Advanced Notification of PyCL Ransomware

Security Advisory AE-Advisory 17-17

Criticality Critical

Advisory Released On 3 April 2017

Impact

Encrypts files in the infected machine rendering them inaccessible

Solution

Refer to the “Solution” section below

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new family of Ransomware called PyCL that is being tested in the wild and said to be distributed through EITest into a well-known exploit kit called RIG EK. It was noticed that PyCL was only distributed for a day and does not securely encrypt files. This means that the ransomware may have had its test run and may be back more advanced and powerful. Further information is explained in the Threat Details section below.

Threat Details

Origin:

The name PyCL Ransomware comes from its programming language. Therefore the probable name of the malicious file is “cl.py” but it may also be reached in different names.

Distribution:

Security researchers noticed that EITest (a known exploit kit) was sending visitors to the RIG exploit kit which was distributing PyCL ransomware. This was done through hacked websites that redirected visitors to the RIG exploit kit, which in return, tries to exploit vulnerabilities found on an infected machine in order to install the ransomware. According to a security researcher, EITest was distributing both Cerber which is a family of ransomware known to have caused a ruckus over the past year and PyCL, however PyCL was only distributed for one day.

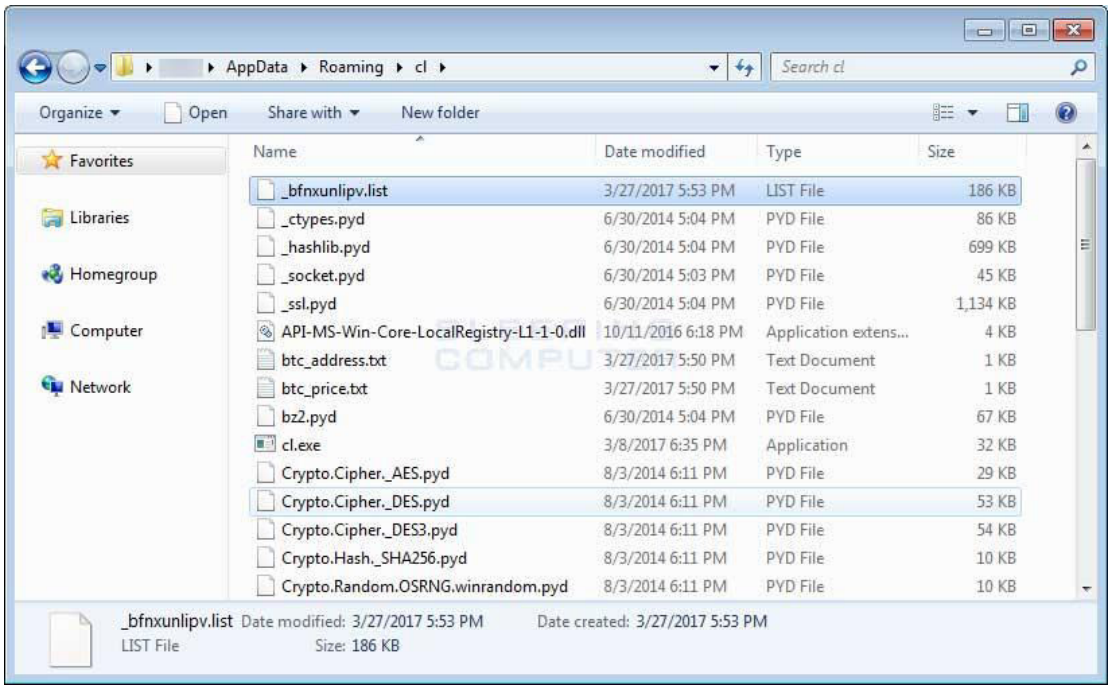
R...	Protocol	Requ...	X-HostIP	Host	URL	Body	Content-Type
200	HTTP	GET	185	.ru	/ip	561	text/html; charset=utf-8
200	HTTP	GET	188.225.37.141	warm.ships.net	/?oq=hoPUqJbBVPwG0ikOBdM1yIoPAFpF9fiv2BDTmEWfh5KArxeIMg51z6LRVvQ6...	38 085	text/html;charset=UTF-8
200	HTTP	GET	188.225.37.141	warm.ships.net	/?ct=sround&qtuif=3266&q=wH3QMvXcJwDGFYbGMvrESaNbNknQA0K...	10 021	application/x-shockwave-flash
200	HTTP	GET	188.225.37.141	warm.ships.net	/?ct=diamond&oq=l-E8_svKLB5aALnjEzWL1EzzopdBFhCofio30GGyhOe...	5 625 739	application/x-msdownload

Malware Technical Details:

Security researchers also claim that one of the files contained in the NSIS installer for PyCL is a file called “user.txt”. This file contains the string “xkwctmmh” which is sent to the command & control (C&C) server during every request. This indicates that the ransomware may be a part of an upcoming RaaS (Ransomware-as-a-service) and entities should be aware of such threats.

Encryption method:

PyCL Ransomware is distributed as an NSIS (Nullsoft Scriptable Install System) installer that has a Python package used to encrypt a computer and a tutorial on how to pay the ransom. PyCL also communicates back to the C&C server at each stage of the process so that it provides debugging/status information to the attacker. When the PyCL installer is executed, the tutorial files will be extracted to the **"%AppData\Roaming\How_Decrypt_My_Files\"** folder and the Python components will be extracted to the **"%AppData%\cl"** folder.



The installer will then connect to the C&C server at "**170.254.236.102/status/?status=IS&u=xkwctmmh&sub=1"** followed by execution of "**%AppData%\cl\cl.exe**". CL.exe is a Python script compiled into an executable which encrypts the computer and once it has been executed, it will start to encrypt the files of the infected system.

First, PyCL will check if the user has administrative privileges, if yes, then it will delete all shadow volume copies using the command:

```
c:\windows\system32\vssadmin.exe delete shadows /all /quiet
```

It then connects to the C&C server again and sends a HTTP POST request to "**http://170.254.236.102/init/**" which will send the:

- Victim's Windows version
- Whether the victim has administrative privileges or not
- Screen resolution
- Processor architecture
- Computer name and username
- MAC Address of the primary Network Adapter

The C&C server responds with:

- RSA-2048 public encryption key
- Bitcoin payment address
- Ransom amount in bitcoins
- Ransom amount in USD (United States Dollars)

This information is then saved into the following files which are located in the "**%AppData%\cl"** folder:

- Public_key.txt
- Btc_address.txt
- Btc_price.txt
- Usd_price.txt

PyCL then generates a list of files to encrypt and stores this list in "**%AppData%\cl\filelist.txt".**

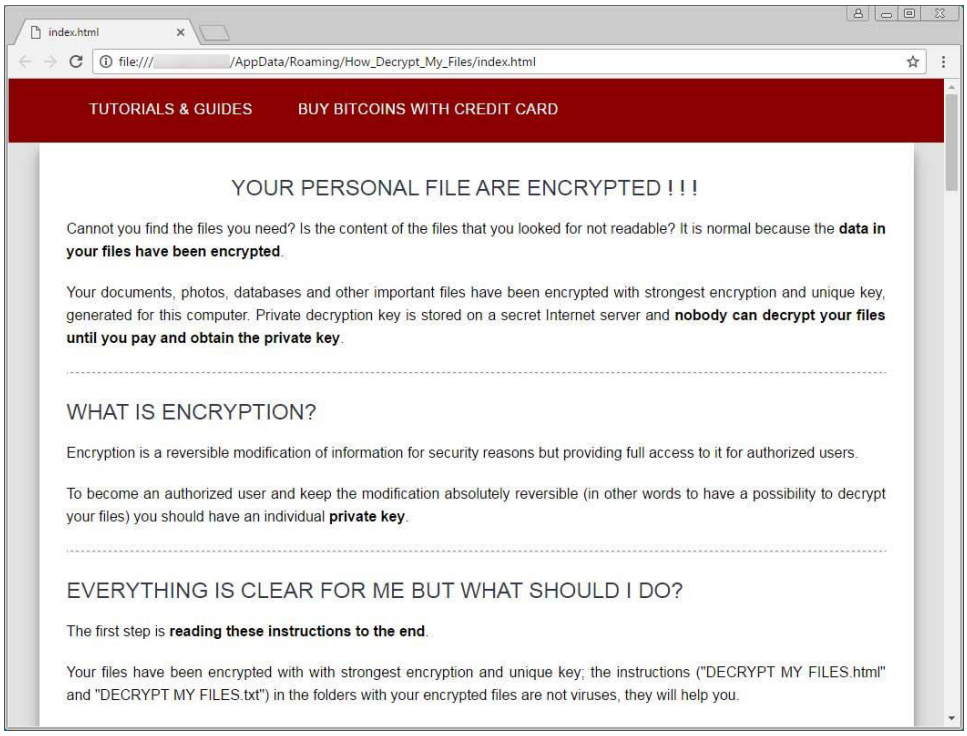
When generating the list, it will skip files that are located in the following folders:

- WINDIR
- APPDATA
- LOCALAPPDATA
- ProgramData
- ProgramFiles
- PROGRAMW6432
- $RECYCLE.BIN
- ProgramFiles (x86)

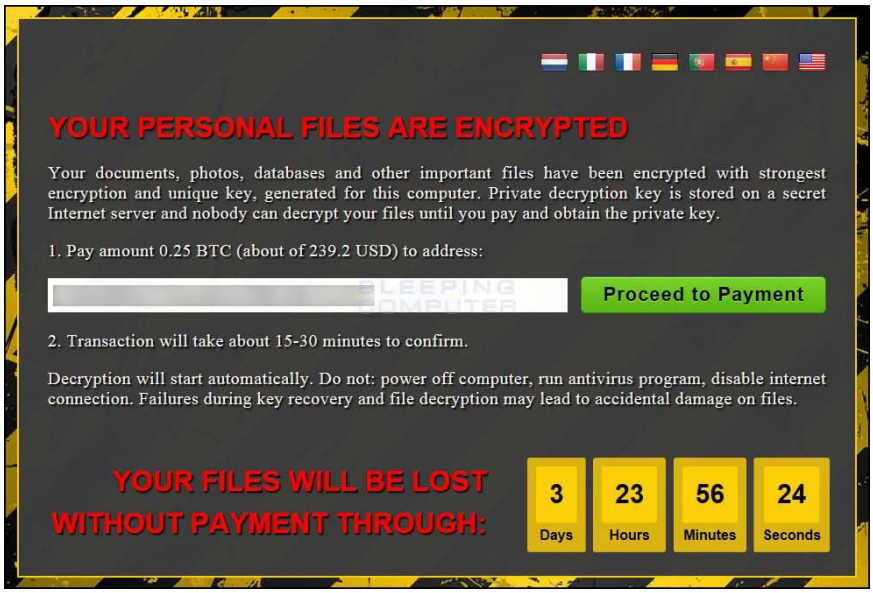
It will then encrypt all files in the list that it generates with a unique AES-256 encryption key for each file. The list of files and each file's decryption key is saved ion a random named file in the CL folder. This folder is then also encrypted with an RSA-2048 public encryption key that was previously received from the C&C server.

Once the above is done, the ransomware is coded in a way that the original files are not deleted, so you still have access to the original unencrypted files even though there is an encrypted copy of the files.

When all of the above is done, it will then create a link on the desktop called **"How Decrypt My Files.lnk**" that opens "**%AppData%\Roaming\How_Decrypt_My_Files\index.html**" file. This file is a tutorial on how to pay the ransom to the attacker and get the files back. Researchers were able to capture a small portion of the ransom note as demonstrated in the screenshot in the next page:



It will then execute **UI.exe** which will display the lock screen as seen below:



This lock screen contains a 4 day timer, the bitcoin address of the victim and the ransom amount wanted. If "**Proceed to Payment**" is clicked, it will open the ransom

note from the C&C server. If a payment has been made, it will automatically decrypt the files on the computer.

Although, aeCERT strongly recommends that ransom amounts should not be paid whatsoever and that the malware should be removed from the infected machine as paying will be an action of supporting criminals and encouraging them to spread ransomware more.

Other Technical Details:

```
Hashes of Main Components:

Installer: 80d402f38ff9849ea5e9f8a126e00f423ca1b4f1121c8059aebed8336bfc6f30

CL.exe: fc2f4904fa71ec4c1e3c73cbac03a57d701409634e3a8a23b05d15edca28d7de

UI.exe: b01d1230f31200a5f195b7f44fcc552a71b9bfe131f7b8eccd2466eb66a952dc
```

```
Network Communication:

http://170.254.236.102/status/?status=IS&u=xkwctmmh&sub=1 - Issues by NSIS
Installer

http://170.254.236.102/init/  - On Execution of CL.exe to retrieve key and
other info

http://170.254.236.102/status/?status=FS&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - Begin generating list of files to encrypt.

http://170.254.236.102/status/?status=FC&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - End generating list

http://170.254.236.102/status/?status=ES&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - Begin Encrypting Files

http://170.254.236.102/status/?status=EC&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - End Encrypting Files

http://170.254.236.102/get_private_key/?btc=[bitcoin_address] - Check if pa
yment has been made

http://170.254.236.102/status/?status=DS&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - Begin Decrypting

http://170.254.236.102/status/?status=DC&btc=[bitcoin_address]&u=xkwctmmh&s
ub=1 - End Decrypting

http://170.254.236.102/help/?btc=[bitcoin_address] - Online tutorial
```

Solution

- Avoid opening suspicious files and links in emails from unknown users.
- Always back up important data daily
- Always show file extensions if you are using Windows operating systems as some malware hide the real extension of their files
- Filter executable files in your e-mail (block any attempt of sending and receiving any .exe files)
- Disable files running from AppData and LocalAppData folders unless needed by a specific application known by the user

Best Practices

These are the best practices that are recommended to be followed:

- Ensure all IT systems (OSs, applications, websites, AV…etc.) are updated.
- Ensure that your security systems are current, can inspect deeply and can detect and prevent phases of attack plan.
- Ensure relevant third party and support vendors are aware and accessible encase of an infection.
- Probe any anomalous network and system behavior and examine it. Make sure your system is not infected.
- Remind users to be particularly careful and watch out for phishing and spear-phishing emails. Be cautious when opening e-mail attachments and check if the file extension corresponds to the file name.
- Only response to trusted emails and only visit trusted websites as a precaution.
- Plan or review your incident response procedures with all necessary parties (not only IT groups). Explore how the planned response against such infection.

- Monitor any suspicious and anonymous IP sources or destinations in your network. Keep track of these IPs and make sure they are not reported as suspicious or malicious addresses.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae