Analysis of the Australian Web Threat Landscape

Christopher Ke, Jonathan Oliver and Yang Xiang

Deakin University,
221 Burwood Highway, Burwood, Victoria 3125, Australia
Trend Micro
606 St Kilda Road, Melbourne, Victoria 3004, Australia

Abstract. This report discusses threats on the Australian web landscape. We analyse web logs and provide statistics on what is happening to the average Australian user of the world-wide web. The analysis covers aspects such as the volume and timing of web threats attacking Australians and the source geography of the malicious activity. We look at a case study of a web attack that had global reach and describe the impact of this attack on Australian web users.

Keywords: Web Threats, Web Security, Australian Threat Landscape, National Broadband Network, NBN.

1 Introduction

Australia is a remarkably Internet-dependent country with a relatively small population. The Internet has become vital for Australia's day-to-day working and living. In 2009 the Australian Government launched its $43 billion National Broadband Network (NBN) project, which aims to provide superfast broadband to Australian homes and workplaces [6]. The Internet offers attackers a powerful infrastructure to compromise victims' systems.

An Australian Research Council (ARC) Linkage Project on web threat research, supported by the ARC, Deakin University, Macquarie University, and Trend Micro, was launched in February 2013. We are processing data from the WRS (Web Reputation Solution) and the SPN (Smart Protection Network) systems developed by Trend Micro [1, 2]. The primary source of data used in this study is the WRS data source which each day collects 4.8 TB of data, consisting of 10 billion queries. Of these 10 billion queries, 14.38 million queries are identified as malicious.

The dataset in the WRS and the SPN systems is comprised of Trend Micro customer opt-in URL filtering records and feedback data. In the dataset, we are able to observe the diversity of malicious activities occurring all over the world. However, from an Australian perspective, we focused on the web threats which attacked Australian computer users and/or which are hosted in Australia. As Trend Micro products currently take a substantial portion of the computer security market share in Australia, it is believed the data is informative and representative of the day-to-day situation of Australian cyberspace. This report describes the web threat landscape of Australia.

2 Statistical Report

2.1 Definition of Terms

Before analysing the statistical data, we need to define the terms used in this report.

A “web hit” is an HTTP/HTTPS transaction initiated by a browser or other program. It may be a GET or POST transaction. In simple terms, a web hit is when a browser downloads a URL. Downloading a web page typically has multiple web hits, since each image and other component of the page are downloaded separately.

A “web threat” is a malicious page or script on a web server. There are multiple types of web threat including:

- Landing pages of exploit kits and other pages which attempt to download malware onto the users system,
- Phishing web pages,
- Compromised pages on legitimate web servers that redirect the user's browser to other malicious pages – such as landing pages, and
- Command and Control (C&C) servers

Hence, a malicious hit is a transaction where Trend Micro WRS has identified before the time of the web request that the web traffic was malicious.

2.1 Web Threats Attack Australian Internet Users

We monitored the live web traffic for a two-week period in May 2013. On average, computers from nearly 600,000 distinct public IPs in Australia surfed the web sites through HTTP/HTTPS protocols on the Internet every day, which generated approximately 200,000,000 web hits per day.

Over 400,000 requests from around 80,000 IPs were issued to malicious web pages. On a typical day, one in seven or eight active Australian Internet addresses had been exposed to one (or more) web threats. However, the real ratio of users exposed to web threats will be lower as many desktops are most likely to access the Internet through NATs (Network Address Translators).

To further investigate the behaviour of Australian Internet users, we collected time-windowed volumes of web/malicious hits issued by the IPs situated in Australia. Fig. 1 shows the daily traffic distribution between 1st May and 15th May in 2013. The peak days were all workdays whilst the numbers of web hits substantially decreased during the weekends. As for the ratio of malicious traffic, the curve reversely vibrates along with the volume changes of web hits. The average percentage of daily malicious hits was 0.31%, but numbers could be as low as 0.21% and as high as 0.43% during workdays and holidays respectively. Similar disproportionate trends also occurred in the hourly distribution of a typical weekday, 15th May 2013 but the deviations were even bigger, as demonstrated in Fig. 2, where the smallest percentage is 0.19% in the work hours and the largest one is 0.46% around 4am.

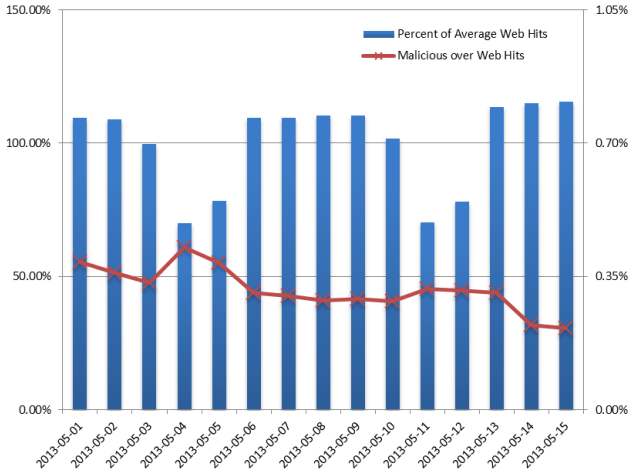

Fig. 1. Daily traffic distribution between 2013-05-01 and 2013-05-15 by Australian users

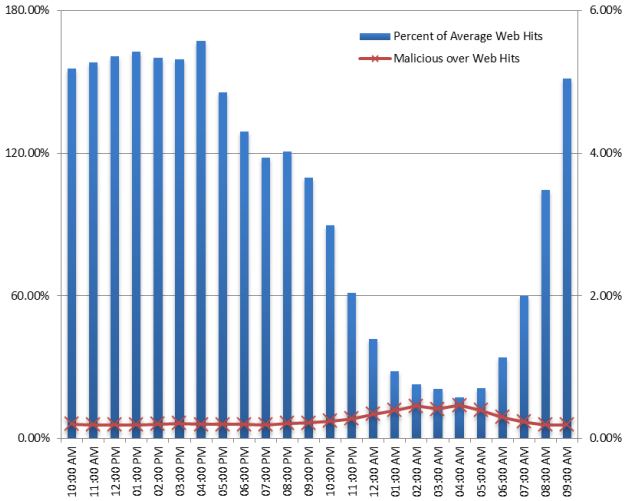

Fig. 2. Hourly traffic distribution between 2013-05-15 10AM and 2013-05-16 9AM (AEST) by Australian users

Fig. 3 lists the countries of the web hosts where the traffic originating from an Australian user went to a malicious web site or malicious page were hosted.
As expected, the US is the number one, but AU was ranked 7th, which indicates that some attacks were specifically targeted at Australians.

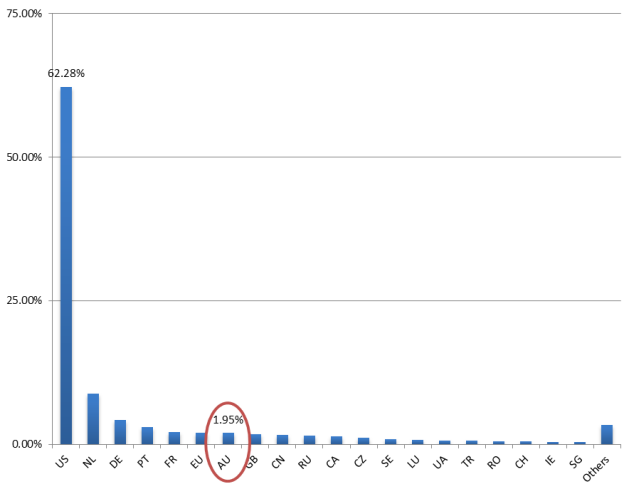

Fig. 3. Malicious host country ranking

We categorised the Trend Micro products into consumer products, business products, email products and others, and proportions of their contribution are displayed in Fig. 4. Just above half of malicious traffic was triggered by business product users whilst consumer product users accounted for over a third.

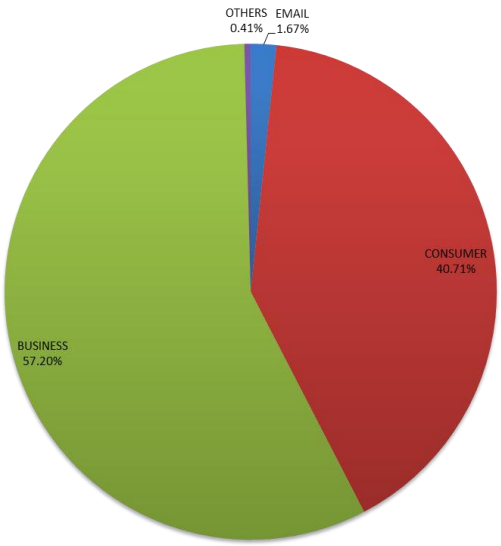

Fig. 4. Malicious hits detected by different product types

2.2 Web Threats Hosted in Australia

We are also interested in the traffic where the destination servers were hosted in Australia. Our sample included 40,000,000 visits per day to Australian web sites attracted around, in which about 16,000 hits were identified as malicious. As can be seen in Fig. 5, the distribution also links to the calendar of workdays and weekends, but the ratio of malicious hits remains nearly constant (0.04%).

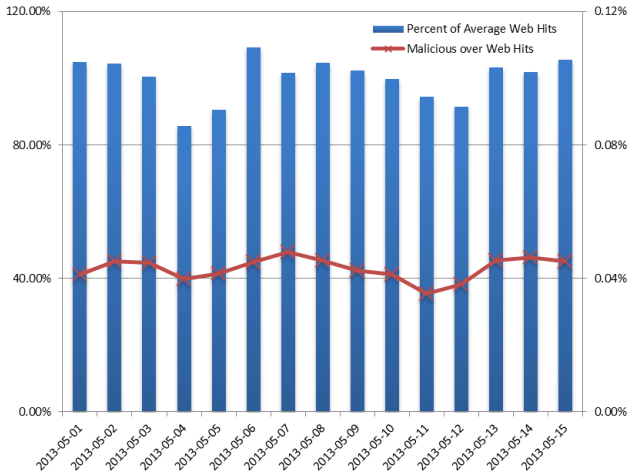

Fig. 5. Daily traffic distribution between 2013-05-01 and 2013-05-15 by Australian servers

Also, the victim country ranking for web hits on web servers hosted in Australia are listed in Fig. 6. AU being the first ranked in Fig. 6 is to be expected due to the majority of visitors to Australian web sites are Australians. Looking at the details of the WRS data, the traffic was generated from visiting web pages delivered by CDN (Content Delivery Network) and AWS (Amazon Web Service), which naturally resulted in special regionalised attacks if the malicious pages are hosted in compromised web sites that employ these services.

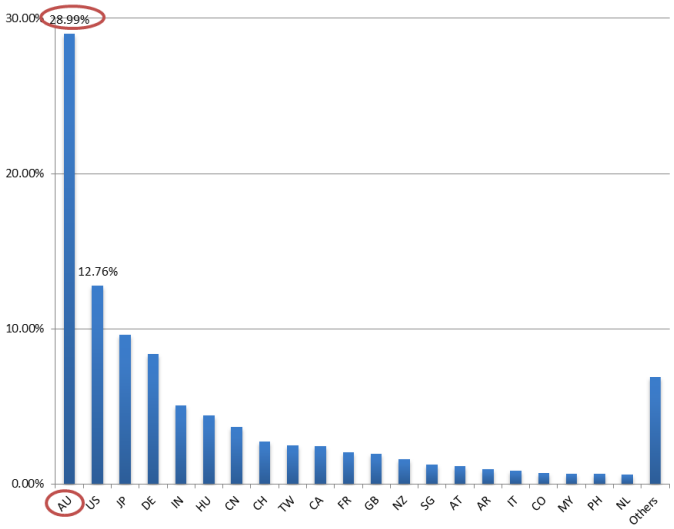

Fig. 6. Malicious victim country ranking for servers hosted in Australia

3 Examples of Typical Web Attacks

To give an understanding of a web attack, we examined two typical web attacks that were related to the Boston Marathon bombing occurred on 15 April 2013.

- A spam run that took the victim's browser to a Blackhole Exploit Kit (BHEK) landing page, and
- A spam run that attempted to infect users with the Kelihos worm

3.1 Blackhole Exploit Kit

The BHEK outbreak was initiated with a piece of spam.

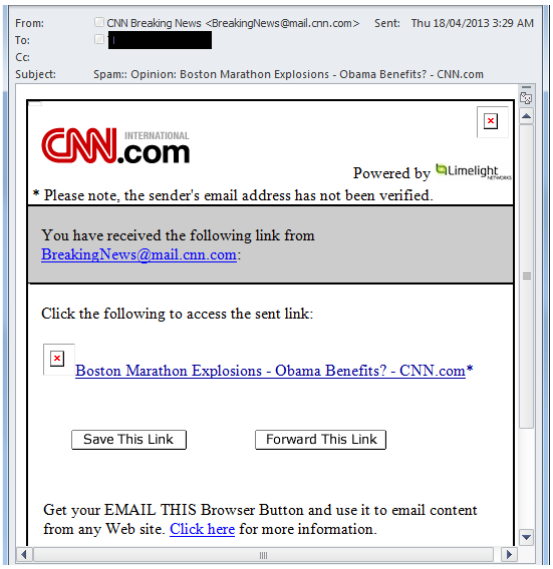

Fig. 7. Spam that initiated the Blackhole Exploit Kit attack

The links in the spam went to pages on compromised web servers – the link would go to one of 24 compromised web servers hosting web pages involved in this attack:

Table 1. Compromised web pages involved in the Blackhole Exploit Kit attack

Compromised Web Pages	
XXXspil.dk/cnn_boston.html	XXXknu.ac.kr/cnn_boston.html
XXXmforsakringar.nu/cnn_boston.html	XXXergo.ru/cnn_boston.html
XXXess-link.net/cnn_boston.html	XXXsmann.cz/cnn_boston.html
XXX-ptjc.com/cnn_boston.html	XXXstrok.com.ua/cnn_boston.html
XXXgroup.com/cnn_boston.html	XXXalarmowy-112.pl/cnn_boston.html
XXXrthanab.com/cnn_boston.html	XXXnaprawkonsumenta.pl/cnn_boston.html
XXXkitchen.co/cnn_boston.html	XXXofchristparish.org/cnn_boston.html
XXX21.ru/cnn_boston.html	XXXgym.pt/cnn_boston.html
XXXee.net/cnn_boston.html	XXXichter.dk/cnn_boston.html
XXXnens.se/cnn_boston.html	XXXkiev.ua/cnn_boston.html
XXXhany.co.nz/cnn_boston.html	XXXvast.com/cnn_boston.html
XXXichter.com/cnn_boston.html	XXXngedu.org/cnn_boston.html

If the recipient clicked on the link in the spam, then the user's browser would be redirected by the page cnn_boston.html to the landing page:

hxxp://thesecondincomee.com/news/agency_row_fixed.php

This was carried out by the location.replace javascript syntax, or the meta refresh html syntax, as shown below:

```
<html>
<title>BBB - gathering report</title>
<script type="text/javascript">
<!--
location.replace("hxxp://thesecondincomee.com/news/agency_row_fixed.php");
//-->
</script>
<noscript>
<meta http-equiv="refresh" content="0; url=hxxp://thesecondincomee.com/news/agency_row_fixed.php">
</noscript>
</head>

<h1>You will be redirected to process</h1>
<h4 style="color:#364dbc;">We must complete few security checks to show your transfer details:</h4>
<h3>Be sure you have a transfer reference ID.<br />You will be asked to enter it after we check the link.<br><br>Important: Please be advised that calls to and from your wire service team may be monitored or recorded.<br /></h3>
<h3>Redirecting to Complain details... Please wait...</h3>
</html>
```

If the user's browser downloaded the agency_row_fixed.php script, then as is typical of a BHEK [4, 5] the landing page would interrogate the browser for its environment, and deliver exploits suited for the victim's system. If the exploitation is successful then the user's system will be infected with malware in the Cridex family (specifically BKDR_CRIDEX.CHX [7]) being deployed on the victims computer. Once infected, the malware will monitor for the user's browser for strings related to online banking, and steal information being typed in. For example this particular variant will monitor and detect when Australian users visit the ANZ or the NAB websites (see [7] for details).

The vast majority of this attack was blocked by spam filters, so we only observed a total of 2,914 attempts to access these compromised web pages. Australia had a total of 21 attempts to access one of these pages, which ranked 13th in the distribution of this attack, as shown below:

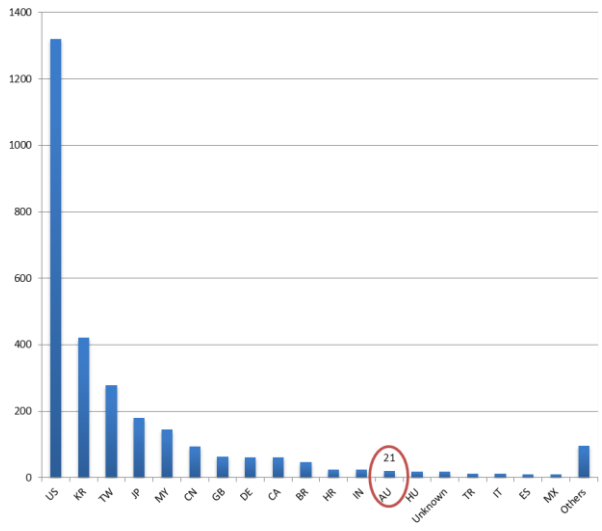

Fig. 8. Blackhole Exploit Kit victim country ranking

We tested these 24 compromised web servers a week after the initial attack (on the 24th April). Of these 24 servers, 12 still delivered the compromised page a week later, while the other 12 delivered 403 and 404 error codes.

3.2 Kelihos Worm

Another web attack using the Boston Marathon intended to infect users with a Kelihos worm. This attack was also initiated by spam:

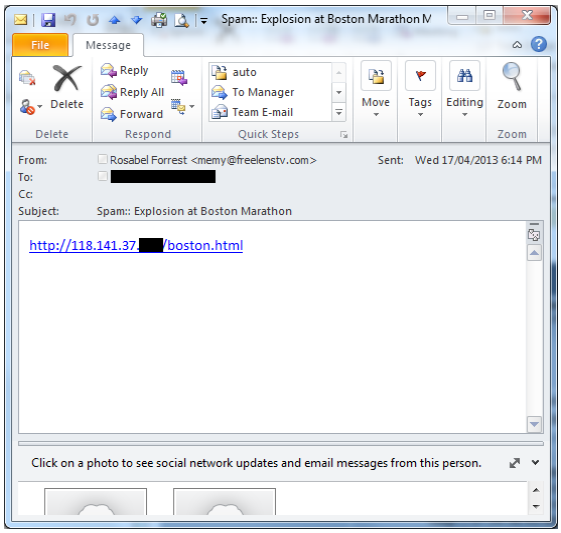

Fig. 9. Spam that initiated the Kelihos worm attack

In this situation, the attack was far more direct – the link in the spam led directly to a malicious web server that was delivering malware to victims.

If a person clicked on the link in the spam then the victim's browser would present a page with a YouTube video on it. While the video was being shown, the iframe tag in the page would connect to the malicious web server, which would exploit CVE-2013-0422 [3].

Fig. 10. YouTube video where Kelihos worm hides behind

CVE-2013-0422 would be exploited by a .jar file (with a random name such as 9uq.jar) which would drop and then execute the malware file boston.avi_____.exe.

There were 42 malicious web servers attempting to show victims YouTube videos of the event while infecting them with the Kelihos worm:

109.87.205.xxx
110.92.80.xx
111.184.108.xxx
118.141.37.xxx
…
94.28.49.xxx
95.69.141.xxx

This attack was on a far larger scale - we observed 212,125 attempts to access these malicious pages. As expected, the number one target was web users in the USA, while Australia had a total of 2429 attempts to access one of these pages, which ranked 14th in the distribution of this attack, as shown below:

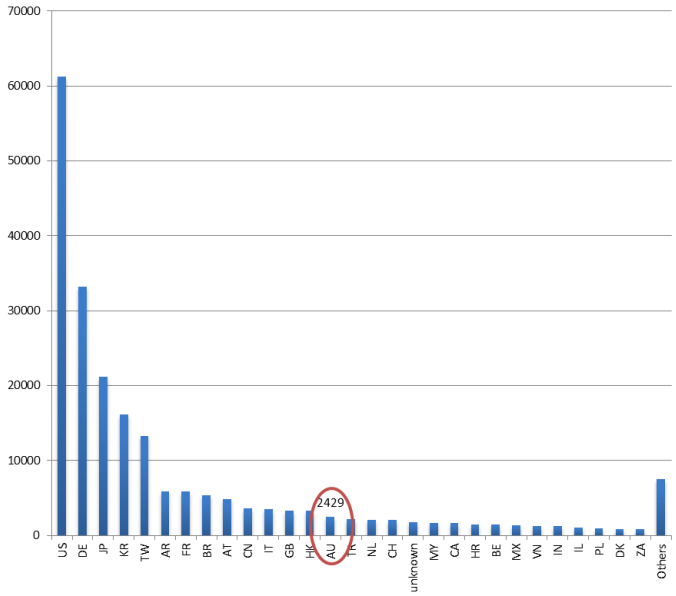

Fig. 11. Kelihos worm victim country ranking

The Kelihos worm does a range of malicious activity including (i) installing the worm on removable drives – and hiding it the folder, (ii) stealing FTP credentials and (iii) harvesting email addresses [8].

4 Conclusion

This report explored various aspects of threats on the Australian web landscape. We have provided statistics on the volume and timing of web threats impacting Australians. We describe the source geography of where those web threats originate, and also looked at where the victims were located when they were exposed to malicious web hosts located in Australia.

Though Australia is geographically isolated in the Southern Hemisphere, it is attracting a significant volume of web threats. Within the sample processed for this report, approximate 1 in every 2,500 (0.04%) web hits originating from Australia is malicious in nature. On a typical day, approximately 1 in 8 Australian IPs are exposed to one or more web threats, resulting in Australian users being victim to 3% of the world web threat attacks.

How does this compare to rest of world? Is there an average, are we above or below it?

5 Acknowledgement

This work was supported by ARC Linkage Project LP120200266.

6 References

1. http://cloudsecurity-apac.trendmicro.com/solutions-and-services/spn-feature/web-reputation-service.aspx
2. http://www.trendmicro.com.au/cloud-content/us/pdfs/about/ds_smart-protection-network.pdf
3. http://blogs.technet.com/b/mmpc/archive/2013/01/20/a-technical-analysis-of-a-new-java-vulnerability-cve-2013-0422.aspx
4. http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf
5. http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf
6. http://www.minister.dbcde.gov.au/media/media_releases/2009/022
7. http://about-threats.trendmicro.com/us/malware/BKDR_CRIDEX.CHX
8. http://blog.trendmicro.com/trendlabs-security-intelligence/kelihos-worm-emerges-takes-advantage-of-boston-marathon-blast/