

Lao Computer Emergency Response Team – Lao People's Democratic Republic

1. Highlight of 2018

1.1 Summary of Activities

- Co-Organized the 1st Cyber Security Workshop for government and private technical officers on 03-04 September 2018 in Vientiane Capital, Lao PDR.

1.2 Achievements & milestones

- Law on Prevention and Combating Cyber Crime

2. About LaoCERT

2.1 Introduction

Lao Computer Emergency Response Team (LaoCERT) is the national CERT of Lao PDR, under, Ministry of Post and Telecommunications and it develop on capacity building for its staffs in the field of cyber security with other CERTs organizations in the region to against with cyber-attack. LaoCERT has been promoted to public and has been known among IT social, government agencies, private organizations in Laos PDR as well as international CERTs and LaoCERT was a member of APCERT in 2014. This annual report will describe activities and operation of LaoCERT in 2018.

2.2 Establishment

LaoCERT was established in February 2012 by degree 220/MPT as a LaoCERT division under the Lao National Internet Center, Ministry of Post and Telecommunications (MPT), Government of Lao PDR. It was established by following up as ITU-IMPACT recommendations and It has been announcement to become the national CERT equivalent department in 2016, directly under to the Ministry of Post and Telecommunications.

2.3 Resource

LaoCERT currently contain 30 staffs, 7 females and divide into 4 Divisions and technical staff currently holds professional information security certificate as follow:

- Cellebrite Certified Physical Analyst
- Computer Hacking Forensic Investigator

LaoCERT Organization Charts

2.4 Constituency

LaoCERT is a coordination center of cyber security within Laos and also cooperation with international CERT organizations in the field of cyber security. LaoCERT is responsible for incident handling, cyber security protection, disseminating information security and awareness raising for ensuring the cyber safety to all citizens, government agency and private organizations include education institute, banks, internet service providers…etc. in Laos PDR.

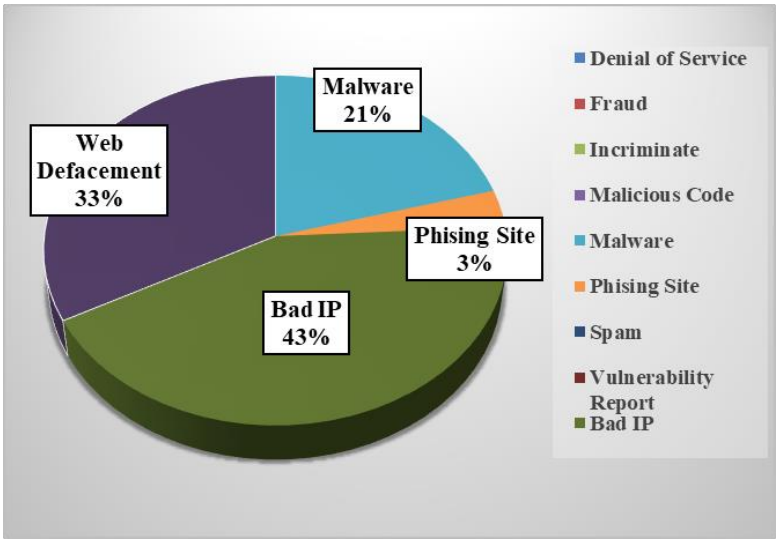
3. Activities & Operations

3.1 Scope and definition

LaoCERT aim to awareness raising on cyber security and solving issue on cyber security incident response as well as to collaboration with other CERT organizations to against with cyber-attack.

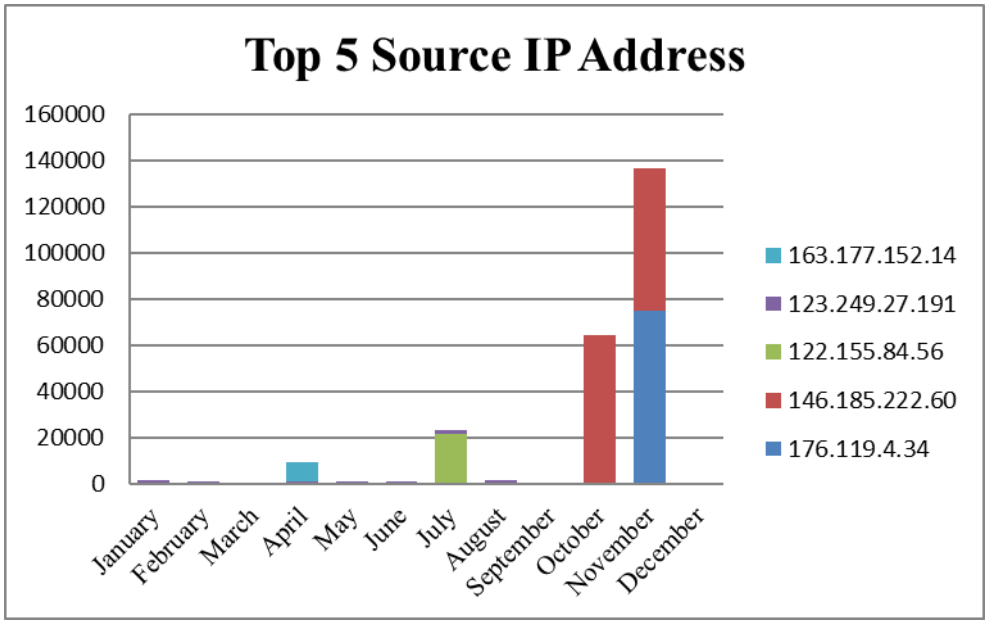
3.2 Incident handling report

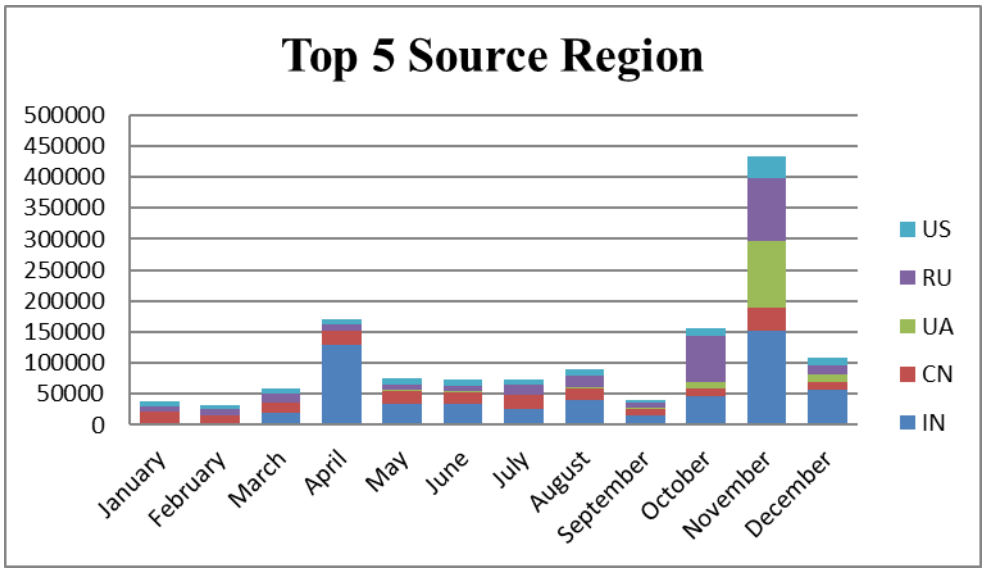
The following graph shows the incidents that happened in 2018.

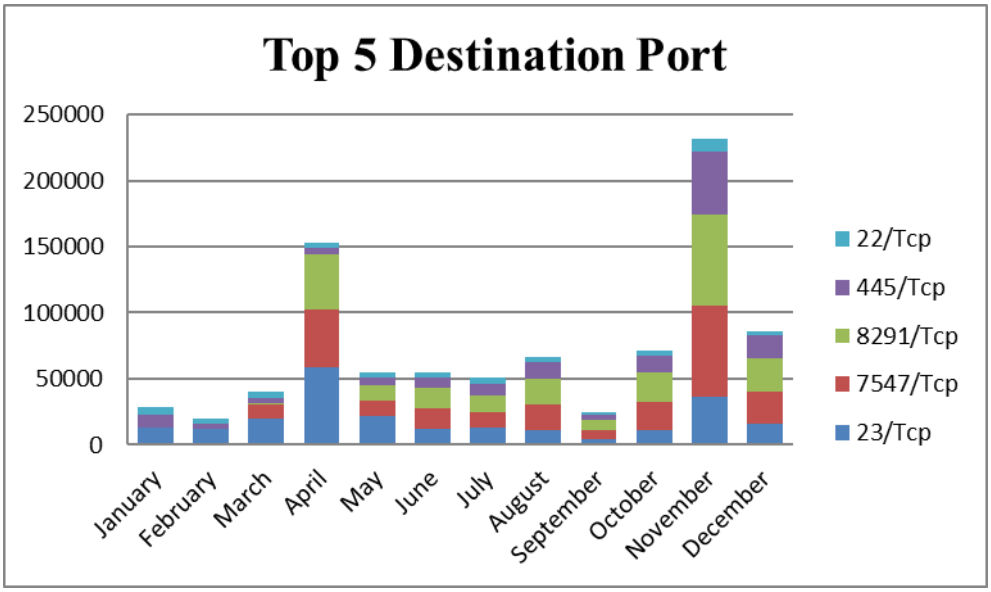


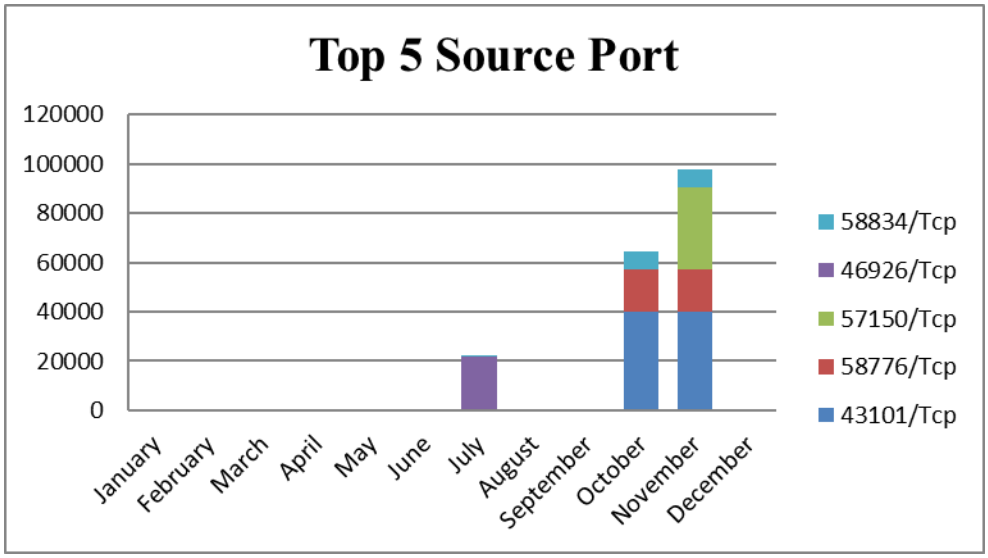
3.3 Abuse Statistics (TSUBAME Sensor)

The following graph shows the top 5 of Source IP Address, top 5 of Source region, top 5 of Destination port and top 5 of Source port statistics obtained by TSUBAME Sensor in 2018.









3.4 Publication

- Website: www.laocert.gov.la
- E-mail: admin@lacert.gov.la
- Tel: +85621 254508 (08:00-16:00) Working hour
- Incident report: report@laocert.gov.la
  (+ 85630 5764222) 24 x 7

3.5 New Services

- Dissemination and advisories on social media and Cyber crime Law to provincial.

4. Events organized / hosted

4.1 Conference and Seminars

- Co-Organized the seminar on Cyber Security Threat Intelligence and Cyber Security Monitoring service on 10th December 2018 in Vientiane capital, Lao PDR.
- Co-Organized the 1st Cyber Security Workshop for government and private technical officers on 03-04 September 2018 in Vientiane Capital, Lao PDR

5. International Collaboration

5.1 International partnership and agreement

- MoU signed with ThaiCERT (ETDA) on 28th December 2018.

5.2 Capacity Building

5.2.1 Training

- Attend the training course on Defense Practice against Cyber Attack from 25th February- 11th March 2018 in Tokyo, Japan.
- Attended the Training Program on Information Security and Internet of Things from 17th – 27th June 2018 in China.
- Attend the Digital Forensics Training from 16th – 20th July 2018 in Singapore.
- Joint the Japan & US training for Industrial Control System Cybersecurity from 10-14 September 2018 in Tokyo, Japan.
- Attend the Certified Incident Management and active Defense Training from 18th – 26th September 2018 in Malaysia.
- Attend the 1st training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 24th – 28th September 2018 in Bangkok, Thailand.
- Attend the training program on Southeast Asia Regional Cybercrime and Intellectual Property Rights Enforcement from 15th – 19th October 2018 in Singapore.
- Attended the training course on Cyber Security Technologies – Recent Trend of Risks and Countermeasures to them from 30 October – 08 November 2018 in Tokyo, Japan.
- Attend the 2nd training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 29th October – 2nd November 2018 in Bangkok, Thailand.
- Attend the 3rd training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 17th – 21st December 2018 in Bangkok, Thailand.

5.2.2 Drills and Exercises (Online)

- Participating the APCERT Drill on 07 March 2018.
- Joint the ASEAN CERT Incident Drill (ACID) on 5th September 2018.

5.2.3 Seminar and conference

- Joint the 1st ASEAN-Japan Cyber Security Working Group Meeting on 19th – 22nd February 2018 in Brunei.
- Attend the ASEAN Cyber Security Strategy Building on 19th – 22nd March 2018 in Singapore.
- Joint the 1st ASEAN-Japan Cyber Security Working Group Meeting on 9th – 10th May 2018 in Bali, Indonesia.
- Attended the 2nd ASEAN Cyber Norms Workshop on 24th – 27th June 2018 in Singapore.
- Attend the Cyber Law International Course on 9th – 12th July 2019 in Singapore.
- Joint the 1st ASEAN-Japan Cyber Security Working Group Meeting on 23rd – 26th July 2018 in Manila, Philippine.
- Attend the Cyber security workshop from 13th-16th August 2018 in Singapore.
- Attend the 3rd Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV from 4th -7th September 2018 in Cambodia.
- Attend the 11th ASEAN-Japan Cyber Security Policy Meeting on 16th – 17th October 2018 in Tokyo, Japan.
- Attended the China-ASEAN Network Security Emergency Response Capacity Building Seminar on May 21st - 25th October 2018 in China.

6. Future Plans

- Implementing the threat monitoring system.
- Planning for Monitoring Critical National Information Infrastructure (CNII).
- Planning for Establishing Government Threats Monitoring (GTM).
- Develop national critical information infrastructure protection mechanism to enhance the robustness of Laos's national infrastructure.
- Expanding awareness data protection Law.
- Drafting National Cyber Security Policy.
- Studying National Cyber Security Strategy.
- Studying and planning to set up the Honeypot, HoneyNet.

- Establishing the project for training of cybersecurity to public and private sector and POC in Lao PDR.
- Planning to set up the Network Monitoring System.

7. Conclusion

LaoCERT is continuing to develop team, we will keep devoting to Incident Handling, network security emergency response and strengthen the cooperation with other security organizations also looks forward to collaborate with internationally cyber security as well as enhance public awareness activities in order to provide the training, seminars and workshop to promote the policy and Law on cybersecurity.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2018

1.1 Summary of major activities

- Collaborate with "Crime Investigation Department (CID)" of Myanmar Police Force to solve the cyber crime cases.
- Giving seminars, workshops and sharing the knowledge to the student of "University of Computer Studies, Yangon (UCSY)", Crime Investigation Department (CID) and "Government Technological College (GTC)".

2. About CSIRT

2.1 Introduction

Myanmar Computer Emergency Response Team (mmCERT) is a national computer emergency response team for handling cyber security incidents in Myanmar and it was a member of APCERT since 2011.

2.2 Establishment

mmCERT was established as a National Computer Emergency Response Team in Myanmar on July 23 2004 and mmCERT/cc (mmCERT coordination center) is strengthening on Dec 15 2010 . The Ministry of Transport and Communication (MOTC) is a leading Ministry of Information Technology and Cyber Security Department Activities in Myanmar and it provides budget to mmCERT/cc since then. In 2016, The Ministry of Communication and Information Technology (MCIT) was changed the name to the Ministry of Transport and Communication (MOTC).

2.3 Resources

Members of mmCERT include from one ministry: Ministry of Transport and Communications (MOTC). The operation of mmCERT was directly managed by Information Technology and Cyber Security Department and total 8 members worked for mmCERT. The 3 members are increased in 2018.

2.4 Constituency

mmCERT has been enhancing for disseminating security information and

advisories and providing technical assistance to his constituencies. These are financial, governmental, research and education, internet service provider, vendor and economy.

3. Activities and Operations

3.1 Scope and definitions

- Create National IT image by cooperating with international CERT teams for cyber security and Cyber crime
- Disseminate Security Information and Advisories
- Provide technical assistance
- Cooperate with law enforcement organizations for cyber crime

3.2 Incident Handling Reports

The following graph shows the incidents that were solved by mmCERT in 2018. According to the results on incident analysis by mmCERT, Intrusion and Information gathering cases were the most prominent incident cases in 2018.

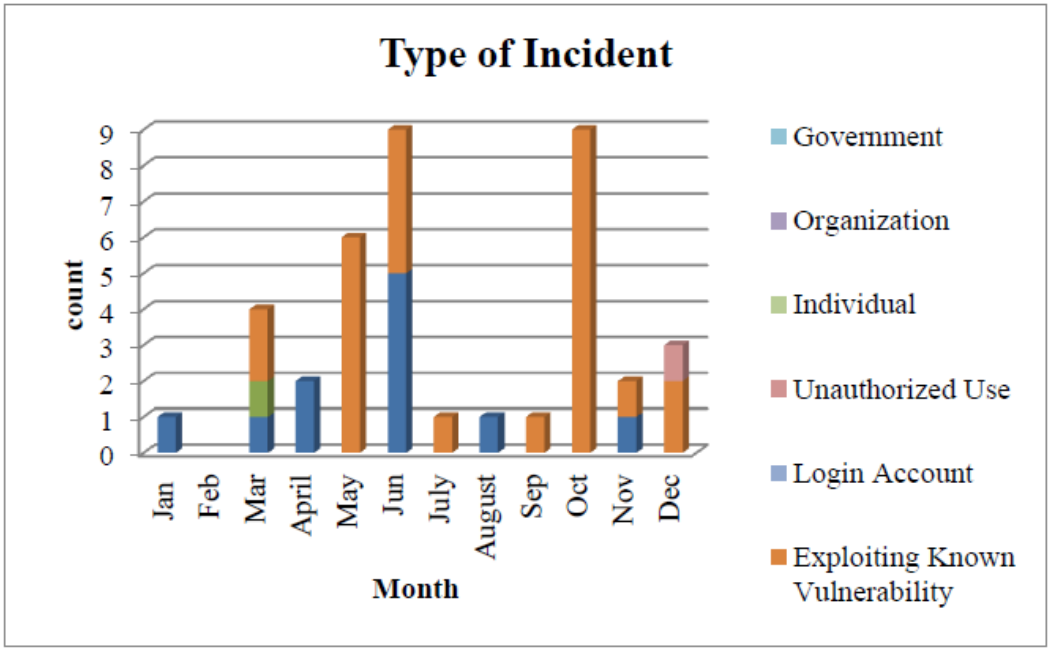


Figure 1 Type of Incident

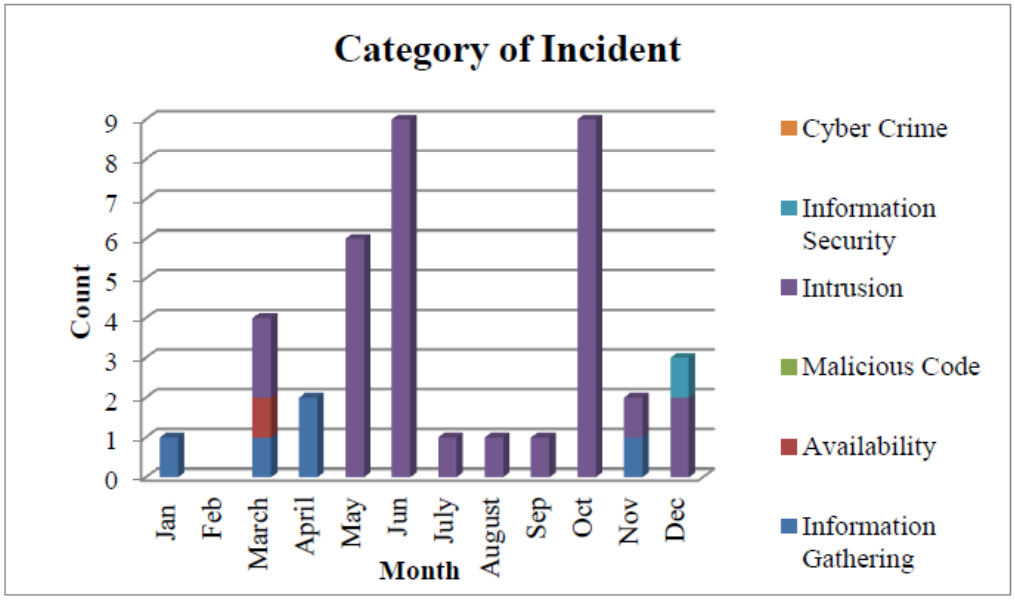


Figure 2 Category of Incident

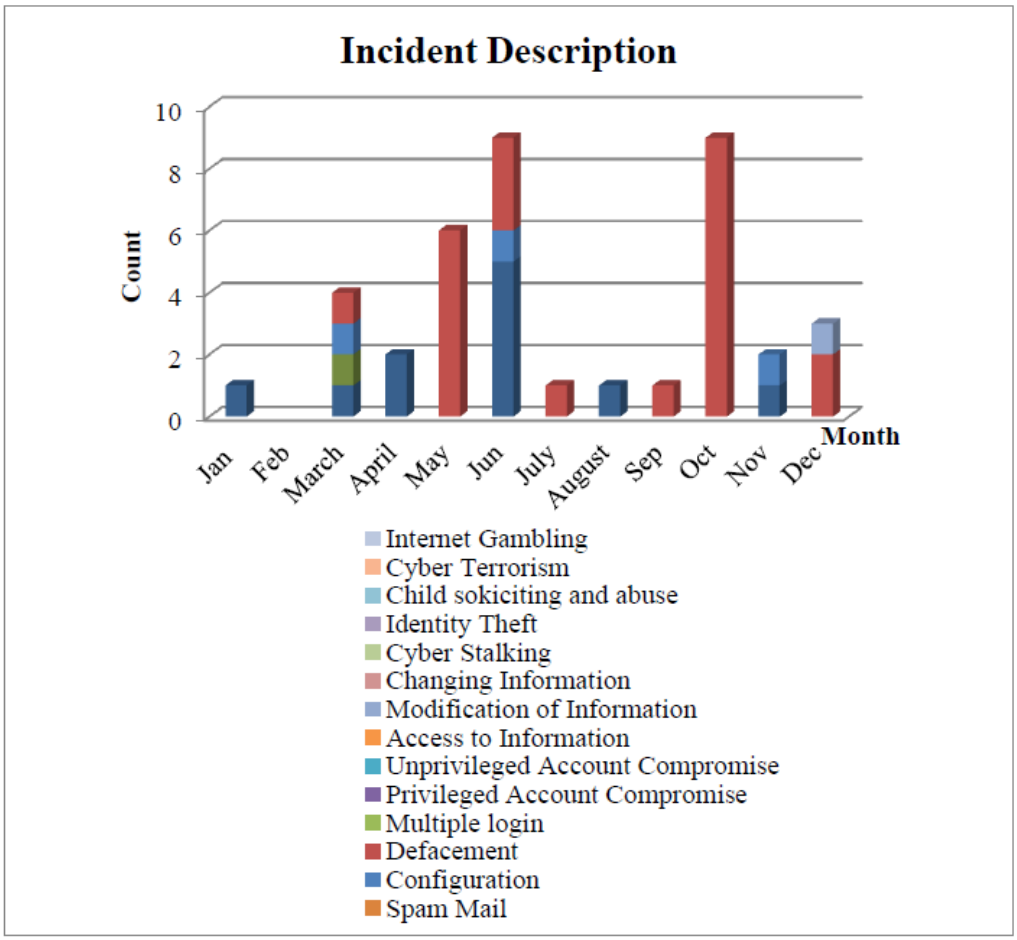


Figure 3 Description

4. Events Organized/Co-organized

4.1 Training

- Giving Internship to the student of "Technological University, Hmawbi" and "Technological University, Meikhtila" on (May – July, 2018)

4.2 Drill and exercises

Drill

- Participating in APCERT Drill on March 7, 2018. APCERT Drill 2018 Title is "Data breach via malware on IoT"
- Participating in ACID Drill on September 5, 2018. ACID Drill 2018 Title is "System Vulnerabilities and Crypto currency Mining"

Cyber Exercises

- Participating in ASEAN –JAPAN Cyber Exercise on May 23, 2018.

4.3 Conferences and Seminars

- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on January 1, 2018.
- Participating in All-Round Youth Development Festival 2018 at Mandalay University, Mandalay on August 11-13, 2018.
- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on October 9, 2018.
- Participating in CyberBayKin - Secure a Digital Myanmar Conference at Naypyitaw on November 27, 2018.
- Participating in e-Government Conference & ICT Exhibition 2018 at Naypyitaw on November 27-28, 2018.
- Attending in Cisco Threat Hunting Workshop at Yangon on November 28.
- Giving "Zero-day Malware-Static Analysis" Seminar to public at Bsides Myanmar 2018 (Information Security Conference), MICT Park, Yangon on 16 December 2018.

5. International Collaboration

5.1 Capacity Building

5.1.1 Training

- Attending in "Capacity Building in Policy Formation for Enhancement of Measures

to Ensure Cybersecurity in ASEAN Region" Training at Tokyo, Japan on January 21 to February 8, 2018.

- Attending in "MOTC Staff Training" at Tokyo, Japan on March 2018.
- Attending in "Defence Practice against Cyber Attacks" Training at Tokyo, Japan on February 25 to March 9, 2018.
- Attending in "Cyber Security Technologies--- Recent Trend of Risks and Countermeasure to them" Training at Tokyo, Japan on October 29 to November 8, 2018.
- Attending in "China-ASEAN On-site Network Security" Incident Training at Naypyitaw, on November 13-14, 2018.
- Attending in "The 3rd Training of the ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE" at Thailand on December 17-21, 2018.

5.2 Conferences, Seminars and Workshop

- Attending in "8thASEAN JAPAN Information Security Workshop for ISPs" Workshop at Japan on February 1 -2, 2018.
- Attending in "the 3rd Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries" Workshop at Cambodia on September 6-7, 2018.
- Attending in "China-ASEAN Network Security Emergency Response Capacity Building Seminar" at Shanghai, China on October 21-25, 2018.

  Attending in "Singapore International Cyber Week (SICW)" Conference at Singapore on September 18-20, 2018.
- Participating in "The 4th ASEAN-Japan Information Security Joint Working Group
- Meeting and CIIP Workshop" at Seda Vertis North Hotel, Philippines on July 23-26, 2018.
- Attending to "Workshop on Cyber Security" at Singapore on August 16 - 18, 2018.

6. Future Plans

6.1 Future projects

- Government Security Operation Center
- Government Secure Service Network
- Penetration Testing Labs
- Forensic Lab

7. Conclusion

As being mmCERT is a developing team, we are trying very much for to be a developed and matured team by elaborately doing Incident Handling, Cyber Security Researches, efficiently providing Technical Advisories, Trainings, Seminars and Workshops to Constituencies, Computer and Technological Universities' Students effective Capacity Building to our Technical Team members, enhancing Public Awareness Activities and promoting International and National Co-operations for CERT Activities and doing Research on Log Data Analysis as much as we can.

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. Highlights of 2018

1.1 Summary of major activities

MNCERT/CC has successfully organized MNSEC 2018 annual event which has covered pretty large scope and allowed the participants to exchange their experience and knowledge.

"Kharuul Zangi 2018" and "Kharuul Zangi U18 2018" cyber security competitions have been held successfully by MNCERT/CC.

1.2 Achievements and milestones

Year 2018 was a full of achievements for MNCERT/CC. One of the main activities was providing its member organizations with security threat news feeds, recommendations, consulting and trainings.

One of the key achievements of this year was continuation of "Kharuul Zangi U18 2018" cyber security competition which was organized among high school senior grade students. Prizes for winners have been expanded with Cisco CCNA training course vouchers and University matriculation vouchers. Goal of the competition is to provide the knowledge of possible danger caused by cybercrime and appropriate knowledge about internet usage and to enhance cyber threat awareness for high school students.

Key achievements continued to MNSEC 2018 event which has been organized with new features such as villages, electronic badge and registration fee.

2. About MNCERT/CC

2.1 Introduction

"Mongolian Cyber Emergency Response Team / Coordination Center" (MNCERT/CC) is a non-governmental organization which established in 2014 and has been performing its function under the guidance and regulation of Mongolian National Security Council. MNCERT/CC is responsible for incident response and monitoring, disclosing the cyber security related information and knowledge to public, developing and broadcasting the methodology to prevent from cyber threats, providing its member organizations with cyber security details and training, as well as acting as coordinator to defend Mongolian cyber environment.

2.2 Establishment

"MNCERT/CC" was established on March 15th, 2014 and founded on following grounds: Based on the component of information security of the Mongolian National Security Concept and National program for Cyber security, the 48th resolution was approved by Mongolian State Great Hural (State Great Assembly) in 2010:

- Objective 2.2 "Establish a system to respond on cyber threats and incidents, develop national CERT, expand cooperation with organizations that have similar operations (e.g. APCERT, FIRST, CERT/CC) (Implementation date 2010-2012, financial source – foreign loan & aid)"
- Objective 4-1 "To strengthen capacity of the organization obligated to provide security on state's data and information (Implementation date 2010-2015, financial source – foreign loan & aid)"

2.3 Resources

According to the Non-governmental organizations code of Mongolia, the founders of MNCERT/CC have appoint the steering committee with seven members and consultant team with three members on November, 2015. In 2016, two members have been added to the steering committee which became totally 9 members. The members of steering committee and consultant team consists of the professionals and researchers in information technology field especially in cyber security and a legal advisor.

Human resource:

- Board Chairman – 1
- Chief Executive Officer – 1
- Officer–2
- Incident Handler – 2
- Analysts–2
- Legal advisor - 1
- Consultant – 3

2.4 Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks
- Mobile Operator Companies

- Universities
- MonCIRT and DCERT
- General public

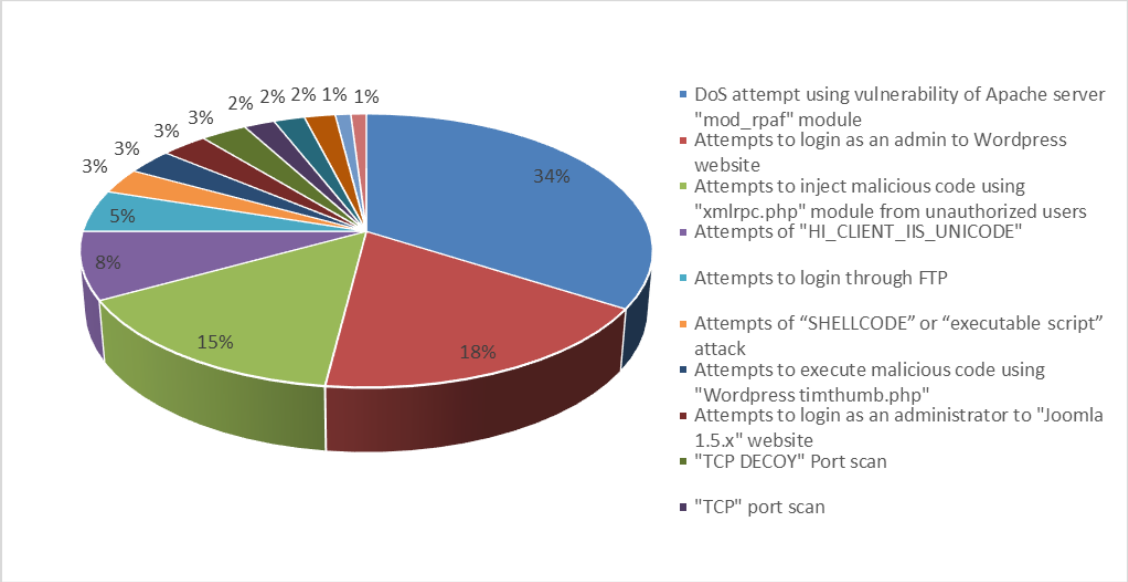
3. Activities & Operations

3.1 Scope and definitions

MNCERT/CC's constituency covers various types of organizations such as business companies, private sector organizations, banks, universities, non-governmental organizations and general public. MNCERT/CC provides services such as discussion, training, security information and feed, recommendation, consulting, research and analysis report and coordination with other local and international CSIRTs for its member organizations as well as provides and improves cyber security awareness of general public.

3.2 Abuse statistics

The summary of acitivities carried out by MNCERT/CC during the year 2018 is given in the following chart. This chart shows about summary of the critical incidents and attempts that were registered: DoS attempt using vulnerability of Apache server "mod_rpaf" module 34%, attempts to login as an admin to Wordpress web site 18%, attempts to inject malicious code using "xmlrpc.php" module from unauthorized users 15%, attempts of HI_CLIENT_IIS_UNICODE 8%, attempts to login through FTP 5%, attempts of SHELLCODE or "executable script" attack 3%, attempts to execute malicious code using "Wordpress timthumb.php" 3%, Attempts to login as an administrator to "Joomla 1.5.x" website 3%, "TCP DECOY" port scan 3%, "TCP" port scan 2%, attempts to content-disposition 2%, attempts to access admin.php 2%, attempts to access using calendar.php 2% and attempts to access using Mambo upload.php 1%.



4. Events organized / hosted

4.1 Training

4.1.1 CISSP Training

We have organized CISSP training in Ulaanbaatar, Mongolia during 07-11th May 2018. The training has been held with full support of Team Cymru who provided with all expenses of CISSP instructor and Official guide to the CISSP CBK fourth edition books for attendees. The training has been conducted without any fee for our constituency.

The training has covered overall 30 attendees who are majored in IT security managers and engineers, security analysts, system administrators, IT auditors and university instructors from various industries such as governmental organizations, banking and financial sectors, data center, mobile operators and universities. All of the attendees have been provided with Official guide to the CISSP CBK fourth edition books.

CISSP training has been held for the first time in Mongolia. MNCERT/CC team and all the training attendees expressed huge gratitude to Team Cymru that they made significant contribution to Mongolian security sector.

4.1.2 MISP Training

MNCERT/CC have organized MISP (Malware Information Sharing Platform) training with the support of CIRCL on 03th October in Ulaanbaatar, Mongolia. Mr. Steve Clement from CIRCL has been invited as an instructor. The training covered 21 security specialists and system administrators from our constituency and it gave a great overview and knowledge for using MISP platform. CIRCL team and Mr. Steve

Clement made a great contribution to Mongolian security field.

4.1.3 Local training and workshop

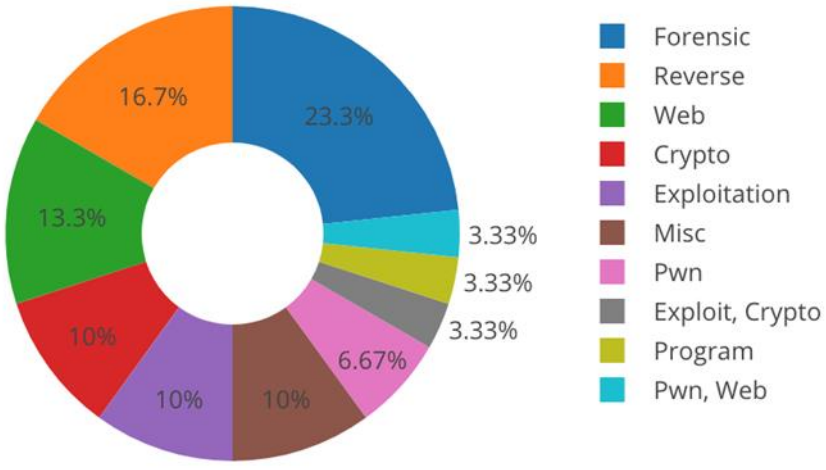
MNCERT/CC have conducted two training and workshops among security engineers of public and private sectors during MNSEC 2018 event. The workshop topics were "Linux hardening" and "Windows forensics", which instructed theoretically and practically by MNCERT/CC security researcher and analyst.

4.2 Drills & Exercises

4.2.1 "Kharuul Zangi 2018" National Cyber Security Competition

MNCERT/CC organizes a cyber security contest named "Kharuul Zangi" in order to promote the real life challenges and proper knowledge of cyber security to general public. We have successfully organized "Kharuul Zangi 2018" competition between 22nd September to 05th October of 2018, in collaboration with Mongolian national data center, Golomt Bank, National cyber security department, "SafeBit" LLC and "MSTRide" LLC. 1st stage was designed to be completed online while the 2nd and 3rd stages had to be completed onsite using the network and systems designed by the organizers. Out of 132 teams of 396 members, 30 teams qualified from the 1st stage. Total of 46 tasks of 8 categories have been given to be completed at 1st stage and 34 tasks have been completed out of them by the competitor teams.

At 2nd stage, 26 teams have participated the contest and the organizing team of competition prepared 30 tasks of 10 types at this stage. The tasks are shown in the following chart.



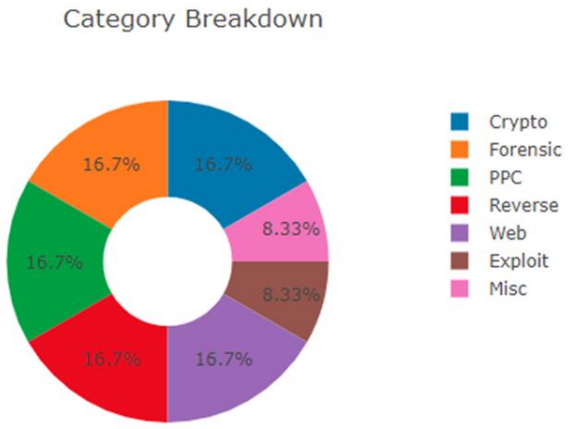
After the 2nd stage, 10 teams were qualified to final stage. 3rd stage of the competition has been held on 03th October 2018, at MNSEC 2018 event.

Topic of the 3rd stage was Mortal Combat, famous game introduced in 1995. Score board of final stage is shown in following picture.

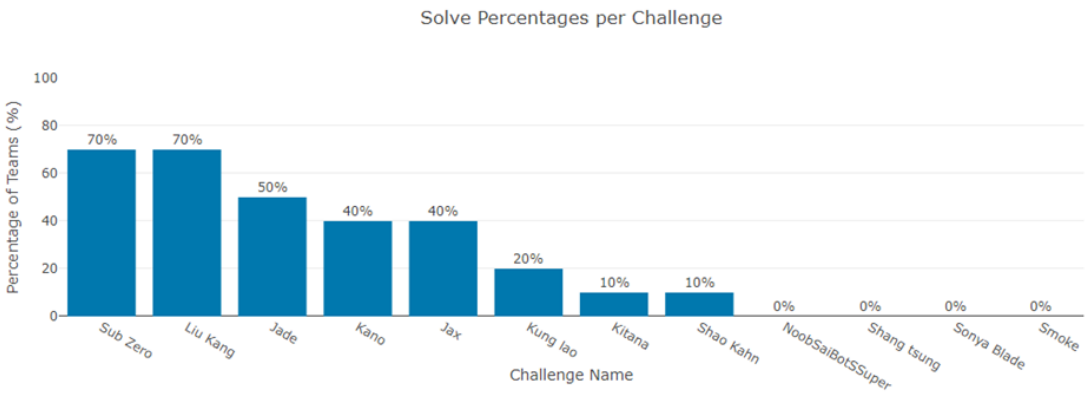
1	#MongolianEmpire	-	-	856	-	-	1000	-	919	991	-	-	-	3766
2	dEspAGitO	-	1000	856	-	-	-	-	-	991	-	-	-	2847
3	0x32d7	-	-	856	-	-	-	-	919	-	-	-	-	1775
4	n$	-	-	856	-	-	-	-	919	-	-	-	-	1775
5	TeamPB	-	-	-	-	-	-	-	-	-	1000	-	-	1000
6	M	-	-	-	-	-	-	-	919	-	-	-	-	919
7	YMGNBYB	-	-	856	-	-	-	-	-	-	-	-	-	856
8	k11even	-	-	-	-	-	-	-	-	-	-	-	-	0
9	wp	-	-	-	-	-	-	-	-	-	-	-	-	0
10	TSOO	-	-	-	-	-	-	-	-	-	-	-	-	0

Score board of final stage

Final stage had 12 tasks with types of crypto, forensic, ppc, reverse, web, exploit and misc which is shown in the following chart.



Following diagram shows the quality of teams and how the tasks completed.



4.2.2 "Kharuul Zangi U18 2018" Cyber Security Competition

MNCERT/CC has initiated and organized cyber security competition named "Kharuul Zangi U18" among the high school students under the age of 18 on April 2018. The competition goal is to provide knowledge about possible danger caused by the cybercrime and to increase cyber threat awareness for high school senior grade students.

Totally 216 competitors of 54 teams have challenged for the competition. Participants increased by 52 than the previous year. 1st stage of the competition had been held onsite while the final 2nd stage had been onsite. High school senior grade students had great interests to this kind of competition and had informed to be more prepared for next Kharuul Zangi U18. As viewing the competitors and their instructors, we found that participants of previous contest Kharuul Zangi 2013 have trained their next generation and made them to attend this competition.

4.3 Conferences and seminars

4.3.1 MNSEC 2018 Event

Information technology (IT) benefits the business world by allowing organizations to work more efficiently and maximize productivity. Faster communication, electronic storage and the protection of records are advantages that IT can bring in your enterprise. Nevertheless there are challenges to overcome in order to continue the development of IT sector. The lack of skilled human resource, legal environment, software and hardware infrastructure for the Information Technology sector in Mongolia and information security is one of them. Therefore, we have organized MNSEC 2018 event on 04th and 05th October of 2018 at the Corporate Convention

Center providing the opportunity to share experience, necessary information, knowledge, technology and new solution within the security community. We have been organizing this event annually since 2012 in Information technology and cyber security field of Mongolia. The goal of this event is to improve cyber security in alliance with government agencies and private sectors by discussing current issues and solutions regarding Mongolian cyber environment.

MNSEC 2018 event has been conducted successfully with the great contribution from JPCERT/CC, APNIC, Palo Alto Networks Unit 42 and CIRCL. Experts from above organizations and CSIRTs have been invited to the event and made great presentations about cyber espionage in Asia and Mongolia with case study.

MNCERT/CC team have a special thanks to these organizations and experts that continuously support us namely Adli Wahid from APNIC, Katsuhiro Mori from JPCERT/CC, Steve Clement from CIRCL and Bradley Duncan from Palo Alto Networks Unit 42.

This event covered some of the most popular topics in cyber security field, therefore about 250 representatives, engineers and technical specialists have participated and shared their knowledge & experience. Participation included from sectors such as financial institutions, universities, government agencies, mobile operators and internet service providers.

5. International Collaboration

5.1 International partnerships and agreements

- APCERT
- TEAM CYMRU
- FIRST
- APWG
- MICROSOFT

5.2 Capacity building

5.2.1 Drills & exercises

- Participated in APCERT Drill 2018 on March, 2018

5.2.2 Seminars & presentations

MNCERT/CC attended to the following international seminars and meetings:

- FIRST TC on March in Osaka, Japan.
- FIRST AGM on June in Kuala Lumpur, Malaysia.
- APCERT AGM 2018 on October in Shanghai, China.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2019.

Events, conferences and drill to participate are as follows:

- APCERT Annual General Meeting 2019 on October in Singapore.

Local activities to organize are as follows:

- MNSEC 2019 Cyber Security Event
- "Kharuul Zangi U18 2019" Cyber Security Contest among high school students
- "Kharuul Zangi 2019" Cyber Security Contest among IT specialists.
- Local cyber drill among member organizations.
- Local training for our constituency
- Initialize and share threat intelligence feed through MIS, introduce it to out constituency.

7. Conclusion

2018 was the year of great success and progress for MNCERT/CC, especially for the local cooperation, the number of our members increased and the cooperation and services for them have improved.

We are looking forward the year 2019 to be a more progressive year in both local and international stage and greater collaboration with APCERT and other international organizations.

MOCERT

Macau Computer Emergency Response Team Coordination Centre – Macao

1. Highlights of 2018

1.1 Summary of Major Activities

During the year 2018 MOCERT has provided the following activities in addition to the base Incident Response and Early Waning through

- Publication of industry specific notification of potential information security issues;
- Publication of broadly affecting issues that affect web servers of Macau origin be they government, industry or other;
- Assisted in the Capture the Flag (CTF) – Cyber Security Challenge information security competitions for public to enhance awareness on cyber-attacks and information security;
- Maintenance of a website as point of reference for MOCERT services;
- Involved in the TSUBAME Working Group;
- Participated in the APCERT Drill 2018 as Player and Observer;
- Article publications in a local magazine called "Macau-ICT";
- Development of MOCERT cyber threat intelligence (MOCERT-CTI) system

1.2 Achievements & milestones

MOCERT has launched a Cyber Threat Intelligence (MOCERT-CTI) System which is able to automatically collect threat intelligence from open-sources and trusted parties. This MOCERT-CTI, along with another integrated Incident Response Management system, will be beneficial to MOCERT's constituencies to deal with incidents handling tasks more effectively.

2. About CSIRT

2.1 Introduction

MOCERT (Macau Computer Emergency Response Team) is a non-profit service funded by MANETIC (Macau New Technologies Incubation Centre), an organization that is supported through industry sourced funding.

The mode of operation provides for an environment for MOCERT to be self-determined, and agile to changes required for an evolution of the service that is required to be provided as the computer security landscape changes in Macao.

MOCERT's core services are an evolving set of computer security issue collection, analysis and notification that encompasses public and industry specific advisories; Provision of a computer incident reporting facility that assist in security issues reactively, as they are reported, or proactively, from collected network evidence in the regional ASN; Provision of behavioral changes campaigns through educational activities for public.

2.2 Establishment

MOCERT started operations in late 2009 and it was in the validation of the services at the end of 2009 that MANETIC formally established and launched MOCERT as a public facing service on the 8th February 2010. Since then, and in a short time, the services have evolved in a manner that is appropriate to the size of the constituency it serves, Macao.

2.3 Resources

The staffing for the MOCERT service is sourced from MANETIC's pool of computer security professional and support staff. As of the year ending 2018 there are two (2) staff providing the service with eight (8) additional support staff.

2.4 Constituency

The constituency of Macau Computer Emergency Response Team Coordination Centre (MOCERT) shall be the internet users of Macao be they from government, businesses, or home users.

3. Activities & Operations

3.1 Scope and definitions

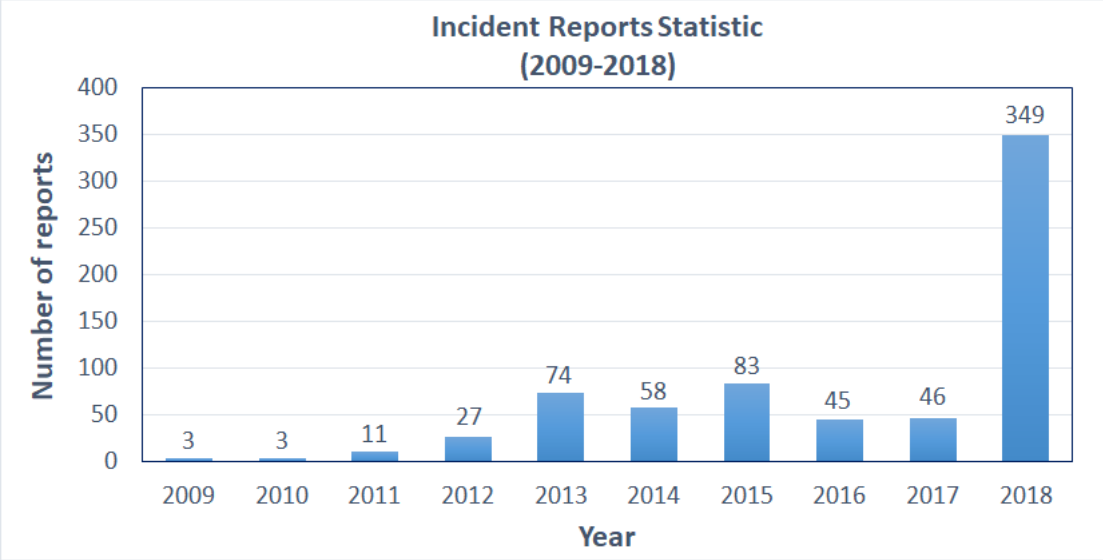
Macau Computer Emergency Response Team Coordination Centre (MOCERT) is managed by Macau New Technologies Incubator Centre in providing Macao with computer security incident handling information, promoting information security awareness, as well as coordinating on an international and local level, computer security issues, advisories, incident response, and research for the Macau public and local enterprises.

3.2 Incident handling reports

Incident reports are increasing as there is an increase in the natural reports being

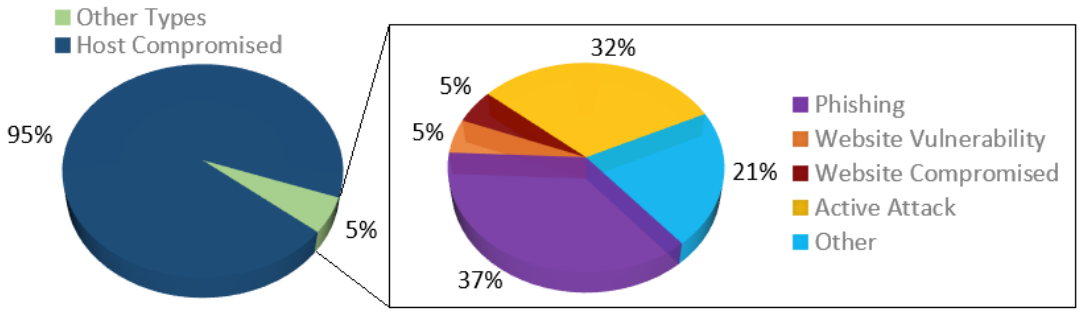
submitted, but also the increase is due to the addition of a service that proactively warns website owners of security issues. Sources of incidents are from three distinct channels.

1. Reported by Web
2. Reported by E-mail message
3. MOCERT initiated from incident discovery activity.



3.3 Abuse Statistics

The following pie graph denotes the abuse distribution as noted for the year 2018. The numbers are drawn from the incidents handled.



3.4 Publications

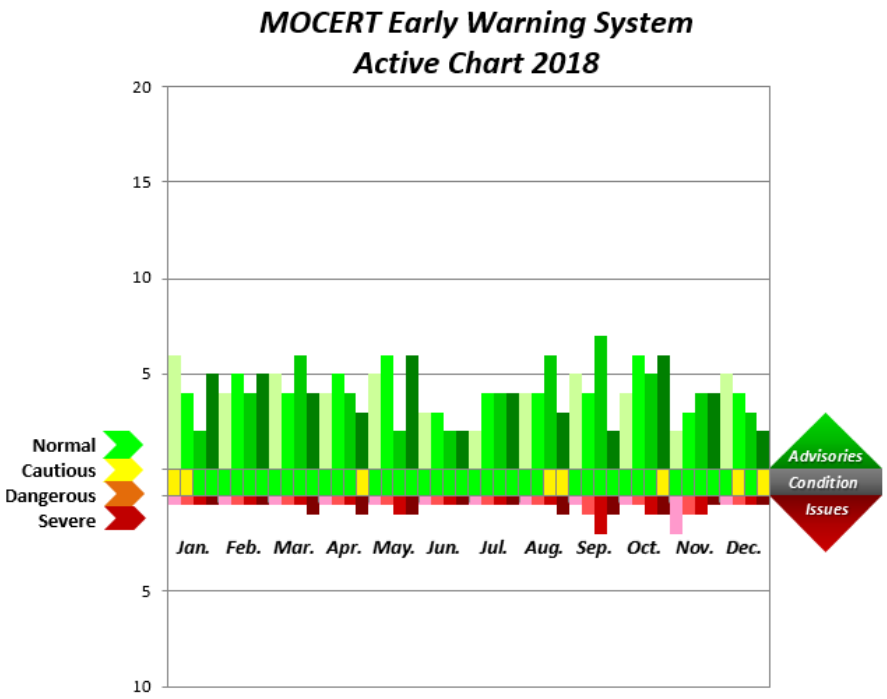
3.4.1 Articles

MOCERT published articles in a local magazine called "Macau-ICT". The magazine is distributed free of charge to the constituency.

- Macau-ICT ISSUE 28
  Title: Everything is a Record
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=38:issue-28&catid=3:macau-ict&tmpl=component
- Macau-ICT ISSUE 27
  Title: IP Surveillance Cameras: What Do You Need to Know
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=37:issue-27&catid=3:macau-ict&tmpl=component
- Macau-ICT ISSUE 26
  Title: Vulnerability Assessment vs. Penetration Testing
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=36:issue-26&catid=3:macau-ict&tmpl=component

3.5 Early Warning Notices

A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency. The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 211 postings in 2018 with 196 postings being Advisories, and 15 Issues.



4. Events organized / hosted

4.1 Training

Staffs in MOCERT service a provided on the job training of incidents along with formal attendance to courses and seminars that first show the need for computer security, followed by personnel certification is practical.

4.2 Conferences and Seminars

MOCERT assisted in a Capture the Flag - Cyber Security Challenge event hosted by a local company, NetCraft Information Technology (Macau) Co. Ltd. This was the first Capture the Flag competition in Macau in order to enhance public awareness of cyberattacks.

5. International Collaboration

5.1 International partnerships and agreements

MOCERT maintains and promotes international partnership and agreements that promote a clean and safe internet.

5.2 Capacity Building

5.2.1 APCERT Online Training

MOCERT participated in APCERT online training courses held in 2018.

5.2.2 Drills & exercises

- APCERT Drill

The involvement in 2018 in the APCERT drill included as a Player and Observer.

6. Future Plans

6.1 Future projects and operation

Future projects mainly focus on the improvement of MOCERT's Threat Information Sharing Platform and provision of IT security consultancy services for the constituency. MOCERT will provide on demand training courses, incident handling services, and hold cybersecurity events for the constituency. Also, MOCERT will continue to collaborate with local and international members on incident handling and information sharing.

7. Conclusion

2018 has been a year where MOCERT launched a cyber threat information sharing platform. The major challenges up ahead are collaborating with local enterprises and organizations to provide solutions that meet their IT security requirements as further security consultancy services are sought. The changes envisaged will be beneficial to MOCERT's constituencies as the platform is progressively being improved to promote a clean and safe Internet.

MonCIRT

Mongolian Cyber Incident Response Team – Mongolia

1. About MonCIRT

1.1 Introduction

A Mongolian Cyber Incident Response Team (MonCIRT) is a Non-Governmental, Nonprofit organization with the objective of securing Mongolian education and public cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services. We perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents, internet threats
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Improve information security awareness, literacy, provide comprehensive trainings.
- Provide a comprehensive view of network security risks, attack methods, vulnerabilities, and the impact of attacks on information systems and networks;
- Provide information on incident and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Such other functions relating to cyber security as may be prescribed

MonCIRT services are available for society and educational sector.

The MonCIRT helps the Internet community deal with its immediate problems and analyzes the scope and nature of the problems. To increase awareness of security issues and help organizations improve the security of their systems, we continue to disseminate information through multiple channels:

- telephone and email
  - hotline: + 976 - 70113151
  - email: info@moncirt.org.mn
- World Wide Web: http://www.moncirt.org.mn/

1.1.1 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2011 MonCIRT operate as sole national CSIRT of Mongolia. From 2012 operate MNCERT/CC at Data Center as NGO.

Now MonCIRT acts as the focal point for cyber security for the Mongolian internet society, especially educational sector.

1.1.2 Workforce

MonCIRT currently has a total of 6 constant staffs such as: executive director-1, experts 3, the bookkeeper 1, system administrator-1. Most of our staffs works part-time.

1.1.3 Constituency

Currently MonCIRT's constituency encompasses the Public users (citizens, business companies, private sector organizations, NGO and general public) of Mongolia and whole universities, institutes, colleges, high schools and other educational organizations.

2. Activities & Operations

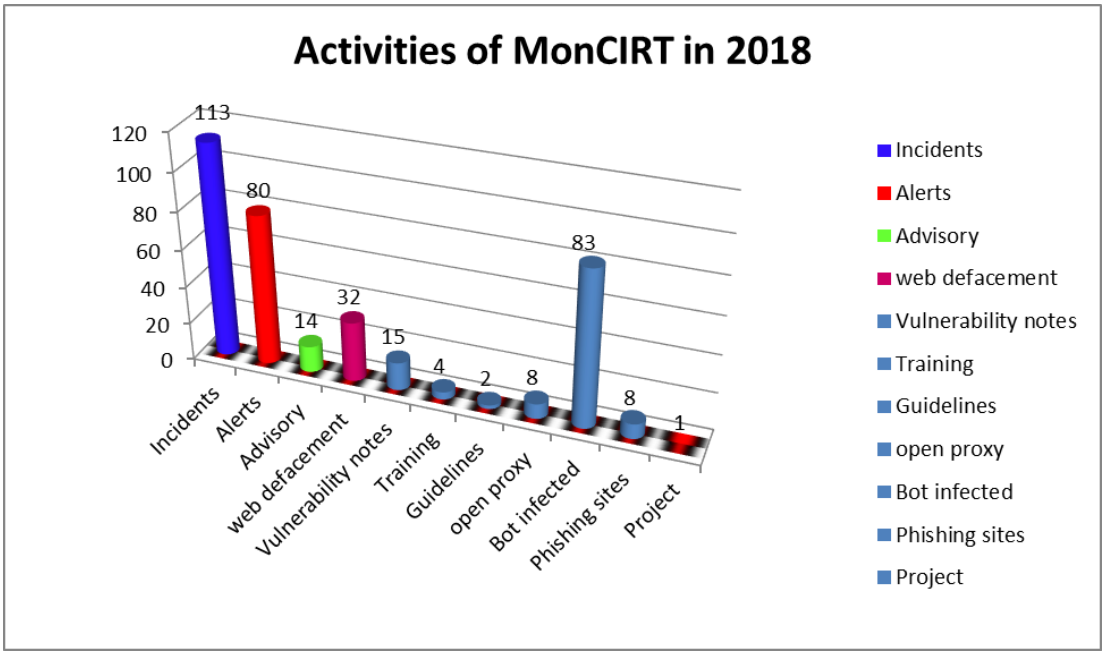
2.1 Summary

Innovation breeds opportunity in any areas. Web and mobility innovations focus on ease of use, availability, and building large user audiences, but they breed opportunity for cybercrime. Security typically comes later, after a period of breaches and security issues put the issue front and center. Through 2018, we are in the midst of this security period. The summary of activities carried out by MonCIRT during the year 2018 is given in the following table:

Activities	Year 2017
Security Incidents handled	113
Security Alerts issued	80
Advisories Published	14
Vulnerability Notes Published	15
Security Guidelines Published	2
Trainings Organized	4
Mongolian Website Defacements tracked and advised	32
Open Proxy Servers tracked	8

Bot Infected Systems tracked	83
Phishing (mirror) web sites tracked and removed	8
Projects	1

The following chart depicts the distribution of various types of activities of the MonCIRT



2.2 Incident trends

MonCIRT working to create organization's trust to us as reliable security center which can share sensitive information about security compromises and network vulnerabilities. Our connection with the Security Solution, Service & Consulting (SSSC) LLC and Communication, Information Technology School of Mongolian University of Science and Technology contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of connection with SSSC's monitoring system, IPS and Tsubame system and sharing of attack data we able to obtain a broad view of incident and vulnerability trends and characteristics.

During the year 2017 MonCIRT handled several incidents related with Coin mining attacks explode, Mobile malware attack, Weaponized Artificial Intelligence attack, Phishing, and identity theft.

The number of cybersecurity incidents threatening to Mongolian educational institutes

and business organizations is climbing at an alarming rate. Cybercriminals are growing more sophisticated in both the type of attacks they attempt and their ability to carry them out.

Organizations are beginning to understand that a security compromise is not a matter of if, but when. But they need better tools that will enable them to fight back with the same level of sophistication as the cybercriminals who attack them.

2018 was a watershed year for data breaches, with hacks targeting the systems of universities and business companies like National University of Mongolia, National Medical University, Tavanbogd, MAK, Erdenes Tavan Tolgoi, Ochir Undraa e.t.c. MonCirt observed that more than 12000 records were compromised in just those six incidents. With more than 40000 personal data records compromised overall, 2018 became a record-breaking year.

In 2018, the number of data breaches rose 30 percent from 2017, and the number rose 34.5 percent from 2017 to 2018.

Data breaches will continue to escalate, especially now that organized crime groups are turning to cybercrime. Here's a list of some of the biggest internet threats faced Mongolian Internet users in 2018.

Advanced Persistent Threats

Advanced persistent threats (APT) are especially worrisome for IT teams because, like the name implies, these attacks persist, stealthily, for months and even years. They move laterally through the IT infrastructure and steal data while avoiding detection.

Many APT solutions of Mongolian companies and universities are ineffective.

While many security solutions focus on network-level APT attacks, the most prevalent and successful attacks tend to come through applications, such as email and web access."

Weaponized Artificial Intelligence

Cybercriminals are using AI for nefarious purposes. As we observed there was about 20 cases that bad actors tried to use AI in 2018. There have been several attempts that a spear phishing Twitter campaign used AI for automation and to increase success rates. As we see cybercriminals innovate, it won't be long before they adapt machine learning to create ever more effective new threats.

Phishing

Phishing is not a new cybercrime tactic, but despite growing awareness of the problem, organizations are still struggling to stay ahead of the sophisticated social engineering techniques used in phishing attacks. In 2018 the 63 organizations and educational institutes became a victims of phishing attacks like email attachments or links, web-based drive-by or download (multiple responses were permitted).

Scammers are not missing a beat. Often masquerading as trusted companies, they bait users into disclosing sensitive personal information. These techniques are also used to insert malware and bots into corporate networks — therefore we organized 4 trainings in organizations on how to avoid phishing attacks.

We teach IT specialists of companies on new technology that can protect companies - remote browser isolation. It can insulate endpoints from web-borne threats because it executes all the code remotely, in a safe environment, so it never reaches the end user's device or computer.

Mobile Malware

For 2018 about 130 students of universities and colleges, more than 300 employees of companies had faced an attempted mobile malware attack. We expect the number of mobile malware attacks to continue to increase in 2019. Most of that malware comes from third parties, but it has also been found embedded in apps sold through app stores. The number of mobile malware variants is also growing. The lineup includes Trojans, ransomware and keyloggers. Attackers don't always exploit vulnerabilities to infect mobile devices — oftentimes, unsuspecting users give access permission to the malicious apps, like embedded adware, when they install what they think is a legitimate app.

As we see the third-party app stores host most mobile malware.

Ransomware in the Cloud

We haven't seen the end of the evolution of ransomware yet. In 2018 there was 1 case of ransomware attacks at cloud services of iTools.mn.

Cloud providers are an enticing target because they store massive amounts of data and have large numbers of customers. However, because big providers make for tough adversaries, hackers looking for lower-hanging fruit are more likely to attack smaller services.

IoT Botnets

In 2018, we received report that 6 internet connected TV-smart bords of NUM cracked in two minutes.

While organizations are very enthusiastic about adopting IoT technologies, many are not aware of the exposure created by vulnerabilities in the IoT ecosystem. And because they often lack visibility into their own ecosystems, it would be easy for them to lose track of data that flows through their corporate networks and not even realize that they'd been hacked.

Identity theft.

Nearly 320 Mongolians have been affected by identity theft, according to a 2018 online survey organized by us.

Publicly available numbers from Cyber crime department of Mongolian Policy tell a similar story.

Coin mining a big growth area in cybercrime

Types of cyberattacks vary from year to year. Lately, cryptocurrency coin mining is in vogue in Mongolia since 2016.

"Coin mining represented the biggest growth area in cybercrime in Mongolia with detections up 500 percent. Overall coin-mining activity increased by 13,000 percent in 2017 in Mongolia.

Coin mining requires a lot of computing power. In 2018 we observed in 68 companies cryptojacking attempts that Coin miners tried to add computers to their arsenal.

From January through December 2017, the MonCIRT received 368 email messages and more than 300 hotline calls reporting computer security incidents or requesting information. More than 100 of these messages, information was related with real incidents and we provided with recommendations.

2.3 New services

2.3.1 Anti new attacks System

We started to develop "Anti new types of attacks" System (Blockchain attacks, Cloud attacks, IoT attacks, Cross platform attacks, Mobile attacks) together with Communication and Information Technology school of Mongolian University of Science and Technology. We expected that thanks to this system the number of network attacks to educational networks will decrease about 50 percent.

3. Events organized / co-organized

3.1 Training / Education

To create awareness and to enable users to implement best practices, MonCIRT is organizing workshops and training programs on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from MonCIRT staffs.

The MonCIRT offers different training courses. These courses derive from the practical work of the MonCIRT staffs, providing introductory and advanced training for technical staff and the management of network security management, configuration, incident response and are centered around broader Internet security issues and security practices.

Courses offered in 2017 included the following:

- *Coin mining attacks types*
- *Struggle with mobile attacks*
- *Information and Network security risk management.*
- *Fundamentals of Incident Handling and Management*

In addition MonCIRT organized following workshops:

« Workshop on "Deploy Organization's SOC" on May 11, 2018

« Workshop on "Protecting child in Internet environment" on September 21, 2017

3.2 Drills

In 2017 MonCIRT organized local network security drill-VI involving all state universities and 14 private universities, institutes.

Cyber Drill VI was planned and culminated in the conduct of a three days exercise between November 05-07, 2018. It was conducted as a 'no-fault' exercise, with the strategic level objective being to test and evaluate Mongolia's educational sector's incident management arrangements in order to most effectively address an cyber threats.

The exercise was run, as much as possible, with participants playing from their normal operating environments using everyday communications. It was coordinated from a central control cell in Mongolian University of Science and Technology, where events from a consolidated master list were passed on to the players for their responses. The problems or incidents in the exercise were all simulated – no live systems were involved.

Cyber Drill VI became the powerful contribution in communicating of security officers, incident handlers, network administrators of universities and in security information sharing. In addition it was the second successful experience in incident coordination.

3.3 Conferences, Seminars

In order to create awareness and build Network Security skills within the constituency MonCIRT conducted the following conferences, seminars, workshops successfully:

a. MonCIRT was one of the partner in organization of annual conference of National Military University dedicated to "Mongolian national security issues". The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker on this conference.
b. Prof Khaltar T and Mr Khadkhuu A (executive director) invited and participated in seminars, conferences organized both in Mongolia or abroad and made some presentations on behalf of MonCIRT, for example "Information security of business and government agencies" conference in Moscow, Russia, March 20, 2018 organized by CNews, "IT&Security Forum 2018" conference in Kazan, Russia, May 25-26, 2018 and IDC Roadshow, Ulaanbaatar, April 11, 2018.

4. Achievements

4.1 Presentations

MonCIRT's board director participated and presented in Information security conferences in Mongolia and Russia as key speakers. In these conferences they have presented following presentations:

a. Conducted presentation during the IDC Roadshow conference organized by IDC on theme "Information Security trends in Digital Transformation Era".
b. Conducted presentation during the "IT&Security Forum 2018" conference in Kazan on theme "Self financing experience of MonCIRT".

In addition Lectures and presentations have been made by members of MonCIRT in various workshops and seminars conducted in the country.

4.2 Publications

The MonCIRT published 14 advisories and 15 vulnerability notes in 2018 on our facebook page (https://www.facebook.com/MonCIRT/). Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround.

MonCIRT Security Practices

MonCIRT security practices are easy-to-implement guidance for experienced system administrators. The practices are technology-neutral, so they apply to many operating systems and platforms. Practices available in the repository of MonCIRT and include the following:

- *Network security practices*
- *Overview of network security*
- *Computer Network Security Alternatives*
- *Network security measures* e.t.c.

Other Security Information

The MonCIRT captures lessons learned from handling incidents and vulnerability reports and makes them available to users of the Internet through a social pages and web site archive of security information.

4.3 Certification & Membership

No Certification and Memberships obtained in 2018.

5. International and Domestic Collaboration

5.1 MoU

No any Memorandum of Understandings signed in 2018.

5.2 International incident coordination

Upon request of some security teams and departments of companies from Europe, USA we handled incidents related to 8 phishing web sites installed illegally in Mongolian web servers.

6. Future Plans

6.1 Future projects

No future projects planned in 2018.

6.2 Future plan

We plan to reorganize board structure, management staffs and expand our operation, establish new services aimed on Business sector's networks, public networks. Following are the future plans:

- Development and implementation of own Intrusion prevention & alert system

7. Conclusion

For MonCIRTs' constant and developing activity it is necessary financial support. Therefore we signed MOU with MonPass CA LLC and in 2018 MonPass CA LLC financed most of expenses of MonCIRT.

Due to constant financial difficulty MonCIRT gives the basic attention on the new financing strategy, proactive and quality management services including educational program, awareness campaigns, presentations and publications.

Henceforth, MonCIRT shall focus on extending and empowering its constituency area involving more and more companies, creating membership. Thus, MonCIRT will act as an real general private sector oriented CSIRT and in future.

All the events organized by MonCIRT during the year 2018 were very successful. We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "MonSec" while finding new ways to reach an even wider audience.

MonCIRT shall continue to participate in regional events such as the Annual APCERT drill and will join to FIRST.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).
Nisora tower, 207. Tokyo street. Bayanzurkh district. Ulaanbaatar, Mongolia and
Incident Response Help Desk
Phone: +976-70113151
Fax: +976-70113151

MyCERT (CyberSecurity Malaysia)

Malaysian Computer Emergency Response Team – Malaysia

1. HIGHLIGHTS OF 2018

1.1 Summary of major activities

23-24 February 2018	Participated in the APCERT Steering Committee Meeting, Kathmandu, Nepal.
7 March 2018	Participated in the APCERT Drill 2018.
24-29 Jun 2018	Local Host for 30th Annual FIRST Conference Kuala Lumpur.
18-27 September 2018	Conducted a capacity building training under the Malaysian Technical Cooperation Program (**MTCP**) attended by selected APCERT members titled "Certified Incident Management and Active Defence Training".
18 September 2018	Conducted the OIC-CERT Cyber Drill 2018 with the participation from the APCERT members with theme "Crypto-currencies Risk and Emerging Threats".
24-28 September 2018	Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (**CSM-ACE**) 2018.
27 September 2018	Organised the National ICT Security Discourse (**NICTSeD**), Kuala Lumpur.
21-24 October 2018	Participated in the APCERT Annual General Meeting (**AGM**) & Annual Conference 2018, Shanghai, China.
26-29 November 2018	Conducted the OIC-CERT Annual Conference 2018 with the theme "Cyber Threats to the Public: Social Network and Mobile Apps" in Shiraz, Iran.

2. ABOUT CYBERSECURITY MALAYSIA

2.1 Introduction

CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Communications and Multimedia Malaysia (**MCMM**) with a vision of being a globally recognised National Cyber Security and Specialist Centre by the year 2020. CyberSecurity Malaysia provides specialised cyber security services which are among them:

i. Cyber Security Emergency Services:
   - Security Incident Handling; and
   - Digital Forensic.

ii. Security Quality Management Services:
   - Security Assurance; and
   - Information Security Certification Body.

iii. Cyber Security Professional Development and Outreach:
   - Info Security Professional Development; and
   - Outreach.

iv. Cyber Security Strategic Engagement and Research:
   - Government and International Engagement; and
   - Strategic Research.

v. Industry and Research Development.

2.2 Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (**MyCERT**) on 13 January 1997 under the Ministry of Science, Technology and Innovation. In 2018, CyberSecurity Malaysia is transferred to the Ministry of Communications and Multimedia Malaysia (**MCMM**). CyberSecurity Malaysia is committed in providing a broad range of cyber security innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace.

2.3 Cyber Security Incident Management

CyberSecurity Malaysia managed security incidents through the Malaysia Computer Emergency Response Team (**MyCERT**), which is a department within CyberSecurity Malaysia. The agency is a leading point of reference for the Malaysian Internet community when faced with cyber security incidents. MyCERT facilitates the mitigation of cyber threats against Malaysia's Internet users particularly on cyber intrusion, identity theft, malware infection, and cyber harassment among others.

MyCERT operates the Cyber999 Help Centre and the Malware Research Centre that provide technical support for incident handling and malware advisories and research respectively. More information about MyCERT can be viewed at: *https://www.mycert.org.my/en/*.

2.3.1 Cyber999 Help Centre

MyCERT operates the Cyber999 Help Centre providing an avenue for Internet users and organisations to report or escalate cyber security incidents that threatens their personal or organisational security, safety or privacy. Channels for reporting cyber abuses and grievances to MyCERT's Cyber999 help centre are available at MyCERT's website at:

https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/443/index.html

MyCERT's Cyber999 help centre, has responded to approximately 10,699 incidents, with about 92% incident resolution in 2018. Majority of the incidents reported to in 2018 were related to intrusion, malware and online fraud.

2.3.2 Malware Research Centre

Another valuable service from MyCERT is the malware research with the establishment of the Malware Research Centre (**MRC**). The centre has been in operation since December 2009 and functions as a research network for analysing malware and cyber security threats. The centre conducts research and development work for mitigating malware threats, producing advisories, monitoring threats and collaborating with other malware research bodies.

2.3.3 Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cyber security incidents within Malaysia that are reported either by the Malaysian public or international organisations will be resolved by assisting the complainants with technical matters. If an incident involves international cooperation, CyberSecurity Malaysia will request trusted parties in that country or constituency, of which the origin of the case, to assist in resolving the security issues.

3. ACTIVITIES & OPERATIONS

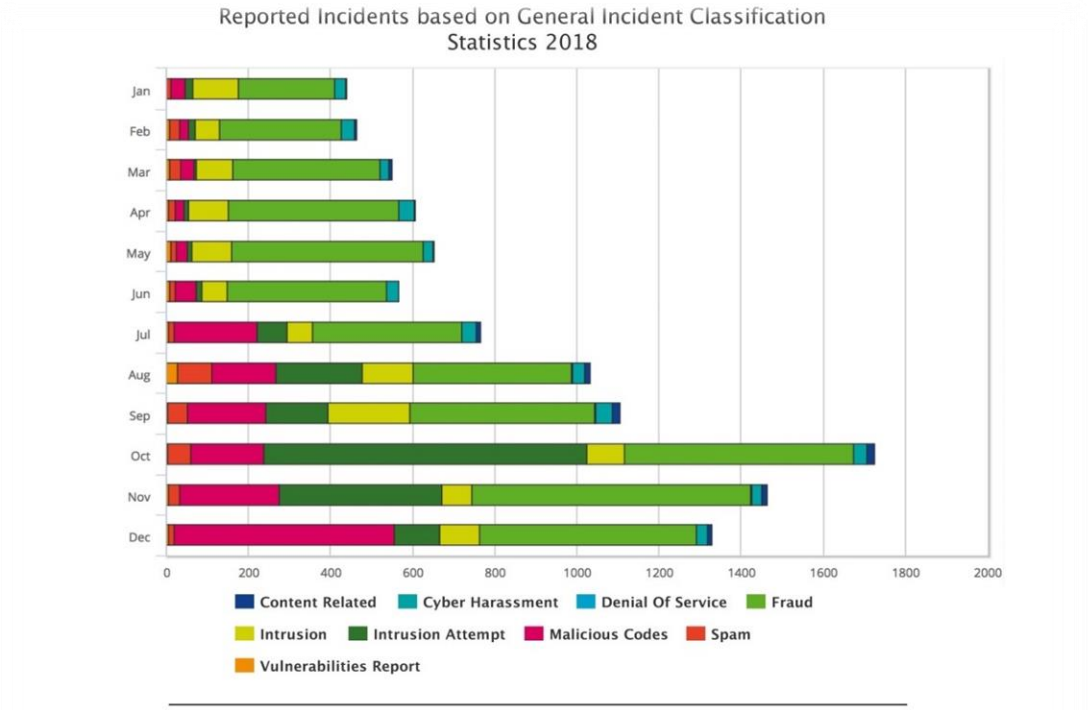
3.1 Incident Handling Reports and Abuse Statistics

CyberSecurity Malaysia receives reports from various parties within its constituency as well as from other constituencies. These include home users, private sectors, government sectors, security teams from abroad (foreign CERTs), Special Interest Groups, as well as through the internal proactive monitoring by CyberSecurity Malaysia's staff.

CyberSecurity Malaysia through MyCERT in 2018 had proactively produced 11 advisories and 8 alerts to inform its constituency on issues relating to cyber security. The specific list of the advisories, alerts and summary reports can be viewed at: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/index.html

There was a decreased in intrusion incident in 2018 as compared to 2017. Most of the incidents reported were related to fraud. This was followed by intrusion.

The following chart shows the reported incidents managed by CyberSecurity Malaysia for 2018:



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	6	8	2	3	2	12	14	17	19	14	12	111
Cyber Harassment	27	31	22	38	24	28	33	30	42	30	25	26	356
Denial of Service	0	0	1	1	1	0	1	1	1	1	2	1	10
Fraud	234	297	357	414	467	389	363	386	451	557	680	528	5123
Intrusion	110	59	89	97	96	63	62	123	199	94	71	97	1160
Intrusion Attempt	19	17	7	11	10	13	73	212	152	786	396	109	1805
Malicious Code	36	22	31	23	29	51	204	156	191	178	243	536	1700
Spam	10	24	28	16	13	12	13	82	47	55	27	15	342
Vulnerabilities Report	1	7	8	5	10	9	5	28	4	4	6	5	92
TOTAL	439	463	551	607	653	567	766	1032	1104	1724	1464	1329	10699

Chart 2: Reported Incidents in 2018

Further information on Cyber999 statistics can be viewed at:
https://www.mycert.org.my/statistics/2018.php

4. EVENTS INVOLVEMENT AND ACHIEVEMENTS

CyberSecurity Malaysia actively participated in cyber security events such as trainings, seminars, conferences and meetings. The agency has contributed its competencies in the following events:

4.1 Cyber Drills

CyberSecurity Malaysia, participated in three (3) cross-national Cyber Drills in 2018 namely the APCERT Drill, the ACID Drill, and the OIC-CERT Drill. The agency was the Executive Controller of the Malaysia National Cyber Drill.

4.2 Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2018. One of the topics is "Incident Handling & Network Security".

4.3 Presentations

CyberSecurity Malaysia's representatives had been invited to give presentations and talks at international conferences and seminars. Among the participations include the APCERT Malware Mitigation Working Group held during the 2018 APCERT AGM & Conference in Shanghai, China, FIRST TF CSIRT in Kuala Lumpur, Malaysia, Annual FIRST Conference in Kuala Lumpur, RSA Conference in San Francisco, USA and FIRST TC in Amsterdam.

4.4 Research Papers

CyberSecurity Malaysia actively contributed research papers to journals and conference proceedings. Amongst others, the list of papers is provided below:

i. *Cyber Threat Intelligence: Issues and Challenges.* Published in Institute of Advanced Engineering and Science
ii. *Cyber Parenting Module Development for Parents*. Published in International Academy of Technology, Education and Development
iii. Classification of Malware Analytics Techniques: A Systematic Literature Review. Published in Science and Engineering Research Support Society [SERSC]

iv. Content Based Fraudulent Website Detection Using Supervised Machine Learning Techniques. Published in Springer

v. Bridging the Gap Between Organisational Practices and Cybersecurity Compliance: Can Corporate Promote Compliance in Organisation? Published in International Journal of Business and Society

vi. Simulating Command Injection Attacks on IEC 60870-5-104 Protocol in SCADA System. Published in Science Publishing Corporation

vii. Cyber Force Establishment: Defence Strategy for Protecting Malaysia's Critical National Information Infrastructure Against Cyber Threats. Published in Academic Conferences and Publishing International Limited

viii. A Study on Security Vulnerabilities Assessment and Quantification in SCADA Systems. Published in Medwell Publishing

ix. Denial of Service: (DoS) Impact on Sensors. Published in IEEE Xplore

x. A Management Framework for Developing a Malware Eradication and Remediation System to Mitigate Cyberattacks. Published in Springer

xi. Towards Stemming Error Reduction for Malay Texts. Published in Springer

xii. Developing Digital Parenting Program Using Blended Learning Approach. Published in American Scientific Publishers

xiii. Malware Forensic Analytics Framework Using Big Data Platform. Published in Springer

xiv. Measuring Sensor to Cloud Energy Consumption. Published in ACM

xv. Modelling Malware Prediction Using Artificial Neural Network. Published in IOS Press

xvi. Possible Conditions of FTE and FTA in Fingerprint Recognition System and Countermeasures. Published in IEEE Xplore

xvii. High Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution. Published in MDPI

xviii. Video Spam Comment Features Selection Using Machine Learning Techniques. Published in IEEE Xplore

xix. Comparison on Scorecard and Dashboard in Smart Water Monitoring Application. Published in ACM Digital Library

xx. State of the Art Intrusion Detection System for Cloud Computing. Published in Pakistan

xxi. Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. Published in OIC-CERT Journal of Cyber Security

xxii. Developing a Competency Framework for Building Cybersecurity Professionals. Published in OIC-CERT Journal of Cyber Security

4.5 Social Media

In 2018, CyberSecurity Malaysia received continuous invitations to speak in events with regards to cyber security at the local radio and television stations. CyberSecurity Malaysia also actively disseminates security concerns through social media such as Facebook and Twitter, which is done through MyCERT. As of now, the MyCERT Facebook Page has about 52,053 likes and the MyCERT Twitter has 3,241 followers.

5. INTERNATIONAL COLLABORATION

Malaysia's National Cyber Security Policy identified international cooperation as one of the areas in enhancing cyber security. In line with this, CyberSecurity Malaysia is active in establishing collaborative relationships with foreign parties.

5.1 Working Visits

CyberSecurity Malaysia conducted working visits to relevant organisations overseas to further enhance the country's cyber security posture. The objective of the visits is to seek potential collaborations in the area of cyber security.

This agency also received working visits from foreign organisations that have similar objectives. Among them are:

i. Romanian National Institute for Research and Development in Informatics (ICI Bucharest), Romania;
ii. National Commission of Cryptology (CNG), Senegal;
iii. Alibaba Security Response Center (ASRC), China;
iv. Cybersecurity Philippines CERT, Philippines (CSP-CERT);
v. Ministry of Interior Cambodia;
vi. Computer Emergency Response Team Ghana (CERT-GH).
vii. Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Centre (ID-SIRTII/CC), Indonesia;
viii. Badan Siber Sandi Negara (BSSN), Indonesia;
ix. Moroccan Computer Emergency Response Team (maCERT), Morocco;
x. Indian Computer Emergency Response Team (CERT-IN), India;
xi. Qatar Computer Emergency Response Team (Q-CERT), Qatar;
xii. Tonga National Computer Emergency Response Team (CERT.to), Tonga; and

xiii. Daimler AG, Jerman.

5.2 Memorandum of Understanding (MoU)

CyberSecurity Malaysia in 2018 has signed MoUs with the following organisations in matters pertaining to cyber security:

i. Cyber Security Philippines Computer Emergency Response Team ORG. INC, Philippines;
ii. National Center for Cyber Security Technology, Taiwan; and
iii. ALIBABA Security Response Center, China.

5.3 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia are:

i. The Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), CyberSecurity Malaysia is facilitating cooperation and interaction among the member countries;
ii. The Deputy Chair of the APCERT; and
iii. The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action.

6. FUTURE PLANS

CyberSecurity Malaysia strives to improve service capabilities and encourage local Internet users to report cyber security incidents to the Cyber999 help centre. The development of new and better reporting channels and further promotion of services through the mass media are aspects that will proactively be intensified.

To achieve world-class capabilities, CyberSecurity Malaysia will relentlessly encourage its employees to obtain certifications in cyber security. In addition, the personnel are encouraged to attend trainings, give presentations and write publications at international security platforms. This will assist them to improve their contribution in knowledge and experience sharing in the cyber security field. The personnel are also encouraged to develop in-house tools used in mitigating security threats to assist the public and industry to secure and utilise their assets when performing online activities.

To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with the local and international security organisations through the establishment of formal relationship arrangements such as the MoUs and agreements.
This agency will continue to organise national events such as the Cyber Security Malaysia – Awards, Conference and Exhibition (**CSM-ACE**), which is an annual event providing awareness, training and awards to information security professionals, and the National ICT Security Discourse to boost the cyber security awareness among the youth. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, will spearhead the collaboration and organise international events such as the OIC-CERT Annual Conferences.
With such understanding, CyberSecurity Malaysia supports newly established local and international Computer Security Incident Response Team (**CSIRT**) by providing advice and assistance especially in becoming members to international security community such as the APCERT, FIRST and OIC-CERT.

7. CONCLUSION

CyberSecurity Malaysia observes a reduction in cyber incidents that were reported to the Cyber999 Help Centre in 2018 compared to the previous year. This agency will continuously work with international allies to generate useful cooperation in safe guarding the cyber environment.
In line with the Malaysia's National Cyber Security Policy that emphasised on capacity and capability building, mitigation of cyber threats and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cyber security processes, human capability and technology. CyberSecurity Malaysia will also continue its commitment to seek for new edges in cyber security and to be a catalyst in developing the industry.
International cooperation and collaboration are important facet in mitigating other cyber security issues. As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. CyberSecurity Malaysia will continue to establish and support cross border collaboration either through bilateral or multilateral platforms such as the APCERT and the OIC-CERT. CyberSecurity Malaysia will continuously pursue new cooperation with cyber security agencies regionally and globally in the effort to make cyber space a safer place for all.

SingCERT

Singapore Computer Emergency Response Team- Singapore

1. Highlights of 2018

Singapore Computer Emergency Response Team (SingCERT), Singapore's national CERT, is part of the Cyber Security Agency of Singapore (CSA). SingCERT serves as a trusted point of contact for cyber incident reporting for the members of the public, private businesses and international CERTs around the world.

In 2018, SingCERT received 5,863 incident reports from its constituency and foreign partners, which is a 22.6% increase from the 4,782 incidents reported in 2017. Over the years, the number of alerts and advisories released by SingCERT has also increased, with 68 being released in 2018 compared to 38 in 2017 (i.e. 79% increase).

Against the backdrop of the rising trend in cyber incidents, CSA launched three initiatives aiming at promoting cybersecurity awareness and fostering a cybersecurity community in 2018:

i. *2nd Edition of Singapore Cyber Landscape*
Highlights facts and figures on significant cyber threats and incidents in Singapore for 2017.

ii. *Cybersecurity Awareness Campaign – "Cyber Tips 4 You"*
Focuses on promoting four cybersecurity tips and information to enable internet users to better safeguard their digital assets.

iii. *Cybersecurity Awareness Campaign – "Be Safe Online"*
Focuses on helping businesses better protect themselves against the increasing frequency and sophistication of cyber attacks.

2. About SingCERT

2.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is Singapore's national CERT, serving as a trusted point of contact for cyber incident reporting to the

members of the public, private businesses and international CERTs around the world. It was set up to facilitate the detection, resolution and prevention of cyber security related incidents on the internet. Besides providing technical assistance and identifying trends in hacking activities, SingCERT also works closely with other security agencies and Internet Service Providers (ISPs) to resolve cybersecurity incidents.

SingCERT's Contact Information:

- Website: https://www.csa.gov.sg/singcert
- Email: singcert@csa.gov.sg

2.2 Establishment

SingCERT was first set up in October 1997 by the Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015.

CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology and industry development for Singapore's critical information infrastructure. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.

2.3 Resources

SingCERT publishes specific threat alerts and advisories that affects its constituency on the SingCERT website (https://www.csa.gov.sg/singcert). These are broadcasted through the SingCERT subscribers mailing list, and CSA's Facebook and Twitter platforms.

CSA also maintains a website - GoSafeOnline (https://www.csa.gov.sg/gosafeonline) - to provide cybersecurity trends and tips for individuals and businesses.

2.4 Constituency

SingCERT primarily serves the local constituency comprising members of the public and private businesses in Singapore.

3. Activities & Operations

3.1 Scope and definitions

SingCERT provides technical assistance and facilitates communications in response to cybersecurity related incidents affecting our constituency, and collaborates with foreign

CERT partners in handling cross border cyber threats.

SingCERT also monitors and evaluates global cyber threats and vulnerabilities, and publishes alerts and technical advisories with recommended prevention and mitigation measures.

3.2 Incident handling reports

SingCERT receives incident reports via email and phone, and will assess and follow up with the respective agency or service provider to coordinate and carry out further remediation.

In 2018, SingCERT received 5,863 incident reports from its constituency and foreign partners, a 22.6% increase from 2017 (i.e. 4,782 incidents reported in 2017).

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
Number of Incident Reports	1,222	2,871	651	1,119	**5,863**

Figure 1: Number of Incidents Reported to SingCERT (2018)

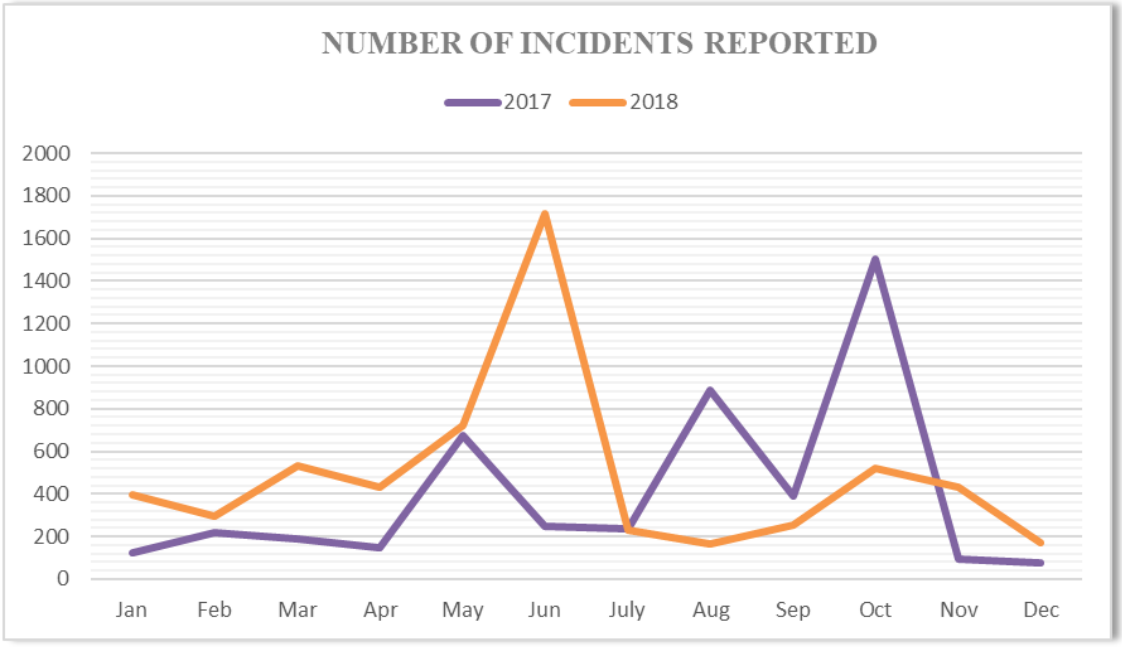


Figure 2: Comparing the Number of Incidents Reported to SingCERT (2017 to 2018)

3.3 Abuse statistics

SingCERT receives numerous incident reports on different forms of cyber attacks. Some of the common cyber threats observed in Singapore are website defacements, phishing websites and ransomware. In 2018, there were 3800 reported phishing incidents, a 7.9% increase from the previous year.

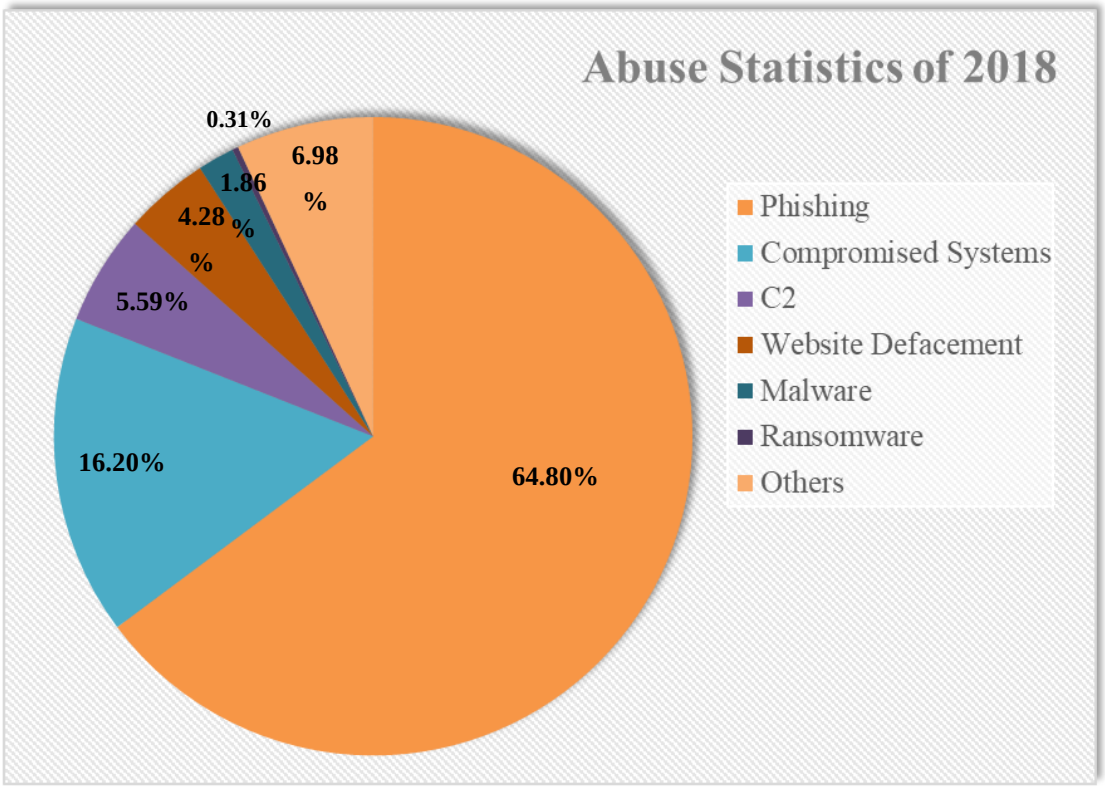


Figure 3: Abuse Statistics (2018)

3.4 Publications

3.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories on widespread, emerging cyber threats with recommended mitigation measures and solutions to raise security awareness about the current cyber landscape.

The following chart shows the increase in alerts and advisories issued by SingCERT in 2018 as compared to 2017.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2017	0	2	1	1	3	5	2	2	3	4	8	7	38
2018	8	3	2	9	4	5	6	2	8	8	5	3	63

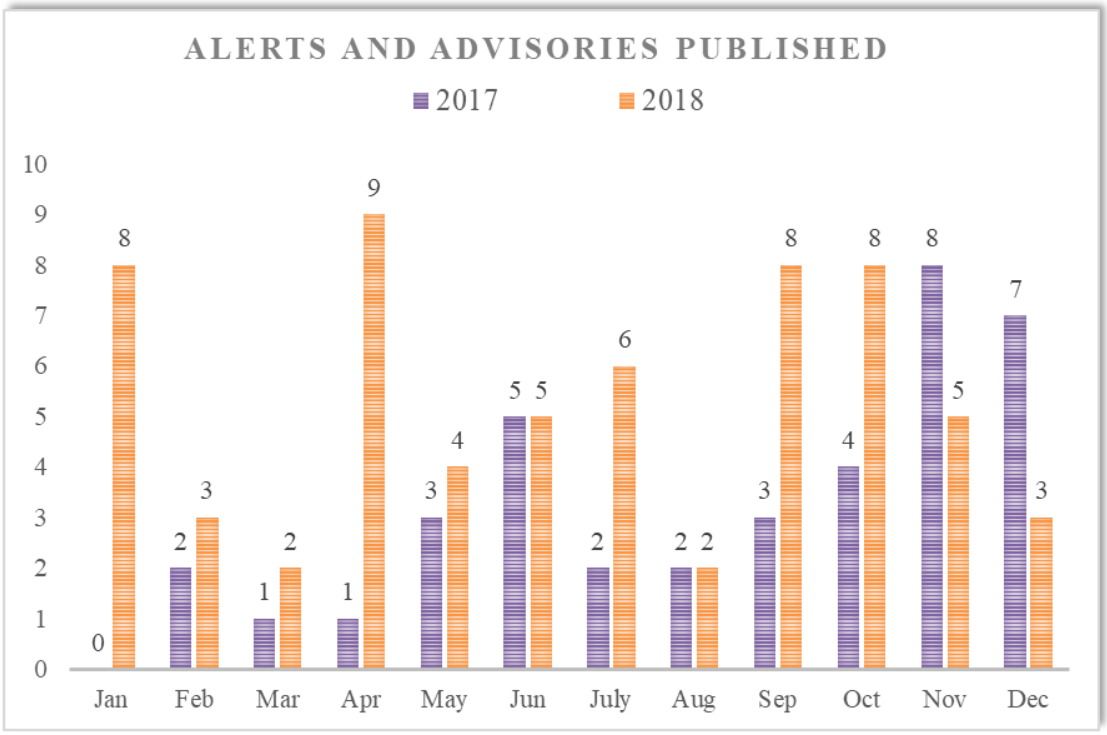


Figure 4: Comparing the Number of Alerts and Advisories Published (2017 to 2018)

In 2018, 63 alerts and advisories were published on SingCERT's website (https://www.csa.gov.sg/singcert/news/advisories-alerts/) in the following chronological order:

Date	Title
04 Jan	Alert on Security Flaws Found in Central Processing Units (CPUs)
08 Jan	Alert on Digital Currency Mining Malware
09 Jan	Advisory on Critical Zero Vulnerabilities Within Dell EMC Data Protection Suite
09 Jan	Alert on Western Digital NAS Drive Vulnerabilities
12 Jan	Advisory on Important Microsoft vulnerabilities affecting Office, .NET Framework and ASP.NET

13 Jan	Alert on Intel Active Management Technology (AMT) Issue
26 Jan	Technical Advisory on Electron Framework Critical Protocol Handler Vulnerability
31 Jan	Alert on WordPress Websites Infected with Browser
01 Feb	Alert on Cisco Adaptive Security Appliance (ASA) Critical Vulnerability (CVE-2018-0101)
02 Feb	Advisory on Critical Security Bug in Oracle's MICROS POS System
02 Feb	Alert on Firefox Browser Critical Vulnerability (CVE-2018-5124)
13 Mar	Technical Alert on the Distributed Denial of Service (DDoS) Amplification Attacks Using Memcached
22 Mar	Alert on security flaws in Advanced Micro Devices (AMD) processors
03 Apr	Alert on Drupal Critical Vulnerability (CVE-2018-7600)
06 Apr	Alert on Debian Beep Package Local Privilege Escalation Vulnerability (CVE-2018-0942)
06 Apr	Alert on Microsoft Malware Protection Engine Critical Vulnerability (CVE-2018-0986)
08 Apr	Alert on Cyber Attacks Leveraging Cisco Vulnerabilities (CVE-2018-0171)
09 Apr	Advisory on Distrust of Symantec
13 Apr	Alert on Microsoft Information Disclosure Vulnerability (CVE-2018-0950)
13 Apr	Advisory on Critical Microsoft Graphics Component Vulnerabilities
20 Apr	Alert on Vulnerability in Oracle WebLogic Server (CVE-2018-2628)
20 Apr	Technical Advisory for Network Administrators to Guard Against Recent Network Malicious Activities
10 May	Alert on Critical Microsoft Vulnerabilities (CVE-2018-8174 and CVE-2018-8120)
15 May	Alert on NagiosXI Security Vulnerabilities (CVE-2018-8733 through CVE-2018-8736)
18 May	Alert on Critical Cisco Vulnerabilities (CVE-2018-0222, CVE-2018-0268 and CVE-2018-0271)
18 May	Alert on Red Hat DHCP Client Critical Vulnerability (CVE-2018-1111)
07 Jun	Alert on "VPNFilter" Malware Infecting Networking Devices Worldwide
08 Jun	Alert on Zip Slip Vulnerability for Archive Files

4 Jun	Alert on Critical Microsoft Vulnerabilities (CVE-2018-8267, CVE-2018-8225 and CVE-2018-8231)
19 Jun	Alert on "SigSpoof" Email Encryption and Digital Signature Vulnerability (CVE-2018-12020)
19 Jun	Alert on Misconfigured Geth Ethereum Client
12 Jul	Alert on WordPress 4.9.7 Security Release
13 Jul	Alert on Cisco Security Updates (CVE-2018-0369 and CVE-2018-0341)
20 Jul	Protecting Your Personal Data
20 Jul	Technical Advisory on Measures For Protecting Customers' Personal Data
26 Jul	Alert on Intel Management Engine Vulnerabilities (CVE-2018-3627, CVE-2018-3628, CVE-2018-3629 and CVE-2018-3632)
27 Jul	Alert on Vulnerability in Oracle WebLogic Server (CVE-2018-2893)
16 Aug	Alert on Vulnerability in Oracle Database Server (CVE-2018-3110)
24 Aug	Alert on Critical Apache Struts 2 Remote Code Execution vulnerability (CVE-2018-11776)
03 Sep	Alert on Privilege Escalation Vulnerability in ANTlabs Internet Gateway Products
13 Sep	Alert on Critical Microsoft Vulnerabilities (CVE-2018-8440, CVE-2018-8475, CVE-2018-0965, CVE-2018-8439 and CVE-2018-8449)
24 Sep	Alert on Cisco Video Surveillance Manager Default Password Vulnerability (CVE-2018-15427)
24 Sep	Alert on Critical Out-Of-Band Adobe Acrobat Vulnerability (CVE-2018-12848)
24 Sep	Alert on Microsoft JET Database Engine Vulnerabilities (CVE-2018-8392 and CVE-2018-8393)
28 Sep	Alert on 14 High-Severity Vulnerabilities in Cisco Products
28 Sep	Technical Advisory on DNSSEC Root Zone Key Signing Key Rollover
29 Sep	For Facebook Users: Alert on Facebook Security Breach
03 Oct	Alert on 47 Critical Vulnerabilities in Adobe Acrobat and Adobe Reader
11 Oct	Alert on 12 Critical Microsoft Vulnerabilities for October 2018 Patch Tuesday
13 Oct	Updated Advisory on Ransomware
16 Oct	Alert on Multiple Vulnerabilities in PHP

16 Oct	Alert on PHP 5.6 and 7.0 End-of-Life
18 Oct	Alert on Linksys E Series Routers Vulnerabilities (CVE-2018-3953, CVE-2018-3954, and CVE-2018-3955)
18 Oct	Alert on Multiple Security Vulnerabilities in Oracle's Enterprise Products
24 Oct	Alert on Drupal Critical Vulnerabilities
05 Nov	Technical Advisory on Vulnerabilities in Bluetooth Low Energy Chips by Texas Instruments (CVE-2018-16986 and CVE-2018-7080)
08 Nov	Alert on Critical Apache Struts 2 Remote Code Execution Vulnerability (CVE-2016-1000031)
08 Nov	Alert on Nginx Vulnerabilities (CVE-2018-16843, CVE-2018-16844, and CVE-2018-16845)
10 Nov	Festive Shopping Advisory for Shoppers and Online Merchants
22 Nov	Alert on Adobe Flash Player Vulnerability (CVE-2018-15981)
05 Dec	Alert on EternalSilence, a New Variant of EternalBlue and EternalRed Abusing UPnP Services on Routers
13 Dec	Alert on Windows DNS Server Vulnerability (CVE-2018-8626)
21 Dec	Alert on Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-8653)

3.4.2 Singapore Cyber Landscape

The 2nd edition of the Singapore Cyber Landscape publication was released on 19 June 2018, highlighting facts and figures on significant cyber threats and incidents in Singapore for 2017.

The publication provides an overview of the frequency and scope of cyber attacks in Singapore, raising awareness of cyber threats among stakeholders, including the general public and businesses so that they can take appropriate actions to defend against such threats.

More information about the report, including a downloadable copy, is available via https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2017.

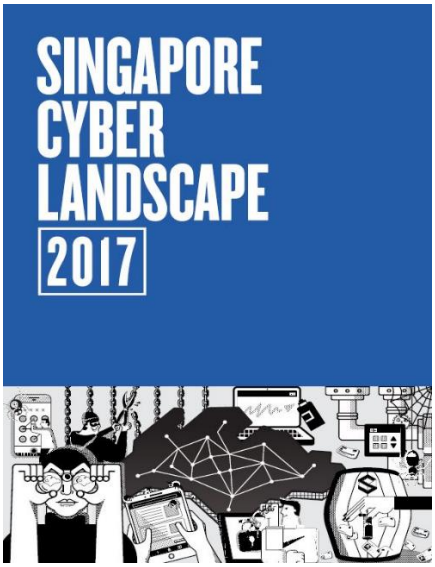


Figure 5: Singapore Cyber Landscape 2017

3.4.3 National Cybersecurity Awareness Campaign

CSA launched two cybersecurity awareness campaigns to educate individuals and businesses on the how and what they can do to protect themselves online and against cyber attacks.

Cybersecurity Awareness Campaign – "Cyber Tips 4 You"

This campaign was launched on 3 May 2018 and focuses on promoting four cybersecurity tips and information for internet users to better safeguard their digital assets. The four cybersecurity tips are namely to (i) use an anti-virus software, (ii) use strong passwords and enable Two-Factor Authentication (2FA), (iii) spot signs of phishing and (iv) update their software as soon as possible. More information about the campaign, including a downloadable copy, in four languages, is accessible via https://www.csa.gov.sg/gosafeonline/resources/cyber-tips-4-you-flyer.

Cybersecurity Awareness Campaign – "Be Safe Online"

This campaign was launched on 16 May 2018 and focuses on helping businesses better protect themselves against the increasing frequency and sophistication of cyber attacks by enhancing their cyber defence capabilities and digital risk management. More information about the campaign, including a downloadable copy, in four languages, is accessible via https://www.csa.gov.sg/news/publications/be-safe-online

4. Events organised & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2018

The ASEAN CERT Incident Drill (ACID) is an annual drill that Singapore has been hosting since 2006, to strengthen cybersecurity preparedness and cooperation within the region.

On 5 September 2018, SingCERT successfully conducted the 13th iteration of ACID. More than 100 participants from 10 ASEAN Member States (AMS) and 5 Key Dialogue Partners participated in the drill. The participants were put through a series of scenario injects that are designed based on prevalent cybersecurity threats. The theme "*System Vulnerabilities and Cryptocurrency Mining*" was chosen given the increasing prevalence of online payment systems which have created highly-valued cryptocurrencies such as Bitcoins, Monero, Ethereum and Ripple. Cryptocurrency mining actors have been actively targeting vulnerable systems such as Content Management System and web-servers running on outdated software to add to their cryptocurrency mining resources.

4.1.2 Government Bug Bounty Programme

Singapore's Government Bug Bounty Programme (GBBP) is part of an ongoing initiative to build a secure and resilient Smart Nation. The first GBBP took place from 27 December 2018 to 16 January 2019 and welcomed 400 ethical hackers globally to look for security weaknesses in the Government systems.

This programme was organised in partnership with HackerOne – the world's largest community of cybersecurity researchers and white hat hackers. By bringing together a community of cyber defenders who share the common goal of developing a safe and resilient cyberspace, the GBBP aims to build a shared sense of collective ownership over the cybersecurity of Government systems and websites, which is vital to achieve Singapore's Smart Nation goals.

4.2 Conferences and seminars

4.2.1 Singapore International Cyber Week 2018

Singapore International Cyber Week (SICW) is Singapore's most established annual cybersecurity event, providing a platform for cybersecurity experts from around the world to discuss, network, strategise and form partnerships in the cyberspace. More details about the event can be found at https://www.sicw.sg.

CSA organised the 3rd SICW from 18-20 September 2018 on the theme "Forging a Trusted and Open Cyberspace". It reflects the importance of trust and openness in cyberspace, given the fast-evolving and complex cybersecurity landscape. SICW hosted more than 7,000 cybersecurity experts from the region and beyond, as well as 250 exhibitors, sponsors, and speakers.

4.2.2 Cybersecurity Awareness Alliance

CSA drives awareness efforts through the Cybersecurity Awareness Alliance, a collaboration between public and private sector organizations as well as trade associations, to raise awareness and adoption of cybersecurity measures. Alliance members actively give talks to schools, businesses and the community at various platforms.

5. International Collaboration

5.1 Training

SingCERT participated and benefitted from the following APCERT training topics that were arranged by TWNCERT:

Date	Title	Presented by
03 Apr	Analysis of a Compromised Linux Server	APNIC
05 Jun	Performing Forensics on an Azure Virtual Machine	Microsoft
07 Aug	Shaoye Botnet – Android Malware & DNS Hijacking	TWNCERT
04 Dec	Inside the APCERT Drill: Player, Observers, EXCON and OC	AusCERT

5.2 Drills & exercises

5.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2018

The Asia Pacific Computer Response Team (APCERT) Cyber Security Drill tests the response capabilities of leading Computer Security Incident Response Team (CSIRT) within the regions.

The annual APCERT Cyber Security Drill was held on 7 March 2018 with the theme "Data breach via malware on IoT", to test the response capabilities of member teams in responding to real incidents and issues that exist on the internet. As a member of the

APCERT Drill Working Group, SingCERT participated in the planning and creation of the drill, and was also part of the ExCON team conducting the drill.

5.2.2 ASEAN-Japan Cyber Exercise

The ASEAN-Japan Cyber Exercise seeks to validate and improve information sharing mechanism, with the aim of enhancing the partnership among policymakers of ASEAN Member States (AMS) and Japan. It consists of two types of exercises, the first being the Cyber Exercise, and the other being a Table Top Exercise.

In 2018, Singapore co-chaired the ASEAN-Japan Information Security Policy Meeting. CSA was involved as a member of the ASEAN-Japan Cyber Exercise Working Group. The working group not only focuses on conducting the exercise but also in business-as-usual and crisis coordination. SingCERT participated in the cyber exercise held on 18 May 2018 with two objectives:

- To enhance capability and readiness of national coordination for cyber incident
- To establish secure communication method assuming actual information sharing

5.3 Conferences, Seminars & Presentations

5.3.1 APCERT Annual General Meeting (AGM) and Conference 2018

SingCERT attended the APCERT Annual General Meeting (AGM) and Conference held in Shanghai, China, from 21-24 October 2018. This is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies.

During the APCERT AGM, SingCERT presented the plan to host the event alongside SICW 2019, and was selected to host the event in 2019.

5.3.2 Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an organisation and recognised global leader in incident response. FIRST brings together a wide variety of security and incident response teams including product security teams from the government, commercial, and academic sectors. In addition, FIRST Technical Colloquia & Symposia provide a platform for FIRST members and invited guest to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams. More details about the organisation can be found at https://www.first.org.

As a member of FIRST, SingCERT attended the FIRST Conference and Technical Meeting for National CSIRTS held in Kuala Lumpur, Malaysia from 24-30 June 2018 and the Technical Colloquium in Osaka, Japan from 14-16 March 2018.

6. Future Plans

For 2019, planning and discussions are in progress for the following:

S/n	Description	Category
1	Singapore Cyber Landscape	Publications
2	4th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	APCERT Annual General Meeting and Conference	Events Organising & Hosting
4	14th iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT | CC

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

1. ABOUT SRI LANKA CERT | CC

1.1 INTRODUCTION

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT | CC) is the national centre for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and respond to cyber security threats and vulnerabilities.

1.2 ESTABLISHMENT

As the national CERT of Sri Lanka, Sri Lanka CERT | CC acts as the central hub for cyber security of the nation. It is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks.

Sri Lanka CERT was established on 1st of July 2006 as a subsidiary of Information and Communication Technology Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka.

Sri Lanka CERT is directly under the Ministry of Digital Infrastructure and Information Technology since August 2018.

1.3 WORKFORCE

The Sri Lanka CERT | CC has a total staff strength of fourteen (14) team members consisting of a Chief Executive Officer, Director Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Information Security Engineers, Associate Information Security Engineers, Information Security Analysts, Associate Information Security Analysts, Head of Human Resources and Administration and a driver/office assistant. This team is supported by six (06) undergraduate interns.

All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), Cisco

CCNA and CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)2.

1.4 CONSTITUENCY

Sri Lanka CERT's constituency encompasses the entire cyber community of Sri Lanka (private and public-sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government. Based on the availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

2. ACTIVITIES & OPERATIONS

2.1 INCIDENT HANDLING SUMMARY

Sri Lanka CERT|CC being the national contact point for all cyber security related matters, receives numerous incident reports/complaints relating to the country's national cyber-space from both domestic and international partners.

The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems operated by international organizations.

This report presents an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the year of 2018. Based on the said date, following observations can be made;

i. Financial frauds targeting local importers and exporters have seen an increase over the past several years. Financial frauds on local importers and exporters have increased more than 300% when compared to 2017.
ii. There has been an increase in the spread of ransomware and malicious software during the year of 2018, where sensitive data belonging to both individuals as well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.
iii. A significant number of phishing attacks targeting financial sector

organizations were recorded in 2018.

iv. Majority of the reported incidents fall in to the category of social media related incidents. Among the social media incidents, Facebook related incidents were the highest.

In addition, Sri Lanka CERT was able to conduct digital forensics investigations for the following types of investigations during the year 2018.

i. Credit card frauds
ii. Image enhancements for identifying objects on videos and images
iii. Mobile phone investigations
iv. Recovery of deleted information
v. Email frauds

Cyber-security related incidents reported to Sri Lanka CERT have decreased in the year 2018 compared to previous years. In 2018, a total of 2598 incidents were reported to Sri Lanka CERT while it was 3907 during the year 2017. This may be due to several reporting options for the people to report such incidents.

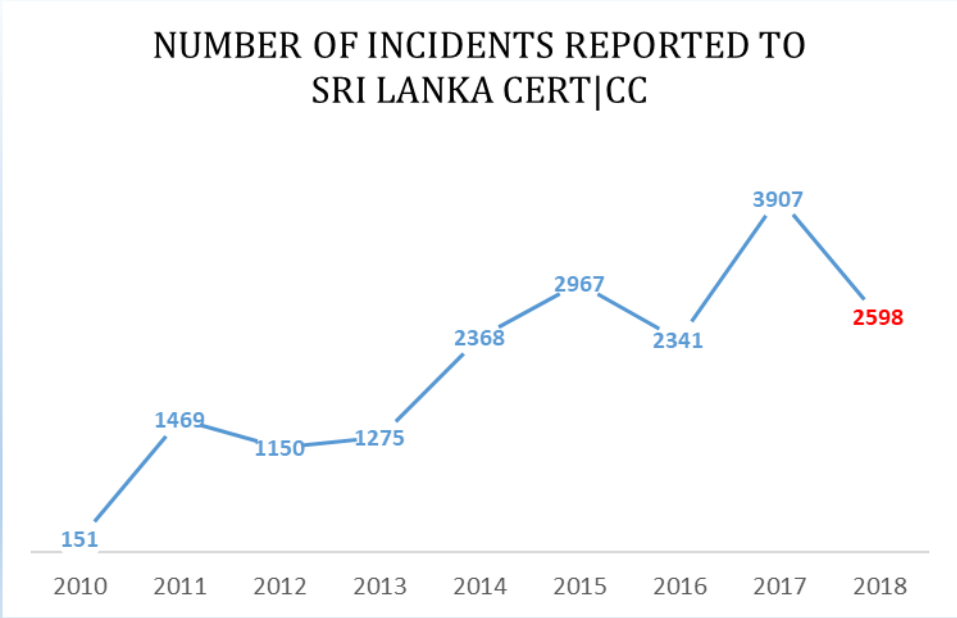


Figure 1. Growth of the number of incidents reported

Type of Incident	Number of Incidents
Phishing	12
Abuse/Hate/Privacy Violation	11
Ransomware	08
Scams	07
Malicious Software issues	11
Financial Frauds	21
Web site Compromise	09
Hate/ Threat emails	07
Intellectual Property violation	06
Unauthorized Access	-
DoS/DDoS	01
Social Media related incidents	2505
Total	2598

Table 1. Types of incidents

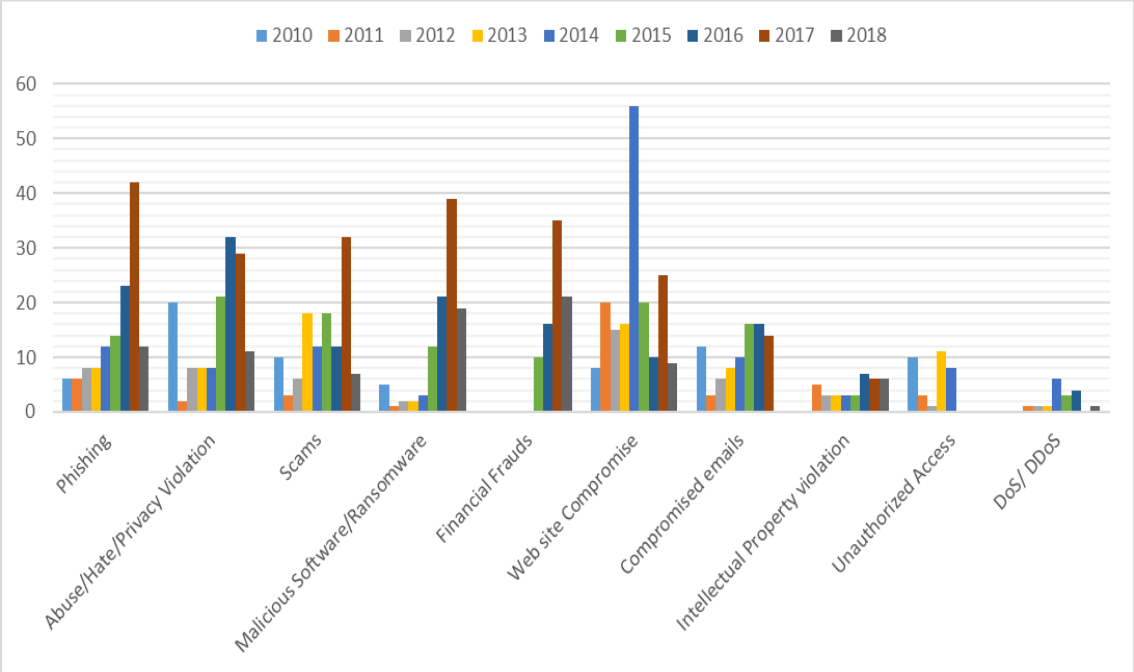


Figure 2. Growth of the types of cyber security incidents

2.2 CONSULTANCY SERVICES

Sri Lanka CERT|CC continues to provide consultancy services to government and non-government agencies

Typical consultancy services provided during the period include;

- Security assessments for more than 140 government ministries/departments/statutory boards web sites.
- Security assessments for several public sector systems
- Security assessments for several private organizations.
- Consultancy for a government bank for conducting Security Assessments for their systems
- Consultancy for a government bank for procurement of SOC solution
- Consultancy for a government bank for procurement of ATP solution
- Forensics investigation for suspected data deletion for a private company
- Security assessment for LGC2
- Security assessments for few nationally important applications developed through ICTA
- Security assessments for few nationally important applications developed through the line ministry

2.3 TRAINING / EDUCATION SERVICES

Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences. This includes Chief Innovation Officers (CIOs), System Administrators, Banking and Telecom Sector Staff, Law enforcement authority staff, Tri-forces, Students, Engineers and the General Public.

1. Awareness Program and Training Sessions

i. Two Information Security Policy Development Sessions at SLIDA
ii. Two Government CIO - IS Policy Development workshop
iii. Cyber Security, IT Security & Licensing Guidelines Breakfast Session for Government CIOs
iv. Training on Information Security delivered for law enforcement officers
v. Train the trainer program for Court Management Assistants
vi. Bar Association ICT course-session on cyber security
vii. SLAS class 1 officer program on Cyber Security

viii. Cyber security awareness program for Colombo District school principals
ix. Awareness session for parents of the SOS children village
x. Open Source Investigation training for law enforcement
xi. Internet Safety Session for 100 School Principals at Viharamahadevi Balika Kiribathgoda
xii. Awareness session on Internet threats and mitigations at Lyceum International School AL teachers
xiii. Training for executive staff of MAS holdings
xiv. Awareness Session on Cyber Crime & Social Media
xv. EDUCSIRT Training Program
xvi. Diploma - Gender Based Socialization, session on cyber security
xvii. ICC Sri Lanka Event - on cyber security
xviii. CEB engineer's awareness session on SCADA security
xix. Cyber Security Training for SLAS officers
xx. INSSL presentation on Fake news and mitigation
xxi. Training for parents of grade 8-10 students
xxii. Digital Forensic Workshop for law enforcement
xxiii. Two awareness sessions for government officers on the importance of website security. Approximately 150 senior and middle level management staff were participated.
xxiv. PGIM Lecture Series
xxv. Family Health Bureau, session on cyber security
xxvi. Social Media and Internet related complaints handling training for law enforcement
xxvii. Cyber Security training for Immigration Officers
xxviii. Launch Ceremony of MSC program of Informatics
xxix. Infotel Exhibition
xxx. The Signal Corps Exhibition
xxxi. NCPA police officer training
xxxii. Army Signal Corps 75th Anniversary
xxxiii. Basic Internet and Open source investigations for law enforcement officers
xxxiv. Email security and document protection for PSD
xxxv. Mobile Phone related Cybersecurity Awareness- Awadahanaya Program
xxxvi. National Police Academy training course on cyber security
xxxvii. BCIS Seminar session on transnational crimes

xxxviii.Online security session for school children

2. Awareness through Electronic/Print Media

i. News paper articles
(Lankadeepa, Dinamina, Sudnaytimes, Ada newspaper, Daily mirror, Rivira, Island paper, ada irida paper etc)

ii. Monthly updates for media (voice)
(Sirasa, Ceylontoday, LakFM vioce, SLBC, Rivira, HiruFM, , Swarnawahini, ShriFM, VFM etc)

iii. Live TV programs
Doramadalawa – ITN program-10pm to 12p
Rupavahini – Chakrawata – 10pm-12pm program
SiyathaTV 15min x 2 programs
BASL organized TV program on Rupavahini 10-11 am

iv. Liver Radio programs
RanONE FM 45 min live program
Shadda Radio 1 hr program

v. Entire year update for media (voice)
(LakFM, Siyatha, Sirasa, VFM, RidamFM, Derana Radio,SithaFM etc)

3. Annual Cyber Security Week 2018

Since 2008, Sri Lanka CERT|CC has been conducting an annual security awareness programme titled Cyber Security Week (CSW). This international event attracted the attention of the local as well as regional information security professionals. Cyber Security Week 2018 was held in the months of October and November 2018, and featured a series of events including the following;

- Hacking Challenge, 10th October 2018 at Lavender Room, BMICH
  Hacking Challenge is a contest for IT Professionals to attack or defend an actual network within a given timeframe. The participants were Technical Security Professionals, Network Administrators, System Administrators and students following information security post-graduate courses.

- Cyber Security Quiz: 17th October 2018 at Lavender Room, BMICH
  This competition is open only to students of Sri Lankan Universities and other

tertiary education institutions. The objective of the quiz is to assess the knowledge and to identify and reward the aspiring young information security professionals.

- 11th Annual National Cyber Security Conference - Wednesday 7th November 2018 at Hilton Colombo,
  - This year's theme was "National Importance of Cyber Security"
  - More than 350 participants
  - Published the "National Information and Cyber Security Strategy"
  - Chief guest was Hon. Attorney General of Sri Lanka

- Workshops – Monday 5th, Tuesday 6th and Thursday 8th November 2018 at DLC, SLIDA
  - Android Mobile Application Security (Hands On)-by Sri Lanka CERT|CC
  - Network Forensics Analysis using Wireshark (by Thailand Bank Association Resource person)
  - Incident response and Internet security (by ICANN)

- Supporting events
  - Workshop on Cybersecurity Risk by Palo Alto Networks-8th November 2018
  - Knowledge Sharing Workshop on the Latest Cybersecurity Incidents and their Impact by CERT- Estonia (13th November 2018)
  - Lanka Network Operators Group" Workshop, Tutorials & Conference (01 & 02 November 2018)

2.4 PUBLICATIONS

Website

The Sri Lanka CERT|CC website publishes security related awareness bulletins for the public through News Alerts, Glossaries, Case Studies, Statistics and FAQs.

E-mails

Sri Lanka CERT|CC disseminates security related information through e-mails to its subscribers.

Newsletters

Sri Lanka CERT|CC continues to publish and circulate The Cyber Guardian

e-newsletter to a large number of students, through the SchoolNet- the network connecting secondary schools in Sri Lanka.

Newspapers/media

Sri Lanka CERT|CC continues to educate the general public through the electronic and print media about emerging cyber security threats and vulnerabilities with recommendations on how to safeguard themselves against these attacks.

2.5 OPERATIONAL SUPPORT PROJECTS

It was able to conduct a project to acquire cyber security investigation/assessment resources and enhance the capabilities of staff during the year 2018. This project was funded by government of Sri Lanka.

2.6 SPECIAL PROJECTS

Project Name	Description and Activities
○ Government Website Audit	○ Vulnerability assessments for 120 government websites
○ National Certification Authority (In progress)	○ Procurement of two data centre locations for production and backup sites were completed ○ Procurement of auditor is ongoing ○ Implementation and testing is ongoing
○ National Security Operations Center (In progress)	○ This project was transferred to CERT from ICTA ○ Procurements are in progress.

3. NEW SERVICES

3.1 CYBER SECURITY MANGED SERVICES

Sri Lanka CERT was delivering cyber security managed services for three government organizations and one private sector organization during the year of 2018.

4. ACHIEVEMENTS

4.1 NATIONAL CYBER SECURITY STRATEGY

The government of Sri Lanka, committed to keep the nation safe, secure and prosperous, by introducing Sri Lanka's first Information and Cyber Security Strategy which will be implemented over period of five years from 2019 to 2023. Sri Lanka CERT developed the National Information and Cyber Security Strategy of Sri Lanka with the support of

stakeholders and obtained the cabinet approval for the strategy on 16th October 2018.

Our strategy aims to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digital technology, and facilitate growth, prosperity and a better future for all Sri Lankans.

Our strategy is underpinned by six pillars, (1) establishment of a governance framework to implement national information and cyber security strategy, (2) enactment and formulation of legislation, policies, and standards to create a regulatory environment to protect individuals and organizations in the cyber space, (3) development of a skilled and competent workforce to detect, defend and respond to cyberattacks, (4) collaboration with public authorities to ensure that the digital government systems implemented and operated by the them have the appropriate level of cyber security and resilience, (5) raising awareness and empowering citizens to defend themselves against cybercrimes, and (6) development of public-private, local-international partnerships to create a robust cyber-security ecosystem.

Sri Lanka CERT is in the process of the implementation of the National Information and Cyber Security Strategy.

4.2 RESEARCH AND POLICY DEVELOPMENT

Sri Lanka CERT strengthened its research arm by recruiting a research team. The team conducted several surveys, such as, Youth's Survey on Social Media Awareness and Public Service Managers Information and Cyber Security Readiness Survey.

It has planned to conduct several research and policy development activities aligned with the national information and cyber security strategy.

4.3 CERTIFICATION & MEMBERSHIP

Sri Lanka CERT continues to maintain memberships with following professional organizations;

i. (ISC)2 Colombo Sri Lanka Chapter the local representative organization of International Information Systems Security Certification Consortium.
ii. Membership for Threat Intelligence from ShadowServer.
iii. Membership of FIRST
iv. Membership of APCERT
v. Membership of CAMP, Korea

4.4 TRAINING FOR STAFF

Sri Lanka CERT was able to provide following training and conference participation for its staff

i. Network Security and Penetration Testing Training (Malaysia)
ii. Mobile hacking and security (Malaysia)
iii. SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling (Singapore)
iv. Workshop on International Law (Germany)
v. Underground Economy Conference (France)
vi. KISA training (Korea)
vii. CyFy Conference 2018 (India)
viii. CEH training (Sri Lanka)
ix. RedHat RHCSA training (Sri Lanka)
x. RedHat RHCE training (Sri Lanka)

5. INTERNATIONAL COLLABORATION

5.1 EVENT PARTICIPATION

i. Cybercrime cooperation exercise (Moldova)
ii. KISA Conference (Serbia)
iii. UNCCPCJ meeting (Austria)
iv. FIRST AGM and Conference (Malaysia)
v. COE - TC-Y meeting and Octopus conference (France)
vi. CAMP Annual General Meeting (Korea)
vii. APCERT AGM and Conference (China)
viii. BIMSTEC meeting (India)

5.2 OTHER ACTIVITIES

- Reporting of malicious IP address details received from International counterparts to local ISPs. The International counterparts consists of CERT Bund - Germany, Microsoft, Shadow Server and APCERT Data Exchanger.
- Continuing with network monitoring project "Tsubame" with JPCERT | CC

5.3 INTERNATIONAL INCIDENT COORDINATION

- APCERT Cyber Security Drill
  - Worked as a member of the organizing committee of APCERT Cyber Security Drill 2018
  - Participated for the drill
- Engagements with CERTs in the Asia Pacific region. Sri Lanka CERT has regular operational engagements with CERTs/Information security organizations in other regions of the world and commercial establishments and solution providers (such as Facebook, Google, Yahoo) to resolve phishing and identity theft incidents.

6. FUTURE PLANS

6.1 FUTURE PROJECTS

- Implementation of National Information and Cyber Security Strategy (in progress).
- Development and Implementation of a Security Operations Centre (in progress).
- Establishment of the National Certification Authority through an Act of Parliament (in progress).
- Establishment of sector based CSIRT's (e.g. Telco-CERT).
- Cyber Security Week 2019.
- Cyber Security project with European Union (Cyber4Dev) to implement the provisions of the National Information and Cyber Security Strategy.

6.2 FUTURE OPERATIONS

This section details the changes anticipated in Sri Lanka CERT with regard to staff, equipment and capabilities:

- Sri Lanka CERT shall recruit undergraduate students on internships basis to enhance the information security capabilities of the younger generation.
- Sri Lanka CERT shall continue to operate as a skilled small group of professionals.
- Sri Lanka CERT shall continue to invest on developing the capacity of the staff.

7. CONCLUSION

During the period, Sri Lanka CERT has observed that cyber criminals are targeting small and medium businesses for conducting financial frauds. Most of them were happened through compromising the email accounts.

Sri Lanka CERT was able to carry out a large number of information and cyber security training and awareness sessions during the year 2018, and the demand for such programs are increasing. All the events organized by Sri Lanka CERT during the period were very successful, well attended and were high in demand. Sri Lanka CERT will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security as we have planned.

Sri Lanka CERT is in the process of implementing the National Information and Cyber Security Strategy of Sri Lanka with the involvement of relevant stakeholders. To implement some of the proposed activities of the strategy, Sri Lanka CERT|CC has partnered with NI-CO (Northern Ireland Cooperation Overseas) of European Union to conduct a program called Cyber Resilience for Development (Cyber4Dev) which is jointly funded by the Foreign and Commonwealth Office of UK, Dutch Ministry of Foreign Affairs, and Estonian Information System Authority.

It is expected to operationalize few national level information security related projects during the year 2019 to support the implementation of the National Information and Cyber Security Strategy.

In addition to securing Sri Lanka's cyberspace, Sri Lanka CERT is committed to building a secure information environment in the Asia Pacific region/world with the help of all the CERTs and information security organizations through APCERT/FIRST.

TechCERT

TechCERT – Sri Lanka

1. About TechCERT

1.1 Introduction

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps general public and Sri Lankan organizations keep their computer systems and networks secure.

TechCERT originated as a pioneering project of the LK Domain Registry and its academic partner to provide a safety net for organizations – large and small – against cyber-attacks and emergency situations. TechCERT has collaborative partnerships with several national and global information security organizations that provide latest data on computer and network security threats and vulnerabilities. Issuing security advisories for the public, conducting security and cyber-crime related workshops and public awareness programs on safe use of computers and the Internet, and providing engineering consultancy services are also in its repertoire of services.

1.2 Establishment

TechCERT was originally formed in 2006 and has its origins as a pioneering project of the LK Domain Registry and its academic partners, as a way of providing a safety net for large and small organizations against cyber-attacks and emergency situations. In order to improve the operations and to further develop TechCERT, it was incorporated as an independent not-for-profit organization, affiliated with LK Domain Registry, on 05th September 2016 (Company registration no. GA 3238).

1.3 Resources

TechCERT currently has a technical team of over 20 qualified and experienced professionals. The details of the academic/professional qualifications held by all members of the technical team are given below (most of the team members have multiple qualifications in different areas of information security, computer systems security, network security etc.):

Name	Designation	Qualifications
Prof. Gihan Dias	Chairman	PhD, MSc, BSc Eng (Hons), MIE (SL), Ceng
Dr. Shantha Fernando	Director/ Co-Founder	PhD (TU Deift), Mphil (Moratuwa), MCS (SL), BSc.Eng.Hons (Moratuwa), MIET (UK), MIE (SL), CEng
Mr Dumindra Ratnayaka	Director	BSc.Eng.Hons(Moratuwa)
Dileepa Lathsara	Chief Executive Officer	MSc. BSc Eng (Hons), MIE (SL), CEng, CISSP, C|EH, CPISI (PCI DSS), Certified ISMS Auditor
Kushan Sharma	Engineering Manager	MBA (Colombo), MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, AMIE (SL), MCS (SL)
Kasun Chathuranga	Lead Security Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), RHCE, RHCSA, AMIE(SL), MIEEE
Nalinda Herath	Lead Security Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, CPISI, ITIL, CCNA (Security), AMIE(SL)
Kalana Guniyangoda	Lead Security Engineer	MSc. (Moratuwa), BSc. IT (Hons), GCFA, C|HFI
Sashika Suren	Lead Security Engineer	MSc in Info Sec (UCSC), BICT (UCSC), RHCE, RHCSA, MCTS, GDip in Bus Mgmt
Geethika Wijerathne	Manager Projects & Administration	MSc in Information System Management (Colombo), PMP
Mishra De Silva	Senior Account Manager	MBA (Colombo), BBA (U.S.A), AS (U.S.A), MSLIM
Viraj Madhawa	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya), C|EH
Chathuranga Gunatillake	Information Security Engineer	BEng (Hons) Computer Networks & Security, MBCS, E|NSA, C|EH, CPISI (PCI DSS)
Rajith Jayasekara	Information Security Engineer	MBA (Moratuwa), Bsc. Information and Communication Technology
Vidusha Rathnayake	Information Security Engineer	BSc (Hons)in IT Computer Systems & Networking, RHCSA, C|EH
Anuruddha Hewawasam	Information Security Engineer	BSc. in Computer Science (UCSC), SSCP, CPISI, MIEEE, ACS(SL)
Vishvajith Ihalagama	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)
Priyankara Bandara	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya), C|EH
Asanka Dhananjaya	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)
Dushan Chathuranga	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)

Dilusha Bandara	Information Security Engineer	BSc Information and Communication Technology, CCNA, C|HFI
Ayodya Balasuriya	Information Security Analyst	BSc. Information Systems (UCSC)
Kushantha Rajaratne	Information Security Engineer	BEng (Hons) Computer Networks and Security, OSCP
Yenuka Shachintha	Associate Information Security Engineer	BSc. Information Systems (UCSC), C|EH
Chalana Madusanka	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)
Thusitha Kumarage	Information Security Analyst	BSc (Hons) in IT Cyber Security
Darshana Kithulgoda	Information Security Analyst	Bachelor of Information Technology (UCSC)
Hirushan Thilanka	Associate Information Security Analyst	BSc. Information Systems (UCSC)

1.4 Constituency

TechCERT's constituency comprises its member organizations, private sector organizations, selected governmental organizations and the general public of Sri Lanka. In accordance with the mandate of TechCERT, it provides effective incident response to malicious cyber threats, widespread security vulnerabilities identify and respond to cyber security incidents, conduct training and awareness to encourage best practices in information security and disseminate cyber threat information among Sri Lankan organizations and the general public.

2. Activities & Operations

2.1 Services Provided

TechCERT Managed Security Services include a range of engineering and consultancy services listed below:

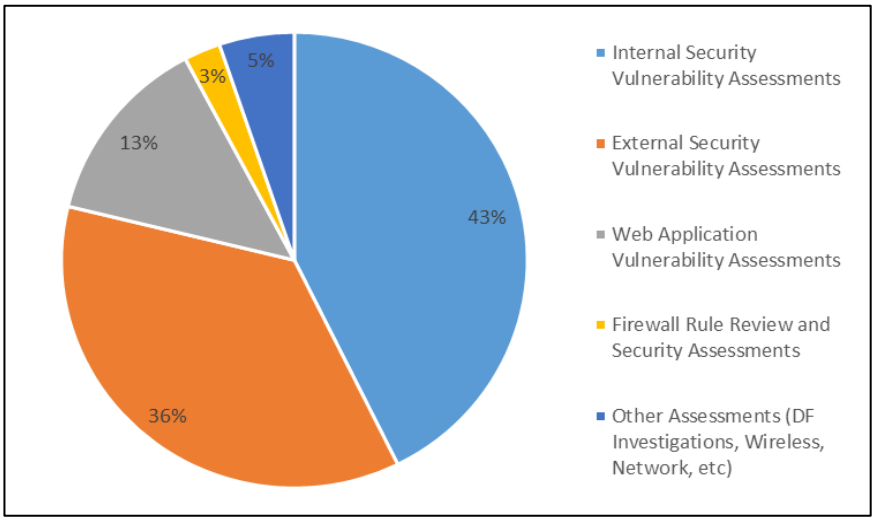
- Network Surveying and Vulnerability Assessments
- Penetration Tests
- Web Application Security Vulnerability Assessments
- Mobile Application Security Vulnerability Assessments
- Firewall Security Configuration Assessment and Rule Evaluation
- Operational Security Assessments
- Router / Switch Security Configuration Assessment
- Wireless Network Security Assessments

- Cloud Security Assessments
- Network Security Architecture Reviews
- Server Security Configuration Evaluation and Implementation
- Application Security Configuration/Vulnerability Assessments
- PCI Compliance Advisory Services
- Source Code Reviews
- Digital Forensics Investigations
- Vulnerability Research and Verification
- Physical and Environment Security Checks
- Information Security Policy Evaluations
- Preparation of IT Security Policy
- TechCERT - Cyber Security Drills
- Attending to Computer Security Incidents
- TechCERT Security Operations Centre (SOC)

2.2 Security Assessments Conducted

The details of security assessments conducted by TechCERT during the year 2018 are as follows:

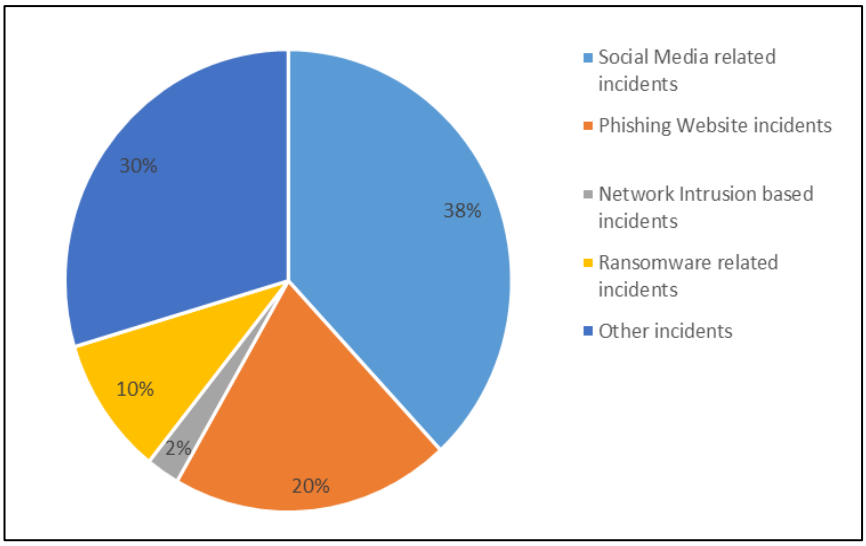
Activity	Count
Internal Security Vulnerability Assessments	2927
External Security Vulnerability Assessments	2477
Web Application Vulnerability Assessments	922
Firewall Rule Review and Security Assessments	174
Other Assessments (DF Investigations, Wireless, Network, etc)	358



2.3 Incident Handling

Throughout the year 2018, TechCERT responded and helped organizations to handle numerous and diverse cyber security incidents and submitted reports pertaining to those incidents. These were reported to us via our hotline, Facebook page, email, clients, Netcraft phishing service, law enforcement units and other security entities.

Activity	Count
Social Media related incidents	126
Phishing Website incidents	6
Network Intrusion based incidents	8
Ransomware related incidents	32
Other incidents	98



3. Alerts and Advisories

TechCERT publishes alerts on various business critical vulnerabilities that are trending at present and relevant solution recommendations through the TechCERT official website https://techcert.lk/en/ throughout the year to spread awareness and knowledge about current security related information among the public.

TechCERT further publishes security facts and best practices on the official Facebook page https://www.facebook.com/techcert.lk/.

4. Events Organized/Hosted

4.1 Organizing Trainings Locally

Over a time frame of several months	Secure Software Development Life Cycle and Best Practices training for Financial Institutes and Telecommunication Companies
8th and 9th of February 2018	Two-day workshop on PCI-DSS v3.2 Implementation (CPISI Certification)
5th of July 2018	TechCERT Annual Workshop on Current Security Trends, Securing the Cloud Environment and Responding To A Cyber Attack.
Over a time frame of several months	Awareness session on email security, password best practices ransomware and physical security for Financial Institutes, Manufacturing and Telecommunication Companies

4.2 Conduct Trainings Internationally

12th of February 2019	Training- "Digital Forensic Analysis with Free and Open Source Tools" training program for APCERT members. Organized by APCERT online training program.

4.3 Cyber Security Drills for Local Organizations

14th of June 2018	TechCERT Cyber Security Drill 2018 – Banking Sector
2nd of August 2018	TechCERT Cyber Security Drill 2018 – Financial Sector
14th of November 2018	TechCERT Cyber Security Drill 2018 – Telecommunication Sector

4.4 APCERT Cyber Security Drill

TechCERT participated in the APCERT Cyber Security Drill as a player. Also TechCERT was in the organizing committee and shouldered the role of EXCON for four teams.

7th of March 2018	Participated in APCERT Cyber Security Drill 2018

4.5 Conferences and Workshops organized by TechCERT

21st of July 2018	Workshop – "CYBER {Smart;}" "RESPONDING TO CYBER ATTACKS" Workshop Conducted for Engineering Students of University of Jaffna, Sri Lanka together with IESL (Information Technology and Communications Engineering Section of Sri Lanka)
20th of December 2018	Seminar – "Blockchain – Future of Trusted Information Systems Awareness Sessions Conducted for Practicing Engineers in Different Fields and Engineering Students of University of Ruhuna, Sri Lanka together with IESL (Information Technology and Communications Engineering Section of Sri Lanka)

5. Future Plans

- In 2018, TechCERT will continue to focus on Information security emergency response work, and strengthen the cooperation with other security organizations to contribute our strength for Internet security.
- Further expanding and developing the technologies in TechCERT Security Operations Centre (SOC).
- Initiate operations in Threat Hunting process of proactively discover malicious behavior to reduce breaches and breach attempts on client networks.
- Enhancing the technologies and technical knowledge of the engineers working on penetration testing and digital forensic investigations operated at TechCERT.
- Implementing Vulnerability Management Systems to integrates and correlates vulnerability scanners to makes vulnerability assessment more convenient and reduce time to remediate, prioritize and document reported risks.

6. Conclusion

TechCERT has been able to consistently improve and expand its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner. As a leader in IT security service provider in Sri Lanka, TechCERT has able to provide security best practices on safe guard of IT infrastructure, mitigate and counter cyber threats successfully by organizing training and awareness programs along with conducting annual TechCERT cyber drills for Sri Lankan Organizations (Financial Organizations, Banks and Telco & ISPs) for the eighth consecutive year in 2018.

Over the last year, there were multiple phishing attacks and ransomware/hacking incidents reported in Sri Lanka in which most of them were able to identified and mitigate before a critical effect on business operations and company assets when compared to previous years. TechCERT was able to successfully respond to most of the incidents reported and assist the relevant authorities to mitigate the threats with minimum effect. TechCERT is confident of its ability and readiness to successfully assist its constituency in computer emergencies by providing pro-active response. In achieving the organizational objectives, the global collaboration and the commitment and dedication of the staff have propelled TechCERT to its present status as a significant player in providing a faster and more efficient service to the clients as well as the public.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. Highlights of 2018

1.1 Summary of key activities

In 2018, ThaiCERT played important role on supporting the National Cybersecurity Preparedness Committee, which is chaired by the Prime Minister to further drive cybersecurity development in Thailand. According to the direction of the Committee, we helped strengthen Critical Information Infrastructure (CII) by identifying 6 CII Sectors: 1) Critical Government Ministries/Agencies 2) Financial Institutions 3) ICT and Telecommunications 4) Transportation and Logistics 5) Energy, Water and Utilities and 6) Healthcare.

Another key achievement was in the area of capacity building. We launched the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), funded by Japan ASEAN Integration Fund (JAIF2.0). The project aims to enhance the capacity of cybersecurity experts and specialists in the ASEAN Member States for protecting government systems and critical information infrastructure. AJCCBC provides 3 training courses, including CYDER (Cyber Defense Exercise with Recurrence), Digital Forensics and Malware Analysis. In 2018, AJCCBC organized 3 trainings for 109 people.

2. About CSIRT

2.1 Overview of ThaiCERT

Founded in 2000, ThaiCERT, a non-profit government funded organization, is the Computer Security Incident Response Team (CSIRT) for Thailand, providing an official point of contact for dealing with computer security incidents in the internet community of Thailand. Apart from coordination and handling the reported incidents, ThaiCERT also provides advisory services to both organizations and individuals, publishes cybersecurity alerts and news, and organizes trainings for the public to enhance knowledge and to raise awareness to people on information security. Currently, ThaiCERT is the operational security unit within the public organization Electronic Transactions Development Agency (ETDA), under the supervision of the Ministry of Digital Economy and Society, Thailand.

2.2 Constituency

The constituents of ThaiCERT are public and private sectors of Internet users in Thailand. ThaiCERT also performs incident coordination with other international entities, where the sources of attacks are originated from Thailand.

3. Activities & Operations

3.1 Incident handling reports

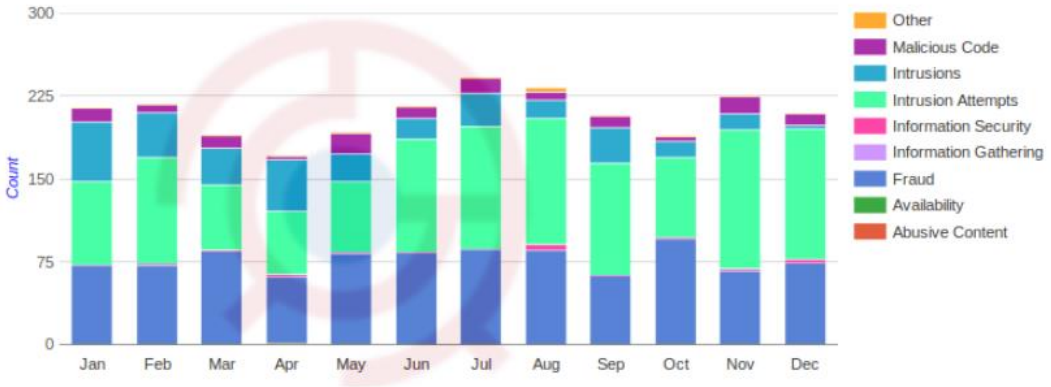


Figure 1: The number of reported incidents in 2018

Via triage, ThaiCERT handled a total of 2,520 reported incident cases (tickets) in 2018, which is a decrease of 22% compared to those of 2017 (3,237 cases). Received reports were approximately 200 cases per month.

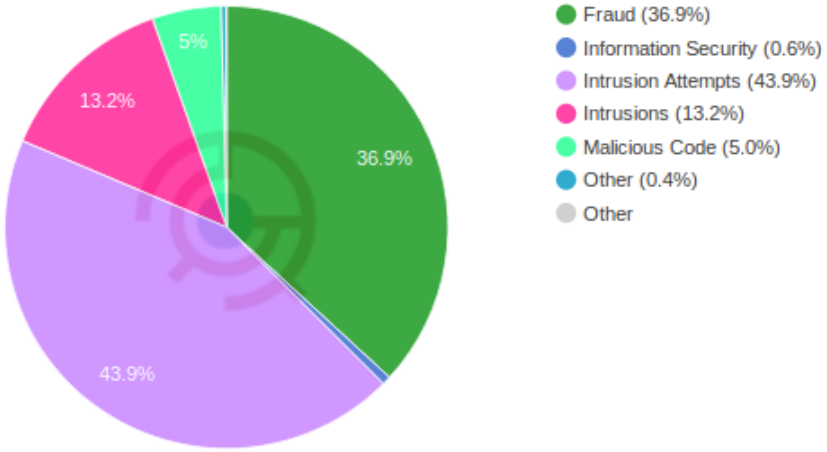


Figure 2: The proportion of reported incidents by incident type in 2018

ThaiCERT classifies incidents using the eCSIRT Incident Classification[1]. In 2018, Intrusion Attempts dominated with 43.9%, followed by fraud at 36.9%, where all fraud cases were phishing, and intrusions at 13.2%. All such information was handled and notified to the relevant parties through e-mail channels.

Figure 3: Top 10 incident reporters in 2018

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents were reported by the ThaiCERT security watch system, comprising 708 cases or 28% of all reports. Fraud, Malicious Code and Intrusions incident reports generally came from automatic feeds. Germany was ranked second (565 cases), followed by the United Kingdom (286 cases).

3.2 Publications

In 2018, ThaiCERT published 5 white papers to provide comprehensive information covering key incidents. ThaiCERT also published a book, CYBER THREATS 2017, to raise awareness. The book can be downloaded from https://www.thaicert.or.th/downloads/downloads.html.

4. Events organized / hosted

4.1 Training

Organized:

- AJCCBC Trainings, Sep Oct and Dec 2018

[1] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

4.2 Drills, exercises

Participated

- APCERT Drill 2018, Mar 2018
- ASEAN CERT Incident Drill (ACID) 2018, Sep 2018
- ASEAN-Japan Cyber Exercise 2018

4.3 Conferences and seminars

Organized:

- Cybersecurity Boot Camp (organized with financial associations and regulators), Oct 2018
- Thailand CTF 2018, Nov 2018
- Cyber SEA Game 2018, Nov 2018

Co-organized:

- Cybersecurity and Machine Learning training, with CMKL University, Nov 2018

Participated as speaker:

- Cyber Intelligence Asia 2018, Singapore, Mar 2018
- Annual FIRST Conference 2018, Kuala Lumpur, Malaysia, Jun 2018
- Critical Infrastructure Protection & Resilience Asia, Kuching, Malaysia, Jul 2018
- Microsoft Seminar “Security is NOW”, Bangkok, Thailand, Oct 2018
- APCERT AGM 2018, Shanghai, China, Oct 2018
- China-ASEAN Network Security Emergency Response Capacity Building Seminar, Shanghai, China, Oct 2018
- FIRST Regional Symposium for Asia-Pacific, Shanghai, China, Oct 2018

5. Future Plans

- Thailand Cybersecurity Week 2019 Event
- Incident Handling Training, with CMKL University
- Secure Coding Training, with CMKL University

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. Highlights of 2018

1.1 Summary of major activities

In 2018, the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) received 31,093 incident reports from 20 countries and collected 185 vulnerabilities separated in 14 categories.

This year TWCERT/CC also provided 5 cybersecurity trainings for industrial associations, enterprises, and schools, joined 2 international cyber drills, 11 domestic and international cybersecurity conferences and seminars, and hosted the 2018 Conference of Taiwan Cyber Security Notification and Response and the 5th Working Meeting of Taiwan CERT/CSIRT Alliance.

As for TWCERT/CC's services, in addition to the Malware Analysis and Report System (MARS) and the Automatic Incident Reporting System available from 2017, since 2018, TWCERT/CC has become a member of the Common Vulnerabilities and Exposures (CVE®) with the root CVE numbering authority (CNA). To facilitate the disclosure of vulnerabilities and further patching and mitigation hence to prevent the exploitation of vulnerabilities, TWCERT/CC has also released its vulnerability disclosure and coordination policy.

1.2 Achievements & milestones

- Become a member of the Common Vulnerabilities and Exposures (CVE®) with the root CVE numbering authority (CNA) and released its vulnerability disclosure and coordination policy.
- Received 31,093 incident reports from 20 countries, and outbound attacks take the major account in 83.41%.
- Collected 185 vulnerabilities separated in 14 categories; code execution, privilege elevation, and data breach are the first three types of vulnerabilities in 2018.

2. About TWCERT/CC

2.1 Introduction

To build up a stronger and more secure cyberspace in Taiwan, the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) responds to major

cybersecurity incidents, analyzes cyber threats, publishes vulnerability information, and exchanges cyber intelligence with trusted partners around the world. In the year 2018, TWCERT/CC has accomplished several provisional goals and missions:

- To assist the handling of the intrusion incidents in the constituency of .tw domain.
- To announce system vulnerability information.
- To provide trainings, lectures, and reference documents about cybersecurity protection and defense technologies and skills.
- To act as the focal point of Taiwan's international cybersecurity cooperation with other CERTs/CSIRTs in the world.

2.2 Constituency

TWCERT/CC provides cybersecurity services to enterprises and individuals in Taiwan, including incident reporting and handling, intelligence collection and publication, consultation, and assistance.

To enhance Taiwan's cybersecurity capacity, TWCERT/CC leads the promotion of cybersecurity incident reporting, provision of cybersecurity educational resources, and cybersecurity outreaches. TWCERT/CC collaborates and integrates resources with cybersecurity organizations, academic institutions, civil communities, governmental institutions, private enterprises, and CERTs/CSIRTs all over the world. To realize the vision "develop a secure Internet environment, towards a high quality Internet society", TWCERT/CC devotes itself to protect and promote Taiwan's cyber security with emphases on safety, convenience, and efficiency, hence to establish the national cybersecurity collaborative defense system, enhance self-protecting capacity in cyber security industry, cultivate high quality cybersecurity human resources, and strengthen the public-private partnership on cybersecurity issues.

3. Activities & Operations

3.1 Incident Report Handling

In order to against hackers' intrusions and the spread of cyber threats, TWCERT/CC receives cybersecurity incident reports from CERTs, public and private sectors, cybersecurity companies, and individual researchers beyond and behind the border.

TWCERT/CC also keeps expanding its intelligence resources and detecting more malicious or hacked domain names and IPs through collaborations with CERTs, government authorities, enterprises, ISPs, cyber security companies, researchers, and so on while playing the coordinating role among those different units to handle

cybersecurity incidents happen in Taiwan.

In 2018, TWCERT/CC received 31,093 incident reports from 20 countries, and the numbers of the reports we received in recent years are shown in Table 1.

Table 1. Incidents reported to TWCERT/CC in recent years

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018
Total	1,094	6,666	8,126	140,250	15,150	24,116	3,461	4,720	31,093

TWCERT/CC consistently seeks its progress on:

- Prevention: to provide advices and early warnings to avoid the occurrence of similar cybersecurity incidents.
- Reporting: to issue an immediate warning at the time a cybersecurity incident is disclosed or occurs.
- Handling: to provide the technical support and consultation needed and to coordinate the actions of a cybersecurity incident's damage control and recovery.

The types of notifications TWCERT/CC received in 2018 are numbered and shown on a pro rata basis as below:

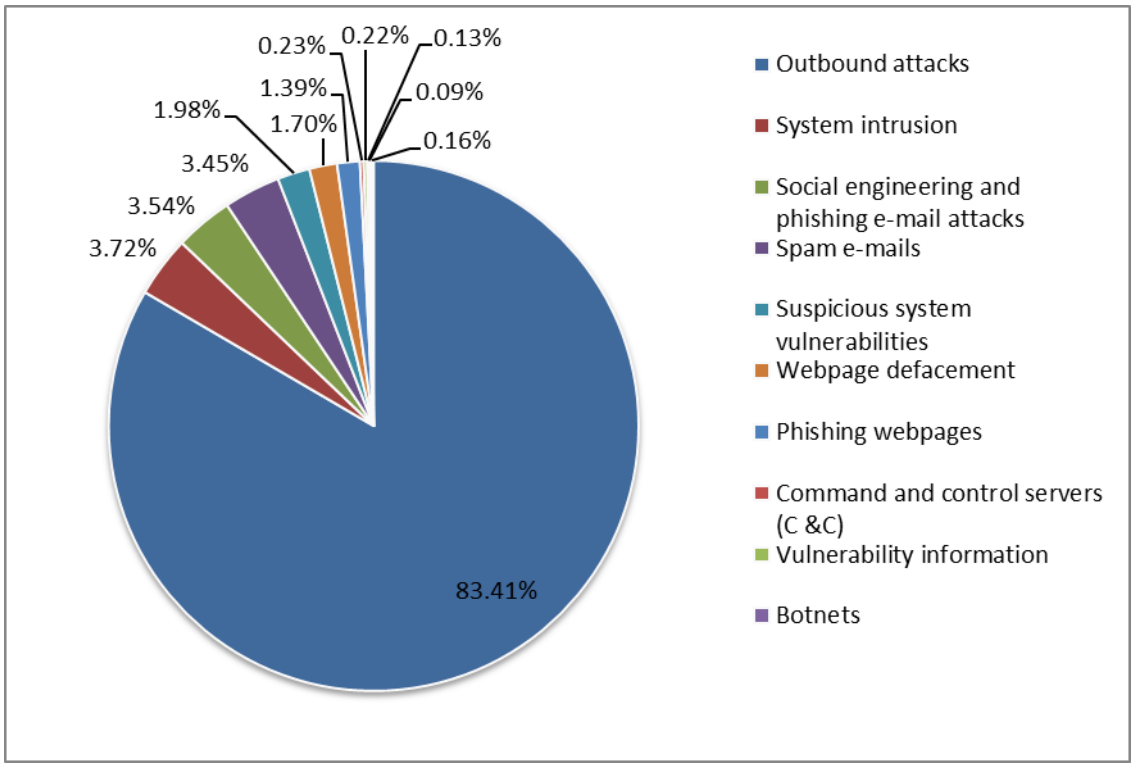


Figure 1. Types of notifications TWCERT/CC received in 2018

3.2 Intelligence Monitoring and Warning

- Vulnerability Announcement

In 2018, TWCERT/CC collected 185 vulnerabilities separated in 14 categories.

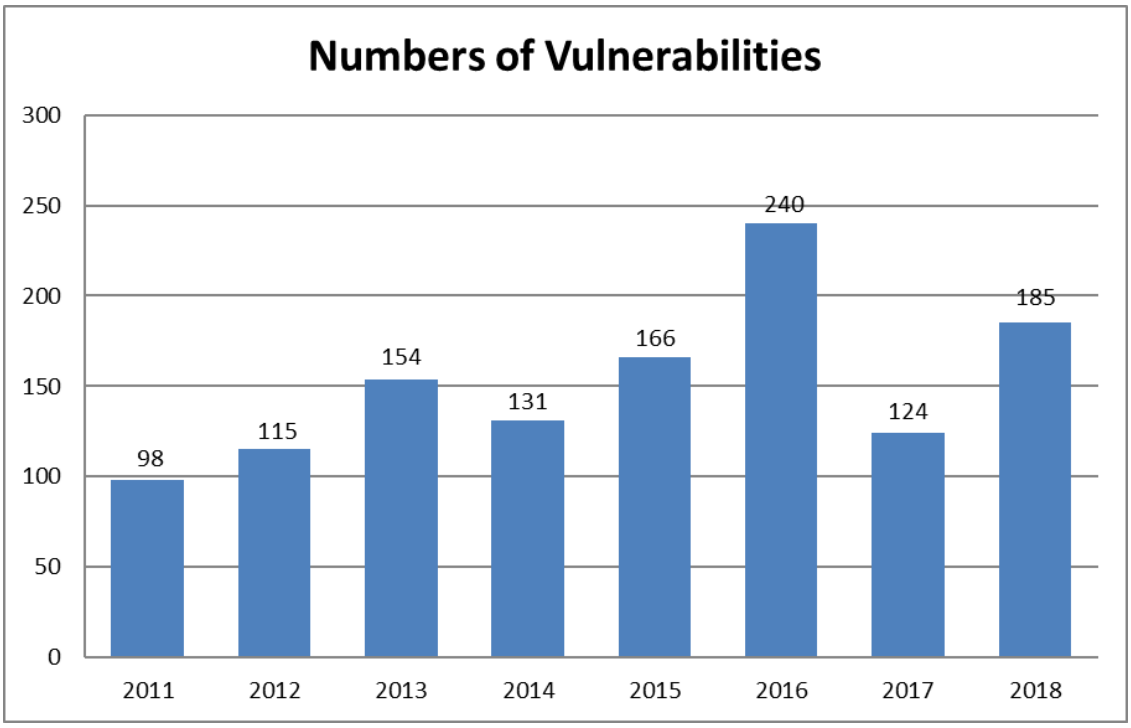


Figure 2. Annual Statistics of Vulnerability by TWCERT/CC

The yearly numbers of vulnerabilities from 2011 to 2018 are shown in Table 2, and the categorized vulnerabilities in the year 2018 is shown in Figure 3.

Table 2. Categorized numbers of the vulnerabilities TWCERT/CC collected in 2018

Category	Number(s)	Category	Number(s)
Http response splitting	1	Memory corruption	14
File inclusion	2	Injection	16
Man in the middle	7	Denial of service	17
Cross-site request forgery	7	Bypass	19
Directory traversal	9	Data breach	20
Cross-site scripting	12	Privilege elevation	24
Overflows	12	Code execution	25

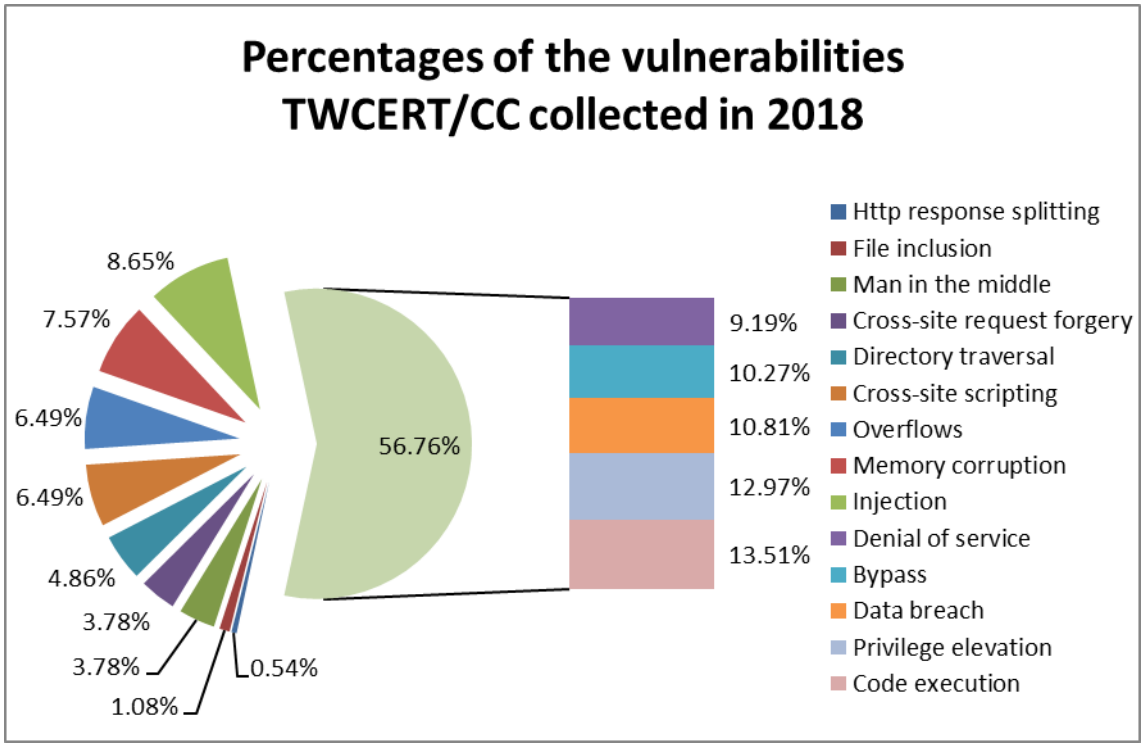


Figure 3. Percentages of the vulnerabilities TWCERT/CC collected in 2018

3.3 Publications

To raise Taiwanese's cybersecurity awareness, every month TWCERT/CC releases an e-newsletter covering important cyber intelligence in the previous month through e-mail as well as TWCERT/CC's official website, Facebook fans page, and blog. The e-newsletter contains TWCERT/CC's recent activities, cybersecurity policies, cyber threats and trends, cyberattacks, vulnerabilities, cybersecurity seminars and events, and the statistics of cybersecurity incident notifications.

3.4 Services

- MARS

In order to prevent data leakage, TWCERT/CC have collaborated with the National Center for High-performance Computing (NCHC) and developed the Malware Analysis and Report System (MARS). Although currently it is only accessible to the public sector, it is preparing to be open to the public.

MARS is developed under the supervision of the Department of Cybersecurity, Executive Yuan. Through the provision of a web-based interface for users to upload files, MARS detects the uploaded files and then generates reports to users of the file detection results to disclose the risks they contain.

- Automatic Incident Reporting System

In October 2017, TWCERT/CC developed the Automatic Incident Reporting System, which is open to the public to facilitate people's reporting of cybersecurity incidents. The System provides web interface and API, and users can choose either of the accesses at their convenience. In addition, the System will send an incident report to the ticking system after receiving an incident report to monitor and manage its conducting process.

- CVE

Since 2018, TWCERT/CC is a member of the Common Vulnerabilities and Exposures (CVE®) with the root CVE numbering authority (CNA).

Operated and maintained by the MITRE Corporation and sponsored by the Office of Cybersecurity and Communications of the United States Department of Homeland Security, currently the CVE is the most frequently used database for publicly known cybersecurity vulnerabilities. Following the CNA rules, TWCERT/CC has designed its vulnerability handling framework as Figure 5 shows to ensure the availability of competent CNAs and access to the vulnerability notification channel when any domestic and international cyber security research institutions, bug bounty programs, CERTs, or computer security incident response teams report vulnerabilities in Taiwanese ICT products.

To facilitate the disclosure of vulnerabilities and further patching and mitigation hence to prevent the exploitation of vulnerabilities, TWCERT/CC has released its vulnerability disclosure and coordination policy and is developing the Taiwan Vulnerability Note (TVN) platform. TWCERT/CC's vulnerability disclosure and coordination policy is available from: http://surl.twcert.org.tw/tCaC6

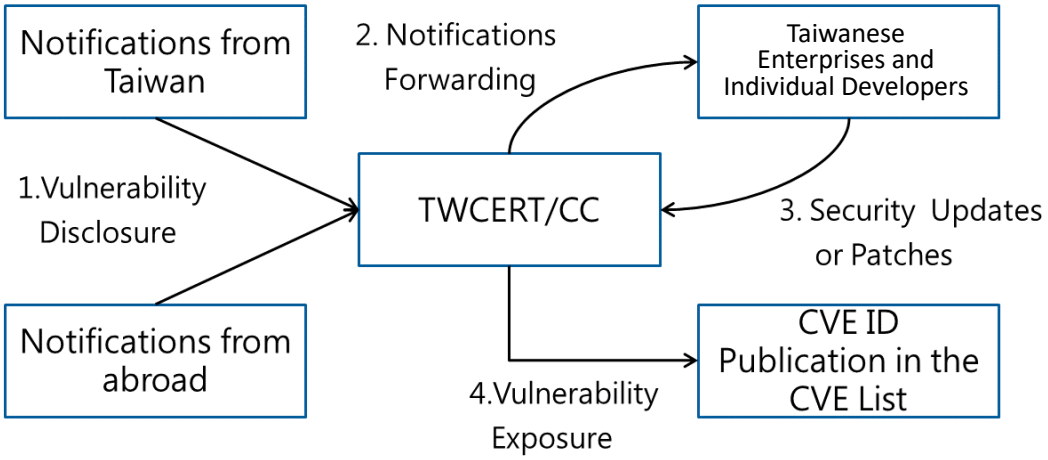


Figure 4. TWCERT/CC's vulnerability handling framework

4. Events organized / co-organized / hosted

4.1 Information Security Training & Activity

In 2018, TWCERT/CC provided 5 cybersecurity trainings for industrial associations, enterprises, and schools to enhance their understandings and capabilities on information and network security with lectures and field practices.

Table 3. List of the trainings TWCERT/CC provided in 2018

Date	Theme of the Training	Institution
2018/FEB/07	Entrepreneurial Cybersecurity Collaborative Defense- Incident Report and Intelligence Sharing	Computer Audit Association in Taipei
2018/MAR/19	Frequent Cybersecurity Incidents and Their Countermeasures within and outside of Offices	National Association of Small & Medium Enterprises, R.O.C.
2018/JUN/27	New Perspectives on Collective Cybersecurity Defense: a Holistic View of Cybersecurity Incident Notifications from Civil Enterprises	Taiwan Internet and E-Commerce Association
2018/AUG/19	Trend and Cases of Cyber Threats	Seminar for Seeding Teachers in Secondary Schools
2018/NOV/29	The Trend and Related Case Studies on Cyber Threats	China Airlines Emergency Security Response Seminar

To raise people's cybersecurity awareness and exchange information and technical skills with cybersecurity talents and ISPs, TWCERT/CC co-hosts and participates in cybersecurity conferences and seminars regularly. In 2018, TWCERT/CC joined 11 conferences and seminars:

Table 4. List of the conferences and seminars TWCERT/CC participated in 2018

Date	Conference/Seminar
2018/APR/18	Symantec Internet Security Threat Report (ISTR) Presentation
2018/APR/27	2018 Asia Pacific Cyber Security Forum

2018/MAY/03	2018 Hackers' Task: Cyber Security War
2018/JUL/09	Honeynet Project Annual Workshop 2018
2018/JUL/12	2018 Taiwan International Cyber Security Organization Summit
2018/JUL/27	HITCON Community 2018
2018/AUG/29	2018 SHIELD CTF Contest
2018/SEP/29	TDOH Conf 2018
2018/NOV/02	2018 Symentec Cybersecurity Forum
2018/DEC/03	2018 IT Month
2018/DEC/14	2018 HITCON Pacific

4.2 Drill

TWCERT/CC participated 2 cyber drills in 2018: one is the APCERT Cyber Drill on March 7, 2018 with the theme of "Data Breach via Malware on IoT", and TWCERT/CC designed its script. The other one was held by the Organization of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) on September 18, 2018. The theme of 2018 OIC Drill 2018 was "Crypto-currencies: Risks and Emerging Threats".

4.3 Conferences and seminars

On October 3, 2018, TWCERT/CC held the 2018 Conference of Taiwan Cyber Security Notification and Response with the theme of "Inevitable Cybersecurity Managerial Responsibilities for Enterprises" and the 5th Working Meeting of Taiwan CERT/CSIRT Alliance in the GIS NTU Convention Center. Around 450 people participated in the Conference, while 15 companies and institutions joined the Working Meeting.

The main goals of the Conference are to increase the participants' understandings about the measures of cybersecurity defense and management, how to establish a computer security incident response team (CSIRT) on one's own, the importance and benefit of cybersecurity incident notifications, and how to comply the Cybersecurity Management Law.

The Conference was divided in 11 sessions. 2 keynote speeches and a forum were held in the morning; the afternoon sessions were separated into the sub-themes "e-commerce cybersecurity" and "cybersecurity incident handling strategies". During the break time, there were 9 cybersecurity companies and communities shared their cybersecurity defensive strategies and ideas of cybersecurity governance. Around the main conference

hall were the booths set up by 15 cybersecurity companies, communities, and units to facilitate matches between the personal and business participants.

The chairperson of National Communications Commission (NCC), Ms. Nicole Chan, said: "As serious cybersecurity incidents happen more and more frequently, we should strengthen and improve our countermeasures of cybersecurity defense and cybersecurity emergency response systems. To address ever-changing cyberthreats, a national collective cybersecurity defense mechanism should be established, and our country's cybersecurity defense capability should be improved comprehensively."

The deputy director of Department of Cybersecurity, Executive Yuan, Ms. Chia-Lin Hsu, also gave a lecture to instruct the implementation of the Cyber Security Management Act and its six sub-laws. Her speech included the duties of public institutions, critical infrastructure providers, public enterprises, and state-sponsored foundations to give a comprehensive legal basis to facilitate the cybersecurity incident notification thus to promote national cybersecurity protection and related works hence to ensure national security and public welfare.

In addition, Mr. Adli Wahid, the APNIC senior cybersecurity expert, also gave a keynote speech to share his experiences in APNIC and FIRST to assist countries to establish their computer emergency response teams (CERTs). He especially underscored that mutual trust is the basis of intelligence sharing between and among the organizations, and the common goal of collaborative cyber defense actions should be to establish a stable and safe Internet environment.

After Mr. Wahid's speech, a forum themed on "the Countermeasures of Cyber Threats in the New Internet Era" was hosted by the deputy director of the Department of Cybersecurity, Ms. Chia-Lin Hsu, and the panelists were the senior Internet Security specialist of APNIC, Mr. Adli Wahid, the director of TWCERT/CC, Dr. Yeong-Jia Chen, the chief secretary of the Small and Medium Enterprise Administration, Mr. Kuo-Liang Chen, and the co-founder of CyCarrier, Mr. Benson Wu.

Nowadays in the Internet era, the importance of cybersecurity issues is increasing. On facing tremendous cyber threats and challenges, necessary cybersecurity protections in compliance with comprehensive cybersecurity policies and standard operating procedures for cybersecurity incident notifications should be taken into the considerations of business administration.

Figure 5. Group photo of the guests in the 2018 Conference of Taiwan Cyber Security Notification and Response

5. International Collaboration

5.1 International partnerships and agreements

Currently, TWCERT/CC is the member of FIRST and APCERT. Aside from its constant participation to the events held by the two international cybersecurity organizations, TWCERT/CC also collaborates with other CERTs in the world to handle cybersecurity incidents and exchange cyber intelligence.

In addition, since 2018, TWCERT/CC is a member of the Common Vulnerabilities and Exposures (CVE®) with the root CVE numbering authority (CNA). TWCERT/CC has released its vulnerability disclosure and coordination policy and is developing the Taiwan Vulnerability Note (TVN) platform to facilitate the disclosure of vulnerabilities and further patching and mitigation hence to prevent the exploitation of vulnerabilities.

5.2 Other international activities

In 2018, TWCERT/CC designed part of the scripts of the annual APCERT Cyber Drill themed on “Data Breach via Malware on IoT” and participated in the Drill on March 7.

The Organization of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) also invited TWCERT/CC to join the 2018 OIC Drill, "Crypto-currencies: Risks and Emerging Threats", on September 18.

6. Future Plan

In the year 2018, TWCERT/CC focused on the cybersecurity promotions and outreaches to the small and medium enterprises. From January 1, 2019, the Taiwan Network Information Center (TWNIC) again takes charge of TWCERT/CC.

In the future, TWCERT/CC will dedicate to advance its services and raise people's awareness of cybersecurity with the following promises:

1. Publish daily vulnerability information and cybersecurity incidents, monthly cybersecurity e-newsletter, and annual report;
2. Release trends, policies, threats about cybersecurity from time to time;
3. Collect and release the latest information of conferences, seminars, and trainings relative to cybersecurity
4. Keep noticing and assisting of cybersecurity incidents as well as improving our technical capability.

7. TWCERT/CC Contact Information

- Website: https://www.twcert.org.tw/
- Facebook: https://www.facebook.com/twcertcc/
- Telephone: 0800-885-066 / +886-2-23414344
- E-Mail: twcert@cert.org.tw

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Highlights of 2018

1.1 Summary of major activities

TWNCERT (Taiwan National Computer Emergency Response Team) aims to support and enhance the government's ability to respond and deal with security incidents. In 2018, TWNCERT received more than seven hundred reports of cyber security incidents from government agencies and published more than two thousand security advisories to government agencies as well as provided consulting and training services.

To raise security capability, TWNCERT conducted a national large-scale cyber security exercise, named Cyber Offensive and Defensive Exercise, as well as launched cyber security competitions for university students. Moreover, TWNCERT held twelve national cyber security seminars, eight Government Configuration Baseline trainings and four Secure Software Development Life Cycle trainings for government agencies.

In 2018, TWNCERT also attended various international events and delivered presentations on cyber security threats at the Honeynet Project 2018 in Taiwan, Meridian 2018 in Korea, APCERT training program, etc.

1.2 Achievements & milestones

This year in Taiwan, TWNCERT managed to encourage major CI sectors and six regional collective defense centers to join as members of the National Information Sharing and Analysis Center and share cyber security information with other members. TWNCERT was reappointed as APCERT Steering Committee member at the APCERT AGM 2018. As the convener of APCERT Training Working Group, TWNCERT convened six APCERT training programs in 2018, including five online training sessions and one training workshop, and a total of 27 APCERT member teams had participated in these programs.

2. About TWNCERT

2.1 Introduction

As a national CERT, TWNCERT acts as the point of contact for the CSIRTs in Taiwan and worldwide for the nation. We aim to enhance the government and CI sectors' ability to respond and deal with cyber security incidents, as well as to conduct technical and

consulting services to government agencies.

2.2 Establishment

TWNCERT was established in 2001, formed by the National Information and Communication Security Taskforce (NICST). TWNCERT is also known as the National Center for Cyber Security Technology (NCCST) domestically, led by the Department of Cyber Security, which is in charge of cyber security policy of Taiwan. The formation of TWNCERT aims to create a government cyber response center that can help optimize the capability of continuous monitoring, task coordination, and incident response and handling in the face of cyber security threats.

2.3 Resources

TWNCERT currently has around 130 full-time employees, and the operation funding comes from the Department of Cyber Security.

2.4 Constituency

TWNCERT dedicates to enhance the capability of incident report and response among government authorities and major national CI sectors. Moreover, TWNCERT coordinates information sharing with various organizations such as Financial ISAC, Academic ISAC, National Communications Commission ISAC, major MSSPs, law enforcement agencies, other CSIRTs in Taiwan as well as cyber security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

Our critical mission activities are

- Incident Response
- Responsible for cyber security incident response in the government and CI sectors and provide effective assists and supports to related agencies to counter when under cyber-attacks or facing threat situations.
- Information Gather

National Information Sharing and Analysis Center (N-ISAC) provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.

- Cybersecurity Drill & Audit

Hold large-scale cyber offensive and defensive exercises, pairing with security audit, cyber health check and penetration test services, to discover cyber security problems of the government and critical infrastructures in time.

- Education & Training

Plan cyber security series competitions and training programs to enhance cyber security education effects and raise cyber security awareness.

- Coordination and Collaboration

Build coordination and communication channels with domestic and foreign incident response organizations; Coordinate with international CSIRTs, cyber security vendors, and other cyber security related organizations.

3.2 Incident handling reports

TWNCERT received more than seven hundred reports on cyber security incidents from Taiwan government agencies, and about one thousand and seven hundred international cyber security incident reports from overseas in 2018.

Additionally, around one hundred and eight thousand security incidents and critical information were shared among N-ISAC members, including CI sector ISACs, major MSSPs, law enforcement agencies, and CSIRTs in Taiwan.

3.3 Abuse statistics

- Government agencies

  Two most reported incident categories from government agencies are Intrusion and Defacement.

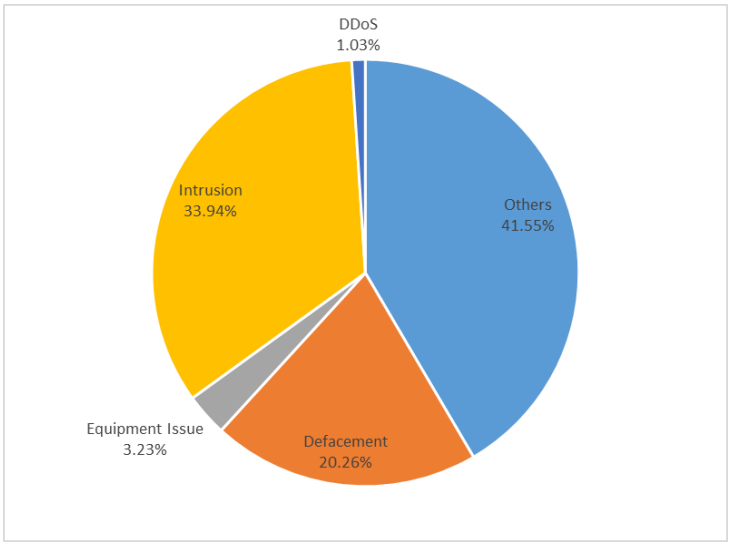


Figure 1 Security incidents from government agencies

- International incident report

  The international cyber security incident reports in 2018 were categorized as in Figure 2. About 40.82% of the incident reports were Malware, followed by Phishing and Attack.

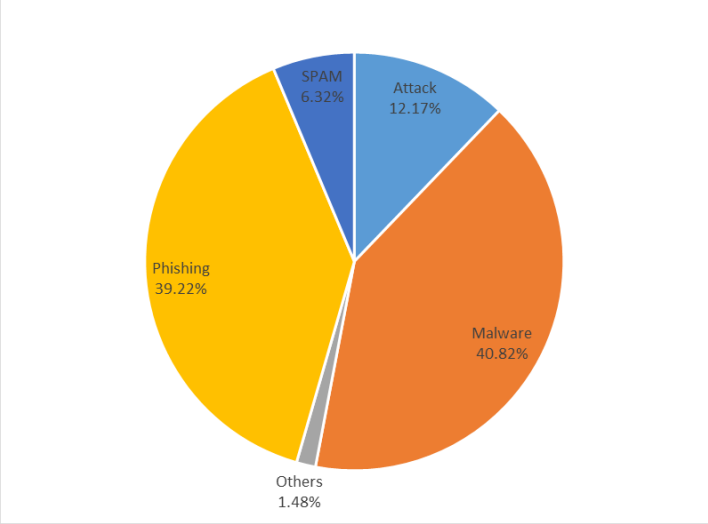


Figure 2 Classification of the international incident reports

- N-ISAC information sharing

  N-ISAC members shared thousands of security incidents and critical information, around one hundred and eight thousand security information in 2018.

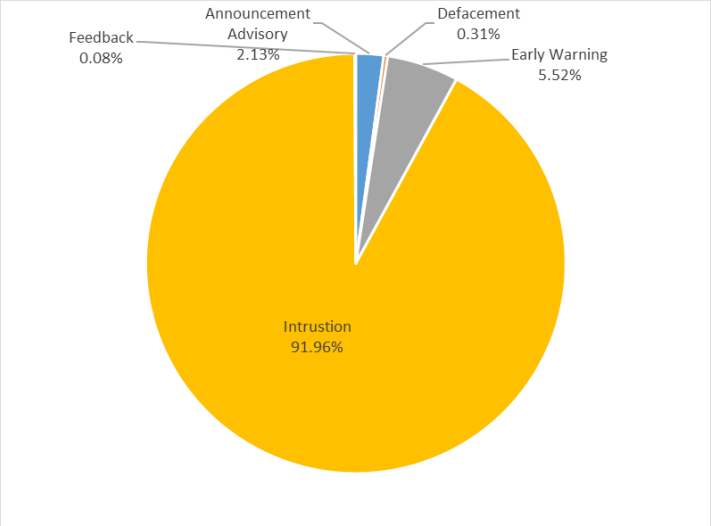


Figure 3 Information sharing distribution of N-ISAC

3.4 Publications

- Website publication

TWNCERT collects and publishes cyber security advisories, news or guidelines via its website. In 2018, TWNCERT published more than one hundred and fifty articles including cyber security news and security alerts on the website.

- Government agencies

  In 2018, TWNCERT published more than two thousand notice advisories to government agencies. The categories were distributed as in Figure 4.

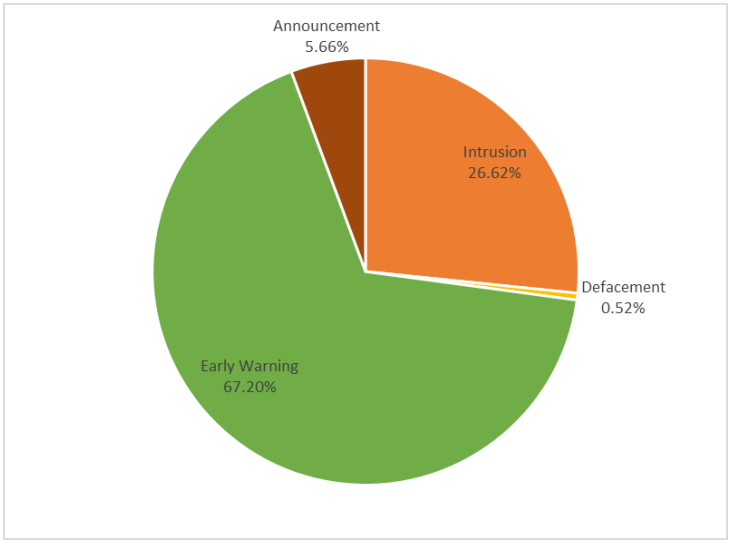


Figure 4 Distribution of government notice advisories

- International incident report sharing

Regarding the international incident report sharing, TWNCERT has reported a total of 1,716 incident reports to 55 countries shown in figure 5.

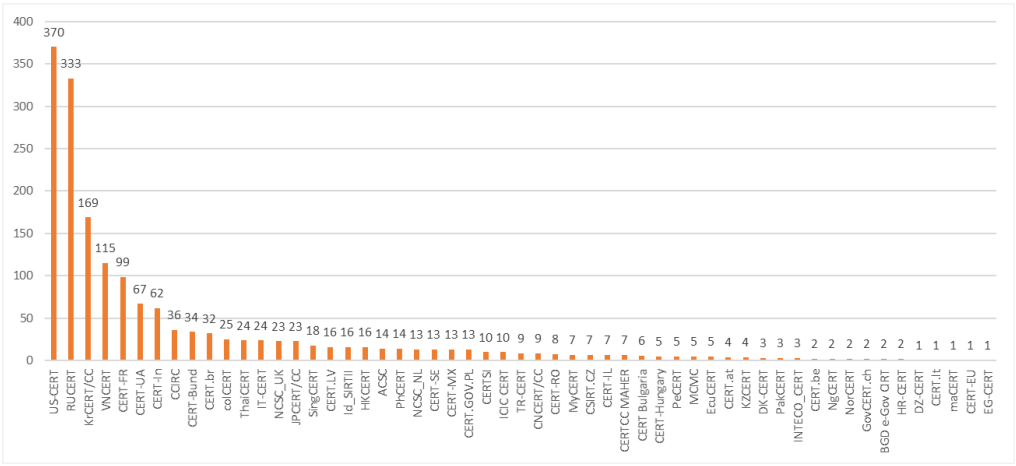


Figure 5 International incident report

4. Events organized/hosted

4.1 Training

In order to better the cyber security among computers and systems of government agencies, TWNCERT held eight Government Configuration Baseline (GCB) trainings to three hundred government technical staffs in 2018. Also, TWNCERT held four Secure Software Development Life Cycle (SSDLC) trainings to more than five hundred government technical staffs.

Moreover, TWNCERT hosts national cyber security workshops and seminars regularly to raise cyber security awareness among government agencies. In 2018, TWNCERT held 12 national cyber security workshops for government agencies.

Figure 6 Cyber security workshops

4.2 Drills & exercises

- Drill

TWNCERT has conducted a national large-scale cyber security exercise, Cyber Offensive and Defensive Exercise (CODE). This year CODE was mobilized relevant domestic agencies, including National Security Bureau, Ministry of National Defense, Office of the President, and local government agencies, to strengthen the preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure (CII) incidents.

- Cyber security competition

To promote cyber security general awareness, TWNCERT launched cyber security series competitions in 2018. It aimed to improve cyber security awareness among university students. There are more than two thousand attendees participated.

Figure 7 Cyber Security Competition

4.3 Conferences and seminars

For N-ISAC members, TWNCERT held quarterly meetings among members, not only discuss issues and problems found during each quarter but also improve information sharing efficiency and effectiveness. In 2018, a total of four member meetings had been held.

Figure 8 N-ISAC Members Meeting

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT is the member of international organizations listed below and actively participates in member activities including organization events, working groups, annual conferences, and other cooperation.

- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- APEC TEL
- Meridian

To further strengthen cooperation, TWNCERT currently has Government Security Program Source Code Agreement with Microsoft, NDA with Fortinet, MOU with four CERTs/CSIRTs and Team Cymru for CSIRT Assistance Program.

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, this year TWNCERT continued to coordinate member teams to provide online training sessions every other month. In 2018, a total of six APCERT training programs, including five online training sessions and one training workshop, have been convened. Moreover, there were 27 APCERT member teams participated in these training programs. To improve the training program, TWNCERT conducted a survey to evaluate the effectiveness of the training program and delivered the statistics results at the APCERT AGM & Conference in October.

Date	Topic	Presenter	Participation Team
2018/2/6	Malware Information Sharing Platform (MISP) in a CERT	AusCERT	AusCERT, CERT Australia, CERT-In, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, MOCERT, MyCERT, SingCERT, Sri Lanka CERT|CC, ThaiCERT, EC-CERT, TWCERT/CC, TWNCERT
2018/4/3	Analyses of A Compromised Linux Server	APNIC	CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, LaoCERT, MNCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC, ThaiCERT, EC-CERT, TWCERT/CC, TWNCERT
2018/6/5	Performing Forensics on and Azure Virtual Machine	Microsoft	AusCERT, CERT Australia, BtCIRT, CERT-In, GovCERT.HK, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, LaoCERT, MOCERT, MyCERT, SingCERT, Sri Lanka CERT|CC, EC-CERT, TWCERT/CC, TWNCERT
2018/8/7	Shaoye Botnet-Android Malware & DNS Hijacking	TWNCERT	CERT-In, CNCERT/CC, GovCERT.HK, JPCERT/CC, KrCERT/CC, MOCERT, MyCERT, SingCERT, Sri Lanka CERT|CC, TWCERT/CC, TWNCERT
2018/10/21	Technical Training: Digital Forensics with a Focus on the Cloud	Microsoft	APCERT AGM Training Workshop
2018/12/4	Inside the APCERT Drill: Player, Observers, EXCON and OC	AusCERT	ACSC, AusCERT, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MOCERT, EC-CERT, TWNCERT

Figure 9 APCERT training programs

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme “Data Breach via Malware on IoT” on March 7th, and solved a set of drill scenario within the given time limit.

Figure 10 APCERT Drill 2018

5.2.3 Seminars & presentations

Below are a portion of international events which TWNCERT participated in 2018.

- APRICOT 2018, February in Nepal
- AusCERT 2018 Cyber Security Conference, May in Australia
- APEC TEL 57, June in Papua New Guinea
- FIRST 2018 and NatCSIRT 2018, June in Malaysia
- Honeynet Project 2018, July in Taiwan
- Black Hat USA 2018 & DEF CON 26, August in the United States
- APEC TEL 58, October in Taiwan
- Meridian 2018, October in Korea
- APCERT AGM and Conference 2018, October in China

6. Future Plans

For the APCERT online training program, TWNCERT will continue to coordinate trainers and participants to provide bi-monthly online training, expands the coordination with other APCERT Working Groups, and participate in APCERT activities such as APCERT Drill. Possible collaboration opportunities with other international organizations will also continue to be a key emphasis to enhance the depth and broadness of the training program further.

7. Conclusion

TWNCERT will continuously enhance the collaboration with government agencies, particularly critical information infrastructure sectors, to build the public-private partnerships and collaborate with local and global CSIRTs to strengthen the cyber security awareness and incident handling capabilities. The critical elements of this strategy will be

- Enhance agency accountability and guide resource allocation
- Expand public-private partnership and introduce quality services
- Defense-in-depth deployment and toward government-wide situation awareness
- Harden IT infrastructure and reduce cyber-attack surfaces
- Check and evaluate regularly, improve through lessons learned
- Cultivate future talents to raise the bar for cyber security

Within the region, TWNCERT dedicates to contribute to the APCERT mission as well as looks forward to domestic and international cooperation opportunities, to achieve the goal of establishing a safe and secure cyberspace for the prosperity of the society.

VNCERT

Vietnam Computer Emergency Response Team – Vietnam

1. About VNCERT

1.1 Introduction and Responsibilities

VNCERT belongs to the Ministry of Information and Communications of Vietnam. It was established in 2005, by the Decision 339/2005/QD-TTg of Vietnam's Prime Minister. The Term 3 of Article 43 (Emergency for network problems) of Decree No. 72/2013/ND-CP dated July 15, 2013 of the Government (on management, provision and use of internet services and online information) regulates:

"Ministries, ministerial agencies, Governmental agencies, telecommunication enterprises, internet service providers, the organizations in charge of national critical information systems protection have to establish computer emergency teams (CERT) to take actions within their competence and cooperate with Vietnam Computer Emergency Response Teams (VNCERT)".

Roles of VNCERT:

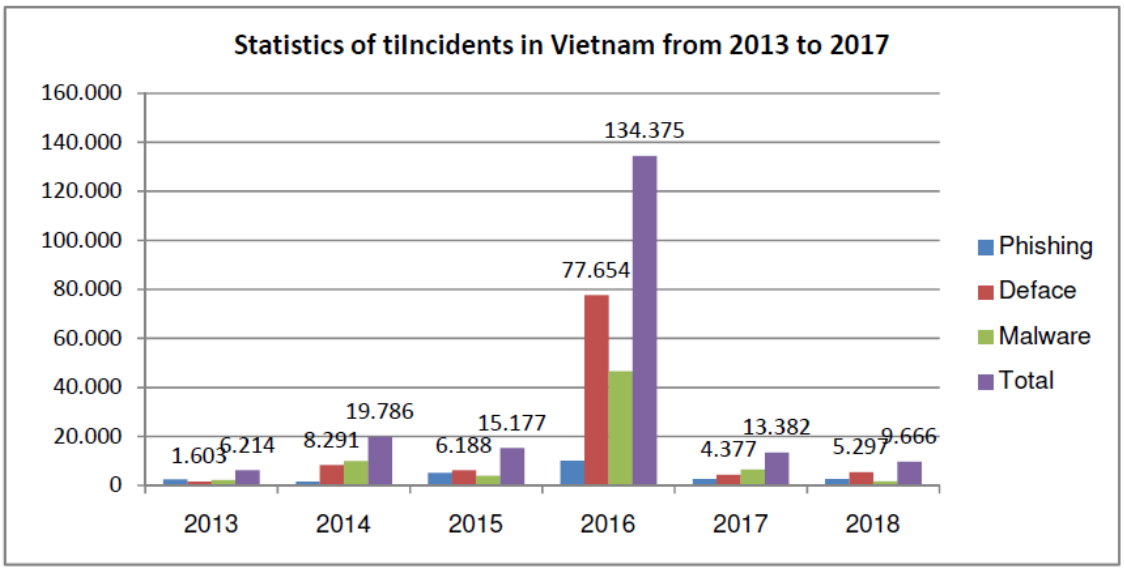
- Being National Coordination Agency for Incident Response nationwide, responsibility for:
  - Performing the function of coordinating incident response activities nationwide; Have the right to mobilize and coordinate members of the Vietnam CSIRT Networks and relevant organizations and units to coordinate in preventing, handling and recovering cyber incidents in Vietnam.
  - Organizing and administering operations of the Vietnam CSIRT Networks with 175 members (Including: specialized units in charge of incidents response, information security or information technology of ministries, ministerial-level agencies, governmental agencies, provincial-level agencies; telecommunications enterprises and Internet service providers (ISP); organizations and enterprises providing data center services; leasing information space; Units managing and operating the national database; specialized units in information security, information technology of banking, finance, treasury, tax, customs, etc...);
- Monitoring and early warning computer network security problems.
- Building and coordinating to build cyber security technical standard.

- Promoting the formation of local CERTs/CSIRTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the other CERTs in the world.
- Supporting Ministry of Information and Communications of Vietnam with activities in information security state management.
- Implementing and deploying the anti-spam activities.

2. Activities & Operations

2.1 Incident handling reports

In 2018, VNCERT processed 9.666 information security incidents (including 2.611 phishings, 5.297 Defaces and 1.758 Malwares).



2.2 Abuse statistics

Security Incidents	2013	2014	2015	2016	2017	2018
Phishing	2.469	1.458	5.104	10.057	2.605	2.611
Deface	1.603	8.291	6.188	77.654	4.377	5.297
Malware	2.142	10.037	3.885	46.664	6.400	1.758
Total	**6.214**	**19.786**	**15.177**	**134.375**	**13.382**	**9.666**

2.3 Incident response coordinating, warning and supporting activities

In 2018 VNCERT had actively issued early warnings to all members of Vietnam

National CSIRTs Network and related organizations about incidents and risks, such as:

- Alerted and required organizations to monitoring, blocking the campaign distributing ransomware GandCrab ver1.0 and 2.0 in end of March 2018.
- Alerted and required all members of Vietnam National CSIRTs Network and related organizations to update Vulnerabilities of Drupal's Content Management Systems in the end of April 2018.
- Detected and alerted APT campaign targets Vietnam's banks and national key infrastructure organizations in July 2018

2.4 Anti-spam activities

In 2018, VNCERT received 56.941 advertising text messages (including advertising emails; advertising SMS over Internet)

2.5 Information security legal framework update on

- Law No. 24/2018/QH14 on Cybersecurity 2018, Issue date 12/06/2018, Effective date 01/01/2019 (New Cybersecurity Law)
- Law No. 86/2015/QH13 on Cyber information Security 2015, Issue date 19/11/2015, Effective date 01/07/2016.
- Decree No. 85/2016/ND-CP dated July 01, 2016 - on the security of information systems by classification.
- Decision No. 05/2017/QD-TTg dated March 16, 2017 - Regulations on the system of National Cyber Incident Response Plans.
- Circular No 20/2017/TT-BTTTT dated September 12, 2017 - Regulations on coordinating and responding to information security incidents nationwide.
- Circular No. 31/2017/TT-BTTTT dated November 15, 2017 on surveillance of information system security.

3. Events organized / hosted

VNCERT had organized:

- Hosted a training courses on Malware Analysis for LaoCERT in VNCERT.
- Hosted workshop and training courses on “Fundamentals of Incident Handling”, instructed by FIRST's experts.

4. International Collaboration

- Participated in 03 international drills:
  - APCERT Annual Drill 2018
  - ASEAN-JAPAN Drill 2018
  - ASEAN CERTs Incident Drill 2018
- Became official member of FIRST

5. Future Plans

- To draft and submit the circular on guiding the organization and operation of incident response teams and job title positions, standards and certificates for members of incident response teams of CSIRT.
- To carry out tasks of the Prime Minister's Decision No. 1622/QĐ-TTg dated October 25, 2017 approving Project on enhancing the cyber security incident response network and increasing capacity of staffs and specialized units in cyber security incident response to 2020, orientation toward 2025.
- To carry out tasks of the Prime Minister's Decision No. 1017/QĐ-TTg dated August 14, 2018 approved the Scheme on monitoring of cyber security of information technology systems and services supporting the e-government operations through 2020, orientations toward 2025.
- To participate international drills.
- To organize national wide drills for Vietnam CSIRT's networks.

Disclaimer on Publications

The contents of the Activity Report on Chapter III are written by each APCERT member teams based on their individual analysis. Responsibility for the information and views expressed in each report lies entirely with the authors.