Sri Lanka Computer Emergency Readiness Team | Coordination Centre

Annual Report 2015

CONTENTS

Contents 2

ABOUT SRI LANKA CERT|CC 4

Introduction 4

Establishment 4

Workforce 4

Constituency 4

Activities & Operations 5

Incident Handling summary 5

Incident Handling Statistics 6

Consultancy services 8

Training / Education services 9

Publications 9

Operational Support Projects 10

Events organized / co-organized 10

Seminars & Workshops 10

Achievements 11

National Cyber security strategy 11

Research and development 11

Certification & Membership 11

New services 12

Setting up sector based CSIRTs 12

National Certification Authority 12

International Collaboration 13

Event participation 13

International incident coordination 13

Future Plans 13

Future projects 13

Framework 14

Future Operations 14

Conclusion 14

ABOUT SRI LANKA CERT|CC

INTRODUCTION

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the 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.

ESTABLISHMENT

As the national CERT of Sri Lanka, Sri Lanka CERT|CC acts as the focal point for cyber security for the nation. It is the single trusted source of advice for 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 July 2006 as Sri Lanka's National CERT, by the ICT 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 registered as a Private Limited Liability Company, and is a fully owned subsidiary of ICTA, which in turn is fully owned by the Government of Sri Lanka.

Sri Lanka CERT|CC is presently under the purview of Ministry of Telecommunications & Digital Infrastructure and is fully financed by the state budget.

WORKFORCE

The Sri Lanka CERT|CC has a total staff strength of fourteen team members consisting of Chief Executive Officer, Manager Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Junior Information Security Engineer, four Associate Information Security Analysts and an officer in charge of HR and Administrative work. This team is supported by three 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].

CONSTITUENCY

Sri Lanka CERT's Constituency encompasses the whole of the cyber community of Sri Lanka (private & 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 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.

ACTIVITIES & OPERATIONS

INCIDENT HANDLING SUMMARY

Given the expertise in the field of cyber security and the capacity to prevent, analyze, identify and respond to cyber security incidents that threaten Sri Lanka's national cyber-space, Sri Lanka CERT|CC continues to work with government, non-government and international organizations.

As the national contact point for matters relating to cyber security incidents, Sri Lanka CERT|CC receives numerous reports from domestic and/or international partners about various cyber security incidents/vulnerabilities that affected/may affect our national cyber-space. Following are some of the different types of incidents reported during 2015 (1st of January – 31st of December);

- Compromised unique IP's extracted from the information collected by automated systems
- Vulnerabilities on applications, operating systems and firmware etc.
- Phishing incidents and various other scams associated with this
- Content related matters such as privacy violations
- Cyber-attacks on various systems and applications

This annual report analyzes the cyber security incident information collected / managed by Sri Lanka CERT|CC in 2015, in order to obtain an overall view of the nature and dynamics of these types of events relevant to the evaluation of the risks targeting the ICT systems in Sri Lanka.

Based on the collected data, the following have been observed;

- Financial frauds targeting local importers/exporters are a relatively new type of incident that Sri Lanka CERT |CC encountered. This happens mainly in the Small and Medium Enterprises (SME) sector where local exporters/importers are exporting or importing various items to or from foreign countries. Hackers have used social engineering techniques to gain access to the email accounts of these businessmen and then sending emails pretending to be their business partner convincing them to deposit money to fraudulent bank account.
- There has been an increase in the spread of ransomware during the year, where sensitive data belonging to both individuals as well as corporate businesses have been stolen.
- It was observed that hackers were not targeting particular organizations when they attempt to compromise company websites. Instead they were targeting vulnerable web servers which may have hosted several web sites of various organizations. Once they compromise the server, hackers could deface multiple sites hosted in that server. In some cases it was observed that the vulnerability was with the content management panel, where the user who has being entrusted to update the site used a simple password to access the content management panel.
- There is an increase in the phishing emails specially targeting email accounts of businessmen. This might be the first step towards targeting those businessmen for financial frauds.

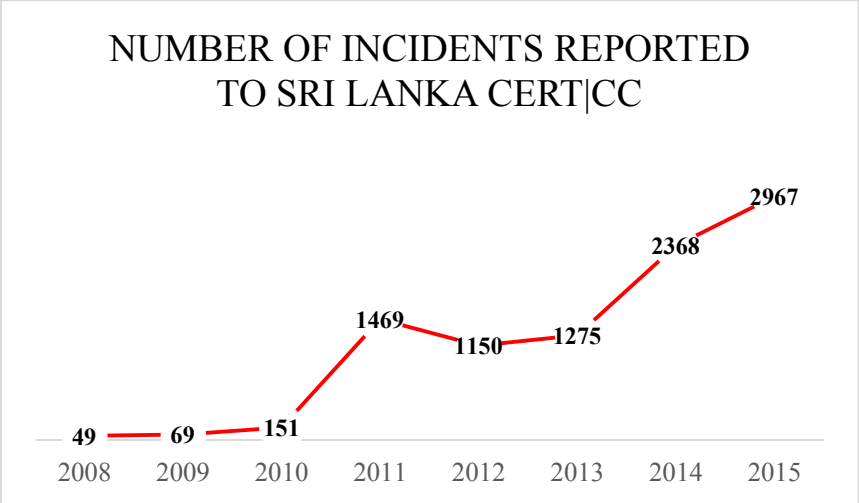
- Phishing mails targeting on-line banking customers continue to pose a problem, and regular complaints are received from banks as well as bank customers.

The above findings lead to the following conclusions:

- Cyber security is a part of every individual and each and every one is responsible for contributing to a secure online environment.
- Attackers might be shifting their focus on targets which can easily be compromised. For example, the average internet user many have comparatively less knowledge on information security and hence be more vulnerable to online attacks.
- Some Website owners believe that confidential information is not stored in the web site hence investing money on the security of the web site is not worth it. But they fail to realize that their compromised Website can be used to host malware sites that have the possibility of becoming a part of a botnet.
- Making the general public, private and public sector organizations aware about various types of cyber threats is a vital part of ensuring that people will gain the benefits of Internet rather than be a victim in the cyber world.

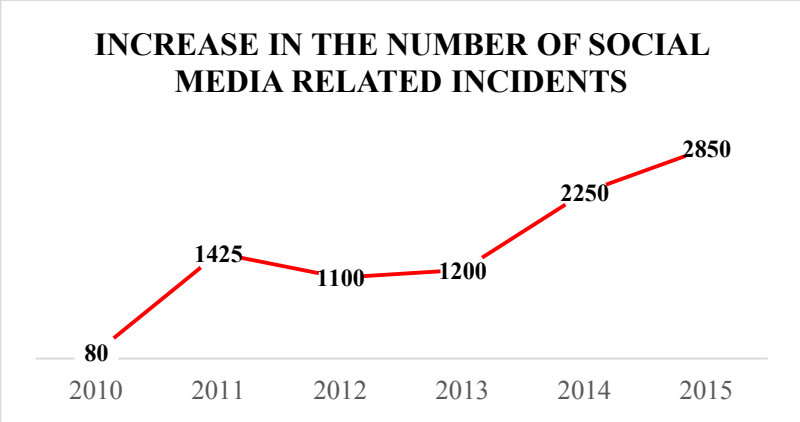
INCIDENT HANDLING STATISTICS

Incidents reported to Sri Lanka CERT have increased to 2, 967 in the year 2015. In 2014 2,368 incidents were reported. This represents a 25% increase in reported incidents compared to the year 2014.



Graph 1: Total number of reported incidents

It was observed that the number of reported cases related to social media have also increased considerably in the past year.

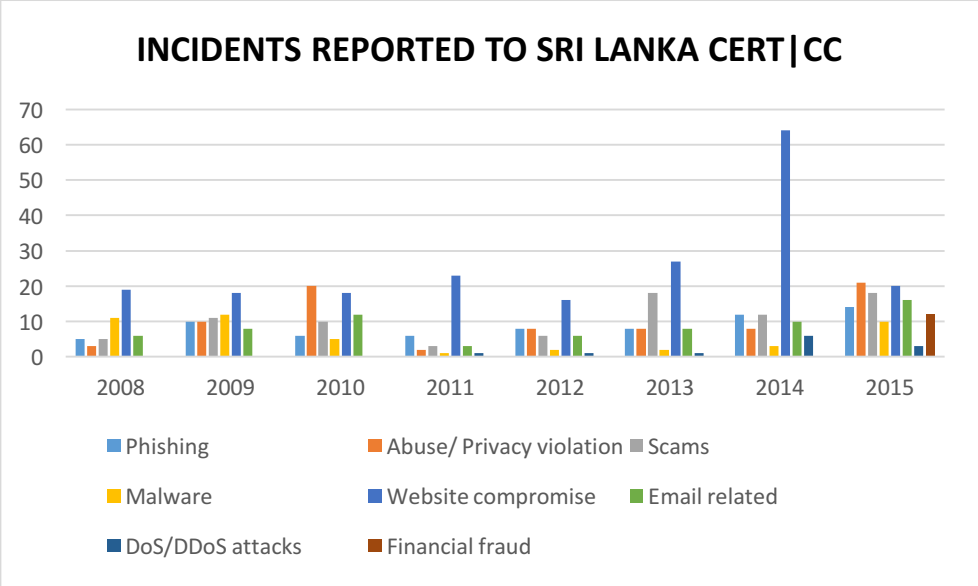


Graph 2: Total number of social media related incidents

The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT during 2015. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	Year 2015
Phishing	14
Abuse/Hate/Privacy violation (via mail)	21
Scams	18
Financial Frauds	12
Malicious Software issues	10
Web site Compromise	20
Compromised Email	16
Intellectual property violation	3
DoS/DDoS	3
Social Media related incidents	2850
Total	**2967**

Table 1: Number of reported incidents in year 2015



Graph3: Types of incidents reported to Sri Lanka CERT|CC from 2008- 2015

From Graph 3 it is evident that attacks targeting Websites are on the increase. Also, new types of incidents such as DoS/DDoS attacks and financial frauds have been reported in 2015.

CONSULTANCY SERVICES

Sri Lanka CERT|CC continues to provide consultancy services in response to requests made, particularly by government departments.

Typical consultancy services provided during the year 2015 include;

- Assisting several government organizations and private sector organizations to develop an Information Security Policy for their organizations.
- Application security and server hardening for a number of government and private sector organizations.
- Application and network security vulnerability assessments for e-Government applications.
- Carrying out technical forensic investigations for the Criminal Investigations Division (CID) of Sri Lanka Police;
  - Credit Card fraud investigations prosecuted under the Payment Devices Frauds Act, 2006, where Sri Lanka CERT serves on the panel of experts through a special gazette notification.
  - Investigating ATM and Credit Card skimming cases.
  - Investigation of Money Laundering cases.
- Carrying out technical forensic investigations for Private sector organizations.
- Assisting government and private sector institutions to secure their operational environment and secure their applications by performing information security policy formulation workshops, network architecture reviews, consulting on secure network and system design and system hardening.

TRAINING / EDUCATION SERVICES

In order to fulfil its mandate to create awareness and build information security skills within the constituency; Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences. This includes CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and the General Public.

During the year 2015 Sri Lanka CERT|CC conducted the following awareness, training and education programs successfully:

- Training sessions for police officers at the Police Training Academy and Police Training College.
- Awareness session for judges.
- Regular press releases to the media about incidents and impending vulnerabilities.
- Awareness programs for School Teachers.
- Cyber Guardian e-newsletter distributed monthly through School Net. This is the fourth consecutive year of this circulation which is widely accepted and read.
- Train-the-trainer on-line safety awareness programs island wide in collaboration with the Ministry of Education for IT Teachers of schools.
- Child on-line safety awareness presentations at private and government schools.
- Participating in regular radio programs, and in particular the "Subarathi" programme conducted by the Sri Lanka Broadcasting Cooperation as part of Sri Lanka CERT's awareness creation campaign.
- Conducting regular training programmes for SOCO (Scene of Crime) officers at the Police training college focussing on Cyber Crime first responder's role.
- National Child Protection Authority - Member of the panel to develop a training module for Ministry of Education for online safely.
- Awareness programs for high level government officers.

In addition, Sri Lanka CERT|CC staff has continued to assist in the delivery of courses in computer security topics at tertiary education institutions.

Sri Lanka CERT|CC was involved in the coordination and organizing of First Responder Training for law enforcement officers at Sri Lanka Police training college. Another training workshop on Live Data Forensics was also conducted for the law enforcement officers of Sri Lanka Police. These were funded by the Council of Europe project titled Global Action Against Cybercrime (GLACY).

As a key strategy, Sri Lanka CERT uses publications developed in-house such as leaflets and posters during public awareness sessions such as seminars, exhibitions and other forums.

PUBLICATIONS

Website

The Sri Lanka CERT|CC website publishes security related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, Case Studies, Statistics and FAQs are among some of the other published items.

E-mails

Sri Lanka CERT disseminates security related information via e-mail alerts to its subscribers. Similarly, the Cyber Guardian e-newsletter that was initiated in mid-2010 is distributed to a large number of students by the Ministry of Education, 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.

OPERATIONAL SUPPORT PROJECTS

Sri Lanka CERT continues to maintain a sensor for the JPCERT/CC hosted TSUBAME Internet Scan Data Acquisition System project.

EVENTS ORGANIZED / CO-ORGANIZED

SEMINARS & WORKSHOPS

- Cyber Security Week 2015;

  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 2015 was held in the month of November 2015, and featured a series of events including the following;

  - Annual National Conference on Cyber Security 2015.
  - Four full-day Workshops for professionals, namely:

    ✓ Technical workshop on "Internet Abuse Handling"
    ✓ Technical workshop on "Network Security in depth"
    ✓ Technical workshop on "Using Cuckoo Sandbox for Malware Analysis"
    ✓ Technical workshop on "Run your own Honeypots"

  - Hacking Challenge: Hacking Challenge is a contest for IT Professionals to attack or defend an actual network within a given timeframe. The invited participants are Technical Security Professionals, Network Administrators, System Administrators and students following information security post-graduate courses.

  - Information Security Quiz: 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.

All these events were well attended and were conducted by international industry experts. The conference and the workshops also saw the participation of information security professionals from APNIC, ICANN and Team Cymru.

- Application Security Awareness Session: A session on application security and CSSLP conducted by (ISC)2.

- First Responder Training: A five day first responder training was conducted by Council of Europe trainers for 15 local law enforcement officers.

- Carrying out training sessions and presentations on Information security for SLAS (Sri Lanka Administrative Services) officers at SLIDA

ACHIEVEMENTS

NATIONAL CYBER SECURITY STRATEGY

Sri Lanka CERT|CC commenced work on the first draft of the national cyber security strategy for Sri Lanka during the year 2015. Stakeholder consultations have been initiated in order to discuss this in detail with the relevant stakeholders during the year 2016 before finalising it.

RESEARCH AND POLICY DEVELOPMENT

The initiation of the research arm of Sri Lanka CERT will add more value to our services in the future. As a first step, the research team has conducted a pilot survey to assess the level of cyber security awareness among citizens of Sri Lanka.

CERTIFICATION & MEMBERSHIP

Sri Lanka CERT continues to enjoy the benefits of membership to the following professional security organizations;

a) Microsoft SCP (Security Cooperation Program).
b) Collaborative agreement with ITU Subsidiary "IMPACT", where Sri Lanka CERT benefits from receiving threat intelligence from the region and is also part of the global incident response teams.
c) International Information Systems Security Certification Consortium, Inc., $(ISC)^2$.
d) Threat Intelligence from ShadowServer.

NEW SERVICES

SETTING UP SECTOR BASED CSIRTS

Sri Lanka CERT|CC initiated the setting up of sector-based Computer Security Incident Response Teams (CSIRTs) in 2010. Typical sectors are Banking, Telecom, Defence and Education.

The rationale for sector based CSIRT's is to ensure that Sri Lanka CERT|CC remains a small, focused national body that functions only as an incident escalation and coordination point and ensures national readiness to tackle large scale incidents effectively.

Sri Lanka CERT|CC launched its first sector based CSIRT for the banking and finance sector called "BankCSIRT" on 1st of July 2014. All of the banks operating in Sri Lanka have joined as members of BankCSIRT and continuing its services with the regulatory blessings of the Central Bank of Sri Lanka. Bank CSIRT is funded by member banks, hosted by the national clearing house Lanka Clear and managed by a Steering Committee chaired by the Central Bank of Sri Lanka. Sri Lanka CERT|CC serves as a member of the Steering Committee, and provides the necessary technical assistance.

Bank CSIRT continued to be in operation during the year 2015 and has successfully resolved a number of security incidents reported by its members during the year. Bank CSIRTs core objectives however remained the same i.e. sharing threat intelligence anonymously using an information sharing platform, and adhering to a baseline information security standard based on ISO 2700. Accordingly, Bank CSIRT continues to protect its constituency from various security threats by taking proactive measures. In addition to its initial services, Bank CSIRT introduced a basic Security Operations Centre (SOC) as an additional paid service to the member banks during the year 2015.

NATIONAL CERTIFICATION AUTHORITY

The Electronic Transactions Act no. 19 of 2006 creates a foundation for the existence of a national certificate authority. With the launch of e-Citizen services and the increased use of online banking and other e-commerce facilities, the use of a digital ID is becoming more important. While the Lanka Government Network (LGN) Certification Authority (CA) for Government establishments and Lanka Sign CA (for Banks) exist, there is a lack of universal acceptance of their certificates.

As a fully own subsidiary of ICTA, Sri Lanka CERT|CC was designated to function as the implementation body for the National Certificate Authority (NCA) of Sri Lanka. The process of setting up the NCA using the provisions granted under the above Act is on-going.

Sri Lanka CERT|CC has completed most of the hardware and software procurements and configurations.

Since there were implementation delays due to lack of funding, NCA is expected to start the operations during the year 2016.

INTERNATIONAL COLLABORATION

EVENT PARTICIPATION

- February 8th – 12th
  ICANN 52|International public ICANN meeting, Singapore.
- May 26th -28th
  CNCERT|CC Annual Conference.
  Wuhan, China
- June 14th-19th
  FIRST AGM and Annual Conference.
  Berlin, Germany
- June 15th -19th
  OCTOPUS Conference.
  Strasbourg, France
- September 6th – 10th
  APCERT AGM and Conference.
  Kuala Lampur, Malaysia
- October 12th – 14th
  2nd PMAP Annual Conference.
  Manila, Philippines

INTERNATIONAL INCIDENT COORDINATION

Sri Lanka CERT|CC actively participated in the APCERT Drill 2015 as the lead team in the organizing committee, a player and an EXCON member.

In addition to the 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.

FUTURE PLANS

FUTURE PROJECTS

The following projects are either in the conceptual stage or just being initiated, and are intended to serve the constituency directly;

- Development of National Cyber Security strategy (ongoing).

- Development and Implementation of a Security Operations Centre (SOC).
- Establishment of the National Certification Authority (ongoing).
- Establishment of sector based CSIRT's.
- Cyber Security Week 2016.

FRAMEWORK

FUTURE OPERATIONS

This section details the changes anticipated in Sri Lanka CERT with regard to staff, equipment and capabilities:

- Continue to recruit undergraduate placement students on internships on an annual basis to enhance the information security capabilities of the younger generation.
- Continue to operate as a small focused group of professionals, but building sufficient skills nationally to combat and prevent cyber-crime.
- Keep the staff up-to date on cyber security threats and technical knowhow by providing adequate training.
- Conducting inter-organisational research in the area of cyber crime victimization and user behavior (e.g. cross- cultural research) which will be useful in guiding policy makers and the law enforcement.
- Expand the aforementioned 'cyber security awareness survey' into a national level survey to gather data that could be useful in identifying training needs when educating the public.

CONCLUSION

Since its establishment in 2006, Sri Lanka CERT|CC has successfully increased the public's awareness of its presence and the nature of the activities it is involved in. It has been possible to achieve this target through the use of seminars, conferences and the use of mass media. This has led to an increase in the number of incidents reported and handled by Sri Lanka CERT|CC in the past consecutive years.

During 2015, majority of the incidents reported to Sri Lanka CERT were related to social networking sites and various malicious activities such as account hijacking and fake account creation. These were typically motivated by revenge, extortion or malicious software distribution.

All the events organized by Sri Lanka CERT during the year 2015 were very successful, well attended and were high in demand. We will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security. In the future, Sri Lanka CERT|CC will find new ways to reach an even wider audience and maintain a calendar of regularly running technical and management training workshops.

Sri Lanka CERT|CC shall continue to participate in regional events such as the Annual APCERT cyber security drill and also welcomes opportunities to collaborate with its sister CERTs in incident coordination and resolution.

Lack of explicit legal regulations regarding the responsibilities for notification, responding, prevention and mitigation of cyber security incidents by the state institutions or companies in the private sector is one of the main difficulties encountered in handling incident response activities and real-time response to such incidents. In this context, we considered it necessary to supplement the national legislation framework with the stipulations contained in certain documents that are found at European level.

In this respect, one of the key achievements this year was Sri Lanka's ratification of the UN Electronic Communications Convention. This was another first for South Asia and ensures greater legal certainty for e-Commerce and e-Business providers who will want to use Sri Lankan law as the applicable law and ensure International validity for such e-Contracts. Ratification of this Convention will also ensure legal validity for Electronic Bills of Lading and other International legal instruments, enhancing the ability for Sri Lanka in its move towards paperless trade facilitation, whilst further strengthening the use of Technology Neutral authentication frameworks under National Certification Authority (NCA) Project.

The other key achievement in this respect was when the Government of Sri Lanka was invited to accede to the Budapest Convention on Cyber Crime in February 2015. This is the only international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. In addition to harmonizing the domestic criminal law for offences connected to provisions in the area of cyber-crime, the main benefit to Sri Lanka from this initiative was the setting up of a fast and effective regime of international cooperation

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.