Clop ransomware

github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Clop.md

albertzsigovits

albertzsigovits/**malware-notes**

Notes and IoCs of fresh malware

1 Contributor | 0 Issues | 27 Stars | 5 Forks

SHA256 hashes

- 6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920
- 6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74
- 70f42cc9fca43dc1fdfa584b37ecbc81761fb996cb358b6f569d734fa8cce4e3
- a5f82f3ad0800bfb9d00a90770c852fb34c82ecb80627be2d950e198d0ad6e8b
- 85b71784734705f6119cdb59b1122ce721895662a6d98bb01e82de7a4f37a188 (unpacked)

References

Targets

Maastricht University (UM) - The Netherlands

Notes

- TA505

- Clop filemarker: `Clop^_-`
- Ransom extension: `.clop` or `.CIop`
- Ransom note: `ClopReadMe.txt` or `CIopReadMe.txt` (https://pastebin.com/rHQ8gzD9)
- Ransom e-mails:

```
servicedigilogos@protonmail.com
managersmaers@tutanota.com
unlock@eqaltech.su
unlock@royalmail.su
unlock@goldenbay.su
unlock@graylegion.su
kensgilbomet@protonmail.com
```

- Using RSA 1024-bit public key
- Then encrypts files with RC4 using 117 bytes of the public key
- Other version uses `Mersenne Twister algorithm`
- Tries to uninstall ESET AV by grepping ProductCode from `callback.log` file:

```
cmd.exe "/C MSIEXEC /x 'ESET ProductCode' /qb"
```

Uninstalls MSC:

```
cmd.exe /C "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

- Other version checks for `MalwareBytes, Webroot, Panda`
- Interesting API call: `OpenPrinterW(L"KJFk23983ruafbuyTHFNIO#wu", 0, 0);`
- Signed with valid certificate
- Check local language via GetKeyboardLayout against hardcoded list: `Georgian, Russian, Azerbaijan`

AV evasion

Tries to disable Windows Defender

```
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t
REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t
REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t
REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t
REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v
"TamperProtection" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiSpyware" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\MpEngine" /v "MpCloudBlockLevel" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Spynet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

Tries to uninstall MalwareBytes

```
cmd.exe /c \"C:\\Program Files\\Malwarebytes\\Anti-
Ransomware\\unins000.exe\" /verysilent /suppressmsgboxes /norestart
```

Seen resources:

- RC_DATAMAKEMONEY
- RC_DATABIGBACK

Seen mutexes:

- FFRRTTOOOTTPPWWZZZLLSS^_-
- MakeMoneyFromAirEathWorld#666Go
- BestChangeT0pMoney^_-666

Ransom note:

```
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong
algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage
encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy
your files irreversibly.
If you want to restore your files write to emails (contacts are at the
bottom of the sheet) and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain
valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the
decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
servicedigilogos@protonmail.com
or
managersmaers@tutanota.com

The final price depends on how fast you write to us.

Clop
```

Yara rules

```
rule clop_ov_carosig
{
  meta:
    author = "Albert Zsigovits"
    family = "Clop ransomware"

  condition:
    new_file and (signatures matches /.*Clop.*/)
}
```