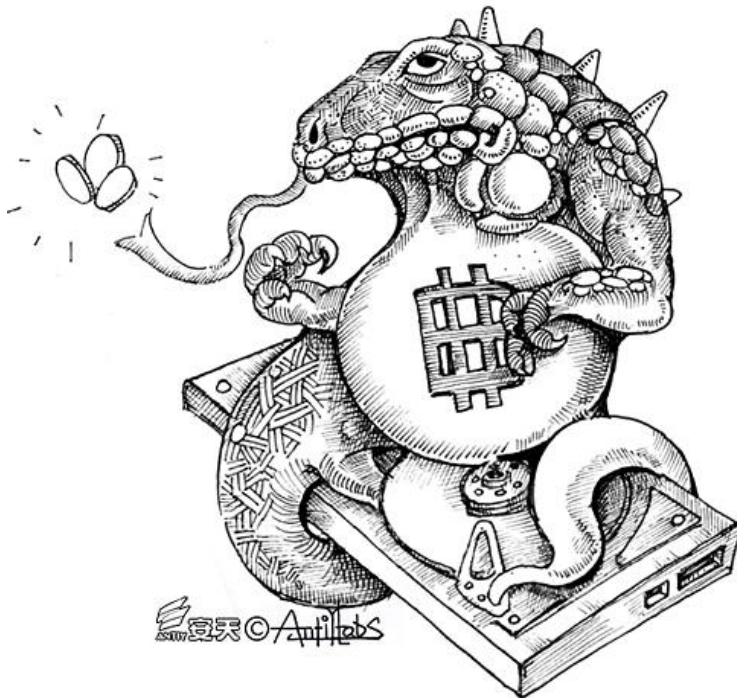




AN ANALYSIS REPORT OF BLACKMAILER TROJAN SPREAD BY EMAILING JS SCRIPT

By Antiy PTA Group



First draft: December 4, 2015, 11: 11



Content

1	INTRODUCTION	1
2	SOCIAL WORK EMAIL SPREAD	1
3	ANALYSIS OF SAMPLE	2
3.1	JS SCRIPT FILE:	2
3.2	SAMPLE ANALYSIS OF CORRESPONDING BLACKMAILER	3
4	TESLA2.X NETWORK FRAMEWORK ANALYSIS	9
5	SUMMARY	11
	APPENDIX 1: REFERENCES	12
	APPENDIX 2: ABOUT ANTIY	12
	APPENDIX 3: TESLACRYPT2.X MD5.....	13

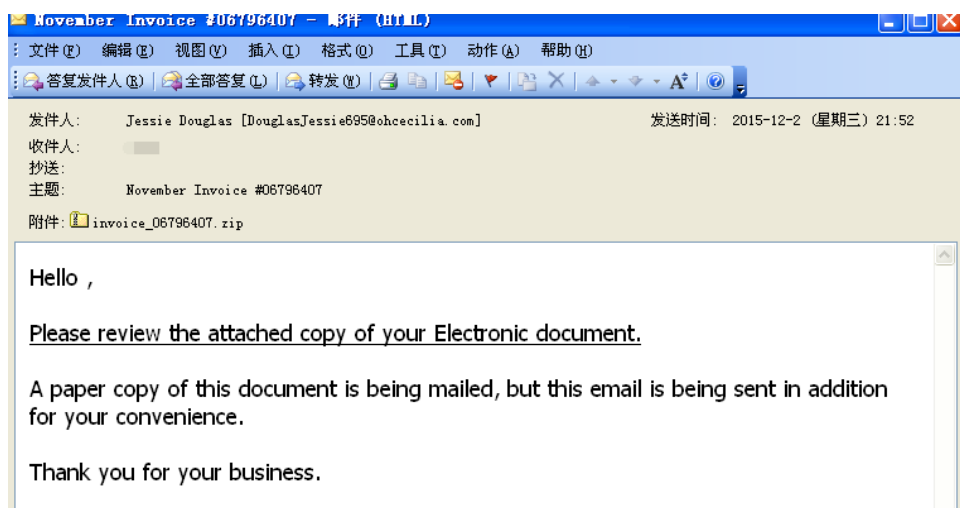
1 Introduction

A new blackmailer variant email with new transmission characters was captured by Antiy Threat Situational Awareness System on December 2, 2015, which was guided by a JS script in compressed package rather than spread by sending binary file load directly.

Antiy PTA group has made an analysis of related incidents and samples. This sample is TeslaCrypt 2.x, a variant of TeslaCrypt. A zip file near to the mail is unzipped to a JS script. After JS script is executed, it will download TeslaCrypt2.x to run, traverse computer files and encrypt 186 kinds of suffix format files, including documents, pictures, audio and etc. After the encryption, it will open blackmailer's homepage to blackmail and ask for 500 USD to decrypt within a specified time. If overdue, 1000 USD is needed. As TeslaCrypt2. X variant changing the way of key calculation with the ECDH algorithm, hackers and victims can negotiate a key without sharing any secret. TeslaCrypt decryption tool released by Cisco ^[1] has been unable to decrypt.

2 Social work email spread

TeslaCrypt2.x spreads by sending plenty of emails, one screenshot of an email is as follows:



It uses "Hello" to address rather than a specific name. The text body is "Please check the attachment, E-mail documents will be mailed to you and this electronic version is sent to you for your convenience ". In order to show the importance of this email, blackmailer emphasizes that the mail is sending by a traditional way. Thus, the recipient may regard it as an important one and check the attachment.

E-mail attachment is invoice_06796407.zip, unzipped as INVOICE_main_BD3847636213.js file which is a downloader used to download TeslaCrypt 2. X and execute.

3 Analysis of sample

3.1 JS script file:

Virus name	Torjan/ js .Downloader.gen
Original file name	INVOICE_main_BD3847636213.js
MD5	0352ACD36FEDD29E12ACEB0068C66B49
Size	6.48KB (6,644 bytes)
Interpretive language	Jscript
VT first update time	2015-12-02
VT detect result	23/52

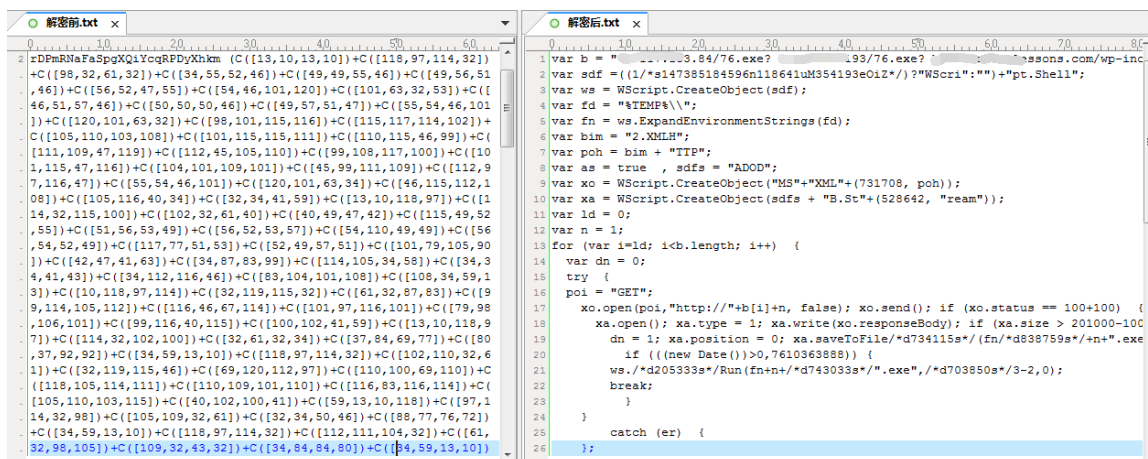
INVOICE_main_BD3847636213.js adopts transformed encryption to avoid antivirus detection, which can self-decrypt by Eval function to obtain clear code. When user double-clicks this JS file, it will download executable files from three network addresses orderly to the Temp directory and execute them. If downloads and runs successfully in the first address, the following two addresses will not download. The network address is divided by space:

74.117.183.84/76.exe

5.39.222.193/76.exe

bestsurfinglessons.com/wp-includes/theme-compat/76.exe

The content contrast of relevant code before and after decryption is as follows:



3.2 Sample analysis of corresponding blackmailer

This variant is similar to previous malicious act in Tesla report and can take another security team IsightPartners' s report for reference [2]. After the samples being executed, it will AES256 encrypt the document, save the recovery file required information to the registry and text files and sends related information to Tor server controlled by hacker.

Virus name	Trojan/Win32.ransomware.gen
Original file name	76.exe
MD5	449C43E250D075D6F19FACB0B51F4796
Processor framework	X86-32
Size	391.0 KB (400,384 bytes)
Format	BinExecute/Microsoft.EXE[:X86]

Time	2015:12:03 06:19:51+01:00
Digital signature	NO
Shell	NO
Compiled language	Microsoft Visual C++ 9.0
VT first update time	2015-12-03
V T detect result	25/52

Samples uses junk instruction and debugging techniques and starts by hanging to read their own data and rewrite to a new hang after decryption process, and determines whether their own path is the specified Application Data file path. If not, it will move to this directory and modify the file name as a random five letters -a.exe, (such as mghsd-a.exe). With creating a fixed mutex value "78456214324124", PTA found it adopted bcdedit disabled security mode and recovery mode in dynamic analysis environment. It creates a startup in the registry:

```
HCUR\Software\Microsoft\Windows\currentVesion\run.
```

Then, it creates multiple working threads, analysis of some key threats is as follows:

- 1) Delete volume shadow copy in system , vssadmin.exe delete shadows /all /Quiet
- 2) Start threat traverse process path, if the path concludes any string of Taskmgr、 procexp、 regedit、 msconfig、 cmd.ex, end related process. Thus, CMD, task manager and process check tools cannot open and thus cannot check and end malicious sample process.
- 3) Another thread is mainly used to connect to the Internet to report information to hackers controlling server, the connected URLs mainly include:

```
ASCII "http://myexternalip.com/raw"
ASCII "https://alcov44uvckrend.tor2web.org/inst.php"
ASCII "https://alcov44uvckrend.onion.to/inst.php"
```

Visit myexternalip.com/raw to acquire outer network IP information of victim host.

Submit information by visiting following network addresses:

Table3-1 Domain names of visiting network

Domain names	IP
regiefernando.me	192.185.5.252
schriebershof.de	78.46.79.167
apotheke-stiepel.com	81.169.145.157
woodenden.com	23.229.206.40
leboudoirdesbrunettes.com	213.186.33.87
Albanytotalwellness.com	66.147.244.93
djepola.com	174.136.13.48
aprenderabailarsevillanas.com	5.56.57.101


```

ASCII "http://regiefernando.me/images/slideshow/sysmisc.php"
ASCII "http://schriebershof.de/tmp/misc.php"
ASCII "http://apotheke-stiepel.com/tmp/misc.php"
ASCII "http://woodenden.com/sysmisc.php"
ASCII "http://leboudoirdesbrunettes.com/wp-content/uploads/misc.php"
ASCII "http://albanytotalwellness.com/wp-content/uploads/misc.php"
    
```

Most files are Get request connection PHP files, parameter formats of the request and data of one request are as follows:

Sub=%s&key=%s&dh=%s&addr=%s&size=%lld&version=%s&OS=%ld&ID=%d&gate=%s

&ip=%s&inst_id=%X%X%X%X%X%X%X , the data that actually sent is as below:

<pre>Sub=Ping&key=F7D8C803858E49F99DD 3F64CEFFF0E8F4CD99737572FED4FC0A 9BD4B01AA7079&dh=34B091E485246FC F9AF47C2F7646FB3581DCE012E64688D 6FF4FEA07BC349C69A23EB960D9BC21E 14352F115BDADE74036985A88E0882C4 656422F077B2F60&addr=1CnQxEQe8oL HWcyiwanuZKMdkFjAf4GRjL&size=0&v ersion=2.2.0&OS=2600&ID=1102&gat e=schriebershof.de&ip=163.125.14 6.191&inst_id=B57F269E9D49E8B...</pre>	
---	---

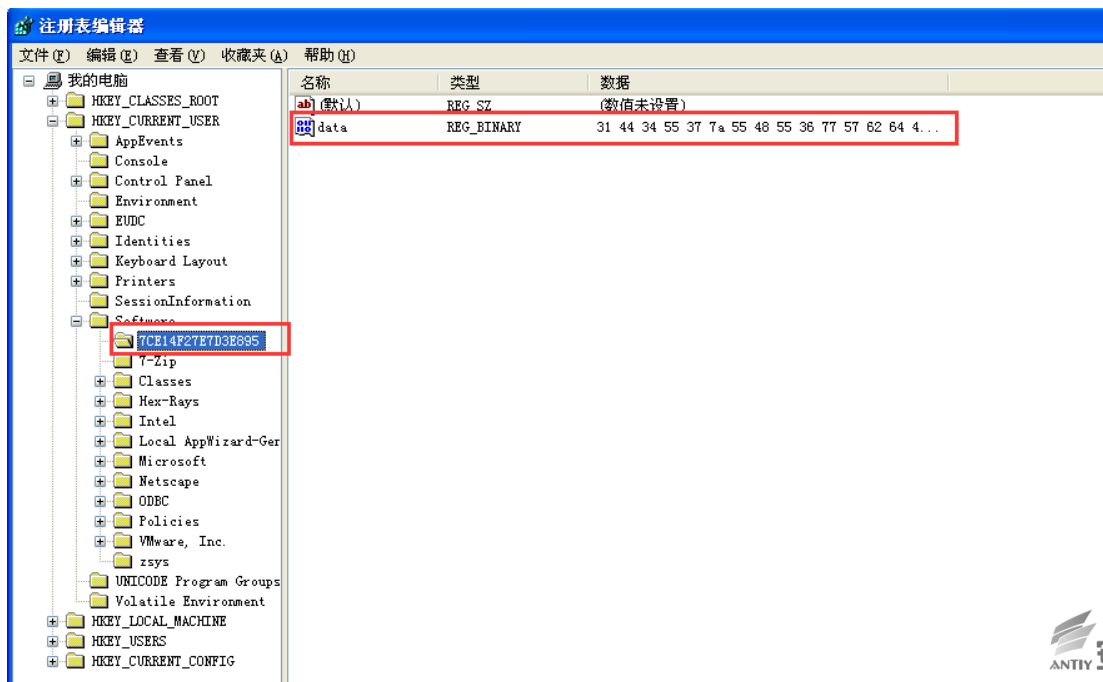
4) Another thread is the malicious core function that encrypts specific suffix file:

First, get all disk information on local system. If it is a local disk and network disk, traverse all disk files. When the file name contains recove, .VVV, release directly. If not, detect file extension. If the extension name matches with any of the following one, it starts to maliciously encrypt files:

```
.r3d .css .fsh .lvl .p12 .rim .vcf.3fr .csv .gdb .m2 .p7b .rofl .vdf.7z .d3dbsp .gho .m3u .p7c .rtf .vfs0.accdb .das .hkdb .
m4a .pak .rw2 .vpk.ai .dazip .hxx .map .pdd .rwl .vpp_pc.apk .db0 .hplg .mcmeta .pdf .sav .vtf.arch00 .dba .hvpl .m
db .pef .sb .w3x.arw .dbf .ibank .mbackup .pem .sid .wb2.asset .dcr .icxs .mddata .pfx .sidd .wma.avi .der .indd .m
df .pkpass .sidn .wmo.bar .desc .itdb .mef .png .sie .wmv.bay .dmp .itl .menu .ppt .sis .wotreplay.bc6 .dng .itm .mlx
.pptm .slm .wpd.bc7 .doc .iwd .mov .pptx .snx .wps.big .docm .iwi .mp4 .psd .sql .x3f.bik .docx .jpe .mpqge .psk .sr
2 .xf.bkf .dwg .jpeg .mrwref .pst .srf .xlk.bkp .dxg .jpg .ncf .ptx .srw .xls.blob .epk .
JS .nrw .py.sum .xlsb.bsa .eps .kdb .ntl .qdf .svg .xlsm.cas .erf .kdc .odb .qic .syncdb .xlsx.cdr .esm .kf .odc .raf .t12
.xxx.cer .ff .layout .odm .rar .t13 .zip.cfr .flv .lbf .odp .raw .tax .ztmp.cr2 .forge .litemod .ods .rb .tor.crt .fos .lrf .odt
.re4 .txt.crw .fpk .ltx .orf .rgss3a .upk
```

Related encryption process and encryption file formats can take Kappa analysis for reference which mainly adopts ECDH algorithm to encrypt the key [3]. Cisco Tesla decryption tool [2] can decrypt Tesla early varieties, the early varieties can save the key to file "key.bat" . And key generation and save of Tesla2.x variants have changed and will be stored in the registry

HKCU\HKEY_CURRENT_USER\Software\HKEY_CURRENT_USER\Software\7CE14F27E7D3E895 , 7CE14F27E7D3E895 is personal identification code, every user is different, which is used by hackers to identify the user on the server. Information stored in the registry is the same as recover_file_*.txt

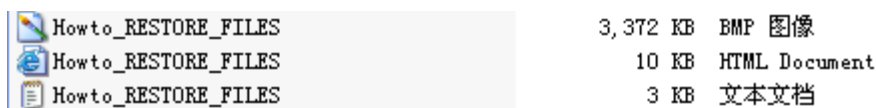


The encrypted data covers the source file and then modifies the file name. In addition to infect local computer, it will try to enumerate computers in a network and infect encrypted files. When all encryption is completed, it will generate recover_file_*.txt in the My Documents directory, its content is as follows:

```

1 161UXbNoRSh8sBeDzJZt2AUSE7mYJzqmvy
2 688ACCCADAA9C4A778B97DE264962C004F7E36A7A2C4C537D96B74447F959CE7
3 0E9BA3CA8593BE2B3DB1FD64EE2A9D117EC924973CDAC97D14B9CA73A9E4C092DB54CA51C2A076EA79CCC50F2A194A00F8F4'
4 8BFA62F2C5F1E1E0
5 76
    
```

And then, it generates Howto_RESTORE_FILES in the following three formats in user desktop and opens which is used to remind users:



Finally, it will pop up a warning page to prompt blackmailer homepage visiting and key encrypted.

And the keys can be got by visiting blackmailer server.

How did this happen?
 Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
 All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
 Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our Secret Server!!! *

What do I do?
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
 If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://alcov44uvcwkrend.paybtc798.com/7CE14F27E7D3E895>
2. <http://alcov44uvcwkrend.btcpay435.com/7CE14F27E7D3E895>
3. <https://alcov44uvcwkrend.onion.to/7CE14F27E7D3E895>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: [alcov44uvcwkrend.onion/7CE14F27E7D3E895](https://alcov44uvcwkrend.onion.to/7CE14F27E7D3E895)
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
 Your Personal PAGES:
<http://alcov44uvcwkrend.paybtc798.com/7CE14F27E7D3E895>
<http://alcov44uvcwkrend.btcpay435.com/7CE14F27E7D3E895>
<https://alcov44uvcwkrend.onion.to/7CE14F27E7D3E895>
 Your Personal PAGES (using TOR-Browser): [alcov44uvcwkrend.onion/7CE14F27E7D3E895](https://alcov44uvcwkrend.onion.to/7CE14F27E7D3E895)
 Your personal code (if you open the site (or TOR-Browser's) directly): **7CE14F27E7D3E895**

To get the key to decrypt files, you have to pay 500 USD. If payment is overdue, you have to pay 1000 USD.

Your files are encrypted.
 To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **09/12/15** the cost of decrypting files will increase **2** times and will be **1000 USD**

Prior to increasing the amount left:
160h 01m 17s

First connect IP: 219.134.48.152

Refresh Payment FAQ Decrypt 1 file for FREE Support

We present a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register Bitcon wallet (click here for more information with pictures)
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

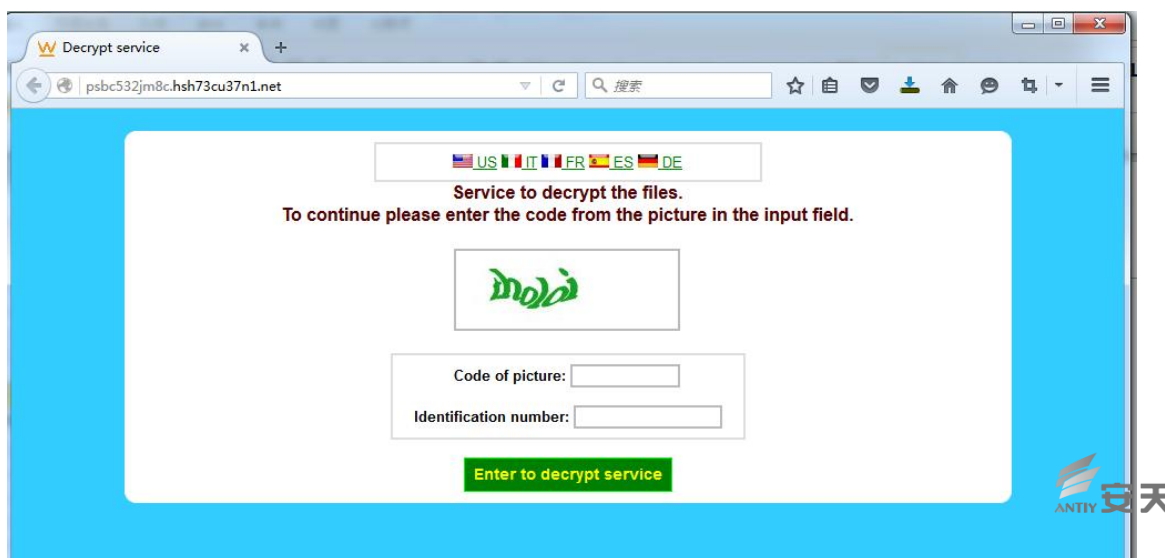
- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- CoinCafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- CEX IO - Buy Bitcoins with VISA/MASTERCARD or Wire Transfer
- btcdirect.eu - THE BEST FOR EUROPE

Some additional sellers:

- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site

4 Tesla2.x network framework analysis

Antiy technicians found that blackmailer network sever hides in Tor network to avoid tracking. Clicking the page that blackmailer provided is as follows: inputing identification number can prevent automated traverse and query of victim information.



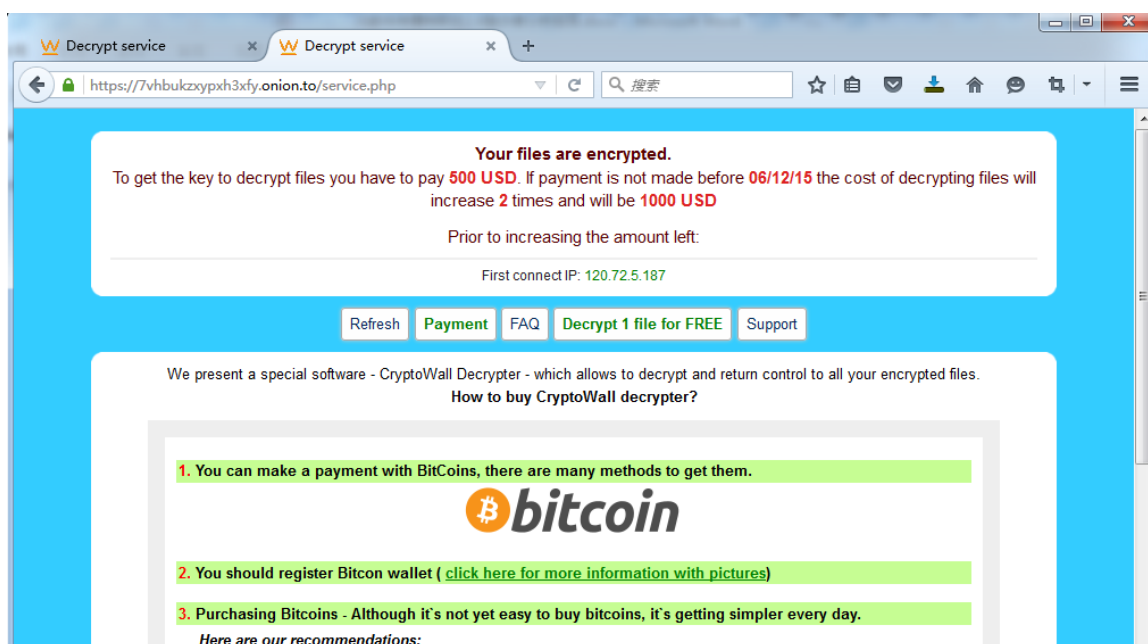
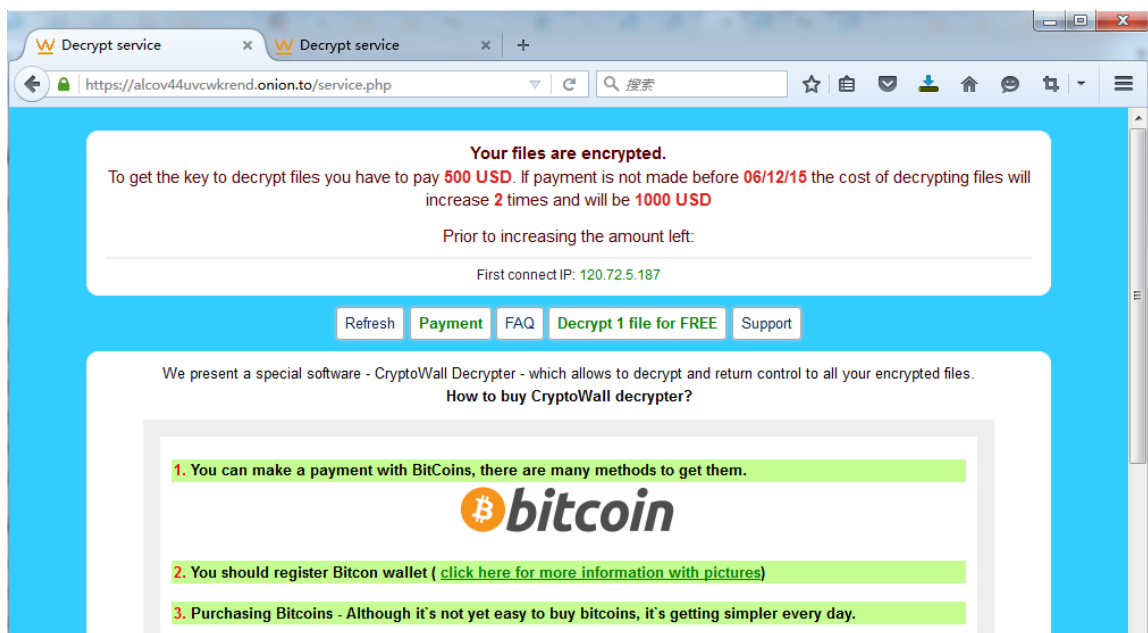
After correlating data, the servers that the following URL point to are the same, which are servers of Tesla (2) x blackmailer variants and the information that queried by the same ID in these three websites is also the same.

psbc532jm8c.hsh73cu37n1.net

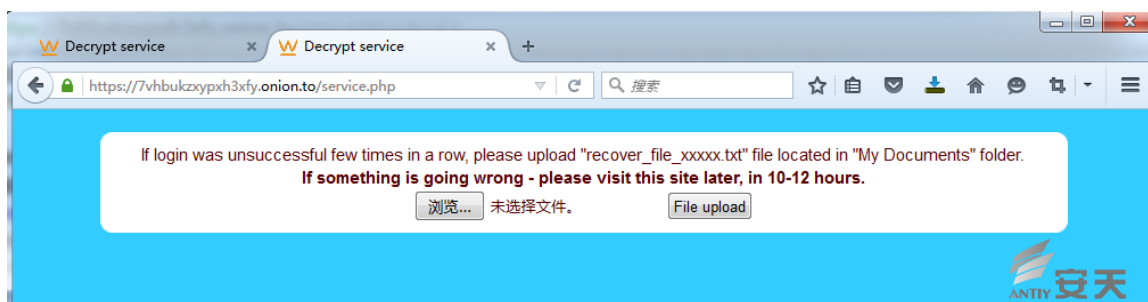
alcov44uvcwkrend.onion.to

7vhbukzypxh3xfy.onion.to

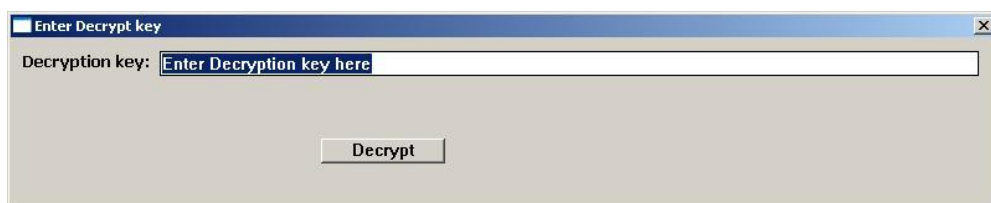
Victim IP120.72.5.187, the data that two URLs returned is the same.



If the reported server of blackmailer is blocked by network security equipment, it cannot receive the encrypted information reported, and the query by personal code in this page will prompt login unsuccessful. In order to be able to provide decryption services, blackmailer has designed a function, that is, save recover_file_xxxxx. txt file upload in "My Documents" folder and then the encrypted information can be got. The diagram is below:



Through a correlation of network framework, a decrypted URL program is found, that is <http://psbc532jm8c.hsh73cu37n1.net/decrypt.zip> MD5 : AE3E2206ACB24A60FF583F2CF0C77E59



It also contains PDB information in C:\wrk\decrypt\decrypt\Release\decrypt.pdb. It can be got that public and private key encryption and decryption algorithm of OpenSSL ECDH is used, which also shows that it adopts ECDH key to encrypt files.

5 Summary

Blackmailer can spread executable PE load through email packaged software by double extension, SCR extension skills, etc. In this campaign, it uses JS format' s disguise to avoid detection and prevention of antivirus software. At the same time, Tesla 2. x blackmailer adopts ECDH encryption algorithm and puts user data in danger, rather than previous reverse get key to decrypt files.

From a past monitoring, we found that the victims of blackmailer malware are from the original individual users widely to business users, or even servers. Antiy has strengthened its detection and defense ability of blackmailer Trojan in its PTD system and IEP system.

As the increasing danger of data security threats, enterprise users also need to defense blind area through competency-based products and effectively improve network security awareness, build defense in depth system, and get threat information through threat information platforms timely to reduce further proliferation of risk.

Appendix 1: References

[1] teslacrypt 和修复工具

<https://blogs.cisco.com/security/talos/teslacrypt>

[2] teslacrypt-2 行为分析

<http://www.isightpartners.com/2015/09/teslacrypt-2-0-cyber-crime-malware-behavior-capabilities-and-communications>。

[3] teslacrypt 2.0 伪装 cryptowall

<https://securelist.com/blog/research/71371/teslacrypt-2-0-disguised-as-cryptowall/>

Appendix 2: About Antiy

Starting from antivirus engine research and development team, Antiy now has developed into an advanced security product supplier with four research and development centers, nationwide detection and monitoring ability as well as products and services covering multiple countries. With a fifteen-year continual accumulation, Antiy has formed massive security knowledge and promoted advanced products and solutions against APT with integrated application of network detection, host defense, unknown threat identification, data analysis and security visual experiences. With the recognition of technical capacity by industry regulators, customers and

partners, Antiy has consecutively awarded qualification of national security emergency support unit four times and one of the six of CNNVD first-level support units. Antiy detection engine for mobile is the first Chinese product that obtained the first AV - TEST (2013) annual awards and more than ten of the world' s famous security vendors choose Antiy as their detection partner.

More information about antivirus engine: [http : //www.Antiy.com](http://www.Antiy.com) (Chinese)

[http : //www.Antiy.net](http://www.Antiy.net) (English)

More information about Antiy against [http : //www.Antiy.cn](http://www.Antiy.cn)

APT products:

Appendix 3: TeslaCrypt2.x MD5

1e20df486a29da12680d0098f95cbf88

b296703818ac3980aceba058b2c3b388

5abd837586f664fa02e3a126824d322f

3722b18641aa6ede7dc102364b583f2e

542d049c074e39af5e25a5d2dd456651

446071be407efeb4e0d7c83bb504774a

ca20df42fbff5178e88ab38538acb79e

c1ee2599617cdb891f290020caba8b8e

5ace41e2990e6196bc50bc72b8494a3e

93e7eb9c02ab7d087e5337e94ddfb1b9

667802f02270c1226b3caf2f07bb7dd4

449c43e250d075d6f19facb0b51f4796

4f453be4dfd17f5628ccda2c6fb3f837

bfbbe661494c651bb2d3949ffde4bace

d39092cb7c4d4e4e1d8f20f90ae20e24

321807acbfdbeabd668705848a9c2136

de0f12ec4cd4a5b002c1ce84425665cc

a3bc6346968b46e31412b80fea9aa3dc

a7dd452baa326abeeca003a14a1114f4

1ddfb5ae1dc258e1bf1c95b5059730b0

38d3009c0f078a44cceb0ef036916df2

616a8c3c655eb1dfa371929a71bc94aa

3fad8d70f49f9cbb5d70efdef85d2d24

7a46e2a5f3ff1c0a8b2974830de0bd29

cbe71af2ddd4c38cc068fca2730a147d