

# ASERT Threat Intelligence Report 2016-06

## Analysis of CryptFile2 Ransomware Server

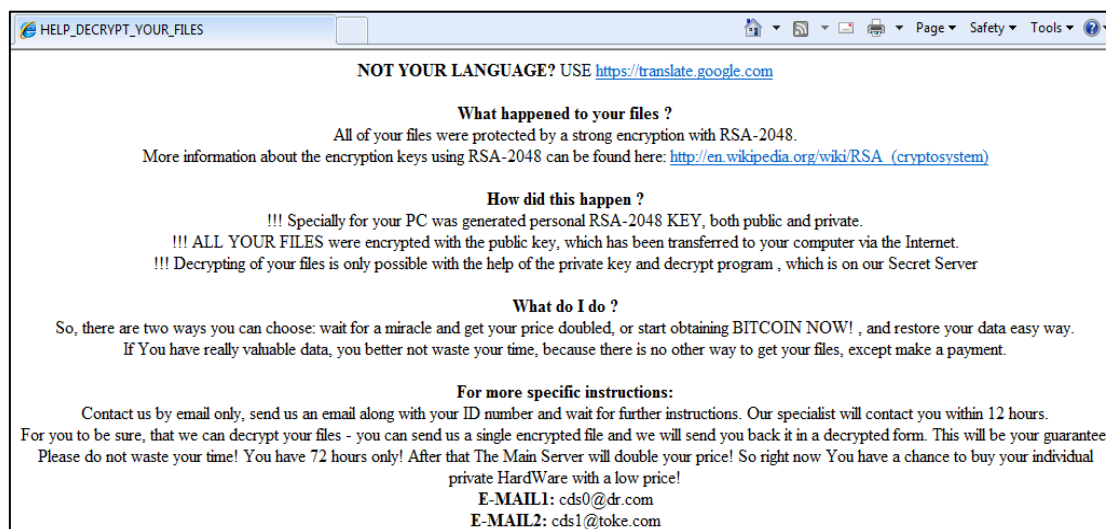
### Introduction

This report describes several elements of a ransomware staging system using the Nemucod malware to deliver CryptFile2 (aka Hydracrypt.A and Win32/Filecoder.HydraCrypt.C) ransomware, an ongoing threat since at least mid-March of 2016. This report reveals TTP's (tactics, techniques, procedures) of threat actors, including insight derived from limited interactions via e-mail. The information in this report is derived from the analysis of a now defunct C2 server/staging site discovered in August of 2016 and is provided to inform detection capabilities and improve defensive posture with regards to ransomware staging and distribution.

While this report focuses on the server-side aspects of a CryptFile2 ransomware operation, an understanding of the endpoint behavior may be obtained from the following reports:

- <https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/HydraCrypt.A>
- <https://www.proofpoint.com/us/threat-insight/post/cryptfile2-ransomware-returns-in-high-volume-url-campaigns>
- <https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfile2-brlock-mm-locker-discovered>

As described in these reports, when the malware detonates, the user is presented with a screen of this nature:


















## Server Side Analysis

The ransomware C2 contained an open directory - [http://5.154.190\[.\]41/uuu](http://5.154.190[.]41/uuu). We have collected 16 distinct instances of the files available via the open directory between August 5, 2016 and August 22, 2016 (just prior to the C2 going offline), providing some visibility into campaign activity. Since we did not obtain access to the C2 panel or a forensic dump, we do not have a complete understanding of the back-end logic. Additionally, ongoing monitoring of the open directory revealed that log files were periodically purged, leading to some limitations of vision. Nonetheless, observations are provided based upon filenames and other context. As analysis was underway, we were able to discover a second server associated with similar threat activity. These are profiled as Server Site #1 and Server Site #2.

### Server Site #1 - [http://5.154.190\[.\]41/uuu](http://5.154.190[.]41/uuu)

The contents of the open directory on server #1 at the point of initial discovery were as follows:

Index of /uuu			
Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">Log_bad_exe.txt</a>	03-Aug-2016 14:02	7.9K	
 <a href="#">Log_bad_js.txt</a>	03-Aug-2016 14:51	70K	
 <a href="#">Log_good_exe.txt</a>	03-Aug-2016 14:07	10K	
 <a href="#">Log_good_js.txt</a>	03-Aug-2016 15:56	64K	
 <a href="#">block/</a>	25-Jul-2016 11:16	-	
 <a href="#">exe.php</a>	02-Aug-2016 19:22	4.9K	
 <a href="#">exe.txt</a>	01-Aug-2016 23:39	181K	
 <a href="#">flags/</a>	25-Jul-2016 11:19	-	
 <a href="#">jbklfdhufidslkfds.php</a>	08-Jul-2016 22:24	3.1K	
 <a href="#">offers.php</a>	14-Mar-2016 18:05	1.6K	
 <a href="#">presentation_loader.php</a>	02-Aug-2016 19:22	4.9K	
 <a href="#">str.txt</a>	03-Aug-2016 16:24	19K	
 <a href="#">style.css</a>	27-Feb-2014 15:09	95K	
 <a href="#">sxgeo/</a>	25-Jul-2016 11:19	-	

Apache/2.2.22 (Debian) Server at 5.154.190.41 Port 80

### exe.php

The file `exe.php` is of note since it was being downloaded by the Nemucod malware mentioned on page 1. This file was identical between August 8<sup>th</sup> and August 22, with an MD5 hash of 61fdc8770e78ce67f63f8bcc2841dfb0.

## exe.txt

The file exe.txt remained the same during the monitoring period, and had an MD5 hash of 757cd97a370c205a89ba8ad8108f8c30. The file exe.txt simply contained a base64 encoded version of a PE binary. Decoding exe.txt back to its PE origins results in a file with the MD5 hash 7199070b699bfa213e88df3d2966e11d.

## Log\_bad\_exe.txt and Log\_bad\_js.txt

These two files are log files containing the date, browser User-Agent value and source IP in a pipe-delimited fashion as follows:

**Figure 1:** Logfile format for Log\_bad\_exe.txt and Log\_bad\_js.txt

```
01.08.2016-18:46 | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.82 Safari/537.36 | 50.207.171.130
01.08.2016-18:46 | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.82 Safari/537.36 | 50.207.171.130
01.08.2016-20:41 | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36 | 136.243.128.115
01.08.2016-20:41 | Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; Media Center PC 6.0; .NET4.0C; W
ebMoney Advisor; .NET4.0E) | 136.243.128.115
01.08.2016-20:41 | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0 | 136.243.128.115
02.08.2016-10:19 | Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko | 95.211.190.198
02.08.2016-13:50 | Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36 | 179.43.148.2
02.08.2016-13:51 | Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0) | 77.247.181.162
02.08.2016-14:23 | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36 | 179.43.148.2
02.08.2016-14:39 | Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:x.xx) Gecko/20090504 Mozilla Firefox/3.0.2.1 | 83.24.168.227
02.08.2016-14:39 | Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:x.xx) Gecko/20090504 Mozilla Firefox/3.0.2.1 | 83.24.168.227
02.08.2016-14:52 | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36 | 212.47.247.88
```

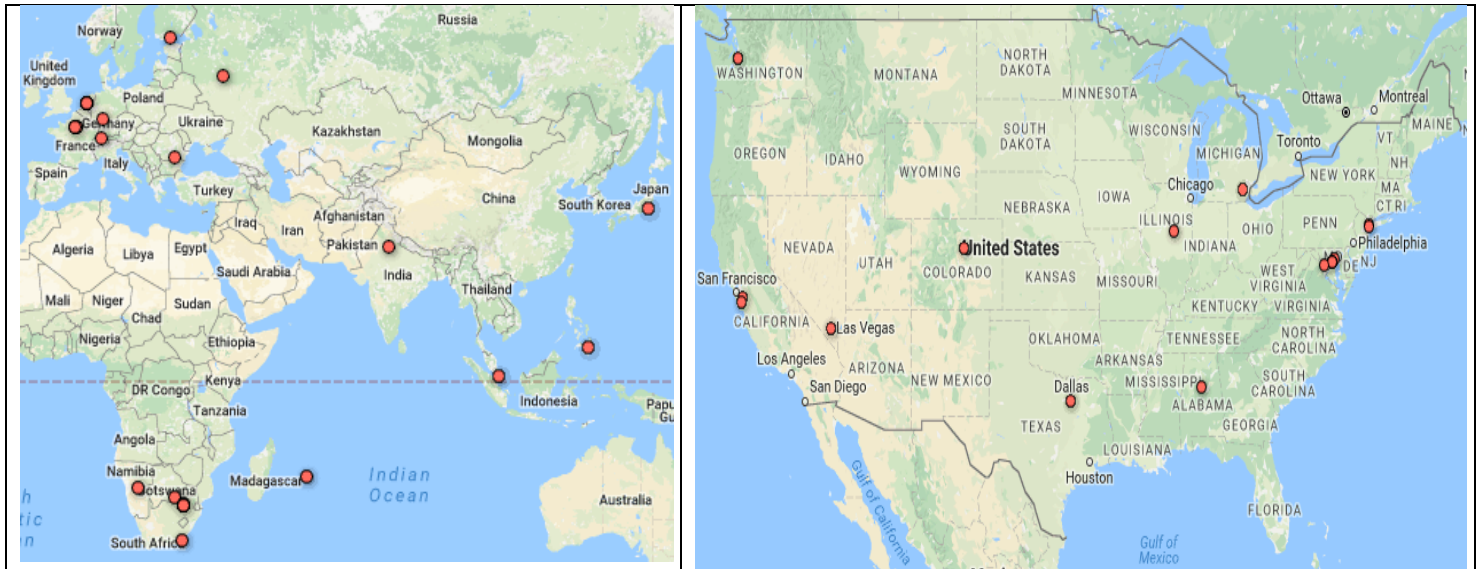
It is likely that the reason for the log files with the name “Bad” is for the threat actor to record unsuccessful exploitation and compromise activity.

## Log\_good\_exe.txt and Log\_good\_js.txt

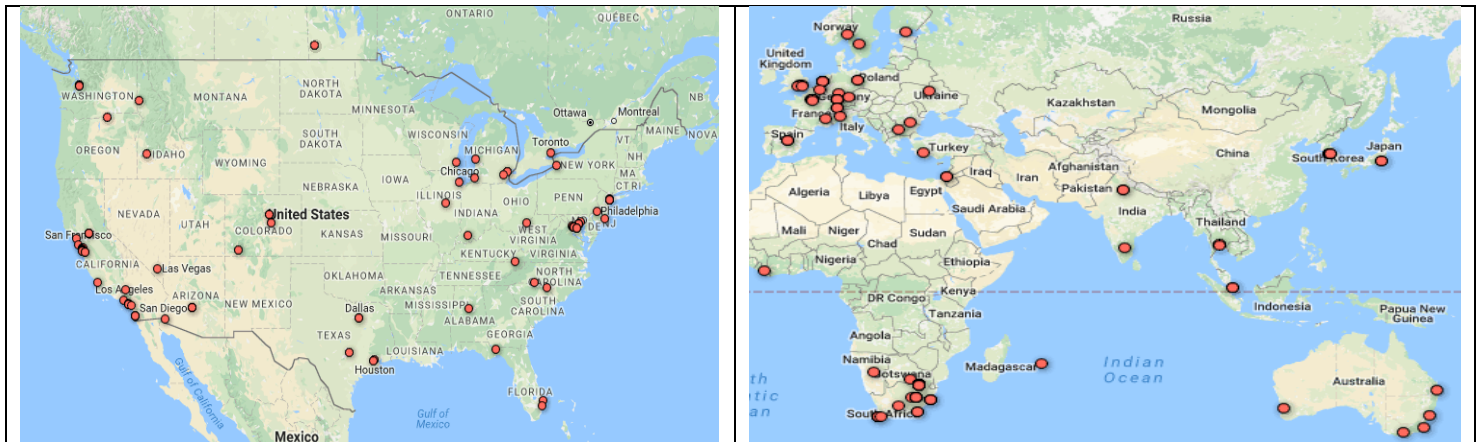
The Log\_good\_exe.txt and Log\_good\_js.txt files are potentially more interesting, because of what “good” may mean (likely this means a successful exploitation or compromise).

The User-Agent value observed during detonation of the malware binary was observed inside all instances of the Log\_good\_exe.txt files, along with evidence of analysis by security researchers using Wget or other browsers to visit the site. The number of unique IP address entries in these log files are low – only forty unique IP’s were observed.

A visual map of the victims reveals that this group was not prolific by ransomware standards, however one should keep in mind that this is one distribution/staging server and does not offer total campaign visibility.

**Figure 2:** Geographical mapping of IP addresses found in Log\_good\_exe.txt

The Log\_good\_js.txt files appear to contain IP addresses of systems that successfully executed the JavaScript and initiated the download, however anyone browsing the open directory also had their IP address logged. The count is higher here, with 232 unique IP addresses represented:

**Figure 3:** Geographical mapping of IP addresses found in Log\_good\_js.txt

One possible explanation for the difference in counts between the IP's that appeared in Log\_good\_js.txt and Log\_good\_exe.txt is the role of host-based security, or network-based security that blocked the download of the binary on the wire.

**Folder /block**

This folder contains the following files:

**bd.php** (not obtainable via open directory)

**head.php** (unauthenticated connection simply displays three periods on a web page):

```
<tr>
  <td class="accordion"><div align="center" class="btn-info">
    <div align="left">...</div>
  </div></td>
</tr>
```

**leftb.php** – lists counts of bots and statistics by country. This page also included a link to a menu that was not accessible during research. The page renders as such:

```
<td width="5%" valign="top" class="alert-info">
<p><strong> Menu:</strong></p>
<div align="left"><a href="jbklfdhufidslkfds.php" >-->Home</a> </div>
```

```
<p><p><strong> Statistics by Country:</strong></p>
```

BOTS ALL COUNTS:

```
0  <p><br>
</p></td>
```

**exe.php**

This the primary ransomware malware file, previously discussed.

**Flags folder**

The flags folder simply holds GIF files of national flags, likely used by the bot panel to display source countries.

**jbklfdhufidslkfds.php**

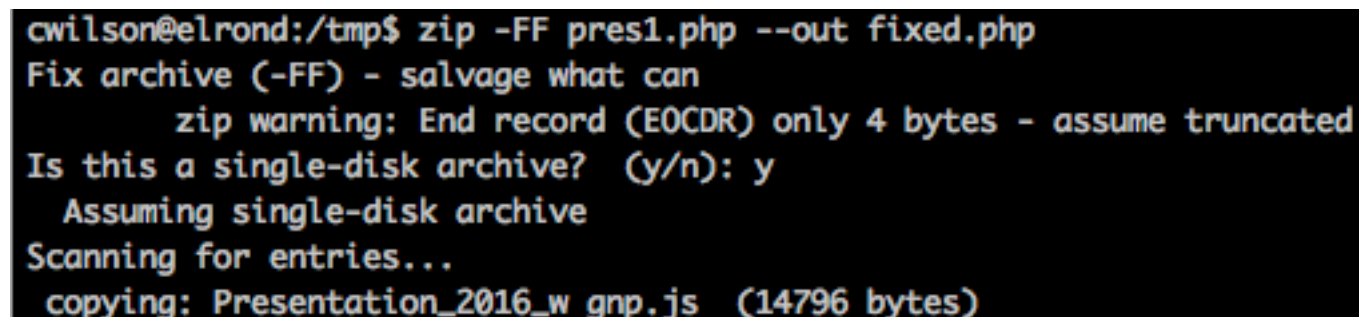
This is a menu page that appears to have only been accessible after authentication. This very unique filename was also discovered on other sites, most notably on 62.75.195[.]136/forse/ that appears to have contained a similar server side kit with an open directory, as discussed later in this paper.

**offers.php** - (not obtainable via open directory)

### **presentation\_loader.php**

This is a ZIP file that was first observed to be damaged or obfuscated in such a manner as to not unzip properly. An attempt to run a forced fix on the archive reveals archived filename details:

**Figure 4:** ZIP file containing Right to Left Override (RTLO) contains JavaScript disguised as a PNG



```
cwilson@elrond:/tmp$ zip -FF pres1.php --out fixed.php
Fix archive (-FF) - salvage what can
      zip warning: End record (EOCDR) only 4 bytes - assume truncated
Is this a single-disk archive? (y/n): y
  Assuming single-disk archive
Scanning for entries...
  copying: Presentation_2016_w gnp.js (14796 bytes)
```

The filename as displayed here by the Unix zip utility, “Presentation\_2016\_w gnp.js” contains the Right-to-left-override (RTLO) trick.

On August 5, 2016, the threat actor appeared to have extracted the file from the ZIP that appears to be named “Presentation 2016 wsj.png” but uses the aforementioned Right to Left Override (RTLO) trick to describe a JavaScript file (.js) as a PNG. This is most likely an attempt to convince users to click on a document that they believe is an image file. This file is heavily obfuscated JavaScript.

On August 6, 2016, the actor updated the file “presentation\_loader.php” at 00:01, just 36 minutes after the modified date of the “Presentation 2016 wsj.png” file. The hash of the file was different, suggesting ongoing efforts to evade hash-based or other static detection mechanisms.

The hash of the presentation\_loader file was consistent between August 8 and August 10, using MD5 hash 3466b3e1c01c43197e1b1919e7da7c70. From August 11 until August 22 (the end of the monitoring period), the MD5 hash for this file is e442a8904d3457f3f7eeb2afe640ffe7.

On August 2, 2016, a user from France uploaded a binary inside a ZIP file to VirusTotal (bb0a9737ae642a30f0728a3cf5a6133d) that contained a filename “Presentation\_Taxes\_2016\_Powerpoint\_.js”. The sha-256 for this file is 03fde3a95a8396413313c8008dc3c5b6a6ac7c8d1edaacd0f72eca1527a36c98. An analysis of the ZIP file reveals Nemucod.



**str.txt**

This file alternated between MD5 hash 130a7eeafa359b0f7beb7ca4526dd495 and MD5 hash 4f4315ef1e82ecbbca437eef0d720a6a, with the former appearing more frequently during the monitoring period.

The hash 130a7eeafa359b0f7beb7ca4526dd495 contains a base64 encoded ZIP file. The ZIP file has the MD5 hash of 4e577d3680b7a1d2eaadbc3fd6212d3c, and uses the same type of filename observed during prior analysis of presentation\_loader.php. Unzipping the file reveals another instance of Nemucod, a JavaScript file with an MD5 hash of e0a51f28714381151dc29193c28dec63 that is obfuscated with the Right to Left Override technique to appear as a PNG file. The output from a Linux unzip plainly reveals the technique as follows:

```
Archive:  str_out.zip
Presentation_2016_w gnp.js: mismatching "local" filename (Presentation_2016_wtAognp.js),
      continuing with "central" filename version
  inflating: Presentation_2016_w gnp.js
```

The file named str.txt with the MD5 hash 4f4315ef1e82ecbbca437eef0d720a6a is very similar, however it drops a ZIP file with MD5 hash of ab600f5d8e01bb228c9f39f7893abca3, which then drops a Nemucod script with MD5 hash 434522ba1b4f3ed815ca1b64f5c2f114.

**style.css**

This file is a style sheet with MD5 hash 266e5a2a4217698315c09c199498eb39. A quick Google search did not reveal other instances of various elements randomly selected from this file, however the style sheet may not be unique to the malware operation.

**The sxgeo folder**

This folder contains two files: SxGeo.dat (MD5: 835bf1be41bcd0ef29262be2c0a81c85) and SxGeo.php (zero byte file during attempted download). This appears to be part of the Sypex Geo geolocation package [<https://sypexgeo.net/ru/docs/>], which is apparently used here to determine the geolocation of compromised IP addresses. Search engine results suggest this package is often used in Russia.

## Server Side Analysis Site #2 [http://62.75.195\[.\]136/forse/](http://62.75.195[.]136/forse/)

Another site containing a similar ransomware server kit was discovered at [http://62.75.195\[.\]136/forse/](http://62.75.195[.]136/forse/) and was contacted by the following malware samples:

Malware hash (MD5)	Compilation Date	Email Contact
a3d9d669e476208e8f30daaad350cfd2	2016-08-02 22:38:46	cx9@dr.com cx9@post.com
f2fa31d8398255a8c92d7e9c07c98b22	2016-08-19 11:31:06	cx9@post.com
9496028dac42c4e6b2d16acd2ba7ab5c	2016-08-24 12:57:07	cx9@dr.com cx9@post.com
f124917597890f966e5d86c82c65d930	2016-09-14 20:23:53	cx9@dr.com cx9@post.com

Analysis timestamps followed compilation timestamps (within a day or two) therefore the compilation date seems to be accurate and not modified.

Every sample mentioned in the table contacted the following two URL's:

- [http://62.75.195\[.\]16/default.jpg](http://62.75.195[.]16/default.jpg)
- [http://62.75.195\[.\]16/forse/point.php](http://62.75.195[.]16/forse/point.php)

These network connections trigger the following network alerts:

[2821561]: ETPRO TROJAN Win32/CryptFile2 Ransomware Fake Image Request

[2022683]: ET TROJAN Win32/CryptFile2 Ransomware Checkin

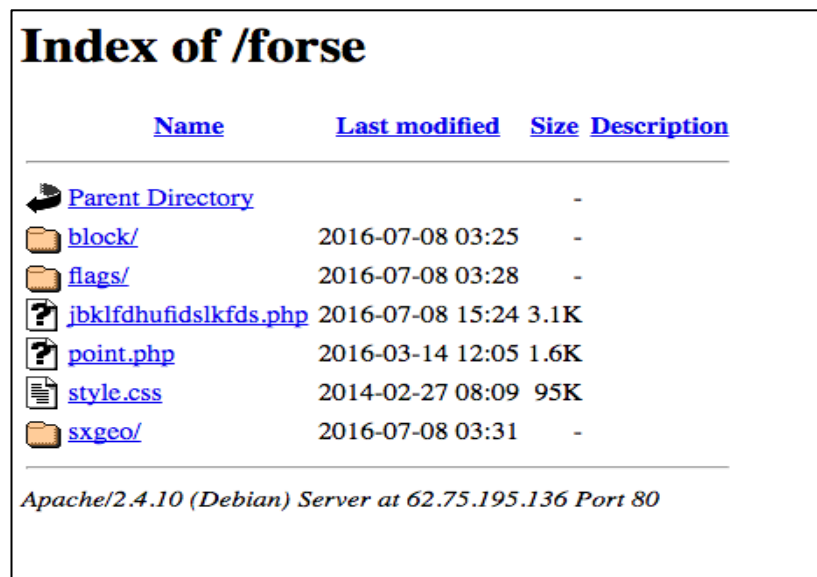
[2821562]: ETPRO TROJAN Win32/CryptFile2 Ransomware Fake Image Response








Just like the other instances of CryptFile2, these samples create a "HELP\_DECRYPT\_YOUR\_FILES" file that is displayed with Notepad. There are two e-mails associated with receiving the ransom payment: cx9@dr.com and cx9@post.com.



The open directory appeared as such:

**Figure 5:** Open directory #2 for CrypeFile2 campaign



Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">block/</a>	2016-07-08 03:25	-	
 <a href="#">flags/</a>	2016-07-08 03:28	-	
 <a href="#">jbkldfhufidslkfds.php</a>	2016-07-08 15:24	3.1K	
 <a href="#">point.php</a>	2016-03-14 12:05	1.6K	
 <a href="#">style.css</a>	2014-02-27 08:09	95K	
 <a href="#">xsgeo/</a>	2016-07-08 03:31	-	

Apache/2.4.10 (Debian) Server at 62.75.195.136 Port 80

We observed a PHP file in the open directory (jbkldfhufidslkfds.php) on this site, with a file modification date one day prior to the previously profiled site #1, indicating timeline overlap that suggests campaign activity. Some of the same directories existed (block, flags, xsgeo) in both site #1 and site #2, however there were distinct files such as point.php on site #2 that did not exist on site #1. Also, the logs were not exposed on site #2, and there was no obvious binary file to download. Accessing point.php did not generate any content or noticeable activity when visiting the site without having authenticated.

## Email Interactions with Threat Actors

Contact with threat actors was pursued via e-mail by a third party who was compromised by the ransomware. This individual then shared the mail details with ASERT. Actors were using tor to send mail, and were corresponding from an email account at the domain toke.com and an account from dr.com.

The third party mailed both cds0[@]dr.com and cds1[@]toke.com on September 13, 2016. A response was received on September 15 from “Frano Bob” using address cds0[@]dr.com asking for the compromise ID. That mail was sent with an X-Originating IP address of 74.208.4.200 (mout.gmx.com) and was received from 149.56.44.254 (IP address associated with OVH, which has been a tor node). This IP has been associated with spam activity [<https://cleantalk.org/blacklists/149.56.44.254>] between August 25 and Sep 23.

An email then arrived from the actor(s) on September 16 from “Robert Deniro” using address cds1[@]toke.com asking for the compromise ID. The wording was as such:

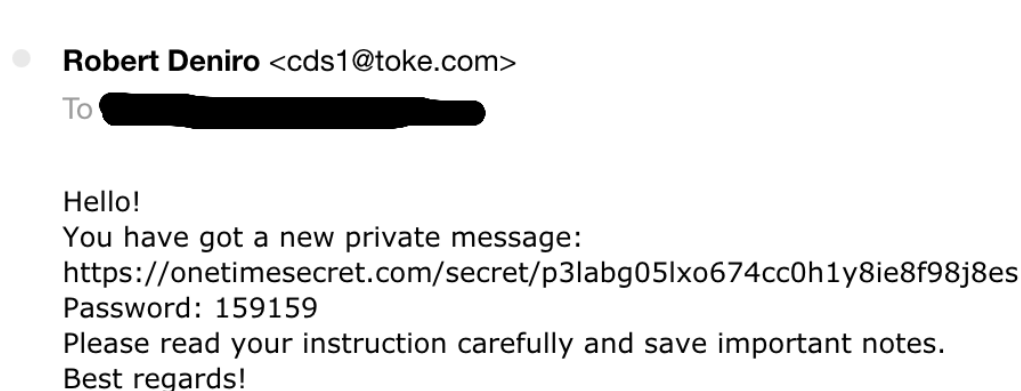
**Figure 6:** Initial response from ransomware threat actors

This was also sent with the same X-Originating IP as the aforementioned mail observed on September 15, (74.208.4.200), with the Received header value of 162.247.72.199. This IP address has also been used as a tor node, and is owned by the Calyx Institute in the US. It has been used for spam at least 327 times between December 28 of 2014 and October 12, 2016 per Cleantalk.org [<https://cleantalk.org/blacklists?record=162.247.72.199>].

The next mail arrived on September 17, from “Robert Deniro” cds1[@]toke.com with the same X-Originating IP as the first two mail messages, and a Received: header value of 197.231.221.211 which appears to be owned by Cyberdyne, in Liberia. The IP, also a tor node, is associated with various types of abuse, from forum spam [<https://stopforumspam.com/ipcheck/197.231.221.211>] to Wordpress hacking activity [<https://www.abuseipdb.com/check/197.231.221.211>] and spam [<https://cleantalk.org/blacklists?record=197.231.221.211>].

After a long period of no response from the victim, our source reported that threat actors wrote back on October 10, prompting him to purchase a decryptor within 48 hours or the price would double. This mail was again from “Robert Deniro” with X-Originating IP of 74.208.4.201 (mout.gmx.de). The Received: header value is 79.172.193.32, owned by Deninet in Hungary. As expected, this IP address is also associated with spam [<https://cleantalk.org/blacklists?record=79.172.193.32>], forum spam [<https://stopforumspam.com/ipcheck/79.172.193.32>] and has been or is currently a tor node.

After providing the ID to the threat actors, the actor replied with an e-mail directing the victim to the onetimesecret.com website with a one-time message and a six digit code required to view the message.

**Figure 7:** Secondary response from threat actors directing victim to payment instructions

This message was sent with an X-Originating-IP header of 74.208.4.201 (as previously observed) and a Received: header value of 176.10.104.240, yet another tor exit node that has been abused by spammers and other threat actors since at least December of 2015.

From here, the victim entered the six digit numeric passcode when accessing the URL on the website onetimesecret.com which then displayed a message from the actors that instructed the victim to send 2 BTC to a specified BTC address. Threat actors here are charging 2 BTC, which was \$1278.58 USD at the time of this writing.

**Figure 8:** Encrypted payment instructions sent via onetimesecret.com website

**Russian translation is now available (2016-09-08)**

S

This message is for you:

Hello.  
You need to pay 2 Bitcoin.  
Wallet to pay for: 121wgRPR1RZvQP1a1QUJpUtPmnZJHrNFj1  
When the pay, let us know, we will issue a software to decrypt your files.  
Thank you.

HELP FOR BUY BITCOIN

1. Create Bitcoin wallet here:  
<https://blockchain.info/wallet/new>

2. Buy 2 BTC with cash, using search here:  
[https://localbitcoins.com/buy\\_bitcoins](https://localbitcoins.com/buy_bitcoins)  
<https://localbitcoins.com/> - on this page you will be able fast and securely buy Bitcoins for cash or by bank transfer,  
just pay attention to the seller's reputation whom you are going to pay. The higher the reputation of seller - the more secure an exchange.

3. Send 2 BTC to this Bitcoin address:  
121wgRPR1RZvQP1a1QUJpUtPmnZJHrNFj1

4. Send any e-mail to:  
cds1@toke.com

(careful: we will only show it once.)

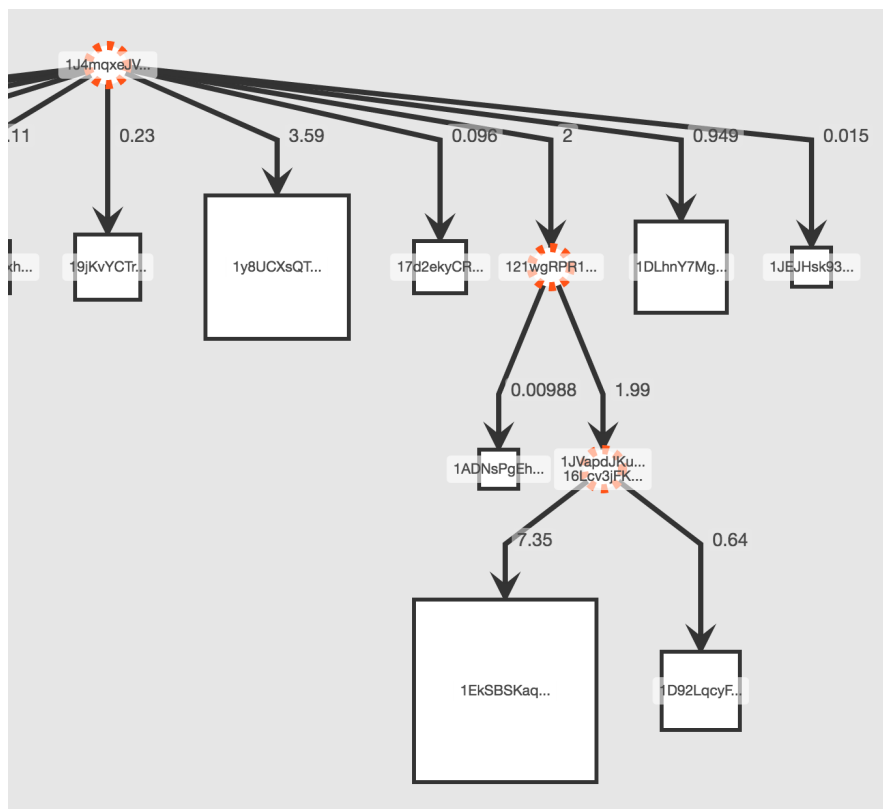
Initially, we observed no transactions involving the address 121wgRPR1RZvQP1a1QUJpUtPmnZJHrNFj1 however it has received 2 bitcoin so far (worth \$1,249.16 at transaction time). This means that the actors are not using unique BTC addresses per potential victim, although it is possible they are using the BTC address only once when payment is received.

On 10/20/2016 at 14:07, someone sent 2BC from 1J4mqxeJVehVRZA13LgioqBdZZf4Ei9Nkb to 121wgRPR1RZvQP1a1QUJpUtPmnZJHrNFj1. 51 Minutes later, actors sent 1.99 BTC to 1JVapdJKuh5zxugZGrxjn9bUcTCzfv75Lj and 0.0098757 BTC to 1ADNsPgEh74VRCSr4ZiTzPLhHtAtAfXqYd.

**Figure 9:** 2 BTC payment to BTC address used by threat actors



**Figure 10:** Another way of visualizing the 2 BTC transaction through blockseer.com



The quality of the language suggests that the actor(s) may not be native English speakers. Note that the dr.com e-mail address is now out of the picture, with all correspondence going to the toke.com address. Anyone can get an e-mail address @toke.com or dr.com via mail.com for free.

**Figure 11:** Ease of obtaining free toke.com and dr.com addresses

**mail.com**  
a 1&1 company

Male

**Date of Birth**  
Month:  Day:

**Country**  
United States

**Desired Email Address**

**Choose a Password**

**Re-type Password**

clubmember.org  
collector.org  
cutey.com  
dbzmail.com  
doglover.com  
doramail.com  
galaxyhit.com  
gardener.com  
greenmail.net  
hackermail.com  
hilarious.com  
keromail.com  
kittymail.com  
linuxmail.org  
lovecat.com  
marchmail.com  
musician.org  
nonpartisan.com  
petlover.com  
photographer.net  
snakebite.com  
songwriter.net  
techie.com  
theplate.com  
**toke.com**  
uymail.com

**Create a new email account**

deliveryman.com  
diplomats.com  
disposable.com  
doctor.com  
**dr.com**  
engineer.com  
execs.com  
fastservice.com

Thankfully, the victim who helpfully came forward was able to migrate to a new system and didn't lose anything important, although not all ransomware victims are as fortunate due to a lack of adequate backup and restore solutions in place.

## Conclusion

Ransomware continues to be a substantial problem for many victims. Every week, ASERT encounters substantial movement involving the ransomware threat landscape as the victim count increases. Threat actors in this case don't appear to be running a huge campaign from the vantage point of the victims profiled herein, however we must be mindful of the fact that this is just one aspect of one ransomware campaign. Since most analysis of ransomware activity tends to focus on endpoint malware activity, encryption method, and in some cases how to decrypt without paying the ransom, visibility into the threat from the server side hopefully provides additional context to this malware family that can be used to enrich situational awareness surrounding this and other ransomware activity.

## About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as “super remediators,” and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at <http://www.arbornetworks.com/threats/>.