TeslaCrypt Ransomware

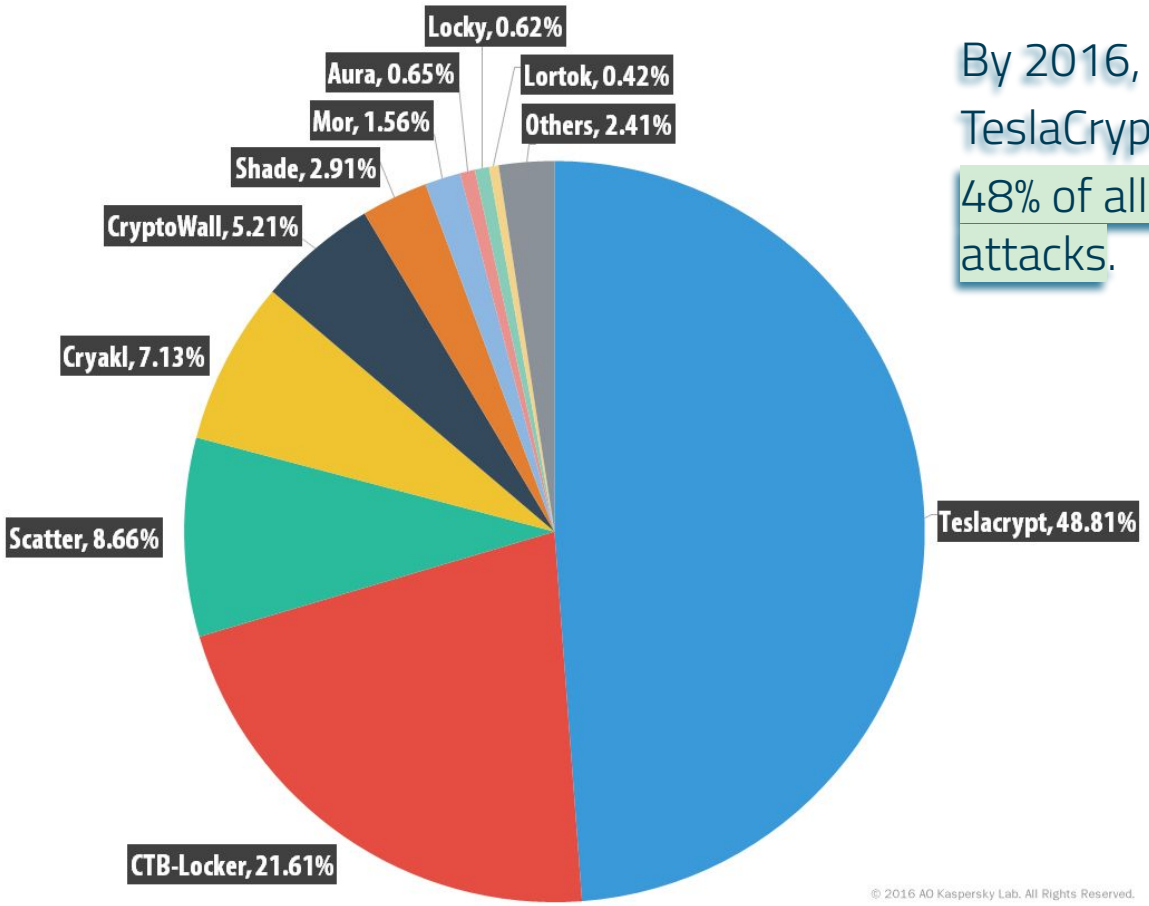
By Gabbie Malhotra, Sam Bedaiwi, Dylan Nelson and Ezequiel Leon

Intro to TeslaCrypt

TeslaCrypt was a ransomware trojan that targeted game-play data for specific computer games, and for later variants, specific file types.

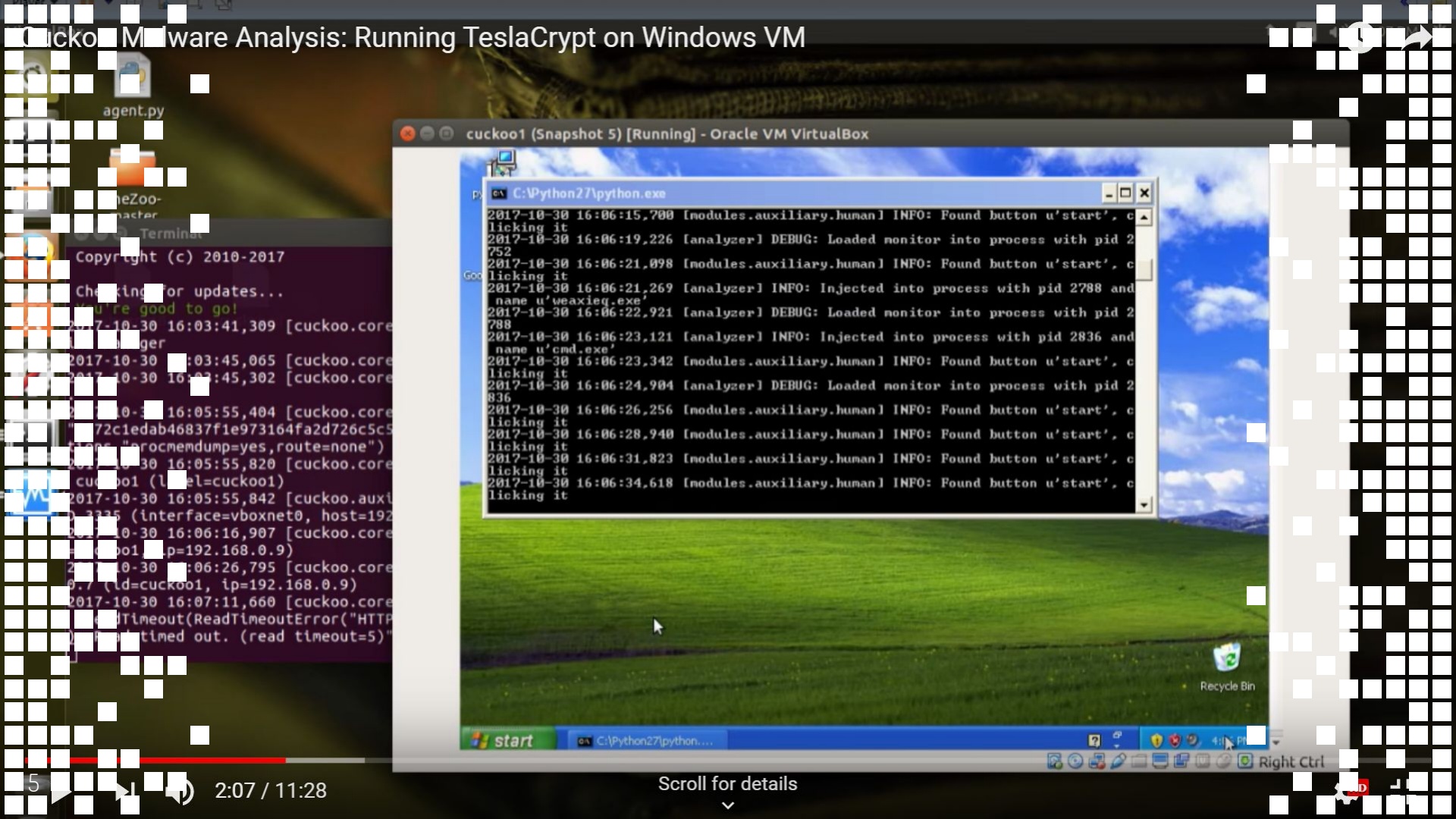
General Information

- Searched for 185 file extensions related to 40 different games
- Newer variants encrypted Word, PDF, JPEG, etc.
- Ransom of $500 worth of Bitcoin
- Now defunct, master key released



By 2016, TeslaCrypt made up 48% of all ransomware attacks.

Cuckoo Malware Analysis: Running TeslaCrypt on Windows VM



2:07 / 11:28

Scroll for details

Static Analysis

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	484	3378	1

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests
9	9	7

Angler Exploit Kit

- Uses a memory-resident, file-less mechanism called Bedep that minimizes the observable footprint of an infection. Bedep can download additional malware payloads and initiate advertising click-fraud activity.

- It exploited several Adobe Flash Player zero-day vulnerabilities in early 2015. Exploit kits distributing commodity-style malware rarely exploit zero-day vulnerabilities.

Dynamic Analysis

It works by encrypting files and then locking those files away for ransom. After encrypting popular file types with the AES-256 encryption algorithm, TeslaCrypt holds the files for a ransom of $250 to $1000

What user does the process run as?

The process runs as Admin. Doesn't really matter who is logged in. As long as it finds an exploit (using an exploit kit called "**Angler**"), it then starts to target system files and even (*by adding a Run key to the Windows registry*) ensures persistence across reboots. It used an exploit found in Adobe Flash (CVE-2015-0311). Angler is then exploited via and injected HTTP iFrame. (which is basically an HTML element that allows external webpage to be embedded in an HTML document.)

An exploit kit is: "A utility program that attackers use to launch exploits against vulnerable programs.
An object - such as a piece of code or string of commands- that takes advantage of a vulnerability in a program to force it to behave unexpectedly.

Encrypted file analysis

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00  ÐÏ.à¡±.á........
00000010  00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00  ........>...þÿ..
00000020  06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00000030  01 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00  ................
00000040  01 00 00 00 FE FF FF FF 00 00 00 00 00 00 00 00  ....þÿÿÿ........

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  36 B8 E5 EC 4B B3 67 FA 10 3A 91 57 81 97 70 D2  6¸åìK³gú.:'W.—pÒ
00000010  00 16 00 00 76 93 F7 F8 D4 00 40 7A C8 84 A2 B5  ....v"÷øÔ.@zÈ„¢µ
00000020  D8 F9 CA F6 1D D6 5F 66 55 C4 9E 30 E0 89 29 C6  Øùʏö.Ö_fUÄž0à‰)Æ
00000030  D7 2A 41 BB 9C B1 64 B6 74 14 D8 CD D7 7F 05 80  ×*A»œ±d¶t.ØÍ×..€
00000040  8B 6D 17 B0 1C B1 27 B5 1B F9 30 DA 3D 6E 6D AC  ‹m.°.±'µ.ùOÚ=nm¬
```

Unencrypted Excel file with headers (top) versus encrypted version with header (bottom, outlined in red). (Source: Dell SecureWorks)

To ensure persistence across reboots, the malware adds a Run key to the registry:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"*<random string>*":"*<full path to copied malware in %AppData%>*"
An identical key is also added to the HKCU hive in the victim's profile.

Version Information

Version — TeslaCrypt malware version (The first version analyzed by CTU researchers was 0.2.5, and the latest version as of this publication was 0.3.6a.)

What are some indicators of suspicious activity?

Encrypts system files which makes the system unresponsive and inaccessible.

Suspicious activity for this can be identified as modified files within the windows registry.
It infects the following file extensions:

.exe
.msconfig
.regedit
.procexp
.taskmgr

After infecting those file types, it then renames them into:

.encrypted
.ecc
.ezz
.exx

Network Activity:

The HTTP GET request it makes is to notify its C2 server of a new infection.
After encrypting a specific list of files, it connects to the command and control server via the TOR anonymity network using different TOR proxy servers along with specific details as base-64 encoded parameter. As for its ransom payment server, it also resides within the TOR network as a hidden service.

“The malware uses the Tor anonymity network for command and control (C2) and does not require network connectivity to encrypt files, which complicates detection, prevention, and remediation.”

- The fact that it uses the TOR anonymity network makes it harder to detect or run network traces to identify where it came from.
- Unlike ransomware families such as CryptoLocker and CryptoWall, preventing TeslaCrypt from communicating with its C2 server does not prevent encryption. TeslaCrypt does not send beacons to its C2 server after sending the 'Ping' and 'Crypted' messages.

General file extensions that are targeted

Table 2. File extensions targeted by TeslaCrypt.

.7z	.map	.m2	.rb	.jpg
.rar	.wmo	.mcmeta	.png	.cdr
.m4a	.itm	.vfs0	.jpeg	.indd
.wma	.sb	.mpqge	.txt	.ai
.avi	.fos	.kdb	.p7c	.eps
.wmv	.mcgame	.db0	.p7b	.pdf
.csv	.vdf	.DayZProfile	.p12	.pdd

These are just a few of the files extensions that it targets..

There are many many more.

Quick summary

- Teslacrypt is a Ransomware variant
- File-encrypting ransomware continues to be a growing trend in malicious software. TeslaCrypt joins CryptoWall, CTB-Locker, and TorrentLocker as the top active ransomware threats.
- Prominent signs of malicious behavior: HTTP GET requests and encrypted files.

Identification

Since TeslaCrypt is a ransomware trojan, you won't realize you have it during the encryption process

Changes:

- Many file extensions will be changed to .ecc, .exx, .ezz or .encrypted
- A file named Help_Restore.HTML will be added to your desktop
- Your desktop background will change

Background

All your documents, photos, databases and other important files have been encrypted
with strongest encryption RSA-2048 key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can
decrypt your files until you pay and obtain the private key.

If you see the main encryptor red window, examine it and follow the instructions.
Otherwise, it seems that you or your antivirus deleted the encryptor program.
Now you have the last chance to decrypt your files.
Open http://tkj3higtqlvohs7z.aw49f4j3n26.com or http://tkj3higtqlvohs7z.dfj3d8w3n27.com ,
https://tkj3higtqlvohs7z.s5.tor-gateways.de/ in your browser.
They are public gates to the secret server.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
1FBt6ieMSt8q8pkMjrUPy17Cupq3a27D3n
Follow the instructions on the server.

If you have problems with gates, use direct connection:
1. Download Tor Browser from http://torproject.org
2. In the Tor Browser open the http://tkj3higtqlvohs7z.onion/
   Note that this server is available via Tor Browser only.
   Retry in 1 hour if site is not reachable.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
1FBt6ieMSt8q8pkMjrUPy17Cupq3a27D3n
Follow the instructions on the server.

HELP_RESTORE.html

Threat Indicators:

50.7.138.132	IP address	TeslaCrypt C2 server
46.4.20.40	IP address	TeslaCrypt C2 server
178.63.9.48	IP address	TeslaCrypt C2 server
94.242.216.5	IP address	TeslaCrypt C2 server
94.242.216.63	IP address	TeslaCrypt C2 server

sshowmethemoney.com	Domain name	TeslaCrypt malicious proxy
jjeyd2u37an30.com	Domain name	TeslaCrypt malicious proxy
63ghdye17.com	Domain name	TeslaCrypt malicious proxy
42k2bu15.com	Domain name	TeslaCrypt malicious proxy
42k2b14.net	Domain name	TeslaCrypt malicious proxy
42kjb11.net	Domain name	TeslaCrypt malicious proxy
2kjb9.net	Domain name	TeslaCrypt malicious proxy

Quarantine

Best preemptive option is to backup all your files.

- Make sure it is saved offline as Teslacrypt can target recovery files and delete them

Ensure your system and browsers are updated

Block access to Tor and I2P via a firewall

- Blocking the connection between your device and the call-home server can disarm a ransomware attack

Escalation

In the event that your computer had been compromised, there wasn't anything you could do if your files were not backed up except pay the ransom price.

Containment

Scope

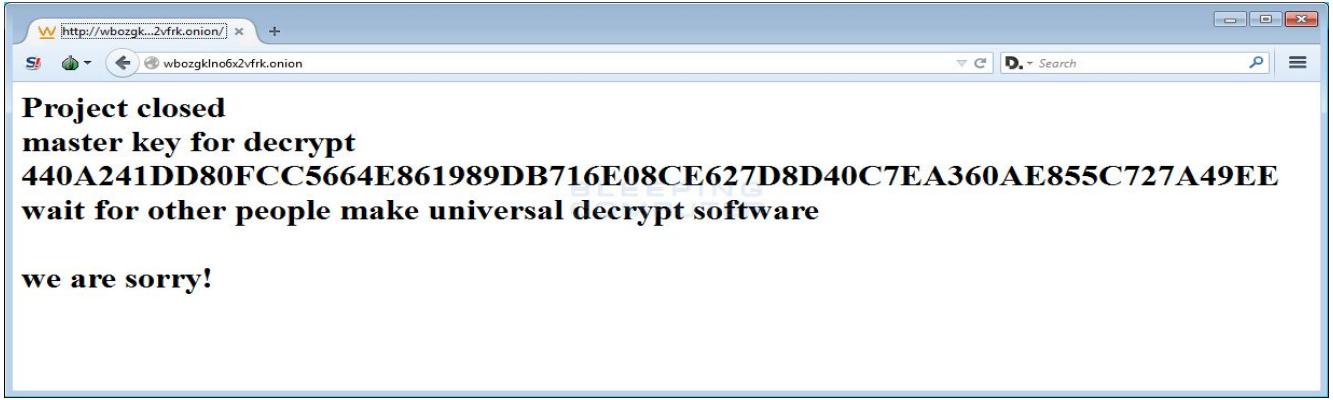
In the beginning Teslacrypt ransomware mainly targeted video game files but it later on was able to target pdf, word, and image files. In the first four months of its appearance a total of 1,231 victims visited the TeslaCrypt page to attempt to decrypt a file, 139 individuals paid 0.5 to 2.5 bitcoins, and 20 individuals paid the full $1,000 through PayPal for the total amount of $76,522. The popular games that were targeted by the Teslacrypt ransomware are: World of Warcraft, Day Z, League of Legends, World of Tanks and Metin2, Call of Duty, Star Craft 2, Diablo, Fallout 3, Minecraft, Half-Life 2, Dragon Age: Origins, The Elder Scrolls and specifically Skyrim related files, Star Wars: The Knights Of The Old Republic, WarCraft 3, F.E.A.R, Saint Rows 2, Metro 2033, Assassin's Creed, S.T.A.L.K.E.R., Resident Evil 4 and Bioshock 2.

Severity

The damage that can be done by the Tesalcrypt ransomware could range from just a from just game files being encrypted to file formats from productivity suites such as Open Office and Microsoft Office, as well as formats associated with creative applications. Decrypting the compromised files was near to impossible without the decryption key leaving the user to lose the files or paying the ransom to recover the files.

Solution

The only way to decrypt your file is with a decryption key. Luckily , in 2016 an ESET researcher reached out in the support chat and asked if they would release the master key for decryption. To his surprise they released the key.



Solution

You can now download and use a Teslacrypt Decryptor provided by ESET.

https://support.eset.com/kb6051/

THANKS!

Any questions?