2017

A Sri Lankan hacking case study

Ishan Senarathna
Deakin University

Matthew Warren
Deakin University

DOI: 10.4225/75/5a84fb0495b50
Senarathna, I, & Warren, M. (2017). A Sri Lankan hacking case study. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.64-69).
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/204

A SRI LANKAN HACKING CASE STUDY

Ishan Senarathna, Matthew Warren
Deakin University Centre for Cyber Security Research, School of Information Technology, Faculty of Science,
Engineering and Built Environment, Deakin University, Victoria, Australia
ishan.senarathna@deakin.edu.au, matthew.warren@deakin.edu.au

Abstract

The aim of the paper is to consider how hacking could impact a country that had historically experienced major cyber-attacks. The aim of the paper is to explore a cyber incident that occurred against the Sri Lankan president and how Sri Lankan authorities reacted to the incident. The paper will focus upon the motivations of the attack, the impact of the attack and how Sri Lankan authorities reacted to the situation.

Keywords: Hacking, Government and Sri Lanka.

INTRODUCTION

We have seen a rise in computer misuse at a global level; in many cases “Hackers” have been found responsible for these attacks. Hackers are often characterised as adolescent males in dark bedrooms that can cause damage to global IT systems through using their computers and computer skills. A more romantic perception portrays hackers as being determined cyber knights, who use personal codes of conduct to live by and are reminiscent of the great Arthurian knights (Warren and Hutchinson, 2003). Moreover, “hacker” is what computer-intruders choose to call themselves, not as a criminal pejorative, but as a noble title given to those “soaked through with heroic anti-bureaucratic sentiment” (Sterling, 1993). Hacking then, can describe the determination to make access to computers and information as free as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and the spirit (Levy, 1984).

Contrasting this romantic perception is the way Bruce Sterling (1993), portrays “Hacking” in his book titled ‘The Hacker Crackdown’. In Sterling’s (1993) book, “Hacking” is described as the act of intruding into computer systems by stealth and without permission. However, Sterling’s definition of “Hacking” is broader than the one used routinely by most enforcement officials with any professional interest in computer fraud and computer abuse. The enforcement officials’ focus on “Hacking” relates to crimes committed with, by, through, or against a computer (Warren and Hutchinson, 2003).

But when happens when a country that has never experienced major cyber incidents becomes victim to a high profile cyber incident. In terms of the paper it reflects upon Sri Lanka. Sri Lanka is an island located of the coast of India and has a population of 22 million people, of the Sri Lankan population 7.1 million (32%) are Internet users (CIA, ND).

The paper intends to answer one key research question:

> What were the motives and impacts in relation to the Sri Lankan President’s Cyber incident.

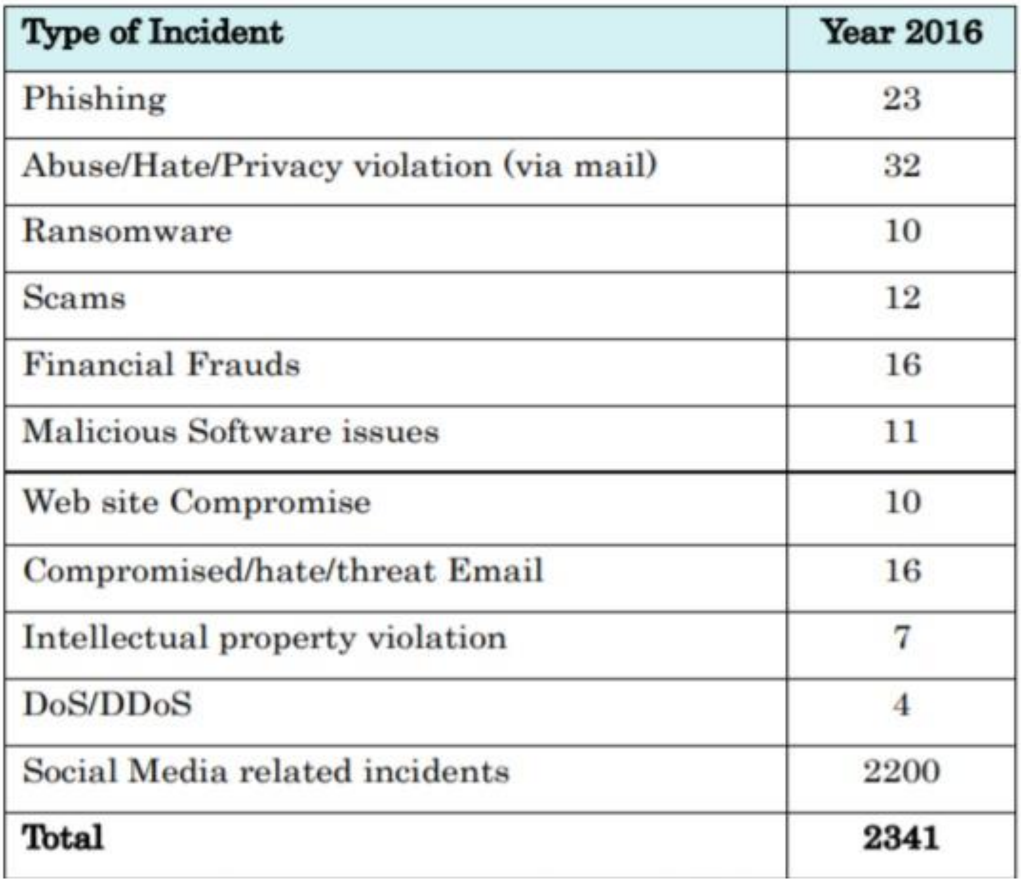
OVERVIEW OF SRI LANKA

The Sri Lankan authorities in anticipation of increased cyber security incidents that Sri Lanka could face and the growing ICT infrastructure across Sri Lanka, the Sri Lanka Computer Emergency Readiness Team | Coordination Centre (CERT|CC) was established as Sri Lanka’s National CERT, by the ICT Agency of Sri Lanka to protect against Sri Lanka’s future Cyber incidents, (Sri Lanka Cert, ND).

The role of the Sri Lanka CERT|CC has developed over time, it has now become 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 (Sri Lanka Cert, ND).

Sri Lanka has had a history of cyber incidents, the following table depicts the distribution of various types of incidents reported to Sri Lanka CERT during 2016 (APCert, 2016). All the incidents reported to Sri Lanka CERT had been resolved satisfactorily.

Table 1: Sri Lankan Cyber Security Profile Incidents (2016) (AP, 2016)



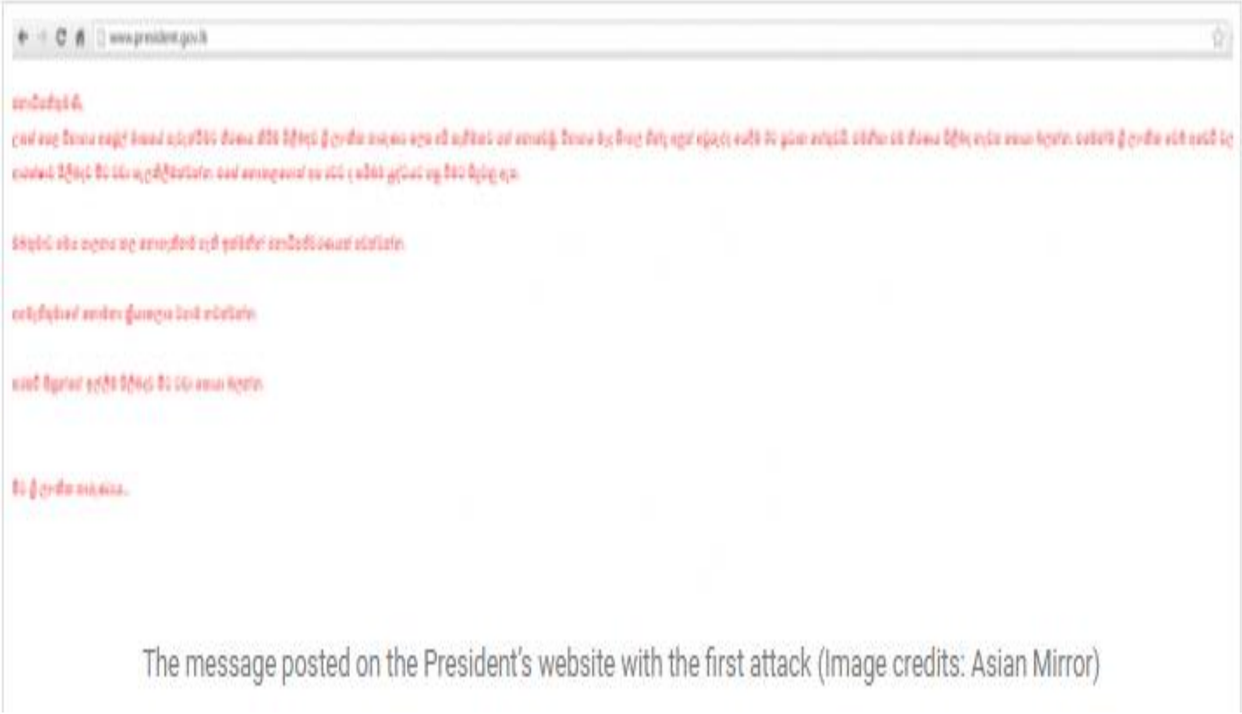
Type of Incident	Year 2016
Phishing	23
Abuse/Hate/Privacy violation (via mail)	32
Ransomware	10
Scams	12
Financial Frauds	16
Malicious Software issues	11
Web site Compromise	10
Compromised/hate/threat Email	16
Intellectual property violation	7
DoS/DDoS	4
Social Media related incidents	2200
Total	**2341**

The majority of issues that have been reported to the Sri Lankan CERT|CC related to social issues relating to social media and related issues such as cyber bullying, the “social media” type of cyber incidents represented 94% of the cases that Sri Lankan CERT|CC had to deal with and would relate to issues such as cyber bullying.

CASE STUDY

On the 25th August the official website of the Sri Lankan President Maithripala Sirisena, (www.president.gov.lk) suffered two cyberattacks on two consecutive days by a group who identified themselves as 'The Sri Lankan Youth' (BBC 2016, DNA 2016, Doole and Thomas 2016, Read Me News 2016, Yahoo, 2016).

The first attack took place on the 25th August 2016, the existing site was removed and replaced with a message. The message that was posted on the home page is shown in Figure1. The president site was hacked on Friday, August 26 with a message being posted in in Sinhala (Wollerton 2016). In the first message, the hacking group made a number of demands to the Sri Lankan government. One of these demands being a request to reconsider the decision to hold the GCE A/Level examination in April rather than in August. In addition, it also commented to the Government to be more conscientious regarding the security of Sri Lankan websites. If no action were to be taken with that regard, the country will have to be face a “cyber war” (Molloy 2016, Read Me News, 2016).



The message posted on the President's website with the first attack (Image credits: Asian Mirror)

Figure 1: The First Hacking Incident

The English translation of the first message from the hacking incident posted in Sinhalese was:

"Dear Mr. President,

We are extremely displeased about the decision to hold GCE A/L in April since the Sinhala/Hindu New Year falls in between the exam dates. Therefore, reconsider that decision. Furthermore, take care of the security of Sri Lankan websites. Or else, we will have to face a cyber war.

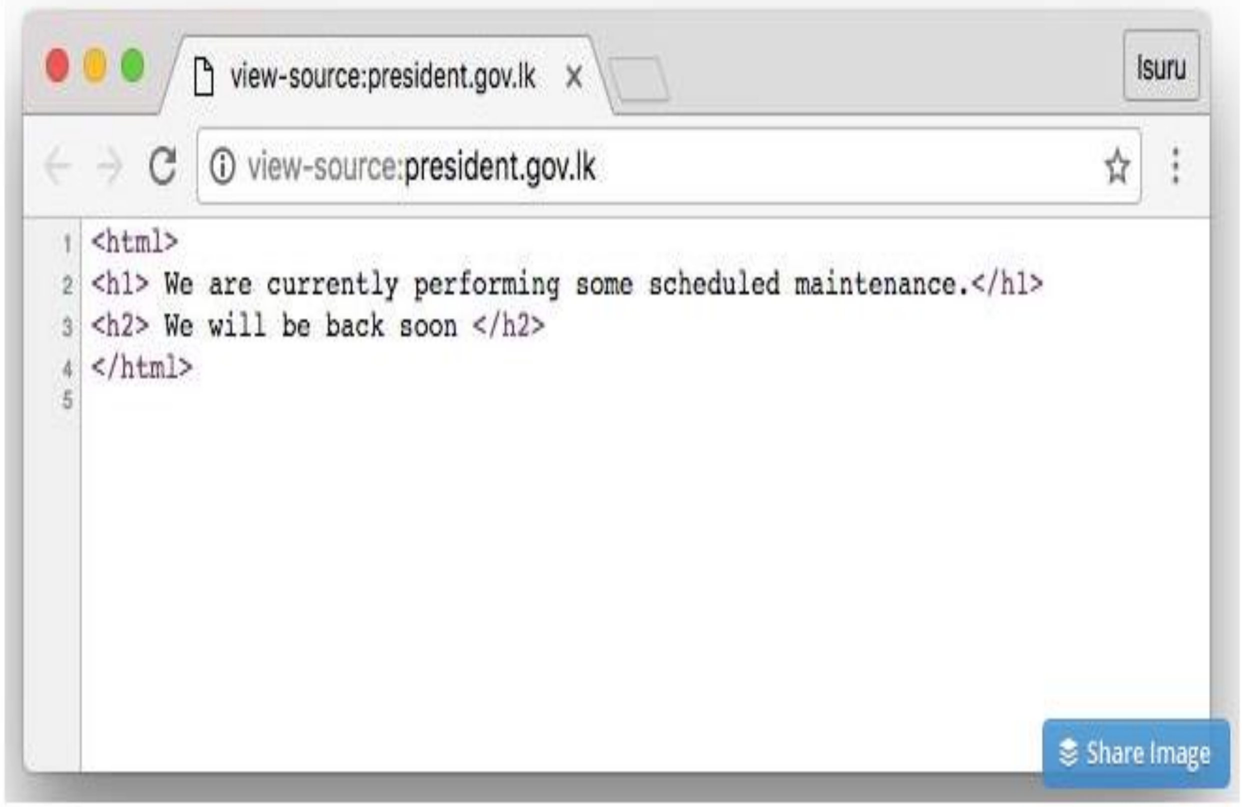
If you cannot control the situation hold a Presidential Election.

Stop the Prime Minister's irresponsible work.
Look more into the problems of the university students.

The Sri Lankan Youth"

The first message posted in Sinhalese was a political message which included the stopping of 'irresponsible conduct' by the Prime Minister and hold a presidential election if the president cannot control the situation. The message also directed the Government to pay more attention to the problems faced by university students.

After the first attack, the site was taken offline for a few hours and then the Presidents site returned to normal operations. But on the 26th August the Presidents site as hacked again, this time a message in English was posted (see Figure 2). The message made no demand, just stating that the site was down for maintenance and the site was quickly restored.



```
<html>
<h1> We are currently performing some scheduled maintenance.</h1>
<h2> We will be back soon </h2>
</html>
```

The HTML page of the president's website after the second attack (Image credits: Isuru Samarasinghe)

Figure 2: The Second Hacking Incident

WHO WAS RESPONISBLE

A group or individual known as the "The Sri Lankan Youth" was suspected to be responsible for the initial attack. Following the incident, a 17-year school boy from Kandy was arrested by the CID (Criminal Investigation Department) for allegedly hacking the website. Further, the CID arrested another 27 year old and charged him with hacking the President's website (Gossip News 2016). Under the Sri Lankan Computer Crimes Act, the unnamed boy who was arrested, and could face a possible fine of Rs. 300,000 (Sri Lankan rupee) and subsequent could face up to three years in jail (Doole and Thomas 2016, Read Me News, 2016).

The Sri Lanka Computer Crimes Act was enacted by the Sri Lankan Parliament and certified by the Speaker as the Computer Crimes Law No. 24 of 2007 with the aim of the protecting Sri Lanka against Cyber Crimes and these was the first arrests in connection to this law (Guardian, 2016).

According to CID, the arrested school boy had illegally accessed more than 37 websites and a Facebook account named 'arrow.lk' had been identified in connection with altering data and entering data (Doole and Thomas 2016). Further, the CID has informed that a group named 'Yakadaya Forums' on Facebook was involved in collecting and sharing information about security weaknesses links to certain hosting websites.(Doole and Thomas 2016).

DISCUSSION

The Sri Lankan President's web-site is a simple news website created for the purposes of disseminating information and news relating to President Sirisena and his activities and a way of connecting to the Sri Lankan public.

The President website was hosted on WordPress, a free and open-source content management system which is a popular choice for people to host their blogs and personal websites (Doole and Thomas 2016, Metzger 2016). The security issue here related to the fact that the WordPress site was not correctly configure and some blame poor security standards on the website as the cause of the problem (Metzger 2016).

The President's website hack was linked to a manipulation of the original program code (script) of the website. The hackers themselves had limited experience who use existing computer scripts or code to hack into computers. They lack the expertise to write their own program code to hack others websites and obtained the information they needed for the hack through the Facebook forums they were linked to (Doole and Thomas 2016). It was also determined that the second hacking incident was also linked to the first hacking incident (Daily News, 2016).

In terms of the paper's research question:

> What were the motives and impacts in relation to the Sri Lankan President's Cyber Incident.

In terms of the motives of the hacking incident the hacker's motivation was to highlight his displeasure that examinations had been scheduled for April, during the traditional Sinhala and Tamil New Year holidays. The motivations reflect that of a young person who was frustrated by the timing of a School exam and decided to hack the Presidents web-site to vent his frustration.

From a forensic perspective, not much information has been shared by the Sri Lankan authorities regarding the situation but following was determined:

1) After the first hacking incident, the Sri Lankan law enforcement agencies took over the operations of the Presidents web-site and very quickly reacted to the second hacking incident;
2) Very quickly the two individuals involved in the incident were identified and arrested by Sri Lankan authorities;
3) The security weakness on the President's WordPress site was quickly identified and corrected;
4) The Sri Lankan authorities used social media to collected information about the attackers and determine which Facebook groups where code exploits and other information had been exchanged.

The damage caused by the incident was limited and only impacted the credibility of the Sri Lankan authorities to protect the Presidents web-site.

The case just highlights a number of issues:

1) The problem of hosting government web-sites on third party web-sites where limited security systems may be in place;
2) The ability of unskilled attackers to use the Internet to download scripts to exploit security weaknesses, in this case being given the script via Facebook forums;
3) The role of media in portraying the defacement of the Sri Lanka Presidents web-site as a major "Cyber incident" and escalating the situation;
4) The capabilities of Sri Lanka authorities to quickly analyse the attacks and respond to the incident and arrest those connected.

CONCLUSION

The case is linked to a Sri Lankan teenager who hacked the president's website to try to reconsider the decision to hold the GCE A/Level examination in April rather than in August. In terms of this incident, it is a classic hacking incident based upon simple motivations of a single individual. The case does highlight the problem that governments have when using third party sites and services on behalf a national government official.

The outcome was that the case against the people arrested was dropped and the teenager behind the incident had to meet the President in person. During the meeting with the Sri Lankan President, he stated "It's our duty to encourage our youngsters to use their talents ethically" (Daily News, 2016).

REFERENCES

AP (Asian Pacific) Cert (2016) Annual Report, URL: https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2016.pdfsite accessed: 7/10/17.
BBC (2016). "Sri Lankan teenager held over hacking of president's website." from http://www.bbc.com/news/world-asia-37214629. site accessed: 7/10/17.
CIA (nd) Sri Lanka, URL: https://www.cia.gov/library/publications/the-world-factbook/geos/ce.html, site accessed: 7/10/17.
Daily News (2016). URL: http://dailynews.lk/2016/11/18/local/99473, site accessed: 7/10/17.

DNA (2016). "Sri Lankan President Maithripala Sirisena's website hacked twice within two days." URL: http://www.dnaindia.com/world/report-sri-lankan-president-maithripala-sirisena-s-website-hacked-twice-within-two-days-2249709, site accessed: 7/10/17.

Doole, C. and Thomas K.C. (2016). "President's website Hack: The Full Story." URL: https://web.archive.org/web/20170118162646/http://www.ceylontoday.lk/print20160701CT20161030.php?id=5042, site accessed: 7/10/17.

Levy, S (1984). Hackers: Heroes of the Computer Revolution, Anchor Press, USA.

Guardian (2016) "Sri Lankan teenager hacks president's website to try to get exams delayed". URL: https://www.theguardian.com/world/2016/aug/30/sri-lankan-teenager-hacks-presidents-website-to-try-and-get-exams-delayed, site accessed: 7/10/17.

Gossip News (2016). "How Harshana and Janith who hacked President Website were cornered." URL: http://www.english.gossiplankanews.com/2016/08/how-harshana-and-janith-who-hacked.html, site accessed: 7/10/17.

Metzger, M. (2016). "Teenager hacks Sri Lankan president's website to protest exams." URL: http://www.scmagazineuk.com/teenager-hacks-sri-lankan-presidents-website-to-protest-exams/article/520647/, site accessed: 7/10/17.

Molloy, M. (2016). "Teenager accused of hacking president's website to try and get exams postponed ". URL: http://www.telegraph.co.uk/news/2016/08/30/teenager-accused-of-hacking-presidents-website-to-try-and-get-ex/, site accessed: 7/10/17.

Sterling B (1993). The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Mass Market Paperback, USA.

Sri Lanka Cert (nd) http://www.slcert.gov.lk/aboutUs.php, URL: http://www.slcert.gov.lk/aboutUs.php, site accessed: 7/10/17.

Read Me News (2016). "The President's Website Was Hacked: Here's What We Know ". from http://www.readme.lk/presidents-website-hacked/, site accessed: 7/10/17.

Yahoo (2016). "Sri Lanka police arrest teen over hacking president's website." from https://www.yahoo.com/news/sri-lanka-police-arrest-teen-over-hacking-presidents-192221299.html, site accessed: 7/10/17.

Warren, M.J and Hutchinson W. (2003). Australian Hackers Ethics, Australian Journal of Information Systems, Vol 10, No 2, pp. 151 – 156.

Wollerton, M. (2016). "Sri Lankan teen hacks president's website to delay exams." from https://www.cnet.com/au/news/sri-lankan-teen-hacks-presidents-website-to-delay-exams/, site accessed: 7/10/17.