Prometheus Ransomware Decryptor

medium.com/cycraft/prometheus-decryptor-6933e7bac1ea

CyCraft Technology Corp September 16, 2021

CyCraft Technology Corp

Jul 13, 2021

·

8 min read

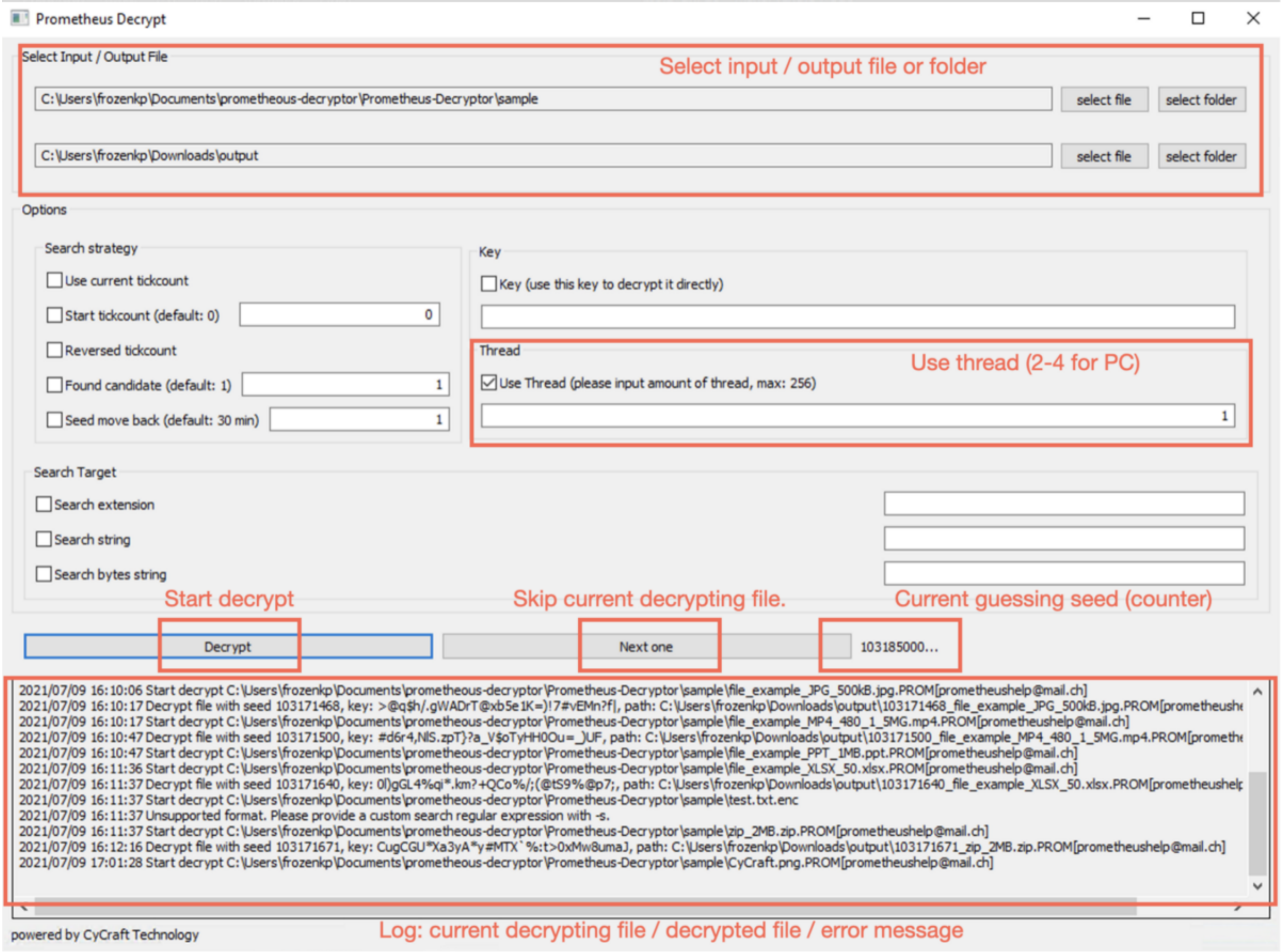
This year, CyCraft has been involved in several cases of Prometheus attacks. Naturally, we attempted to reverse-engineer Prometheus to gain a better understanding of the attack itself, the malware, and the attacker. We discovered that it was possible to recover our customers' encrypted files to some degree. We are sharing this internally developed tool to help other victims recover.

Visit Our GitHub | https://github.com/cycraft-corp/Prometheus-Decryptor
Direct Download | https://github.com/cycraft-corp/Prometheus-Decryptor/releases/download/1.2/prometheus_decryptor.zip

Quick How-to Guide

We provided a GUI version for windows users. All features are supported in the GUI version. If your programming skills aren't developed to a mature level, please follow the steps below to decrypt your files:

1. Choose a file or folder to decrypt.
2. Choose the output file name or output folder.
3. Select "Use thread" and fill in 2–4 for PC. (Threads usually make the decryption routine faster, but it actually depends on the number of your CPU cores)
4. Click decrypt.
5. There is a counter, which shows the current guessing tickcount.
6. The decrypting result will show in the text block below. (There may be multiple possible keys, so the decryption routine will continue to decrypt to find more possible keys. You can press "Next one" to skip the current file.)


Prometheus Decrypt
Select Input / Output File
Select input / output file or folder
select file
select folder
select file
select folder
Options
Search strategy
Key
Thread
Use thread (2-4 for PC)
Search Target
Start decrypt
Skip current decrypting file.
Current guessing seed (counter)
Decrypt
Next one
Log: current decrypting file / decrypted file / error message
powered by CyCraft Technology

C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample

C:\Users\frozenkp\Downloads\output

□ Use current tickcount
□ Start tickcount (default: 0) 0
□ Reversed tickcount
□ Found candidate (default: 1) 1
□ Seed move back (default: 30 min) 1

□ Key (use this key to decrypt it directly)

☑ Use Thread (please input amount of thread, max: 256) 1

□ Search extension
□ Search string
□ Search bytes string

103185000...

```
2021/07/09 16:10:06 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\file_example_JPG_500kB.jpg.PROM[prometheushelp@mail.ch]
2021/07/09 16:10:17 Decrypt file with seed 103171468, key: >@q$h/.gWADrT@xb5e1K=)!7#vEMn?f|, path: C:\Users\frozenkp\Downloads\output\103171468_file_example_JPG_500kB.jpg.PROM[prometheushe
2021/07/09 16:10:17 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\file_example_MP4_480_1_5MG.mp4.PROM[prometheushelp@mail.ch]
2021/07/09 16:10:47 Decrypt file with seed 103171500, key: #d6r4,NlS.zpT}?a_V$oTyHH0Ou=_)UF, path: C:\Users\frozenkp\Downloads\output\103171500_file_example_MP4_480_1_5MG.mp4.PROM[prometh
2021/07/09 16:10:47 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\file_example_PPT_1MB.ppt.PROM[prometheushelp@mail.ch]
2021/07/09 16:11:36 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\file_example_XLSX_50.xlsx.PROM[prometheushelp@mail.ch]
2021/07/09 16:11:37 Decrypt file with seed 103171640, key: 0l)gGL4%qi*.km?+QCo%/;(@tS9%@p7;, path: C:\Users\frozenkp\Downloads\output\103171640_file_example_XLSX_50.xlsx.PROM[prometheushelp
2021/07/09 16:11:37 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\test.txt.enc
2021/07/09 16:11:37 Unsupported format. Please provide a custom search regular expression with -s.
2021/07/09 16:11:37 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\zip_2MB.zip.PROM[prometheushelp@mail.ch]
2021/07/09 16:12:16 Decrypt file with seed 103171671, key: CugCGU*Xa3yA*y#MTX`%:t>0xMw8umaJ, path: C:\Users\frozenkp\Downloads\output\103171671_zip_2MB.zip.PROM[prometheushelp@mail.ch]
2021/07/09 17:01:28 Start decrypt C:\Users\frozenkp\Documents\prometheous-decryptor\Prometheus-Decryptor\sample\CyCraft.png.PROM[prometheushelp@mail.ch]
```

Brief History on Prometheus

The emerging ransomware group Prometheus made headlines last month with Unit42's report. According to the report, which had observed Prometheus for 4 months, victims of the emerging ransomware group total more than 30 in multiple different countries, including the

United States, the UK, and a dozen more countries in Asia, Europe, the Middle East, and South America.

Organizations targeted for attack by Prometheus included government agencies, financial services, manufacturing, logistics, agriculture, healthcare services, insurance agencies, energy, consulting, law firms, and more.

Although Prometheus claimed to be affiliated with REvil (the Russia-based ransomware group attributed to the attack on global meat supplier JBS that succeeded in acquiring an 11 million USD ransom, Prometheus's code and behavior are more similar to Thanos.

Brief History on Thanos — The Possible Predecessor of Prometheus

First observed in 2020, Thanos gained notoriety for its 43 different configuration options as well as being the first ransomware to utilize the evasion technique know as RIPlace.

RIPlace was introduced via a POC exploit in November 2019. Initially, RIPlace could bypass several ransomware defense mechanisms, including AV and certain EDR solutions. It wasn't until a few months later that RIPlace was seen in the wild.

Like other ransomware on the ransomware-as-a-service (RaaS) market, Thanos ransomware does appear to have code overlaps with other ransomware, notably Hakbit; however, just like other ransomware, Thanos does come with customization options and appears to still be under active development.

Usage

Build

```
make win32    # windows 32 bitsmake win64    # windows 64 bitsmake linux    #
linuxmake win32GUI # windows 32 bits GUI (built on windows)make win64GUI # windows 64
bits GUI (build on windows)
```

Command Arguments

```
Usage of ./bin/prometheus_decrypt:  -b string        Custom search with byte value.
(i.e. \xde\xad\xbe\xef -> deadbeef)        Please use ?? to match any byte (i.e. de??
beef)  -c    Use current tickcount. (only support in Windows)  -e string
Search file extension.  -f int        Found candidate. (default 1)  -i string
Input encrypted file.  -k string        Decrypt with this key.  -m int        Move
backward m minutes from the current decrypted seed when guessing the next sample.
(default 30)  -o string        Output decrypted file.  -p int        Use n thread.
(default 1)  -r    Reversed tickcount.  -s string        Custom search with regular
expression.  -t int        Start tickcount.
```

Brute Force Random Seed

Brute force the random seed of a png image from tickcount 0.

```
./prometheus_decrypt -i ./sample/CyCraft.png.PROM\[prometheushelp@mail.ch\] -o
./output/CyCraft.png -e png -p 16
```

In this command, there are 4 arguments:

- i: input encrypted file
- o: output file
- e: search file format
- p: thread count

Reversed Tickcount

Brute force the random seed of a png image from tickcount 100000 in reversed order.

```
./prometheus_decrypt -i ./sample/CyCraft.png.PROM\[prometheushelp@mail.ch\] -o
./output/CyCraft.png -e png -p 16 -t 100000 -r
```

There are 2 additional arguments:

- t: start from 100000
- r: reversed order (100000…0)

Brute force from current tickcount (only for Windows)

Brute force the random seed of a png image from the current tickcount in reversed order. This feature is usually used in reversed order.

```
./prometheus_decrypt -i ./sample/CyCraft.png.PROM\[prometheushelp@mail.ch\] -o
./output/CyCraft.png -e png -p 16 -c -r
```

There is an additional argument:

> c: start from the current tickcount

Decrypt (Encrypt) with a key

Decrypt (Encrypt) a file with a provided key.

```
./prometheus_decrypt -i ./sample/CyCraft.png.PROM\[prometheushelp@mail.ch\] -o
./output/CyCraft.png -k "+@[%T-mZSh+E[^^i{W:dpwnhdL4<b8D4}]]"
```

There is an additional argument:

> k: provided key

Brute force random seed with custom format (regular expression)

Brute force the random seed of a text file with a known string “we had another great”.

```
./prometheus_decrypt -i ./sample/test.txt.enc -o ./output/test.txt -p 16 -s "we had
another great"
```

There is an additional argument:

s: regular expression to match the decrypted file

Brute force the random seed with custom format (bytes pattern)

Brute force the random seed of a png file with its header in hex.

```
./prometheus_decrypt -i ./sample/test.txt.enc -o ./output/test.txt -p 16 -b '89??4e??
0d??1a0a??00'
```

There is an additional argument:

- b: PNG header in hex format.
- The full bytes are “8950 4e47 0d0a 1a0a 0000”.
- We can use ?? to match any byte.

Custom search with bytes pattern is much more convenient than regular expression since there are lots of file format that it can’t be performed by visible characters.

Brute force the random seed for a directory

Brute force the random seed of a png file with its header in hex.

```
./prometheus_decrypt -i ./sample -o ./output -p 16 -m 1 -f 2
```

There are two additional arguments:

- m: Move backward m minutes from the current decrypted seed when guessing the next sample. (default 30) Use `seed-m*60*1000` as the start tickcount.
- f: Found candidate. (default 1)Limit the candidates found. There may be several candidates to a file, limit its candidates can save time.

Since there are lots of files to decrypt, you can press `Ctrl-c` to skip the current guessing file.

Output

Since we match the file with magic number, it might be matched even if a wrong key is provided. Therefore, we keep the decryption process continued to guess. You can terminate it anytime if you find the correct decrypted file.

```
% ./prometheus_decrypt -i ./sample/test.txt.enc -o ./output/test.txt -p 16 -s "we had
another great" Decrypt file with seed 615750, key: +@[%T-mZSh+E[^^i{W:dpwnhdL4<b8D4,
path: ./output/615750_test.txt 2795306...
```

Supported File Format

We match the magic number with https://github.com/h2non/filetype. Here is the file type we currently support:

Image

- jpg — `image/jpeg`
- png — `image/png`
- gif — `image/gif`
- webp — `image/webp`
- cr2 — `image/x-canon-cr2`
- tif — `image/tiff`
- bmp — `image/bmp`
- heif — `image/heif`
- jxr — `image/vnd.ms-photo`
- psd — `image/vnd.adobe.photoshop`
- ico — `image/vnd.microsoft.icon`
- dwg — `image/vnd.dwg`

Video

- mp4 — `video/mp4`
- m4v — `video/x-m4v`
- mkv — `video/x-matroska`
- webm — `video/webm`
- mov — `video/quicktime`
- avi — `video/x-msvideo`
- wmv — `video/x-ms-wmv`
- mpg — `video/mpeg`
- flv — `video/x-flv`
- 3gp — `video/3gpp`

Audio

- mid — `audio/midi`

- mp3 — `audio/mpeg`
- m4a — `audio/m4a`
- ogg — `audio/ogg`
- flac — `audio/x-flac`
- wav — `audio/x-wav`
- amr — `audio/amr`
- aac — `audio/aac`

Archive

- epub — `application/epub+zip`
- zip — `application/zip`
- tar — `application/x-tar`
- rar — `application/vnd.rar`
- gz — `application/gzip`
- bz2 — `application/x-bzip2`
- 7z — `application/x-7z-compressed`
- xz — `application/x-xz`
- zstd — `application/zstd`
- pdf — `application/pdf`
- exe — `application/vnd.microsoft.portable-executable`
- swf — `application/x-shockwave-flash`
- rtf — `application/rtf`
- iso — `application/x-iso9660-image`
- eot — `application/octet-stream`
- ps — `application/postscript`
- sqlite — `application/vnd.sqlite3`
- nes — `application/x-nintendo-nes-rom`
- crx — `application/x-google-chrome-extension`
- cab — `application/vnd.ms-cab-compressed`
- deb — `application/vnd.debian.binary-package`
- ar — `application/x-unix-archive`
- Z — `application/x-compress`
- lz — `application/x-lzip`
- rpm — `application/x-rpm`
- elf — `application/x-executable`
- dcm — `application/dicom`

Documents

- doc — `application/msword`
- docx — `application/vnd.openxmlformats-officedocument.wordprocessingml.document`

- xls — `application/vnd.ms-excel`
- xlsx — `application/vnd.openxmlformats-officedocument.spreadsheetml.sheet`
- ppt — `application/vnd.ms-powerpoint`
- pptx — `application/vnd.openxmlformats-officedocument.presentationml.presentation`

Font

- woff — `application/font-woff`
- woff2 — `application/font-woff`
- ttf — `application/font-sfnt`
- otf — `application/font-sfnt`

Application

- wasm — `application/wasm`
- dex — `application/vnd.android.dex`
- dey — `application/vnd.android.dey`

How it Works

Prometheus ransomware uses salsa20 with a tickcount-based random password for encryption. The size of the random password is 32 bytes, and every character is a visible character. Since the password uses tickcount as the key, we can guess it brutally.

Visit Our GitHub | https://github.com/cycraft-corp/Prometheus-Decryptor
Direct Download | https://github.com/cycraft-corp/Prometheus-Decryptor/releases/download/1.2/prometheus_decryptor.zip

Everything Starts From Security

Prevent cyber intrusions from escalating into business-altering incidents. From endpoint to network, from investigation to blocking, from in-house to cloud, CyCraft AIR covers all aspects required to provide small, medium, and large organizations with the proactive, intelligent, and adaptable security solutions needed to defend from all manner of modern security threats with real-time protection and visibility across the organization.

Engage with CyCraft

CyCraft secures government agencies, police and defense organizations, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, SMEs, and more by being **Fast / Accurate / Simple / Thorough.**

CyCraft powers SOCs using innovative AI-driven technology to automate information security protection with built-in advanced managed detection and response (MDR), global cyber threat intelligence (CTI), smart threat intelligence gateway (TIG) and network detection and response (NDR), security operations center (SOC) operations software, auto-generated incident response (IR) reports, enterprise-wide Health Check (Compromise Assessment, CA), and Secure From Home services. Everything Starts From Security.

Meet your cyber defense needs in the 2020s by engaging with CyCraft at engage@cycraft.com

Additional Resources

- Read our latest white paper to learn , their motivations & how Taiwan organizations retain resilience against some of the most sophisticated and aggressive cyber attacks in the world.
- Is your SOC prepared for the next decade of cyber attacks? Read our latest report on , the challenges to overcome, and the stressors to avoid — includes research from Gartner, Inc. on why Midsize enterprises are embracing MDR providers.
- New to the MITRE Engenuity ATT&CK Evaluations? for a fast, accurate, simple, thorough introductory guide to understanding the results.
- Our CyCraft AIR security platform achieved with zero configuration changes and zero delayed detections straight out-of-the-box.