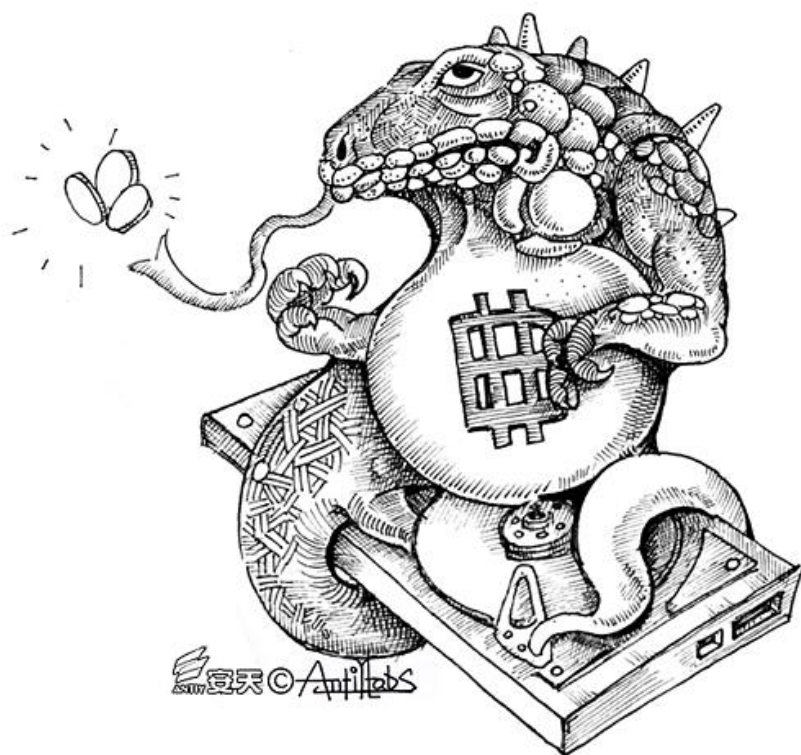




邮件发送 JS 脚本传播敲诈者木马的分析报告

安天追影小组



报告初稿完成时间：2015 年 12 月 04 日 11 时 11 分



目 录

1	概述.....	1
2	社工邮件传播	1
3	事件样本分析	2
3.1	JS 脚本文件:	2
3.2	对应敲诈者样本分析	3
4	TESLA2.X 网络架构分析	8
5	总结.....	10
	附录一：参考资料.....	11
	附录二：关于安天.....	11
	附录三：TESLACRYPT2.X MD5	11

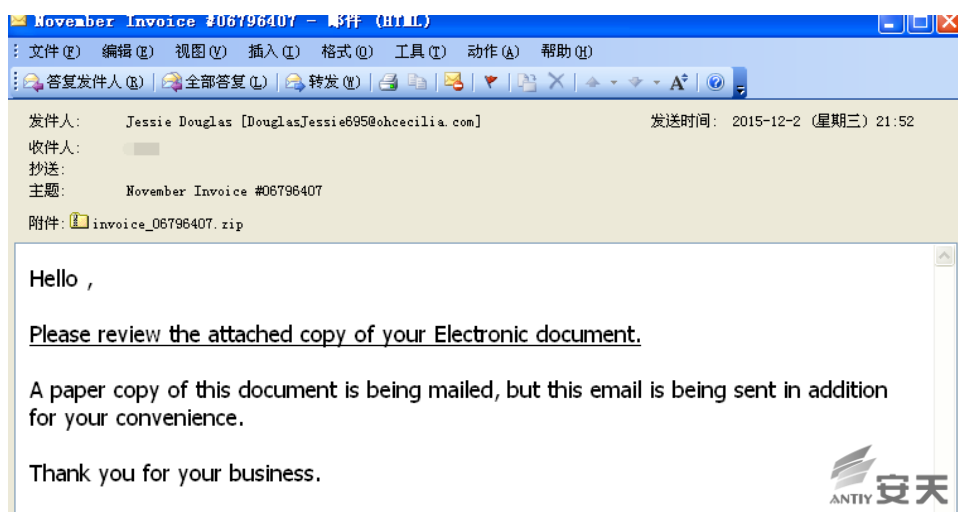
1 概述

安天威胁态势感知系统 2015 年 12 月 2 日捕获到有新的传播特点的敲诈者变种邮件，其不再采用直接发送二进制文件载荷的传播模式，而是以一个存放在压缩包中的 JS 脚本为先导。

安天追影分析小组对相关事件和样本进行了分析。该样本系 TeslaCrypt 的另一个变种 TeslaCrypt 2.x，邮件附近是一个 zip 压缩文件，解压 zip 文件得到一个 js 文件，运行 js 文件，会下载 TeslaCrypt2.x 运行，遍历计算机文件，对包括文档、图片、影音等 186 种后缀格式文件进行加密，加密完成后打开敲诈者的主页，在指定期限内需要支付 500 美元才能得到解密密钥，过期需要支付 1000 美元。因为 TeslaCrypt2.x 变种改变了密钥的计算方式，采用了 ECDH 算法，黑客与受害者双方可以在不共享任何秘密的情况下协商出一个密钥，采用此前思科等厂商发布的 TeslaCrypt 解密工具^[1]已经无法进行解密。

2 社工邮件传播

TeslaCrypt2.x 版本通过发送大量邮件进行传播，邮件截图如下：



邮件直接称呼 Hello，没有给出具体的姓名，邮件正文：“请查收附件，电子邮件的文档会邮寄给您，本电子版本是发送给您方便查看”。为了表明邮件的重要性敲诈者在邮件中强调邮件正通过传统方式邮寄，这样收件人认为可能是重要的邮件而查看相关附件。

邮件的附件为 invoice_06796407.zip，经过解压获得 INVOICE_main_BD3847636213.js 文件，是一个下载者功能，用来下载 TeslaCrypt 2.x 并执行。

3 事件样本分析

3.1 js 脚本文件：

病毒名称	Torjan/JS.Downloader.gen
原始文件名	INVOICE_main_BD3847636213.js
MD5	0352ACD36FEDD29E12ACEB0068C66B49
文件大小	6.48KB (6,644 字节)
解释语言	Jscript
VT 首次上传时间	2015-12-02
VT 检测结果	23/52

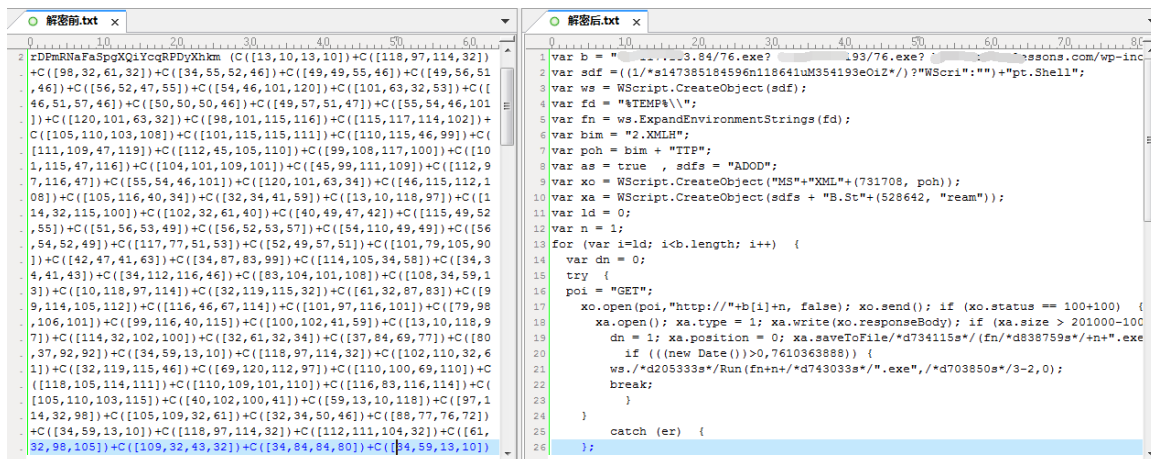
INVOICE_main_BD3847636213.js 文件采用了变形加密躲避杀软检测，通过 Eval 函数进行自解密可以获得明文代码，当用户双击这个 js 文件，其会从三个网络地址顺序下载可执行文件到 Temp 目录下并执行。如果第一个地址下载成功并运行，则后续两个地址就不会进行下载。网络地址以空格分割：

74.117.183.84/76.exe

5.39.222.193/76.exe

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

相关代码在解密前后的内容对照如下：



3.2 对应敲诈者样本分析

该变种和此前的 Tesla 报告中恶意行为大致相同,可以参考另一安全团队 isightpartners 之前发布的报告

^[2]。样本运行后对文档进行 AES256 加密,保存恢复文件所需信息到注册表和文本文件。并发送相关信息给黑客控制的 Tor 服务器。

病毒名称	Trojan/Win32. ransomware. gen
原始文件名	76.exe
MD5	449C43E250D075D6F19FACB0B51F4796
处理器架构	X86-32
文件大小	391.0 KB (400, 384 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015:12:03 06:19:51+01:00
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++ 9.0
VT 首次上传时间	2015-12-03
VT 检测结果	25/52

样本使用花指令以及反调试技术,会以挂起方式启动自身,读取自身数据解密后重写入新的挂起进程,并判断自身路径是不是指定的一个 Application Data 文件路径,若不是则移到该目录并修改文件名为随机 5 位字母-a.exe, (例如 mghsd-a.exe)。 创建一个固定的互斥量值“78456214324124” 动态分析环境下追

影设备也发现了其采用 bcdedit 禁用安全模式、恢复模式，在注册表创建自启动项：

HCUR\Software\Microsoft\Windows\currentVesion\run。

接下来创建多个工作线程，其中一些关键线程行为分析如下：

- 1) 删除系统里的卷影副本，vssadmin.exe delete shadows /all /Quiet
- 2) 启动线程遍历进程路径，如果路径中包含 Taskmgr、procexp、regedit、msconfig、cmd.exe 任意一个字符串则结束相关进程，这样 CMD、任务管理器，进程查看工具无法打开，就无法查看和结束恶意样本进程。
- 3) 另一个线程主要进行联网上报信息给黑客控制的服务器，连接的网址主要有如下几个：

```
ASCII "http://myexternalip.com/raw"
ASCII "https://alcov44uvcwkrend.tor2web.org/inst.php"
ASCII "https://alcov44uvcwkrend.onion.to/inst.php"
```

其中访问 myexternalip.com/raw 获取受害主机的外网 IP 信息。

访问下面的网络地址提交信息:

表 3-1 访问网络域名列表


域名	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"
```

基本上都是 Get 请求连接 PHP 文件，请求中的参数组成格式以及某次请求数据如下：

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%X, 实际发送的数据如下图所示：

<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) 再一个线程就是恶意的核心功能了加密特定后缀文件：

首先获取本地系统上存在的所有磁盘信息，如果是本地磁盘和网络磁盘的话，遍历磁盘所有文件，当文件名含有 recove、.vvv 就直接放行，如果没符合的，就检测文件的扩展名，如果扩展名匹配了下列中任意一个就会开始恶意加密文件：

```
.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
.mdb .pef .sb .w3x .arw .dbf .ibank .mdbbackup .pem .sid .wb2 .asset .dcr .icxs .mddata .pfx .sidd .wma .avi .der .in
dd .mdf .pkpass .sidn .wmo .bar .desc .itdb .mef .png .sie .wmv .bay .dmp .itl .menu .ppt .sis .wotreplay .bc6 .dng .i
tm .mlx .pptm .slm .wpd .bc7 .doc .iwd .mov .pptx .snx .wps .big .docm .iwi .mp4 .psd .sql .x3f .bik .docx .jpe .mpqg
e .psk .sr2 .xf .bkf .dwg .jpeg .mrwref .pst .srf .xlk .bkp .dxx .jpg .ncf .ptx .srw .xls .blob .epk .js .nrw .py.sum .xlsb .b
sa .eps .kdb .ntl .qdf .svg .xlsx .cas .erf .kdc .odb .qic .syncdb .xlsx .cdr .esm .kf .odc .raf .t12 .xxx .cer .ff .layout .od
m .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
```

相关的加密过程以及加密文件格式可以参考卡巴的分析文章，主要是采用了 ECDH 算法进行加密密钥的生成

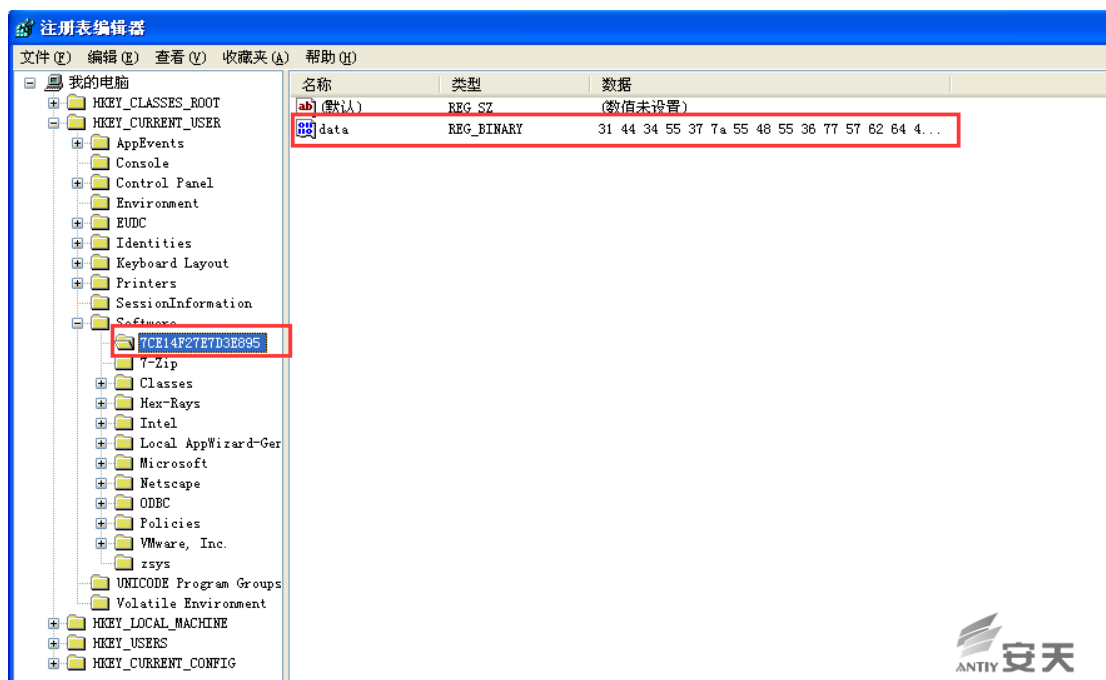
错误!未找到引用源。。之前的思科 Tesla 解密工具**错误!未找到引用源。**可以解密 Tesla 早期变种，其早起

变种会保存密钥到文件“key.bat”。而 Tesla2.x 变种的密钥生成和保存发生变化，会保存在注册表

HKCU\HKEY_CURRENT_USER\Software\HKEY_CURRENT_USER\Software\7CE14F27E7D3E895，其

中 7CE14F27E7D3E895 是个人标识码，每个用户不同，黑客服务器上根据这个标识来识别用户。注册表

中保存的信息和下面生成的 recover_file_*.txt 相同



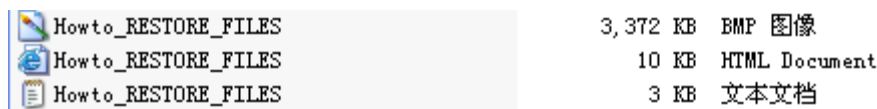
加密后的数据覆盖源文件，然后重新修改文件名。除了感染本机，还会试图枚举网络中的计算机，尝试感染加密其中的文件。当全部加密完成后，就会在 My Documents 目录下生成跟文件恢复相关 recover_file_*.txt 的文件，其中的内容如下：

```

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

```

然后在用户桌面上生成如下三种格式的 Howto_RESTORE_FILES 文件并打开，用来提醒用户用的：



最后弹出警告页，提示访问敲诈者的主页，提示密钥被加密，可以访问敲诈者的服务器获取密钥。

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.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.to/7CE14F27E7D3E895

Your personal code (if you open the site (or TOR-Browser's) directly): **7CE14F27E7D3E895**

需要在指定期限支付 500 美元才能得到解密密钥，过期需要支付 1000 美元。

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 Bitcoin 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:

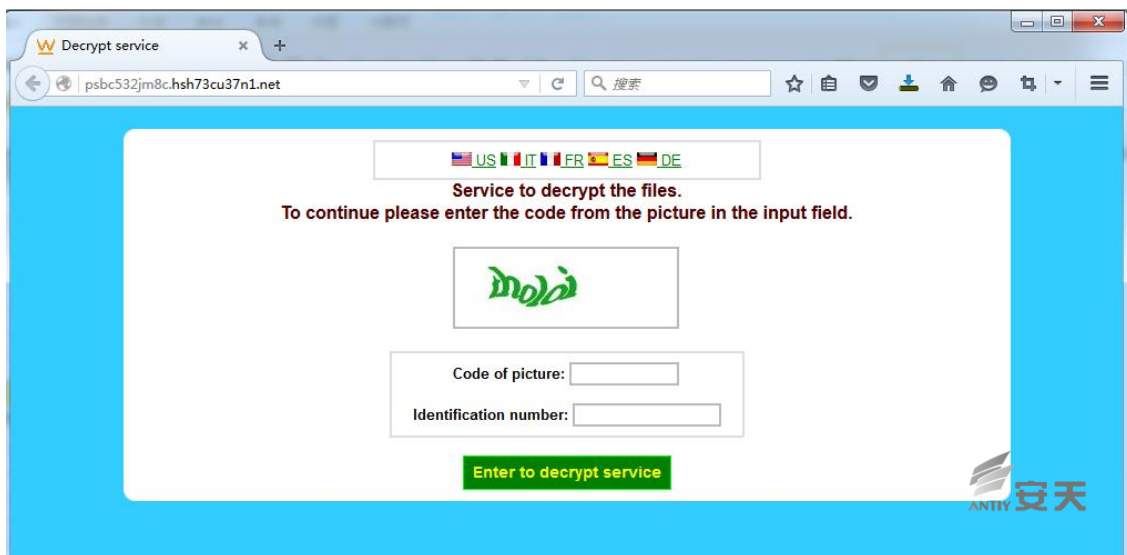
- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [CoinSafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- [LocalBitcoins.com](#) - Service allows you to search 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 网络架构分析

安天分析工程师发现为了躲避追踪，敲诈者的网络服务器是隐藏在 Tor 网络之后。点击敲诈者提供的访问页面效果如下：需要输入验证码，可以防止自动化的遍历查询中毒者信息。



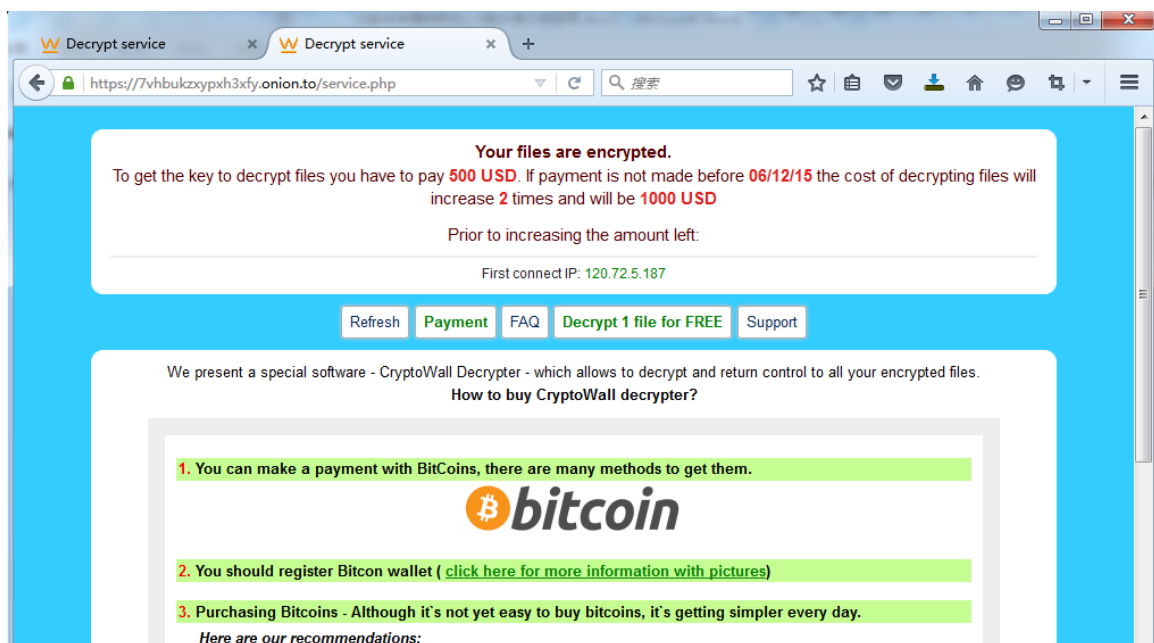
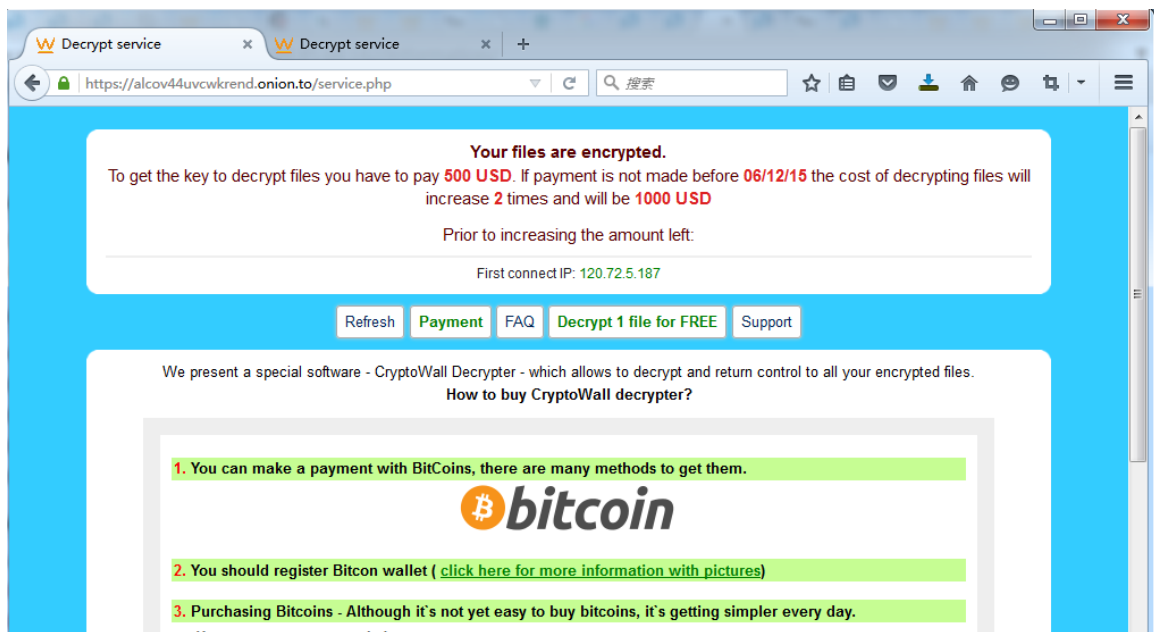
经过关联数据发现下面几个网址的指向的服务器是相同的，都是这个特斯拉 2.x 敲诈者变种的服务器，尝试使用相同的 ID 在这三个网站进行查询到的信息是一样的

psbc532jm8c.hsh73cu37n1.net

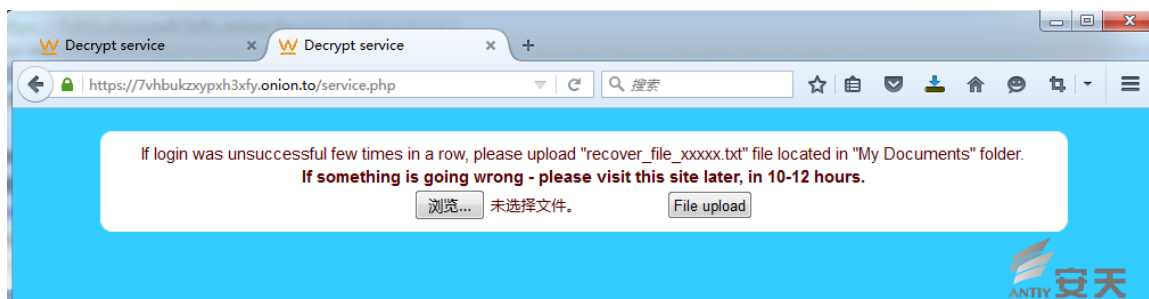
alcov44uvcwkrend.onion.to

7vhbukzypxh3xfy.onion.to

受害者 IP120.72.5.187，可以看到两个网址返回的数据一致，

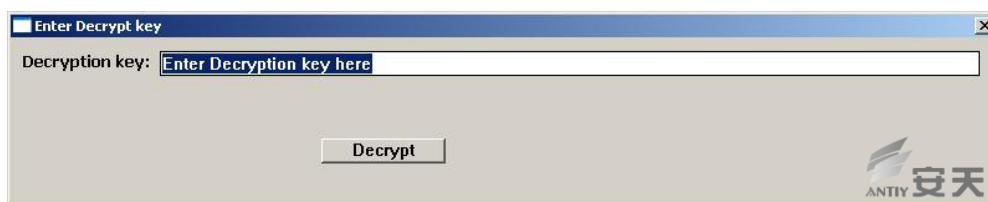


如果敲诈者使用的上报服务器被网络安全设备拦截，无法接收到上报的加密信息，到这个查询页面利用个人码查询的时候，会提示登录不成功，为了能够提供解密服务，敲诈者设计了一个功能就是将“我的文档”文件夹下面保存的 `recover_file_XXXXX.txt` 文件上传即可获取被加密的相关信息。如下图：



通过对网络架构的关联发现一个解密的 URL 程序

<http://psbc532jm8c.hsh73cu37n1.net/decrypt.zip> MD5: AE3E2206ACB24A60FF583F2CF0C77E59



其中包含 PDB 信息 C:\wrk\decrypt\decrypt\Release\decrypt.pdb，从样本功能中可以看到利用 OpenSSL ECDH 方法的公私钥加密解密算法。也印证了这个版本采用 ECDH 密钥对文件加密的密钥进行加密的方法。

5 总结

敲诈者软件此前通过邮件打包传播可执行 PE 载荷，通过双扩展名、SCR 扩展名等技巧进行传播，而在这一轮传播攻势中，其利用 js 格式的伪装性，逃避杀软的检测和防御。同时，特斯拉 2.x 敲诈者采用 ECDH 加密算法，其已经无法再通过此前的逆向获取密钥的方式来解密文件，对用户的数据安全，具有更大的威胁。

从我们过去的监测发现，敲诈型恶意代码的威胁对象，的受害对象，正在从原有的个人用户，广泛的延伸到企业用户，甚至出现了服务器被感染的案例。安天已经在 PTD 探海威胁检测系统、IEP 智甲终端防御系统中，专门强化了对敲诈者木马的检测防御能力。

随着数据安全威胁日益增长，行业企业用户同样需要通过能力型网络安全产品有效改善感知防御盲区，建立纵深防御体系，并通过威胁情报平台及时获取威胁信息。快速发现威胁，降低风险进一步扩散。

附录一：参考资料

[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/>

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：

<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

关于安天反 APT 相关产品更多信息请访问：

<http://www.antiy.cn>

附录三：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