1H TorrentLocker Landscape:

Targeting Even More Victims in Australia

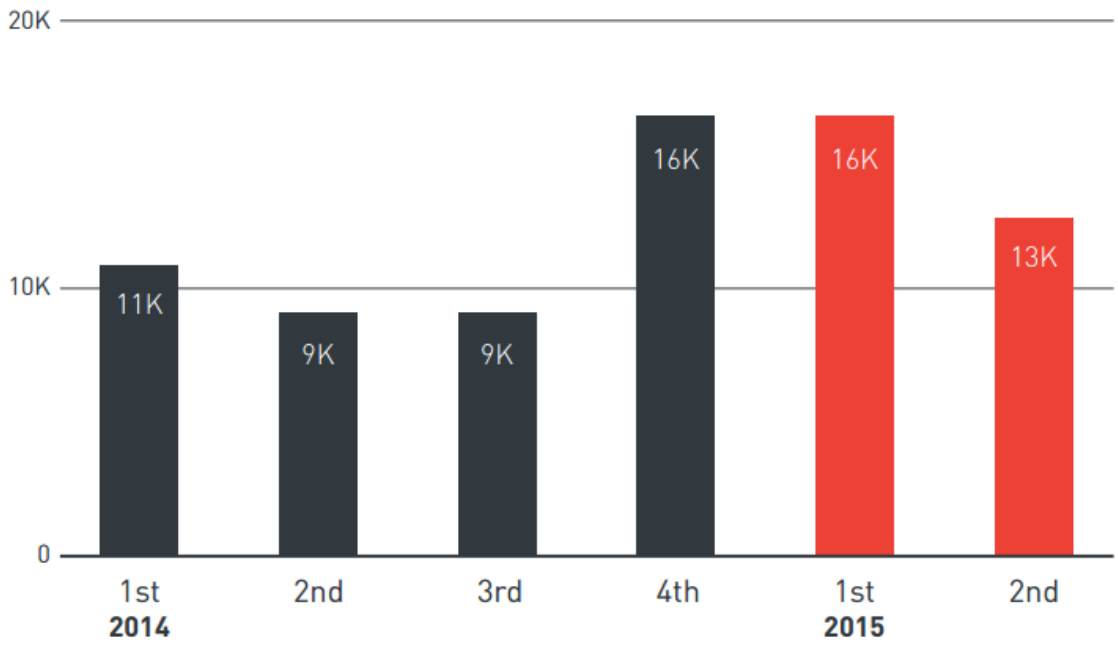
A TrendLabs℠ Primer

TorrentLocker outbreaks[1] have plagued users across several regions for years. A strain of ransomware that uses file encryption to extort money from its victims, TorrentLocker has long been observed in North America, Europe, and Australia. In 2014 we reported our insights on TorrentLocker attacks in Australia for that year, which detailed the malware's usual attack scenario, its use of email spam, and its infection chain.

This paper aims to provide more detail on TorrentLocker infections seen in the first half of 2015, more specifically, details on common evasion techniques and solutions to battle this ongoing threat.

A Quick Background on Ransomware

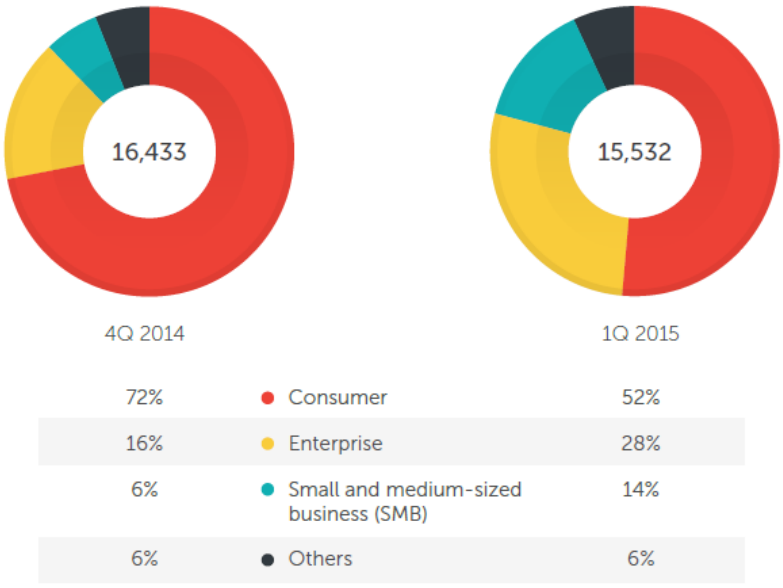
Ransomware is a type of malware that prevents or limits users from accessing their system. To make the infected system usable again, the victim is forced to pay (a ransom) to a remote threat actor thru certain online payment methods.



Ransomware detections (1Q-2014 – 2Q 2015)

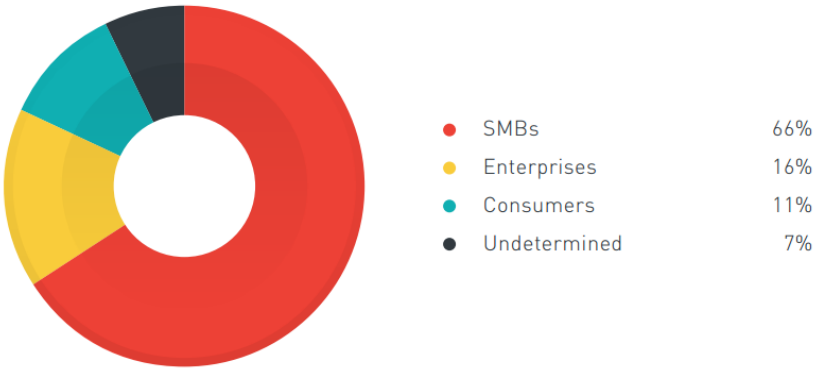
In the first quarter we reported about how ransomware expanded their target base to include enterprises and niche user types. This was evident in our 1Q security report which shows the growing number of ransomware detections for the enterprise segment.

[1] *The use of the term 'outbreak' in this report refers to a spike in ransomware detections versus traditional outbreaks that represent widespread threats like the I Love You virus and the Melissa worm.*



Number of Ransomware Detections by Segment in 4Q 2014 and 1Q 2015

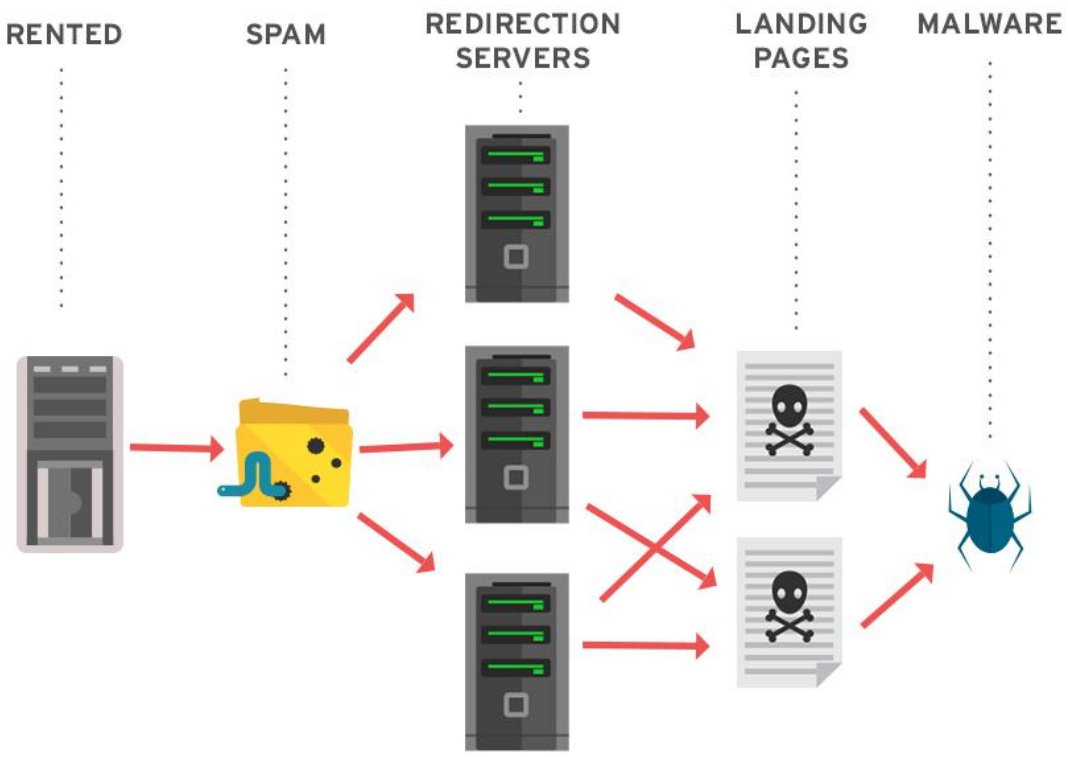
In our 2Q security report, however, we reported our findings on CryptoWall-related URLs in June. Small and medium-sized businesses comprised 66% of CryptoWall-related URLs for that month, followed by the enterprise and consumer segment.



CryptoWall-related URL distribution by segment (June 2015)

TorrentLocker: A Regional Threat

Apart from expanding its target base to include the enterprises, we observed a continuous growth in TorrentLocker outbreaks aimed at Australian individuals and businesses. In the past we have reported that the cause of the outbreaks were spammed messages primarily sent to Australian email addresses and used specially crafted social engineering emails. Below is an infection chain of how a typical spam outbreak carries out TorrentLocker attacks.



TorrentLocker outbreaks

Evasion Techniques used by TorrentLocker

TorrentLocker uses several evasion techniques that are known to bypass spam filters, web reputation, and malware detection. Its ability to utilize these evasion techniques allow ways for the threat to slip through the cracks even if all of your defenses are seemingly in place.

Antispam evasion

TorrentLocker is able to bypass anti-spam filters by sending email to legitimate accounts only. The spammed message are,carefully crafted by mimicking actual parcel tracking and penalty notice emails with accompanying hyperlinks attached.

Moreover, TorrentLocker bypasses IP reputation by making use of legitimate web servers instead of botnets, and uses these compromised web servers to redirect infected systems to malicious websites.

Sandboxes and web reputation evasion

TorrentLocker bypasses sandboxes by adding a CAPTCHA feature to the malicious webpage that carries the malware (example pictured below):

The CAPTCHA field requires users to input letters or numbers, giving cybercriminals a chance to verify that there is an actual person using the infected systems. In addition, the sandbox and web reputation evasion technique allows TorrentLocker to detect antivirus mechanisms that detect drive-by-downloads. TorrentLocker also randomizes the names of the scripts used on the compromised servers.

Newer TorrentLocker techniques employ the use of CAPTCHA fields to verify that an actual person is using the infected computers

An example of how TorrentLocker evades web reputation is its ability to keep the time to live (TTL) records very short. The web service runs on the same server as the DNS service. Hence, once the server is shut down, both services are turned off.

Malware detection

TorrentLocker is known to use standard malware techniques to reduce detection rates. They also heavily use the metamorphism technique by inserting dead code, or a sequence of non-effective assembly instructions. This type of randomness poses a great challenge to pure signature-based static detections.

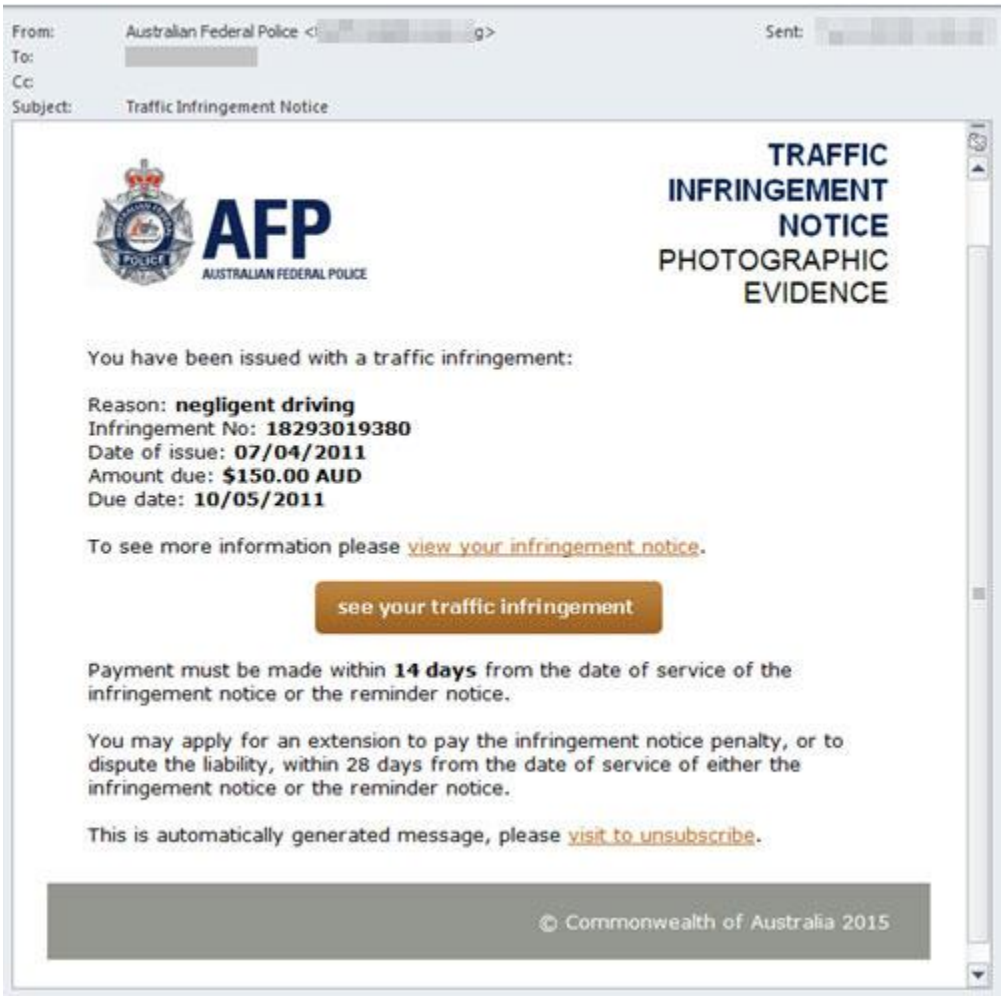
Continuous Surge in Australia

All throughout 2015 we observed many cases of TorrentLocker using various social engineering lures. In April 2015 however, we observed that cybercriminals started using the Australian Federal Police (AFP) as bait. The outbreaks continued until the latter part of May, but seemingly went on hiatus before continuing again in June as the threat returned to focusing on European users.

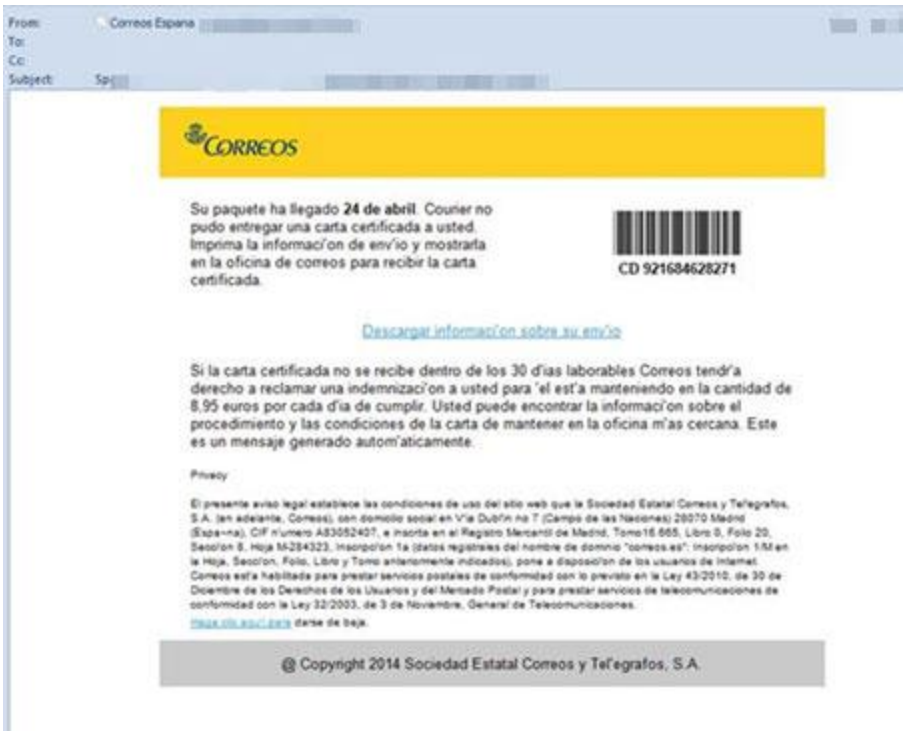
Typical TorrentLocker spam attacks usually occur between 1AM – 9AM. We hypothesize that that this "schedule" was intentional in order to match the email delivery time with the time that workers normally come to work in the morning. Moreover, the emails were seemingly delivered to a carefully selected address list with less than 1% sent to invalid ones. The spam run used email authentication such as DKIM and SPF to bypass spam filters.

Social Engineering Lures

Below are screenshots of sample social engineering lures we've seen related to the outbreak from April to May.



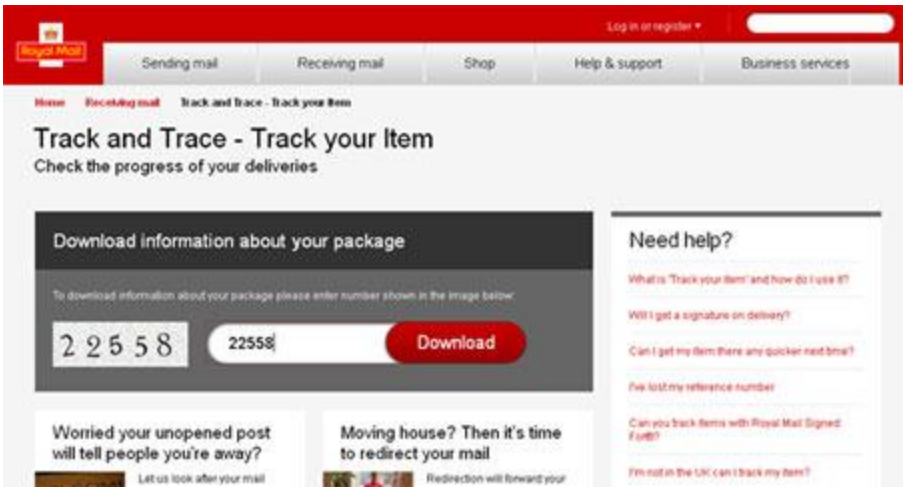
Australian Federal Police



Correos Postal Service

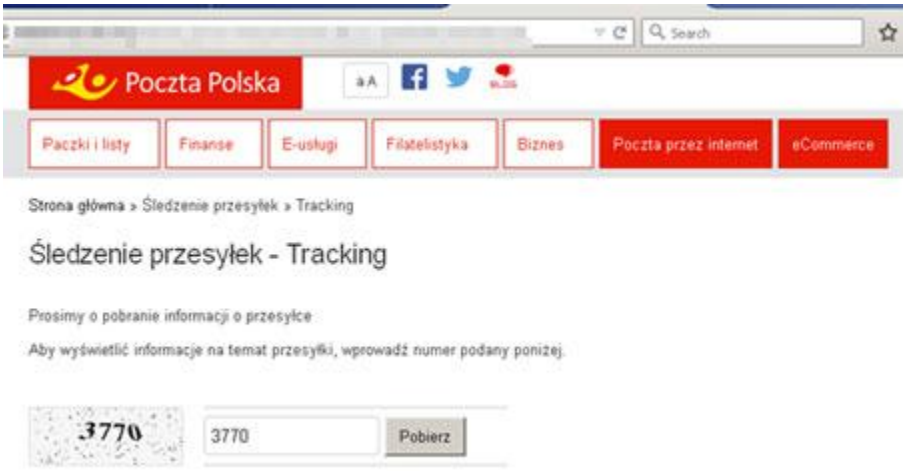
Couriers Please

Upon receiving the spammed email and clicking the embedded links, users get redirected to a Royal Mail landing page that instructs users to track the shipped items.



Fake Royal Mail landing page with instructions for tracking deliveries

Another site redirection related to these TorrentLocker attacks is a fake Poczta Polska site that offers a way to track incoming packages. This eventually leads to the download of the TorrentLocker variant.



Fake Poczta Polska site

Timeline and Downloaded Files

The downloaded files contain the keywords *carta certificada* (roughly translated as "registered letter"), which indicates that the attack targets Spanish-speaking users. Some of the related malicious files we've seen include the following keywords

- Carta cerificada
- "info_ or notice_" for AFP (Australian Federal Police)
- "Informacje przesylki" for Poczta Poland
- "Pacchetto" for SDA Express Courier

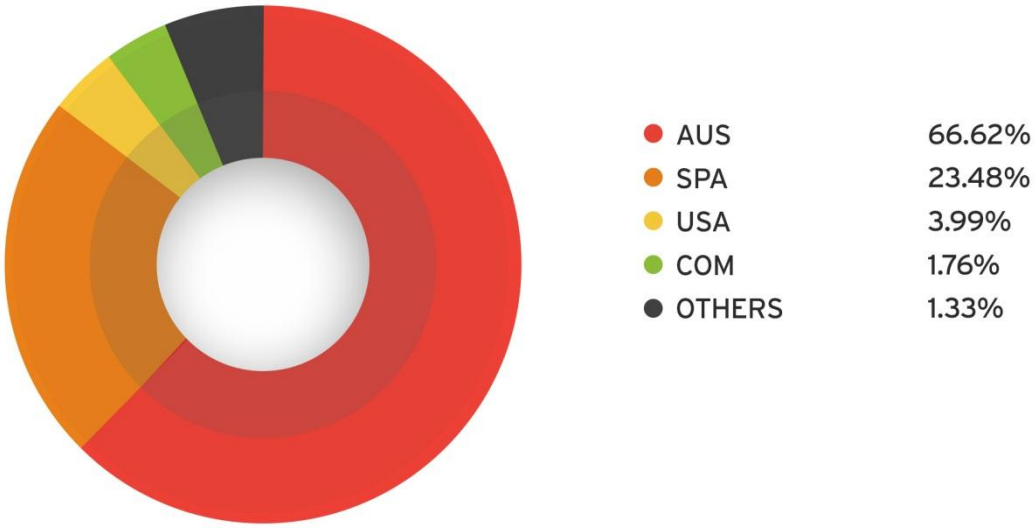
The timeline below shows the ordinance of cybercriminals on how they hosted the domains. The spoofed domains are hosted under a Russian server**.**

Outbreak	Social engineering used in spammed mails and file names
10-Jun	Correo, Poczta, SDA, AFP
13-May	Correo, AFP, Poczta Poland
14-May	Correo, Poczta Poland
15-May	AFP, Royal Mail
12-May	Correo, Poczta Poland
8-May	Correo, Poczta Poland
7-May	Correo, AFP
4-May	Correo
1-May	AFP
30-Apr	Couriers Please, Pack & Send
29-Apr	AFP
28-Apr	AFP, Correo
26-Apr	Correo
23-Apr	Correo
22-Apr	Correo
14-Apr	Correo
8-Apr	Correo
2-Apr	Correo, SDA, PTT
1-Apr	NSW

TorrentLocker outbreak from April to June 2015 included social engineering lures that used Correo, Poczta Poland, AFP, and SDA as the files names

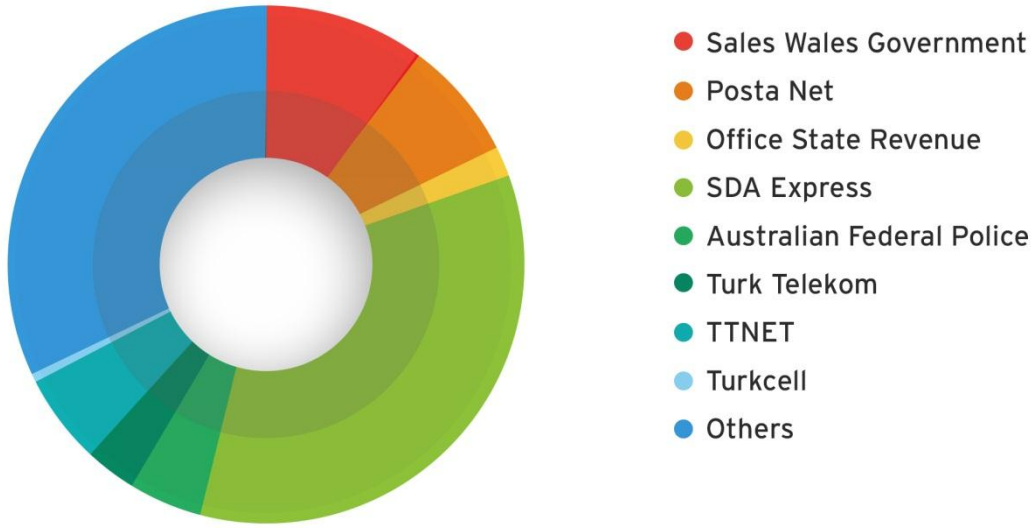
Mail Servers and Spoofed Email Addresses

Here is a closer look into the statistics for the volume of related spam sent. The data below shows our analysis of the data we monitored from Feb 15 to May 18, 2015.



ccTLD/TLD Distribution of Spam Recipients

The volume indicated above was calculated by the domain setup to send spam on different days. Majority of the spammed emails targeted the email domain ".AUS" as indicated by the pie chart above, while the second most spammed email domain was ".SPA".



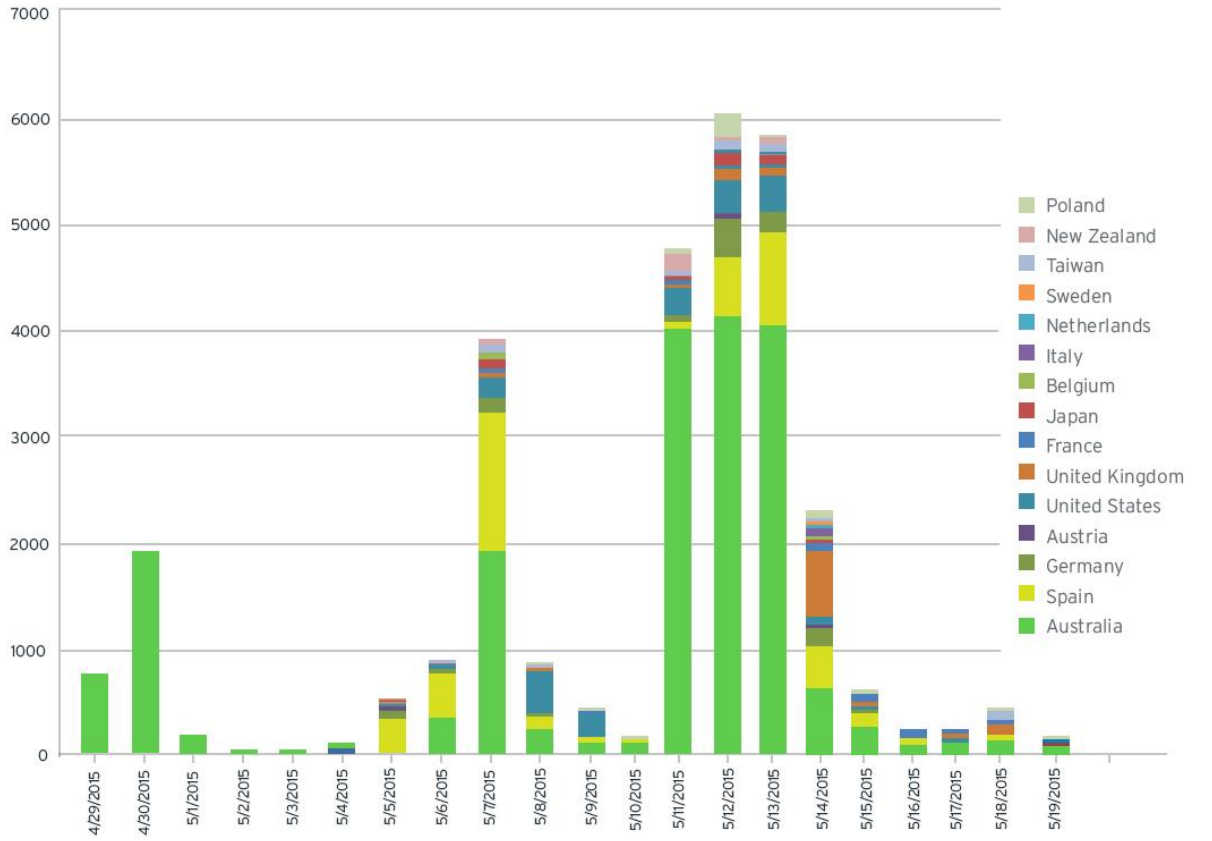
Top Spoofed Domains – Mail Servers

Taking a look at another data set, the graph above shows the top social engineering lures over the same time period (April to May).

We identified the social engineering lures based on the domains used in the spam messages. The "Others" category included targets such as Poczta Poland, a Polish mail service, and the Royal Mail (UK mail service). A common theme of these spammed emails is that the messages aim to alarm its recipients with some level of urgency. Typical inducements used to convince a user to click on the malicious link included: telling the user that a package had been delivered; telling the user that they had received a speeding fine; or telling the user that they had received a tax penalty notice.

Compromised links found embedded in emails

During the course of study, dated April 29 to May 19, we monitored the amount of TorrentLocker-related URLs seen in emails per country. Unsurprisingly, due to the already high volume of the malware in the region, Australia had the highest number (63%) of malicious URLs embedded in emails. Spain (14%) and the United States (6%) are round up the top three countries.



13

Malicious links encountered from emails. Australia ranks first in terms of TorrentLocker-related URLs seen in email.

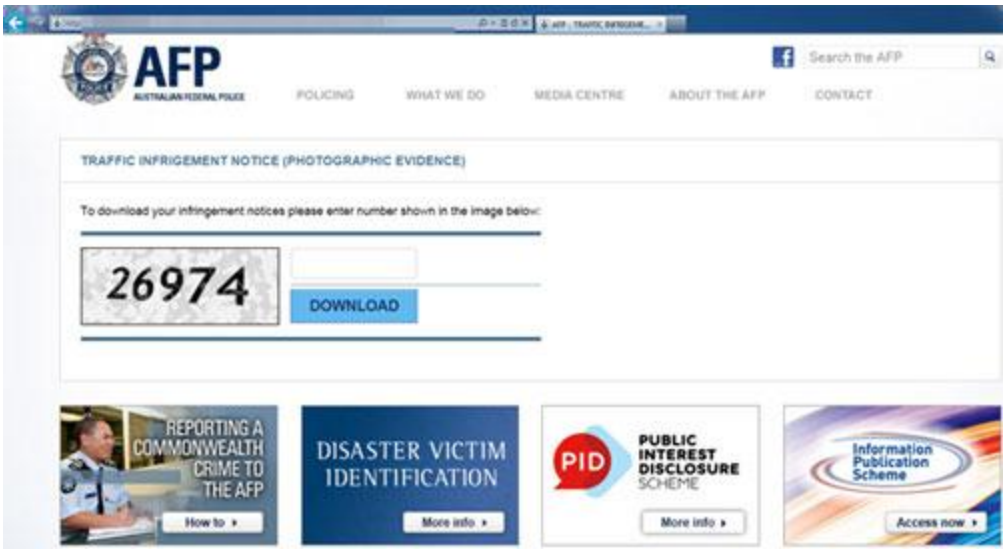
These URLs, which are compromised websites, found in email are commonly injected with */system/log/{random}.php?id={email_address}*.

Is TorrentLocker tricking users?

In order to determine whether TorrentLocker was successfully tricking users, we looked at the number of users visiting the landing pages. If a user attempted to load a TorrentLocker landing page – then they have clicked on the link in the spam.[2]

The most effective campaign we have seen by far took place last May 14 in Australia. The malicious campaign took advantage of the Australian Federal Police as a social engineering lure with a landing page pictured below:

[2] *The data described here is from users who have opted in to send feedback to Trend Micro when they are blocked from visiting malicious websites.*



The table below shows how effective this campaign was in Australia based on access rate. Around 60% of the total number of visits to the spoofed sites came from Australia alone, while some users in Spain also accessed these spoofed domains. This technique, however, was not particularly effective in other countries like Germany, France, and the United States.

Country	Access Percentage
Australia	57.9%
Spain	33.6%
Germany	1.9%
France	1.3%
United States	1.2%
Poland	1.1%
Taiwan	0.8%
United Kingdom	0.7%
New Zealand	0.7%
Netherlands	0.6%
TOTAL	100%

Top 10 countries that accessed spoofed domains

Below is a list of the top 5 domains that were used in this series of attacks:

ho	count(i)
download-notice.com	36%
getinfodata.com	12%
ecorreos24.com	6%
e-correos24.net	6%
ecorreos24.org	6%

Top 5 domains used

Solutions and Insights

With TorrentLocker now targeting more of the enterprise segment, it is more important than ever to enforce user education about the threat - how to know if an infection is present, and what type of security measures should be enforced. Having a file backup strategy for both consumers and enterprises is equally important – TorrentLocker and other types of ransomware heavily bank on users' vulnerability toward losing control of their files – and thus it is highly valuable to be informed how to deal with backing up.

Our online article talks more about the history of ransomware and the necessary security measures to battle this threat: Ransomware: 10 Years of Bullying, Fear-mongering and Extortion.

Strategies against TorrentLocker

Below is a quick rundown of some strategies that enterprises can employ to ensure that TorrentLocker or any other type of ransomware is able to enter your system and network. While having a backup strategy is always important, we recommend the following:

1. Have carefully designed policies that strictly limit the number of people and systems with access privileges for shared data.

2. Deploy an advanced monitoring of incoming email and other traffic that uses real-time threat intelligence to identify malicious emails, compromised URLs and C&C hosts, and contaminated file attachments. **The Trend Micro™ Smart Protection Network™** is a real-time threat intelligence system that gathers global input from millions of collection points and uses big-data analytics to produce up-to-the-minute information about the latest threats. All of Trend Micro's security solutions are constantly updated with the latest intelligence to enable them to identify malicious IP addresses, web addresses, C&C hosts, malicious code hidden in files, and the latest zero-day malware and exploits.

3. Do comprehensive monitoring of network traffic using advanced heuristic, sandbox, and emulation analysis to identify suspicious behavior by attacks both at and within the network perimeter.

4. Have next-generation endpoint technologies in place such as advanced anti-malware which can detect and stop ransomware. Application whitelisting technology can additionally be configured to automatically block any unknown applications/malware/ransomware from executing on your endpoints by only allowing known, good applications (and their associated updates)

5. Conduct training for all end users to minimize the effectiveness of malicious spam and phishing attacks that can infiltrate ransomware into the network. Educating them about social engineering attacks is particularly important as these techniques plays a crucial role in carrying out successful attacks.

No silver bullet

There is no silver bullet to stop TorrentLocker's persistence as the campaigns are growing in operational execution. The damage TorrentLocker brings is continuously causing financial damage and data loss to its victims, and therefore an in-depth defense is required. Attacks involving several components (spam emails, spoofed sites, malware) need multiple layers of defense.

Trend Micro Complete User Protection

A robust, multi-layered endpoint solution can help detect ransomware if it gets past other layers of protection. With an interconnected suite of security capabilities, you can protect against threats like ransomware—no matter where your users are going or what they are doing.

Trend Micro Smart Protection Suites protect your users at multiple layers: endpoint security, email and collaboration security, web security and mobile security. Plus, the suites feature web reputation, file reputation, and behavior monitoring to help detect ransomware files during download or execution.

Trend Micro's Email Reputation Service has heuristic rules which include identifying spam mails using the sender address. Web Reputation Service blocks the URLs found in the spammed messages. Typosquatting domains that spoof the official sites of the Australia Post and the NSW government are also blocked. All related C&C servers and the IP addresses hosting them are listed and blocked.

In addition, Smart Protection Suites give you the broadest range of advanced threat protection for anti-malware, packer variant protection, encryption, device control, data loss prevention, vulnerability shielding, command and control blocking, browser exploit protection, application whitelisting, web threat protection, social engineering attack protection, Census data and more.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com

TREND MICRO™ | Securing Your Journey to the Cloud