Australian Web Threat Landscape (2014)
Observation of TorrentLocker Attacks

Christopher Ke
Yang Xiang
Deakin University
Jon Oliver
Romeo Dela Cruz
Paul Pajares
Adremel Redondo
Lala Manly
Nazario Tolentino
Trend Micro Incorporated
# CONTENTS

Introduction........................................................................................................................................1

Insights on TorrentLocker Attacks..................................................................................................2

Scenario ............................................................................................................................................2

Delivering Email Spam ......................................................................................................................2

Infection Chain................................................................................................................................3

Bitcoin Payment Chain ......................................................................................................................5

Malware Mutation .............................................................................................................................7

Statistical Analysis ............................................................................................................................8

General Web Threat Landscape .........................................................................................................8

TorrentLocker Impact .........................................................................................................................9

Conclusion .........................................................................................................................................12

Acknowledgement .............................................................................................................................12

References ..........................................................................................................................................13

---

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.
INTRODUCTION

TorrentLocker\(^1\) refers to a regional threat with infections found in many regions around the world, including several countries in North America and Europe [1, 2]. Over the last few months, there has been a series of TorrentLocker outbreaks [3, 4, 5], which were aimed at Australian individuals and businesses. The causes of the outbreaks were primarily sent to Australian email addresses; used social engineering carefully crafted for Australia, and had a significant impact on victims’ lives and businesses.

In this report, we are going to provide readers with insights on TorrentLocker attacks based on observations and analysis of data captured by the Trend Micro™ Smart Protection Network™ as well as their influence on the general web threat landscape of Australia.

\(^1\) Even though the malicious software involved identifies itself as “CryptoLocker,” this infection is completely different from the original CryptoLocker. However, both CryptoLocker and TorrentLocker encrypt victims’ data and ransom them for Bitcoins.
INSIGHTS ON TORRENTLOCKER ATTACKS

A TorrentLocker attack uses a combination of email spam, web threats, and malware. Even though each vector does not boast of brand new techniques, when they work in conjunction with social engineering tricks, they make regional attacks highly effective.

Scenario

The following diagram shows how a victim is trapped by TorrentLocker.

In the following sections, we will go through the process of delivering email spam, infecting victims’ systems, and paying off ransom.

Delivering Email Spam

The email spam were carefully crafted. They copied details from genuine parcel tracking and penalty notice emails except for the embedded hyperlinks. In addition, the spam runs were coordinated with their corresponding Domain Name System (DNS) servers to get a Sender Policy Framework (SPF) pass or generate DomainKeys Identified Mail (DKIM) signatures, which enhanced the spam’s ability to penetrate anti-spam systems and arrive in victims’ inboxes.
Infection Chain

After clicking the hyperlink on the email spam, a victim’s web browser went through three steps in the infection chain—URL redirection, landing on a malicious page, and CAPTCHA verification to download the ransomware. The attacker leveraged a variety of tricks in each step to prevent from being identified.

1. **URL redirection:** Most of the web servers used for URL redirection were compromised and injected with a redirect rule, which resulted in a high false alarm rate if domain-level blocking is applied. Also, the redirect rules were quickly taken down either because they were found by the website owners or the attacker deliberately did so. Therefore, the reproducibility for analysis was limited. Furthermore, the syntax of the full URLs kept changing. In November 2014, there were at least five different forms of syntax showing up, listed as follows:

     eid=891913348555349xxxx
     id=1066xxxx
     eid=29773975284719613863652
     3751158729384344863722266
     831413588731859xxxx
     eid=78182419694761732195862
     276998338347532971837998864
     259653657933374xxxx

2. **Landing pages:** These mimicked the official web pages of the Australian POST and the Office of State Revenue of New South Wales. The number of web servers hosting landing pages was relatively small and the attacker used more sophisticated mechanisms to hide server locations:

   - The time to live (TTL) of DNS records was very short—just an hour, so once a DNS record was taken down, the cached domain name resolutions in DNS servers around the world quickly disappeared within an hour.
   - The web service ran on the same server as the DNS service. Hence, once the server was shut down, both services were turned off. In addition, the WHOIs information was counterfeit. The attacker filled in the real official addresses, phone numbers, and so forth of the organisations they mimicked for registering domains. These practices disconnected the correlation among individual
incidents and minimised the risk of being caught in the early stages.

- The relationships between landing page domains and IP addresses were very weak. None of the domains used the same IP addresses at a time and the IP addresses were dynamically allocated by Dynamic Host Configuration Protocol (DHCP). In conjunction with the short DNS TTL described above, the domains could perform fast fluxing to avoid being tracked.

- Some of the landing pages detected visitors’ browser type and only delivered the effective content to Microsoft™ Internet Explorer®.

The table below lists the landing page domains found distributing the TorrentLocker malware in November 2014. In addition to the domains listed below, many further domains were identified as being very similar when their WHOis records were inspected but their maliciousness could not be verified since they did not actively distribute the malware.

<table>
<thead>
<tr>
<th>Australian POST (55 domains)</th>
<th>Office of State Revenue of New South Wales (29 domains)</th>
</tr>
</thead>
<tbody>
<tr>
<td>au-post.com</td>
<td>data-nsw-gov.net</td>
</tr>
<tr>
<td>au-postalservice.com</td>
<td>data-nsw-gov.org</td>
</tr>
<tr>
<td>au-stpost.net</td>
<td>db1-nsw-gov.net</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>post-au.net</td>
<td>state2-nsw-gov.net</td>
</tr>
<tr>
<td>postau.net</td>
<td>state4-nsw-gov.com</td>
</tr>
<tr>
<td>postaust.com</td>
<td>state4-nsw-gov.org</td>
</tr>
</tbody>
</table>

3. **CAPTCHA verification:** This confirmed that the operation was executed by a human. This mechanism protects web servers from being attacked by automation scripts attempting to source samples for researchers and security vendors.
4. **Payload delivery:** When the victim submits the CAPTCHA answer, a ZIP file is delivered from an abused file-hosting site such as sendspace.com to the victim’s computer. The ZIP file contains an executable malware file. The PHP script on the landing page delivers unique links. One sample outbreak with landing page http://up-nsw.gov.org/detailed_info.php used the following file-hosting links:

- https://fs13n3.sendspace.com/dlpro/55d80514c4d20419f547b5bd160ef426/5487c03a/vxj0fm/id_50920949811.zip
- https://fs13n3.sendspace.com/dlpro/85952624fa01ab335913c23c4498f20b/5487c1e8/vxj0fm/id_50920949811.zip
- https://fs13n2.sendspace.com/dlpro/0fb326db3791c23d21898762c9df4b81/5487c214/vxj0fm/id_50920949811.zip
- https://fs13n1.sendspace.com/dlpro/70abb33db12ec9b6b6124f946ae4ea/5487c23a/vxj0fm/id_50920949811.zip
- https://fs13n4.sendspace.com/dlpro/56d96d1b6d2797bed69d2f96ceac2816/5487c2fd/vxj0fm/id_50920949811.zip
- https://fs13n1.sendspace.com/dlpro/5bdee22341c06552d704d0e7cfd0834/5487c31d/vxj0fm/id_50920949811.zip
- https://fs13n1.sendspace.com/dlpro/0ed43ad79aefd484a8d481343fc28c14/5487c53c/vxj0fm/id_50920949811.zip

5. **File execution:** When executed, the malware accesses command-and-control (C&C) servers hosted in Russia. Then, it encrypts files that use 235 of the commonly used file extensions, including .DOCX, .PDF, and .ZIP. Encrypted files have ".encrypted" appended to their filenames once they are locked. The malware deletes the Shadow Copy of the infected system using the vssadmin.exe command. Upon execution, it creates a “new process” called “Explore.exe” and injects the main routine. The encryption routine uses the elliptic curve method. It creates an autostart entry in the registry using the executable file located in %Windows%\{random}.exe and the dropped copy of itself. It drops the encrypted files into the %All Users%\Application Data\{random} path with filenames, sizes, and hashes.

**Bitcoin Payment Chain**

Once the victims’ files are encrypted, the...
malware requires payment in Bitcoins so they can recover their files, as shown below.

**WARNING**
we have encrypted your files with CryptoLocker virus

Your important files, including those on the network (data, USB, e-mail, photos, videos, documents, etc.) were encrypted with our CryptoLocker malware. The only way to get your files back is to pay us. Otherwise, your files will be lost. Retrieving CryptoLocker will not restore access to your encrypted files.

Click here to pay for files recovery

**Frequently Asked Questions**
- [...] What happened to my file?
- [...] How can I get my files back?
- [...] What should I do next?

We noted the following about the user experience at this point of infection:

- The TorrentLocker malware incorrectly tells victims that it is the “CryptoLocker virus.” We believe this is to exploit general brand awareness of the CryptoLocker malware.

- The interface attempts to be very helpful in providing information about how to pay using Bitcoins.

In Australia, the base price is A$598. It displays a warning that the price will double after four days or 96 hours after the user is given the Bitcoin address. To make the transaction, it needs to register a Bitcoin wallet and buy Bitcoins from suggested links. Once the payment is done, cybercriminals will transfer Bitcoins from the given Bitcoin address to their official Bitcoin address typically using a chain of transfers so that the transaction is difficult to trace. The decryption software will only work on the specified infected machine; otherwise it will destroy the files, rendering them unusable.

If users are not located in Australia and New Zealand (ANZ) or Europe, the Middle East, and Africa (EMEA), a generic web page will appear written in English using U.S. dollars as currency. Below are screenshots of payment demands for a selection of victim geo-locations.

The payment process works as shown in the following diagram.
The payment is made through Tor. Users affected by this malware are assigned a code. The payment will be made through a URL with the following format:

- http://{gibberish}.gate2tor.org/buy.php?user_code={xxxxxxx}

As of December 9, 2014, the attacker added a password to the payment URL, as in the following:

- http://r2bv3u64ytfi2ssf.way2tor.org/buy.php?user_code={xxxxx}&user_pass={xxxx}

When a user pays, *Decryption_Software.exe* is provided. The software decrypts the encrypted files.

**Malware Mutation**

The TorrentLocker malware delivered rapidly changes to evade detection by security companies. Traditional approaches to malware detection would have difficulty keeping up with the rapidly changing malware binary. Due to the evasion tricks described in previous sections, collecting and analysing samples are relatively difficult to perform.
STATISTICAL ANALYSIS

In the scope of conducting research, we continuously monitored web threat trends and outbreaks that occur in Australia. The sampling data in this analysis was collected from November 1–30, 2014 by the Trend Micro Web Reputation Service (WRS) and Smart Protection Network [9]. The terms used in this report are defined as those in previous reports in 2013 [10, 11].

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

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

- Exploit kit landing pages and other pages that attempt to download malware onto users’ systems
- Phishing web pages
- Compromised pages hosted on legitimate web servers that redirect users’ browsers to other malicious pages such as landing pages
- C&C servers

Hence, a malicious hit is a transaction that Trend Micro WRS has identified before a web request or web traffic was deemed malicious.

General Web Threat Landscape

In the November data set, Australians surfed the Internet via 16.2 million IP addresses, 1.7 million of whom attempted to visit at least one malicious web page once. In other words, one in 9.52 Australian IP addresses (i.e., 10.5%) was exposed to one or more web threats during the month, which may indicate that Australian Internet users are now more aware of web threats. They also generated 5.47 billion web hits, 11.97 million of whom attempted to visit malicious web pages. The average percentage of malicious over web hits was 0.22%, which is roughly the same as that (i.e., 0.21%) in the December 2013 report. The lowest and the highest numbers were 0.16% and 0.35%, which were recorded on November 21 and 28, 2014 respectively. The following chart depicts the trend in web and malicious hit changes.
The general trend was not significantly influenced by TorrentLocker attacks, as the number of such incidents was still relatively small compared with all malicious activities.

TorrentLocker Impact

The November 2014 data set was extracted from the Trend Micro WRS system where over 10,000 hits going to redirection URLs were found. Around half of the records were confirmed malicious while others were labelled “suspicious” at the time they were clicked. During the analysis, they were all considered TorrentLocker incidents. The chart below reveals outbreaks related to five redirection URL syntax types. We can clearly see that there was only one type before November 22, 2014. Since then, however, the redirection URLs changed more frequently and triggered an outbreak for each syntax change.
The following chart shows the number of web hits for two landing page types. In comparison with the previous chart, we realised why the attacker changed syntaxes; many of the redirection URLs of the first type (i.e., forum.php) have been identified and blocked, so even though there was a URL redirection outbreak starting on November 16, the number of landing page hits remained low. After the syntax changed, another landing page outbreak was triggered.
Based on the statistics, we obtained a basic quantitative understanding of TorrentLocker attacks. However, the attacks still went on beyond the data that was analysed here. As such, further research is urgently required in order to protect people from being attacked by TorrentLocker variants.
CONCLUSION

This report explored various aspects of threats in the Australian web landscape. We have provided statistics on the volume and timing of web threats impacting Australia.

In addition, we examined the TorrentLocker outbreaks that hit Australia over the last few months. We examined the general mechanism as to how an outbreak works and did an in-depth study of the outbreaks that occurred from November 1–30, 2014. We reported about the many and diverse set of evasion techniques employed. Based on the evasion techniques used and the outbreaks that adapted to security measures, we see multi-layer filtering as a more robust approach to protecting users from TorrentLocker variants. In addition, further research is needed to monitor and document the evasion techniques being used and their impact on Australia.

Acknowledgement

This work was supported by the Australian Research Council Linkage Project LP120200266.
REFERENCES


Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2014 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.