

Forum:[Hack Forums](#)

Thread: [Free Ultimate Proxy Checker by Toxic Coder](#)

Djam_01 - October 9, 2024, 5:02 am

The Ultimate Proxy Checker Coded By Toxic Coder v1.0

Download Here : [deleted]

Reviewed by Staff : BTC Clipper

Bastille - October 9, 2024, 6:09 am

Similar case as this one : <https://hackforums.net/showthread.php?tid=6280678>

OP shared a file, compressed in a zip archive, containing the following files :

Few interesting things here :

- Crypto Checker all in one_updated.zip is 17262268 bytes, which is around 17MB
- When we uncompress the archive, Crypto Checker.exe is 800000000, which is around 800MB

Weird number, pretty accurate one for a file

Most online tool used to check if files are malicious have a limit, which is around 700MB, the objective is to discourage the victim to check if the file is malicious

- The read_me.txt file is similar as the read_me.txt file in the thread linked above
- update.exe is also similar as the file we can find in the thread linked above

Crypto Check.exe : this technique is called "padding" or "file padding". I used GHex to inspect the file, here is a screenshot that confirms the padding technique, most of the content (98% is filling with useless bytes) :

After editing Crypto Check.exe and removing useless bytes, we got a 2.6MB file, which is allowed to be uploaded to VirusTotal :

<https://www.virustotal.com/gui/file/887e194407049745c55b8182c30da8d5c8b3e12aa2301a1fa4b0f463c48e8346?nocache=1>

We can see that this .exe runs few commands to exclude some folders to the Windows Defender analysis and executes a dropped file named LZMYBCTLTD.EXE :

```
Code "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference  
-ExclusionPath 'C:\ProgramData'  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference  
-ExclusionPath 'C:\Users\admin\AppData\Roaming'  
"C:\ProgramData\active\LZMYBCTLTD.exe"
```

Regarding the update.exe file, same as the thread linked above, Python script converted to Exe, acting as a BTC Clipper :

Pretty explicit, no need to go further, sharing the reports in case you want to take a look at it :

update.exe :

[*] Virus Total:

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628/detection>

Crypto Checker.exe :

[*] Virus Total :

<https://www.virustotal.com/gui/file/887e194407049745c55b8182c30da8d5c8b3e12aa2301a1fa4b0f463c48e8346/behavior>

[*] TRIA.GE : <https://tria.ge/241009-p65hmavdkr/behavioral1>

[*] ANY.RUN :

<https://app.any.run/tasks/44cfbfdf-d8db-4f8c-b452-ecae68fce588?p=67067c72b875e3a7490f696a>

Last but not least, OP posted many times about the same topic we spoke above :

He had "a big plan" to make money, his plan was maybe to infect HF members, not as long as I'll be there.

Regulus - October 9, 2024, 6:14 am

(Oct 9, 2024 06:09 AM) Bastille Wrote: [\[CITE\]](#) Similar case as this one :

<https://hackforums.net/showthread.php?tid=6280678>

OP shared a file, compressed in a zip archive, containing the following files :

Few interesting things here :

- Crypto Checker all in one_updated.zip is 17262268 bytes, which is around 17MB
- When we uncompress the archive, Crypto Checker.exe is 800000000, which is around 800MB

Weird number, pretty accurate one for a file

Most online tool used to check if files are malicious have a limit, which is around 700MB, the objective is to discourage the victim to check if the file is malicious

- The read_me.txt file is similar as the read_me.txt file in the thread linked above
- update.exe is also similar as the file we can find in the thread linked above

Crypto Check.exe : this technique is called "padding" or "file padding". I used GHex to inspect the file, here is a screenshot that confirms the padding technique, most of the content (98% is filling with useless bytes) :

After editing Crypto Check.exe and removing useless bytes, we got a 2.6MB file, which is allowed to be uploaded to VirusTotal :

<https://www.virustotal.com/gui/file/887e194407049745c55b8182c30da8d5c8b3e12aa2301a1fa4b0f463c48e8346?nocache=1>

We can see that this .exe runs few commands to exclude some folders to the Windows Defender analysis and executes a dropped file named LZMYBCTLTD.EXE :

```
Code "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference  
-ExclusionPath 'C:\ProgramData'  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference  
-ExclusionPath 'C:\Users\admin\AppData\Roaming'  
"C:\ProgramData\active\LZMYBCTLTD.exe"
```

Regarding the update.exe file, same as the thread linked above, Python script converted to Exe, acting as a BTC Clipper :

Pretty explicit, no need to go further, sharing the reports in case you want to take a look at it :

update.exe :

[*] Virus Total:

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628/detection>

Crypto Checker.exe :

[*] Virus Total :

<https://www.virustotal.com/gui/file/887e194407049745c55b8182c30da8d5c8b3e12aa2301a1fa4b0f463c48e8346/behavior>

[*] TRIA.GE : <https://tria.ge/241009-p65hmavdkr/behavioral1>

[*] ANY.RUN :

<https://app.any.run/tasks/44cfbfdf-d8db-4f8c-b452-ecae68fce588?p=67067c72b875e3a7490f696a>

Last but not least, OP posted many times about the same topic we spoke above :

He had "a big plan" to make money, his plan was to infect HF members, not as long as I'll be there. Holy shit that is some INSANELY impressive investigation. Great job!

Bastille - October 9, 2024, 6:20 am

(Oct 9, 2024 06:14 AM)Regulus Wrote: [\[CITE\]](#) Holy shit that is some INSANELY impressive investigation.

Great job!

Thanks buddy ! I like to do these investigations, I have a collection here that is growing up <https://hackforums.net/showthread.php?tid=6276795> , besides it allows me to protect HF members and get rid off scammers.