Sri Lanka Computer Emergency Readiness Team | Coordination Centre

Annual Activity Report 2019

Table of Contents

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. It is mandated with the task of protecting Sri Lanka's Information and Information Systems infrastructure. Its services range from responding to and investigating information security breaches, to preventing security breaches by way of awareness creation, security assessments and security capability building.

1.2 ESTABLISHMENT

As the national CERT, 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 presently serves under the Ministry of Defence.

1.3 WORKFORCE

Sri Lanka CERT|CC has a total staff strength of seventeen (17) team members consisting of a Chief Executive Officer, Chief Operating Officer, Head of Research, Policy & Projects, 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 five (05) 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 2019. As a summary following observations can be made;

i. Number of reported cases related to personal information misuse has been increased during the year 2019.
ii. Financial frauds targeting local importers and exporters have seen a decrease during the year 2019 compared to 2018.
iii. There has been an increase in the spread of ransomware and malicious software during the year of 2019, where sensitive data belonging to both individuals as well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.
iv. A significant number of web site compromises targeting government and private sector organizations were recorded in 2019.
v. 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 provide digital forensics services as follows;

i. Appearing in courts as expert witness for the digital forensics investigations conducted by CERT
ii. Number of forensic work carried out/involved in was more than 24 for the year
iii. Most of them are for the CID (Criminal Investigation Department), CCB (Counterfeit Currency Bureau), FCID (Financial Crimes Investigation Division), Others for some other police stations around the country.

Cyber-security related incidents reported to Sri Lanka CERT have increased in the year 2019 compared to previous year. In 2019, a total of 3566 incidents were reported to Sri Lanka CERT while it was 2598 during the year 2018. The increase is due to the significant number of cases reported for website compromise and privacy related issues.

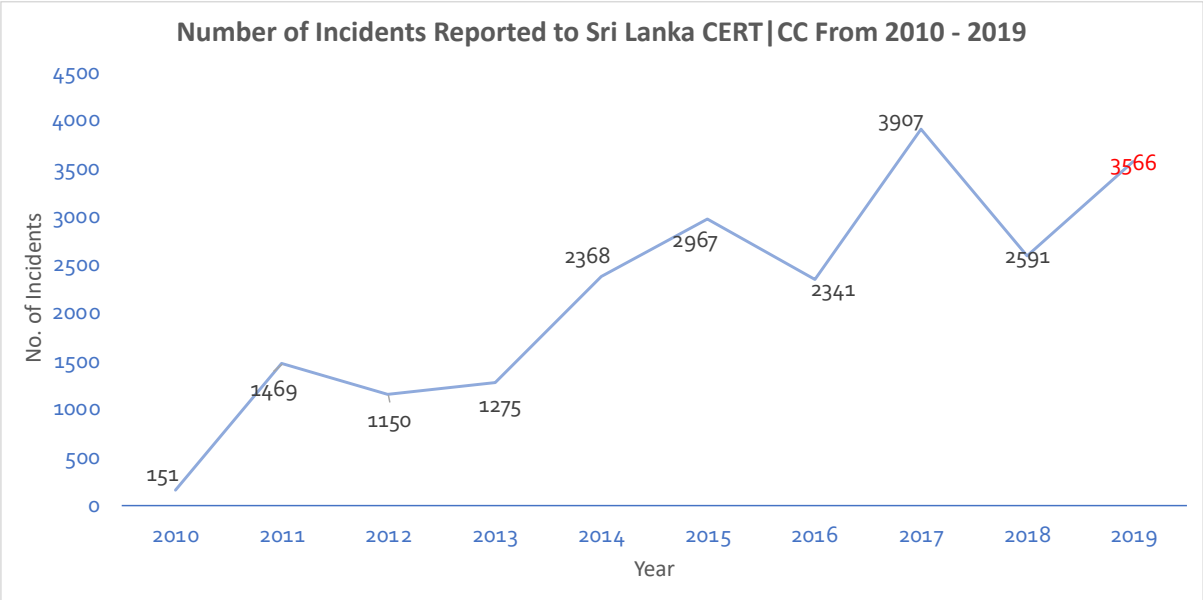

Figure 1. Growth of the number of incidents reported

Incident Type	No of Incidents
File Recovery	1
DDOS	2
Ransomware	11
Abuse/Hate/Privacy violation	307
Malicious Software issues	3
Phone Hacking	1
Scams	5
Phishing	5
Website Compromise	175
Financial/Email frauds	28
Intellectual property violation	1
Server Compromised	2
Social media	2662
Other	363
Total	**3566**

Table 1. Types of incidents

Incident Type	Year									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Phishing	6	6	8	8	12	14	23	42	12	5
Abuse/Hate/Privacy Violation	20	2	8	8	8	21	32	29	11	307
Scams	10	3	6	18	12	18	12	32	7	5
Malicious Software/Ransomware	5	1	2	2	3	12	21	39	19	14
Financial Frauds	-	-	-	-	-	10	16	35	21	7
Web site Compromise	8	20	15	16	56	20	10	25	9	175
Compromised emails	12	3	6	8	10	16	16	14	-	21
Intellectual Property violation	-	5	3	3	3	3	7	6	6	1
Unauthorized Access	10	3	1	11	8	-	-	0	-	
DoS/ DDoS	-	1	1	1	6	3	4	0	1	2
Social Media Incidents	80	1425	1100	1200	2250	2850	2200	3685	2505	2662
Phone Hacking	-	-	-	-	-	-	-	-	-	1
Server Compromised	-	-	-	-	-	-	-	-	-	2
Other	-	-	-	-	-	-	-	-	-	364
Total	**151**	**1469**	**1150**	**1275**	**2368**	**2967**	**2341**	**3907**	**2591**	**3566**

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;

i. Development of Cybersecurity Curriculum for National Police Academy
ii. TEC member of Procurement of VAPT service provider for Bank of Ceylon (BoC)
iii. Police Criminal Records Division (CRD) fingerprint committee for the Automated Fingerprint Identification System (AFIS)
iv. TEC member of Procurement of ATP solution for BoC
v. TEC member of Procurement web development service for Tea Board
vi. TEC member of Procurement of Reserve Management System (RMS) for CBSL
vii. Member of Procurement Committee of e-Passport
viii. TEC member of Procurement of email solution for Bank of Ceylon
ix. TEC member of Procurement of Privileged Access Management (PAM) solution for Bank of Ceylon
x. TEC member of Procurement of ATM AV for BoC
xi. Security assessments for 18 government department web sites
xii. Technical Expert of the President commission on Ester Sunday terrorist attack

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.

a. Awareness Program and Training Sessions

i. Cyber security awareness session for schools (1 session)

ii. Digital forensics training for National Police Academy (3 sessions)
iii. Cyber security workshop for SIS officers
iv. Training sessions for SLAS officers at SLIDA (12 sessions)
v. Cyber Security session for NVQ level 4 students
vi. Information security lecture for Bio informatics Postgraduate/MSc doctors
vii. Training for school IT Tamil teachers via EduCSIRT program (3-day session)
viii. Session on Email security and document protection for STF officers
ix. Cyber Security workshop for OCDS officers
x. Cyber security training for National Police Academy

b. Awareness through Electronic/Print Media

i. Newspaper articles
Provided information for 2 articles

ii. TV programs
01 live session
03 video cuts

iii. Radio programs
17 Voice cuts and one live session

c. Annual Cyber Security Week 2019

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 2019 was held in the months of October 2019, and featured a series of events including the following;

- Hacking Challenge, 8th October 2019 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: 7th October 2019 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.

- 12th Annual National Cyber Security Conference – 15th October 2019 at Hilton Colombo,

  ✓ This year's theme was "Cyber Security…United we stand, divided we fall"
  ✓ More than 400 participants

- ✓ Conducted the awarding ceremony for the winners of Hacking Challenge and Quiz
- ✓ Chief Guest was Hon. Minister of Digital Infrastructure and Information Technology
- ✓ Keynote address was delivered by Dr. Henry Pearson, Cyber Security Ambassador, UK

- Workshops – 9th, 10th & 11th October 2019 at DLC, SLIDA

  - ✓ Securing Internet identifiers and incident Response (Hands On)-by ICANN
  - ✓ Threat detection and Response-Made simple and effective-by CISCO
  - ✓ Threat hunting Techniques and Methods (Hands on)- By Estonian Experts

- Supporting events

  - ✓ Workshop on IT risk assessment for banks
  - ✓ Workshop on IT risk assessment for ISPs

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 2019. This project was funded by government of Sri Lanka.

2.6 NATIONAL PROJECTS

Project Name	Project Status
1. Establish the National Cyber Security Operations Centre (NCSOC) to monitor threats digital government application and critical infrastructure.	Procurement started
2. Establish Root Certification Authority to provide digital certifications to the certification service provides	Ready for commissioning
3. National Surveys to assess cyber security landscape of Sri Lanka a. Critical Information Infrastructure Readiness Survey b. Public Employees Cyber Security Readiness Survey c. National Survey on Citizen Perceptions of Cyber Security (Department of Census and Statistics) d. Supply and Demand Assessment of Cyber Security Professionals	Surveys in progress
4. Development of Information Security Manual for Government Organizations and development Baseline Security Standards	Work in progress

3 ACHIEVEMENTS

3.1 NATIONAL CYBER SECURITY STRATEGY

The government of Sri Lanka ensured its commitment 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.

Sri Lanka CERT is in the process of the implementation of the National Information and Cyber Security Strategy and have initiated several projects during the year 2019.

3.2 RESEARCH AND POLICY DEVELOPMENT

Research and policy development team of Sri Lanka CERT was involved in drafting the Cyber Security Act during the year 2019. The process is ongoing for the enactment of the act through the parliament of Sri Lanka.

3.3 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

3.4 TRAINING FOR STAFF

Sri Lanka CERT was able to provide following local training and conference participation for its staff

i. Discussion with NI-CO team on "CERT maturity model of ENISA"
ii. Discussion with world bank team on “Cybersecurity capacity maturity model”
iii. CISCO security workshop for CERT staff
iv. Cyber Maturity Model (CMM) workshop with Oxford university
v. Participation at ISC2 Sri Lanka chapter meetings

4 INTERNATIONAL COLLABORATION

4.1 EVENT PARTICIPATION

i. FIRST Symposium and TF-CSIRT meeting (Estonia)
ii. CYBERUK 2019 (UK)
iii. HR training (India)
iv. First Annual General Meeting & Conference and NatCSIRT Meeting 2019 (Scotland)
v. International visitors leadership program (Germany)
vi. Japan -US Industrial Control System Training (Japan)
vii. APCERT Annual General Meeting & Conference (Singapore)
viii. nCSIRT workshop (Singapore)
ix. ITU Asia-Pacific & CIS Inter-Regional Cyber Drill (Malaysia)
x. nCSIRT workshop (UK)
xi. CAMP 4th AGM (Korea) -Sri Lanka is in the operations committee

4.2 APCERT

i. Became a member of the APCERT Steering Committee from 2019
ii. APCERT steering committee meetings
iii. Continuing with network monitoring project "Tsubame" with JPCERT|CC
iv. APCERT working group teleconferences- Secure Digital payments
v. APCERT online trainings (3 trainings)
vi. APCERT cyber drill 2019 working group discussions
vii. OIC-CERT cyber drill 2019
viii. APCERT AGM Program Committee Meetings
ix. APCERT AGM and Conference (Singapore)

- Member of the program committee of AGM
- Presented at the Public Conference on "National Information and Cyber Security Strategy"
- Contributed to several APCERT working groups.
- Made new contacts with cyber security related organizations.

4.3 OTHER ACTIVITIES

i. 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.
ii. Continuing with network monitoring project "Tsubame" with JPCERT|CC
iii. Ministerial delegation to Finland and Estonia
iv. NatCSIRT teleconferences
v. ICANN GAC meeting (Japan)
vi. Government delegation to Estonia for e-Governance conference and discussions
vii. Government delegation to Portugal for a Cyber Security Study Tour

4.4 INTERNATIONAL INCIDENT COORDINATION

i. APCERT Cyber Security Drill

- Worked as a member of the organizing committee of APCERT Cyber Security Drill 2019
- Participated for the drill

ii. 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 to resolve phishing and identity theft incidents.

5 FUTURE PLANS

5.1 FUTURE PROJECTS

i. Development of National Vocational Qualification (NVQ) Standards for Cyber Security
ii. Information and Cyber Security Skills Framework for government employees.
iii. Development of a Web Portal to increase citizens' (business, government organizations) awareness on cyber security
iv. Train 2200 government employees with information and cyber security
v. Upgrading Education Sector CERT (EduCERT) with physical premises
vi. Development of e-Learning Modules on Information and Cyber Security
vii. Improving the Information and Cyber Security Readiness of the Government Organizations Maintaining Critical Information Infrastructure (10 organizations)
viii. Development and Implementation of a Security Operations Centre (in progress).
ix. Establishment of sector based CSIRT's (e.g. Telco-CERT).
x. APCERT AGM 2020 with Cyber Security Week.
xi. Cyber Security project with European Union (Cyber4Dev) to implement the provisions of the National Information and Cyber Security Strategy.

5.2 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.

6 CONCLUSION

During the period, Sri Lanka CERT has observed that number of web sites which were compromised has been increased. The main reason for such compromises were due to obsolete Content Management Systems used by those web sites.

It was also observed that financial frauds happening through email compromise is very common as in the previous year and CERT was able to make the public, small business establishments and large corporates aware of such threats in order to stop them from becoming victims.

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 a few national level Information Security related projects during the year 2020 to support the implementation of the National Information and Cyber Security Strategy of Sri Lanka.

Sri Lanka CERT became a member of the steering committee of APCERT in 2019 and expects to contribute to the enhancement of cyber security and improve the collaboration in the region with the support of all the APCERT members.