Sri Lanka Computer Emergency Readiness Team | Coordination Centre

2012 Annual Report

TABLE OF CONTENTS

1. About Sri Lanka CERT 4
1.1 Introduction 4
1.1.1 Establishment 4
1.1.2 Workforce 4
1.1.3 Constituency 4

2. Activities & Operations 6
2.1 Incident Handling Statistics 6
2.2 New services 7
2.3.1 Setting up sector based CSIRTs 7
2.3.2 Blocking Phishing sites 7
3. Events organized / co-organized 9
3.1 Training / Education 9
3.2 Consultancy 9
3.3 Seminars & Workshops 10

4. Achievements 12
4.2 Publications & Other media 12
4.3 Certification & Membership 12

5. International Collaboration 14
5.1 MoU 14
5.2 Event participation 14

6. Future Plans 16
6.1 Future projects 16
6.2 Framework 16
6.2.1 Future Operations 16
6.2.2 Operational Support Projects 16

7. Conclusion 18

1. ABOUT SRI LANKA CERT

1.1 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 responses to cyber security threats and vulnerabilities.

1.1.1 Establishment

As the national CERT of Sri Lanka, Sri Lanka CERT acts as the focal point for cyber security for the nation. It is the single trusted source of advice about 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.

It was anticipated that cyber security incidents in Sri Lanka would increase dramatically due to IT infrastructure growth as a result of the National ICT Policy related activities, primarily, the e-Sri Lanka initiative and ICT revenue generation activities. Sri Lanka CERT therefore 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 the ICTA, which in turn is fully owned by the Government of Sri Lanka.

In early 2011, Sri Lanka CERT | CC, along with its parent body, the ICTA was brought under the purview of the newly formed Ministry of Telecommunications and ICT.

1.1.2 Workforce

Sri Lanka CERT currently has a total strength of nine team members consisting of the Chief Executive Officer, a Principal Information Security Engineer, an Administrative Officer, five Information Security Engineers and an IT Assistant. This team is supported by four 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 $(ISC)^2$ CISSP.

1.1.3 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.

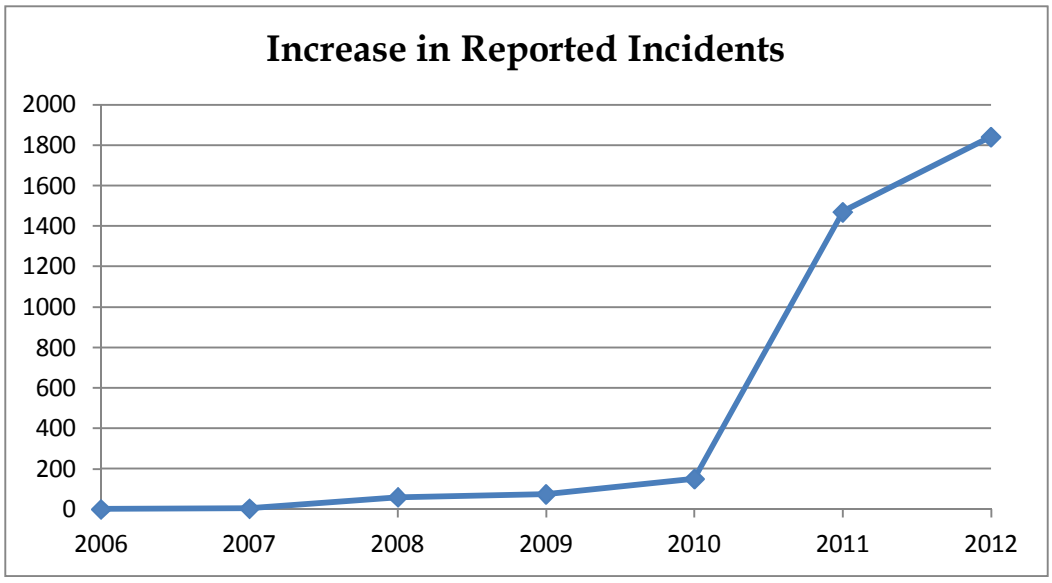
2. Activities & Operations

2.1 Incident Handling Statistics

Incidents reported to Sri Lanka CERT increased to 1,840 in the year 2012. In the year 2011, it was 1,469 incidents were reported. This is a 25% increase in reported incidents compared to the year 2011. The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	No
Phishing	3
Abuse/Privacy	16
Scams	3
Malware	0
Defacements	15
Hate/Threat Mail	1
Unauthorized Access	1
Intellectual property violation	0
DoS/DDoS	1
Fake Accounts	1,800
Total	**1,840**

The following graph depicts the increase in the number of incidents since the inception of Sri Lanka CERT in mid-2006.



2.2 New services

2.3.1 Setting up sector based CSIRTs

Sri Lanka CERT initiated the setting up of sector-based CSIRTs in 2010. Typical sectors are Banking, Telecom, Defence and Education. The Bank CSIRT is already operational while the Defence CSIRT is in its implementation stage and the Telco CSIRT concept paper is awaiting approval from the Telecom Regulatory Commission (TRC) Board, which the intended host body. The Education CSIRT is in the concept phase.

The rationale for sector based CSIRT's is to ensure that Sri Lanka CERT 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.

The net result of setting up sector based CSIRTs and certifying and coordinating the activities of these CSIRTs is that Sri Lanka CERT has now transformed itself to being a true coordinating body.

Sector-based CSIRTs will provide industry specific services to their constituents. For example, The Telco CSIRT will provide content filtering services to ISPs while Bank CSIRT provides vulnerability alerts specific to banking applications and implements security standards to ensure a minimum level of security compliance within the industry.

2.3.2 Incident handling - blocking Phishing sites

Since it takes considerable time to take down the phishing sites targeting local banks of Sri Lanka, a process was established to block the sites locally with the help of TRC (Telecommunication Regulatory Commission) Sri Lanka and the ISPs. This will minimize the damage caused to on-line banking customers during the time of taking down those phishing sites with the help of international CERTs and ISPs.

2.3.3 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 the first 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) CA for Government establishments and Lanka Sign CA (for Banks) exist, the universal acceptance of their certificates is in question. To address this issue, Sri Lanka CERT, ICTA (the apex body for ICT in Sri Lanka) and various stakeholders have come together to form a task force to determine the policies, procedures, governance and service models of the national CA. The end objective is to have a national level body which will effectively regulate the issuing of a number digital certificate classes at affordable prices that are in accordance with the local legislation and international standards.

2.3.3 Vulnerability Assessments – Formal procedure for security testing government websites

In year 2012 all of the government website assessments were carried out according to the formal procedure which was established in year 2011 by Sri Lanka CERT with ICTA and GIDC NOC involvement. ICTA was the primary contact point when dealing with website security assessments for government sites which are hosted at GIDC NOC. Sri Lanka CERT produced all of the assessment reports and final approval for website hosting documents based on a format which was agreed by both ICTA and Sri Lanka CERT.

3. Events organized / co-organized

3.1 Training / Education

In order to fulfill its mandate to create awareness and build IS skills within the constituency; Sri Lanka CERT continues to organize training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and General Public.

During the year 2012 Sri Lanka CERT conducted the following training and education programs successfully:

a. Presentation on "First Responders responsibility on computer related crimes"
b. Seminar series on "Internet safety for School Children" for School Children

Sri Lanka CERT staff has in addition continued to assist in the delivery of courses in Computer security topics at tertiary education institutions.

Publication of leaflets and posters designed for distribution at seminars, exhibitions and other forums is a key strategy for Sri Lanka CERT's awareness campaign.

3.2 Consultancy

Sri Lanka CERT continues to provide consultancy services in response to requests made – particularly from government departments.

Typical consultancy services provided during the year 2011 included;

a. Security Policy development workshops for government organizations
b. Forensics investigation support for Law enforcement
c. Configuration reviews for critical government organization information systems
d. Network Security assessments for several banks
e. Application security assessments for financial institutions
f. Investigation of a financial fraud in a leading bank

3.3 Seminars & Workshops

a. Cyber Security Week 2012

   Since 2008, Sri Lanka CERT | CC has been conducting an annual security awareness program titled Cyber Security Week (CSW). This international event draws attention of the local as well as regional information security professionals.

   The objectives of this program are to:

- Build awareness and update knowledge on key security areas that matter both locally and globally, commercially and personally
- Understand emerging technologies and the security issues pertinent to those technologies
- Provide a meeting ground for like minded individuals with a special interest in information security to forge alliances, share knowledge and experience and build consensus on security issues of the day

The flagship event of CSW each year is the Annual National Conference on Cyber Security.

Cyber Security Week 2012 was held in the month of December, and featured a series of events:

- Annual National Conference on Cyber Security

- Two full-day Workshops for professionals, namely:

  - Technical workshop on "OWASP ESAPI: making it work for you"
  - Technical workshop on "Practical secured software security testing"

- Hacking challenge;

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

4. Achievements

4.2 Publications & Other media

a. Website

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

b. E-mails

Disseminating security related information via e-mail alerts to Sri Lanka CERT website subscribers. The Cyber Guardian e-newsletter was initiated in mid-2011 and is distributed to a large number of students by the Ministry of Education, through the SchoolNet the network connecting secondary schools in Sri Lanka.

c. Newspapers/media

Sri Lanka CERT 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 against these attacks.

4.3 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 "IMPACT". Sri Lanka CERT will benefit from receiving a threat feeds from the region and also form part of the global incident response team

Sri Lanka CERT is represented on the board and steering committee of the Information Systems Security Association (ISSA) Sri Lanka Chapter, and is involved in the planning its membership drive and strategic partnership formation efforts

Sri Lanka CERT is also actively supporting the formation of SLSEC, a proposed online forum where security enthusiasts can get help from fellow security enthusiasts. The forum will be managed by a governing body consisting of Sri Lankan representatives in Sri Lanka as well as overseas. The site will be hosted and managed, by Sri Lankan expatriates.

The most important achievement to-date in this respect is Sri Lanka CERT's role in the setting up of the Sri Lanka Chapter of the International Information Systems Security Certification Consortium, Inc., commonly referred to as the (ISC)², and widely accepted as the global, non-profit leader in educating and certifying information security professionals throughout their careers. The Sri Lankan Chapter was formed with the objective of

disseminating knowledge and providing a common forum for the information security professionals, the (ISC)² credential holders. In addition, the Chapter encourages Information Security certifications among professionals in Sri Lanka. This has now evolved to being a fully fledged association that serves as the main 'focus' group for Information Security Professionals in the country and Sri Lanka CERT continues to facilitate it's growth.

5. International Collaboration

5.1 MoU's

In addition to being members of FIRST and APCERT, Sri Lanka CERT has signed Memoranda of Understanding (MoU) with Microsoft, to be a member of Microsoft Security Cooperation Program (SCP) and with IMPACT, the security arm of ITU.

Sri Lanka CERT has signed MoUs with Team Cymru, Tsubame and Shadowserver; as a result of above MoUs Sri Lanka CERT gets daily statistics for its "Threat Visualization System" which is used for alerting ISPs about possible suspicious network traffic.

5.2 Event participation

March 25th -28th, 2012
APCERT AGM & Conference
Bali-Indonesia

April 20th - May 5th, 2012
USTTI training on cyber security
Washington, USA

June 16th -25th, 2012
FIRST AGM & Conference
Malta

July 6th –8th, 2012
CISSP Asian item writing workshop
Singapore

July 7th –14th, 2012
APISC training (KrCERT|CC)
Seoul, Korea

October 24th – November 3rd, 2012
CyberLympics at HackerHalted
Miami, USA

October 19th – 31st, 2012
USTTI training on cyber security
Washington, USA

November 16th, 2012
Asian Oceanian Computing Industry Organization (ASOCIO) International Conference 2012, Cyberjaya, Malaysia

5.3 International incident coordination

Sri Lanka CERT|CC actively participated in the APCERT Drill 2012 as a player.

In addition to the engagements with CERTs the Asia Pacific region, Sri Lanka CERT has regular operational engagements with CERTs/Information security organizations in other regions of the world and commercial organizations (such as Facebook, Google, Yahoo) to handle phishing, identity theft incidents.

6. Future Plans

6.1 Future projects

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

a. Development and Implementation of the National Certification Authority
b. Implementation of the Telco CSIRT
c. Development and implementation of the Defense CSIRT
d. Conceptualization, development and implementation of the Edu-CSIRT
e. Cyber Security Week 2013

6.2 Framework

6.2.1 Future Operations

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

a. Recruitment of undergraduate students on internships on an annual basis to enhance the information security capabilities of the younger generation.
b. Continue to operate as a small focused group of professionals, but building sufficient skills nationally to combat and prevent cyber crime.

6.2.2 Operational Support Projects

Sri Lanka CERT continues to maintain a sensor for the JPCERT/CC hosted TSUBAME Internet Scan Data Acquisition System project, while collaborating with the Dragon Research Group (DRG) based in Brazil by deploying a sensor to collect and monitor data to identify emerging threats.

Further, it is planned to place the sensors at all ISP networks to cover the IP blocks in order to gather data on attack traffic generating to and from the country. The Sri Lanka Telecom has agreed to place a sensor in the network which will facilitate the coverage of a large part of IP's in the country.

All this information, coupled with the Automated Threat Analysis and Visualization tool will enable Sri Lanka CERT to spot potentially vulnerable incidents at a glance and proceed to take remedial measures.

7. Conclusion

After starting Sri Lanka CERT in year 2006, it was necessary to conduct awareness campaigns to notify the public about our presence and the activities. Through the use of seminars and conferences and through the use of mass media it was possible to achieve this target which resulted increase in number of incidents reported and handled by Sri Lanka CERT in the past consecutive years.

During this year most of the incidents reported to Sri Lanka CERT were related to phishing sites and various activities conducted through social networking sites, 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 2012 were very successful and had huge demand. We will continue to conduct the Annual Computer Security Week and the Annual National Conference on Cyber Security while finding new ways to reach an even wider audience, and also maintain a calendar of regularly running technical and management training workshops.

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

Sri Lanka CERT is committed to build a secure information environment in the Asia Pacific region with the help of all the CERTs and information security organizations through APCERT.