[S2W LAB] Analysis of Clop Ransomware suspiciously related to the Recent Incident (English)

Author: TALON *(BLKSMTH, HOTSAUCE)*

Date: 2020-11-23

Executive Summary

- The ransomware Clop has hit the network of conglomerate and retail giant in South Korea which suspended nearly half of stores due to its attack. We have analyzed the ransomware related to the incident and the summary of the analysis can be seen below.
    - A new variant of the Clop ransomware seems to generate separate key files and store encryption keys for each encrypted files as opposed to the previous behavior of changing the file content and extension and saving the encryption key at the final stage
    - Key File Extension : .cllp
    - Key File Header : Cllp^_-
    - Ransom Note: We have identified that the contact email used in ransom note is identical to the email used by Clop Ransomware on the Dark Web where they leak corporate data when negotiations fails.

- We have also detected the same variant of the ransomware that contained identical signatures on Virus Total (Build time: Nov-21-2020).

Distribution

- We have yet finalized the deploying patterns but we can assume the intrusion technique by referring to previous incidents.
  1. Network intrusion using SMB exploit.
  2. A massive deployment by compromised administrator account of an Active Directory.
  3. Malicious document files distributed as attachments via spear phishing emails.

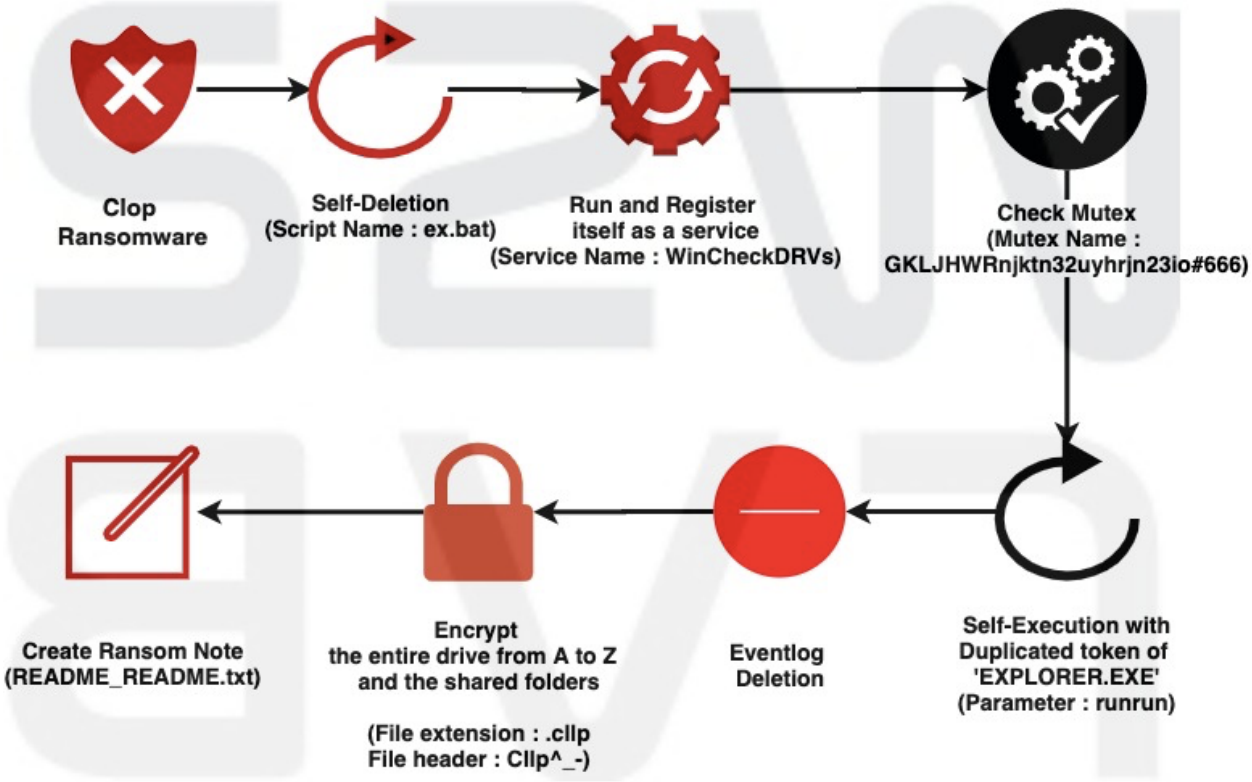
Analysis of Clop Ransomware (#01)

1) Basic Properties (#01, Marker for Relation Analysis)

> **MD5 :** 8b6c413e2539823ef8f8b85900d19724
> **SHA-1 :** 2d92a9ec1091cb801ff86403374594c74210cd44
> **SHA-256 :** 3d94c4a92382c5c45062d8ea0517be4011be8ba42e9c9a614a99327d0ebdf05b
> **Type :** Win32 EXE (PE32 executable for MS Windows (GUI) Intel 80386 32-bit)
> **Build Time :** 2020-11-20 18:18:18

2) Malware Behaviour

Full execution flow of Clop ransomware



Stage1 (Allocates executable code to memory)

- It is configured to be executed by allocating to the memory (VirtualAlloc) so that the structure of the malicious code cannot be understood.

Stage2 (Main code to memory allocation after self-deletion)

- Self-deletion is executed after generating ex.bat file

```
strcpy(ex_bat, "ex.bat");
strcpy(CreateFileA_, "CreateFileA");
strcpy(CreateProcessA_, "CreateProcessA");
strcpy(WriteFile_, "WriteFile");
strcpy(CloseHandle_, "CloseHandle");
strcpy(GetModuleFileNameA_, "GetModuleFileNameA");
strcpy(lstrcpyA_, "lstrcpyA");
strcpy(del_, ":R\r\ndel \"");
strcpy(if_exist, "\"\r\nif exist \"");
strcpy(goto_del, "\" goto R\r\ndel \"");
v20[0] = '"';
v20[1] = '\r';
v20[2] = '\n';
v20[3] = 0;
CreateFileA__ = a2(a1, CreateFileA_);
lstrcpyA__ = a2(a1, lstrcpyA_);
GetModuleFileNameA__ = a2(a1, GetModuleFileNameA_);
CloseHandle__ = a2(a1, CloseHandle_);
WriteFile__ = a2(a1, WriteFile_);
CreateProcessA__ = a2(a1, CreateProcessA_);
GetModuleFileNameA__(0, v26, 260);
result = CreateFileA__(ex_bat, 0x40000000, 0, 0, 2, 128, 0);
v16 = result;
if ( result != -1 )
{
  ARG_01_1040(v15, 0, 256);
  lstrcpyA__(v15, del_);
  sub_1080(v15, v26);
  sub_1080(v15, if_exist);
  sub_1080(v15, v26);
  sub_1080(v15, goto_del);
  sub_1080(v15, ex_bat);
  sub_1080(v15, v20);
  v3 = sub_10E0(v15);
  WriteFile__(v16, v15, v3, &goto_del[16], 0);
  CloseHandle__(v16);
  ARG_01_1040(v10, 0, 68);
  ARG_01_1040(v19, 0, 16);
  v10[0] = 68;
  v10[11] = 1;
  v11 = 0;
  result = CreateProcessA__(0, ex_bat, 0, 0, 0, 16, 0, 0, v10, v19);
}
```

Stage3 (Main malicious code)

- **MD5** : 14B7069B25B04EBA875F264BE4F140DA
- **Build Time** : 2020-11-20 14:35:08

- Infection Routine
  1. Run and register itself as a service
     - Service name : **WinCheckDRVs**
  2. Uses mutex to check if another instance is running (duplication check)
     - Mutex name : GKLJHWRnjktn32uyhrjn23io#666
  3. Self execution
     - Self execute with duplicated token of 'EXPLORER.EXE' and sets "runrun" as a parameter
  4. Run event log deletion command

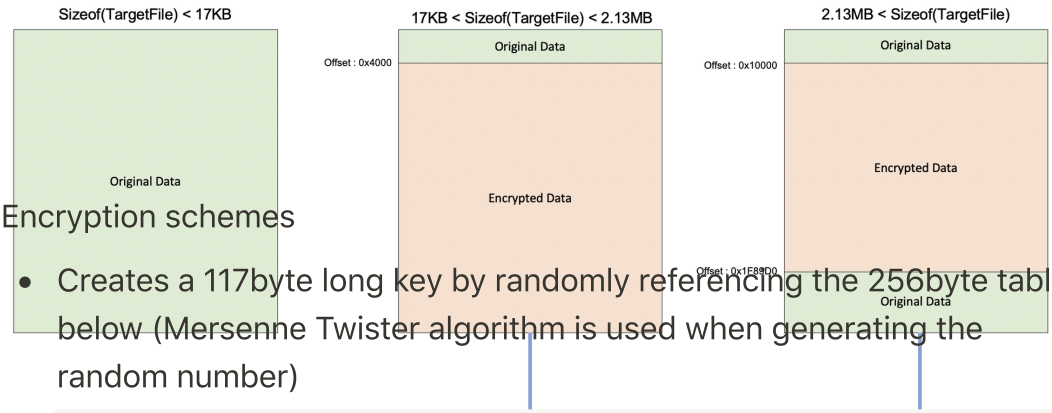
```
cmd.exe /C for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO
wevtutil.exe cl \"%1\"
```

  5. Attempts to encrypt the entire drive from A to Z except Floppy Disk, CD-ROM.
     - RSA Public Key hard coded inside the malware.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCecUuskA+/EYRGu9HUFkpICA
e3MeraGTOS8wa6lZfirCt0oRPARUcF1aNVupKfLeqc02BX+MAn3n15EJpoe1SR
iESj5Z+dJl2WBFaYoV/SBg5EQWganz32HN3dhH037t3vrDP7jsQa2lziD32hLd
SEktD4Gmz87O+0blTQIDAQAB -----END PUBLIC KEY-----
```

     - Skips Desktop path when encrypting files
     - Avoids certain files by matching hash value of file name
     - Clop passes encrypting certain file extensions:
       - .CI0P : Previously encrypted file extension
       - .OCX : Object linking and embedding files (ActiveX)
       - .DLL : Compiled library (dynamic)
       - .EXE : Execution file
       - .SYS : Driver file

    - .LNK : Shortcut file
    - .ICO : Icon file
    - .INI : Initialization file
    - .MSI : Installer file
    - .CHM : Compiled HTML help file
    - .HLF
    - .LNG : Language pack file
    - .TTF : Font file
    - .CMD : Script file
    - .BAT : Batch file
    - .CLLP : Current encrypted ransomware file
- Encryption technique varies depending on the size of target files
    - sizeof(TargetFile) < 17KB : **Passes encryption**
    - 1.7KB < sizeof(TargetFile) < 2.13MB : **Encrypts from 0x4000 to EOF(End of File)**
        - Uses general file input/output method
    - sizeof(TargetFile) < 2.13MB : **0x10000~0x1F89D0 Encryption**
        - MMF method is used to handle large size files efficiently.
        - MMF : Through the Memory Mapped File(MMF), the contents of a file in virtual memory space can be linked enabling an application to write the file directly to the memory.
    - A diagram of encryption method by Clop ransomware



- Encryption schemes
  - Creates a 117byte long key by randomly referencing the 256byte table below (Mersenne Twister algorithm is used when generating the random number)

```
e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 cd ef 34
56 78 9a b1 31 41 51 61 71 81 91 a1 b1 c1 d1 e1 fc 3c 4c
5c 6c 7c 8c 9c ac bc cc dc ec fd 0d 1d 20 12 d3 d4 d5 d6
d7 d8 d9 da db dc dd de df e0 e1 e2 cd ef 83 84 85 86 87
88 89 8a 8b 8c 8d 8e 8f 90 91 92 a3 a4 a5 a6 a7 a8 a9 aa
ab ac ad ae af b0 b1 b2 ab 7f 80 81 82 00 01 02 03 04 05
06 07 08 0b 0c 0e 0f 10 11 12 b3 b4 b5 b6 b7 b8 b9 ba bb
bc bd be bf c0 c1 c2 93 94 95 96 97 98 99 9a 9b 9c 9d 9e
9f a0 a1 a2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff
```

  - 117byte default key is used when creation fails

```
ab 9d 89 0a b9 2b ba fa 19 f2 10 21 4c 9c 6a 7f 3a 31 8b
fd e9 ff fa 6c f1 f1 11 8e b6 c7 81 17 a5 b2 89 ad 1e 78
fa e3 82 83 1b cd 9d 92 ad dc c5 d8 b1 8d 01 1b b2 f1 b9
89 e2 c7 41 71 e2 f7 a3 1d 6c aa 28 0c 6e db 3c f8 fd 10
1f b1 f1 b9 89 8e
```

  - 117byte key is used as RC4 algorithm key to encrypt the original data, then updates
    - It overwrites the encrypted data rather than deleting the original file
  - Key storage file **[encryption target file name]**.cllp is created to manage encryption keys per file
    - Key File Header : Cllp^_- (7byte)

- Key File Data : 117byte RC4 Key (128byte) encrypted by RSA public Key
- 135 bytes fixed in total

6. Tours around shared folders and attempts to encrypt
    - Including Desktop path
    - Identical encrypting schemes is used to encrypt afterwards

7. Attempts to encrypt files from the C Drive
8. Ransom note created in every encrypted file
    - Ransom note file name : README_README.txt
    - Ransom note created by following procedure
        - Extract encoded data in resource section inside malicious code
            - Resource ID : 39339, Resource NAME : ID_HTML
        - Extract the original data by XOR decoding the resource data and the table below

```
JKHfg34789t6y8f9JLKHFUEWir3289457yfnKLSFEj2jk34y57823fjvsdi
```

- When Command line parameter = temp.dat
    1. Reads temp.dat upon execution and attempts to only encrypt the path that has been specified
        - Function exists, however is the option that is not executed from the actual code

Ransom Note

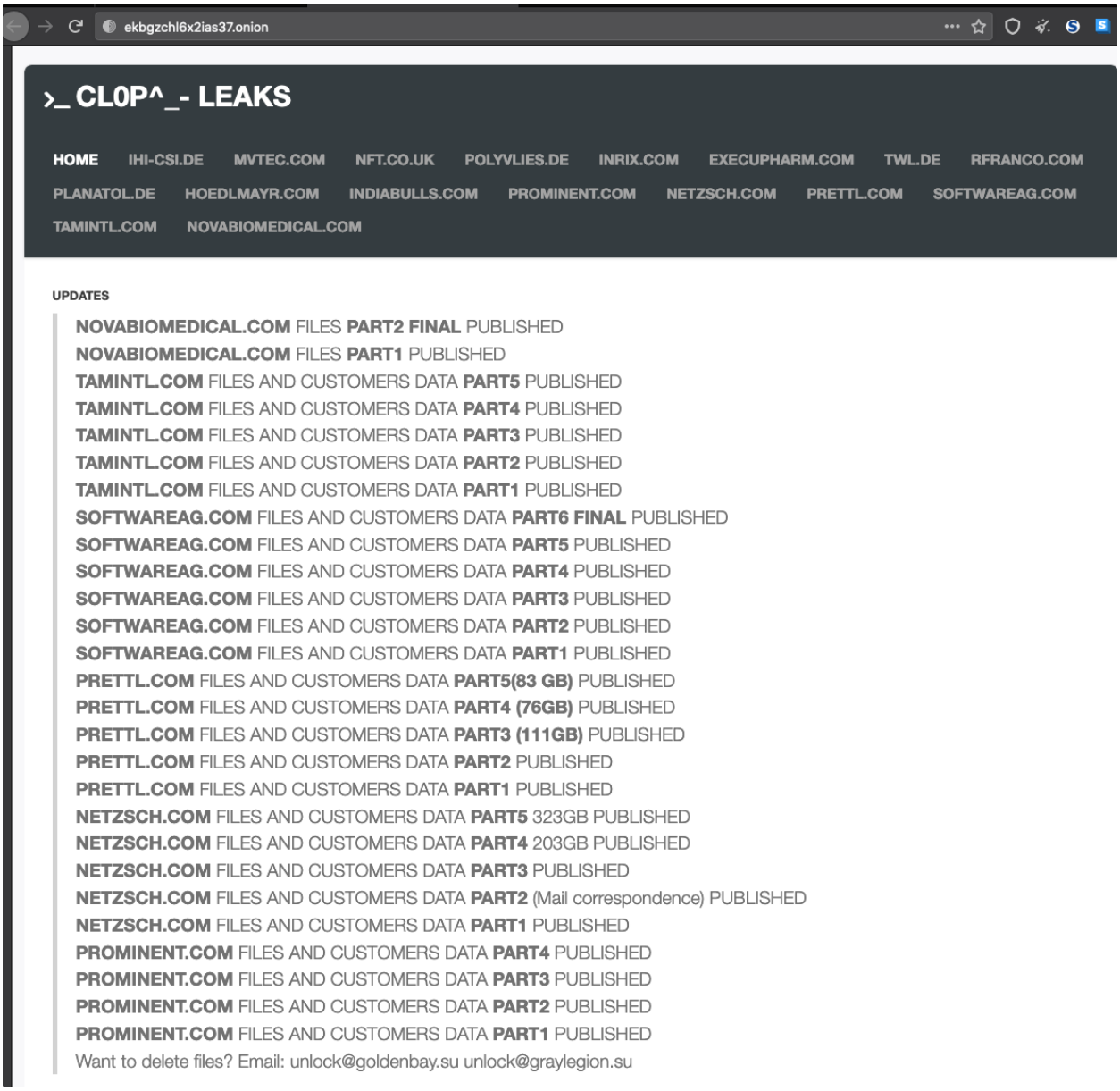

```
HELLO DEAR KMALL *DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. T
THEM* Also, we have stolen very important information from your servers.
for details. If you refuse to cooperate, all data will be published for f
our portal (USE TOR BROWSER): http://ekbgzchl6x2ias37[.]onion/ CONTACTS:
dinoriuss1973@tutanota[.]com AND unlock@support-box[.]com OR unlock@suppo
WRITE TO THE CHAT (USE TOR BROWSER):
http://cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdglsulcsid[.]onion/r
7c5a-4b5d-9e19-3610beadffc6?secret=km2021
```

1) Contact (E-mail)

> dinoriuss1973@tutanota[.]com
> unlock@support-box[.]com
> unlock@support-iron[.]com

- Contact (E-mail addresses) information is identical with the information from the Darkweb website that list-up the Clop ransomware victims (Leaks Website*).

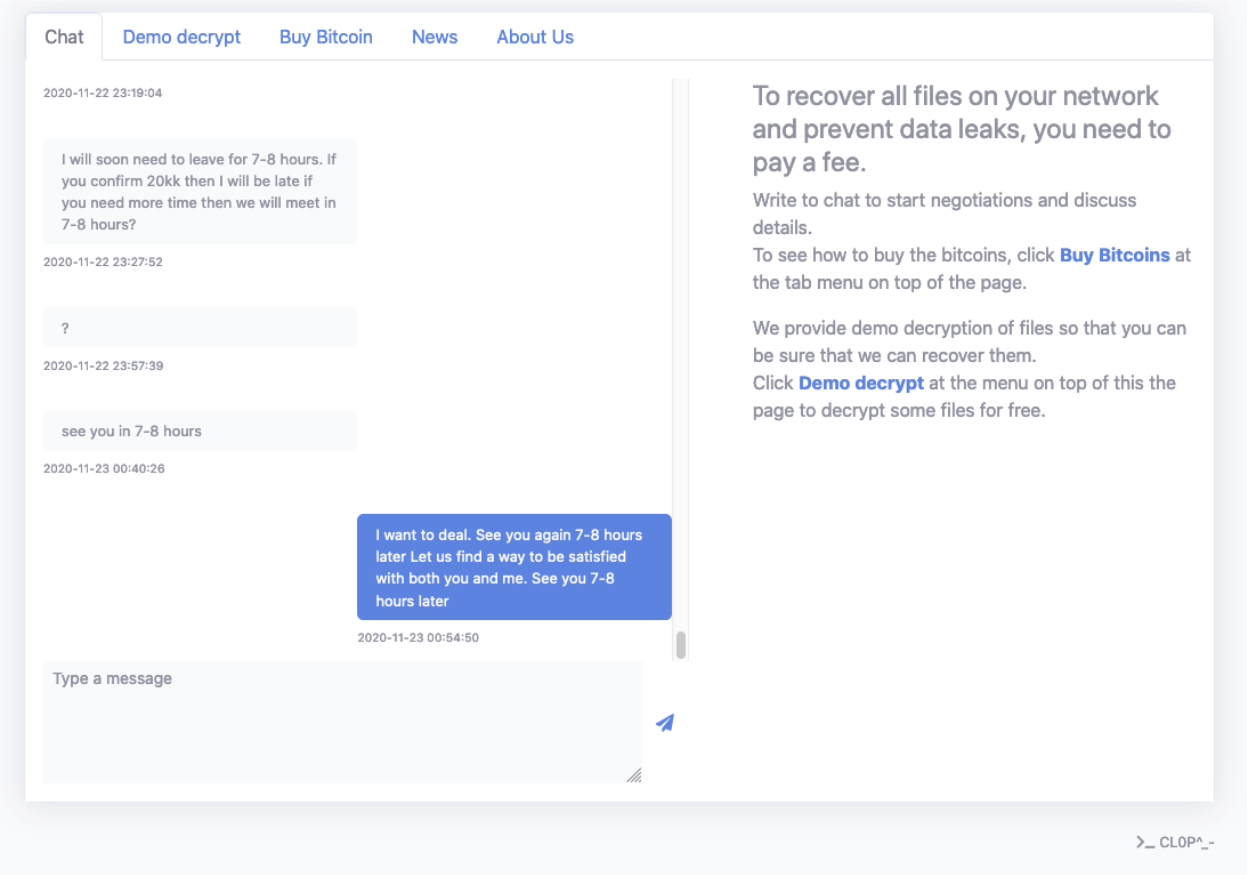
2) Leaks Website of Clop Ransomware (ekbgzchl6×2ias37[.]onion)



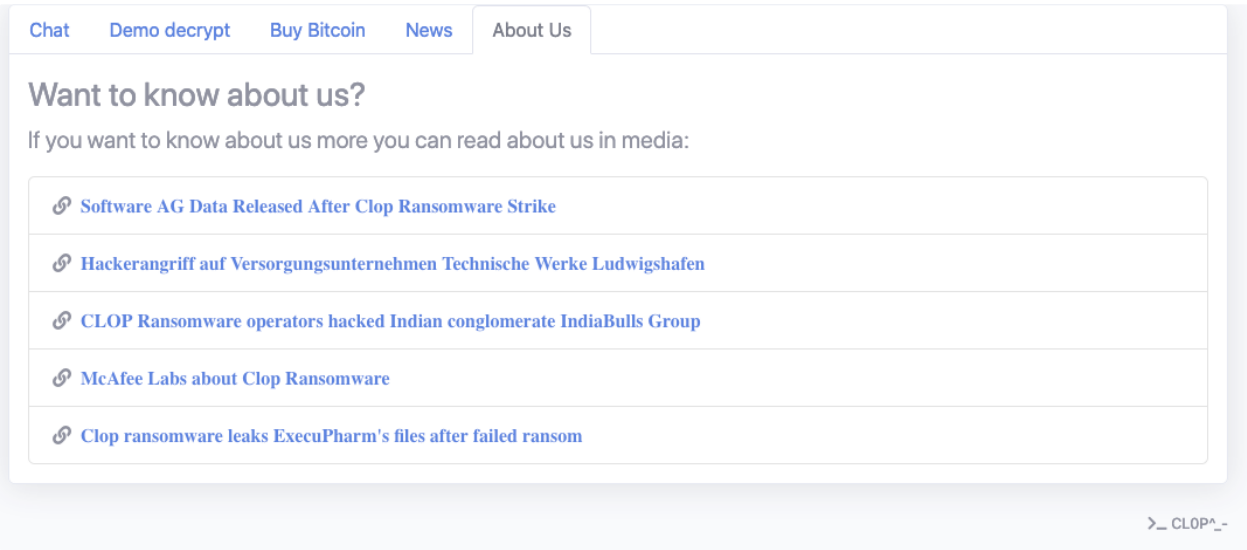
- Number of Clop Ransomware Victims on the Darkweb: 17
- Data uploading cycle for negotiated firm: Approximately 7 days – 1 month
- Uploaded Data
  - Employee credential
  - Employee emails
  - Accounting related information
  - ETC

3) Tor page for negotiation

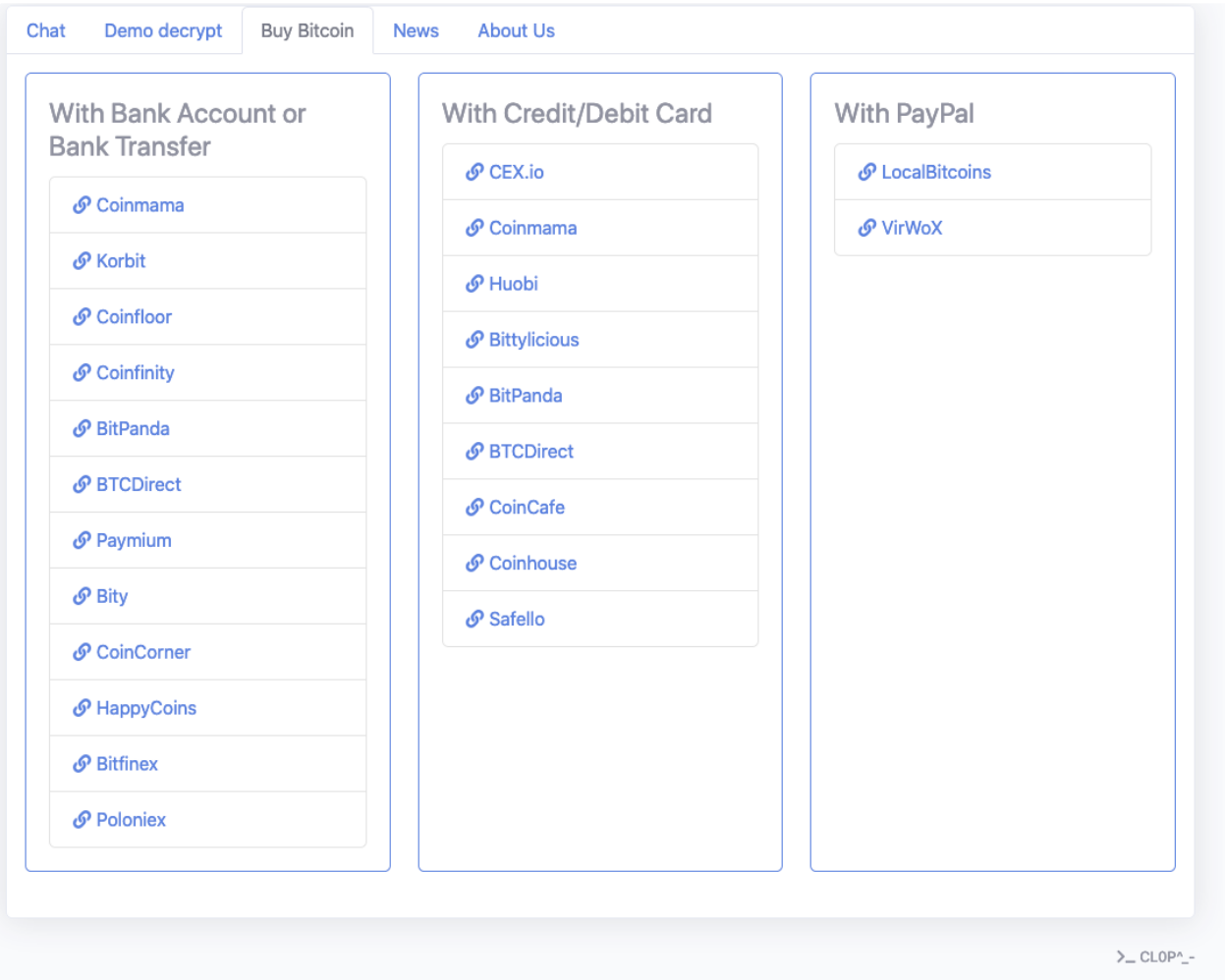
Chat (hxxp://cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdglsulcsid[.]onion)



About Us


Chat
Demo decrypt
Buy Bitcoin
News
About Us
Want to know about us?
If you want to know about us more you can read about us in media:
Software AG Data Released After Clop Ransomware Strike
Hackerangriff auf Versorgungsunternehmen Technische Werke Ludwigshafen
CLOP Ransomware operators hacked Indian conglomerate IndiaBulls Group
McAfee Labs about Clop Ransomware
Clop ransomware leaks ExecuPharm's files after failed ransom
>_ CLOP^_-

Buy Bitcoin


Chat
Demo decrypt
Buy Bitcoin
News
About Us
With Bank Account or Bank Transfer
Coinmama
Korbit
Coinfloor
Coinfinity
BitPanda
BTCDirect
Paymium
Bity
CoinCorner
HappyCoins
Bitfinex
Poloniex
With Credit/Debit Card
CEX.io
Coinmama
Huobi
Bittylicious
BitPanda
BTCDirect
CoinCafe
Coinhouse
Safello
With PayPal
LocalBitcoins
VirWoX
>_ CLOP^_-

Intelligence Analysis

Comparison between current Clop and Clop from first half of the year 2019

	'19 1st	'20 4th
MD5	16900F49B5ED9F240E3E8E71D01202EC	14B7069B25B04EBA875F264BE4F140DA
Keyboard layout to exclude	Russian, Ukrainian, Belarusian, Tajik, Armenian, Uzbek, Kyrgyz, Turkmen	X
Service name	BootServicingSecurity	WinCheckDRVs
Vaccine check	VIPRE Antivirus	X
Mutex	Cash##666	GKLJHWRnjktn32uyhrjn23io#666
Public key	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCCoT6k7uXAUbnmqOL7YlWVhFk6 wLtInGnCHftaRsqvO8NoyCzsjT3UWdl6l4ocV1LaJ4a44gyqL6q3ppslxp4fKzfF g6d+uzeHD9zrYiKn1gNcAdvGslZ4xAaVEjUn14Qe2F4goyS9Lv/pNSJ1bxtaWz59 FNzTRPK+GUdVBCm4HwIDAQAB -----END PUBLIC KEY-----	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCecUuskA+/EYRGu9H UFkpICAgJ e3MeraGTOS8wa6lZfirCt0oRPARUcF1aNVupKfLeqc02BX+MAn 3n15EJpoe1SRya iESj5Z+dJl2WBFaYoV/SBg5EQWganz32HN3dhH037t3vrD P7jsQa2lziD32hLd3y SEktD4Gmz87O+0blTQIDAQAB -----END PUBLIC KEY-----
Extension	.Clop	.Cllp
File size to check	3MB, 2GB	17KB, 2.13MB
File identifier	Clop^_-	Cllp^_-
File encryption algorithm	RC4	RC4
Filename of Ransom note	ClopReadMe.txt	README_README.txt
Resource name of Ransom note	CSIX	ID_HTML
Decoding table of Ransom note	JLKHFVIjewhyur3ikjfldskfkl23j3iuhdnfklqhrjjio2ljkeosfjh7823763647823hrf uweg56t7r6t73824y78Clop	JKHfg34789t6y8f9JLKHFUEWir3289457yfnKLSFEj2jk34y57823fjvsdiogh23f unrjtubh287yutihfgvdfkjrgb34hj
Purpose of hex values	To terminate process	To exclude filenames
Contact Emails	ldtwinj@protonmail.com unlock@eqaltech.su	dinoriuss1973@tutanota.com unlock@support-box.com unlock@support-iron.com
Onion Domain	X	ekbgzchl6x2ias37.onion cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdglsulcsid.onion

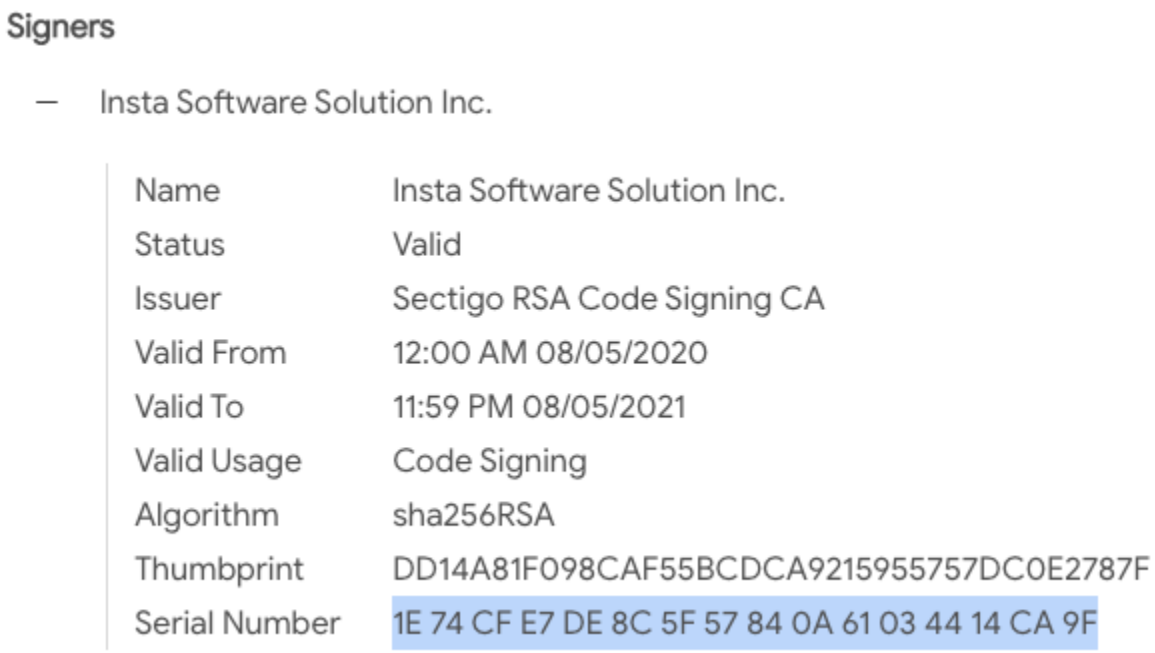
Past Ransom Note

```
!!!Your networks 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 DELETE readme files!!! !!!DO NOT RENAME OR MOVE the encrypted and readme files!!! !!!DO NOT RESET OR SHUTDOWN – files may be damaged!!! 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 3 – 4 encrypted files [Less than 6 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: ldtwinj@protonmail.com and unlock@eqaltech.su Please write to both emails! !!!The final price depends on how fast you write to us!!! Nothing personal just business! Clop^_-
```

Signature information

of other malware similar to recent sample

1



- 11 different malware code MD5 lists that share identical signature information

```
8fc09cb1540a6dea87a078b92c8f2b0a 8b6c413e2539823ef8f8b85900d19724
9246d60c24591855bc1792aa0a672ff7 34f8228a3f12fa9542f1a4181f96edec
731d5ed57434e05c9466107052af5a6a b96f79eb633d0b2c0e79e6d889dac0da
efb886d6eaa54d666dcfde173ae02d81 e3bc953a18fe466cb008184a45c6c858
d014969ab6421bde1419cbd30d0d5ebb a98dc09226b97ddc0d959e0aaa08abe0
8274514bc52e98bb4431ef61109fb15c
```

Clop Ransomware(#02) : Identified using the same signature

#02 : 8fc09cb1540a6dea87a078b92c8f2b0a

Basic Properties

> **MD5 :** 8fc09cb1540a6dea87a078b92c8f2b0a
> **SHA-1 :** 16f48624ea2a575e1bdceb4ac6151d97d4de80b6
> **SHA-256 :** 389e03b1a1fd1c527d48df74d3c26a0483a5b105f36841193172f1ee80e62c1b
> **Build Time** 2020-11-21 15:56:31

- Confirmed that Malware code has been created more recently than #01 Clop Ransomware (8b6c413e2539823ef8f8b85900d19724)

Main features

- Identical method to import the malware activity file with #01 Clop Ransomware(8b6c413e2539823ef8f8b85900d19724)

Results after confirming the code with malware activity

Basic Properties

> **MD5 :** AC0FE3E86F9FC7E5FD08D9E618B601F3
> **SHA1 :** 8C7173BDDE2919B524B22EA257A80360DF33A333
> **SHA256 :** 71DB30A0174795E9387F6A6CCA940359028CAD3BC3B7BEF24B48E150102DB391
> **Build TIme** 2020-11-21 14:43:58

Key strings identified in malware

```
.rdata:00413440 00000014 C (16 bits) - UTF-16LE %s%s.Cllp .rdata:0041345
.rdata:0041345C 00000008 C Cllp^_- .rdata:00413618 00000014 C (16 bits) -
.rdata:00413630 00000040 C (16 bits) - UTF-16LE 666GKLJHWRnjktn32uyhrjn2
0000001A C (16 bits) - UTF-16LE EXPLORER.EXE .rdata:00413690 00000047 C /
%1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\" .rdata:004136F0 0000
16LE WinCheckDRVs .rdata:0041370C 0000000E C (16 bits) - UTF-16LE runrun
00000012 C (16 bits) - UTF-16LE temp.dat .rdata:00413730 0000001C C (16
.rdata:0041374C 0000001A C (16 bits) - UTF-16LE WinCheckDRVs .rdata:0041
BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCecUuskA+/EY
e3MeraGTOS8wa6lZfirCt0oRPARUcF1aNVupKfLeqc02BX+MAn3n15EJpoe1SRya
iESj5Z+dJl2WBFaYoV/SBg5EQWganz32HN3dhH037t3vrDP7jsQa2lziD32hLd3y SEktD4G
END PUBLIC KEY----- .rdata:00413878 00000060 C
JKHfg34789t6y8f9JLKHFUEWir3289457yfnKLSFEj2jk34y57823fjvsdiogh23funrjtub
.rdata:004138D8 0000002A C (16 bits) - UTF-16LE %s\\README_README.txt
```

Result of Similarity

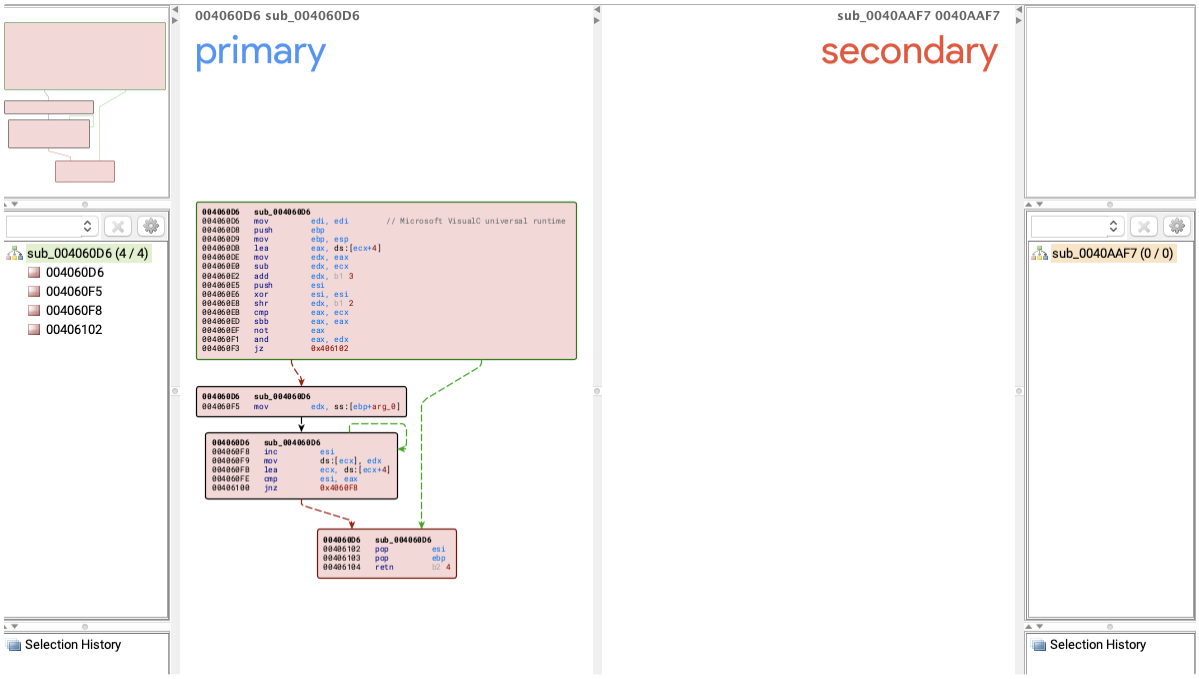
- After analyzing the actual malware code that operates on memory #01 and #02, most of the codes are similar except for some functions (Confidence 99.2% , Similarity : 82.38%)

```
Confidence                    0.992
Similarity                    0.823874
```

Similarity	Confide	Change	EA Primary	Name Primary	EA Secondary	Name Secondary	Cor	Algorithm
1.00	0.99	------…	00401000	sub_00401000	00401000	sub_00401000		edges flowgraph MD index
1.00	0.99	------…	004012D0	sub_004012D0	004012D0	sub_004012D0		edges flowgraph MD index
1.00	0.99	------…	00401420	sub_00401420	00401420	sub_00401420		edges flowgraph MD index
1.00	0.99	------…	00402B20	sub_00402B20	00402B40	sub_00402B40		edges flowgraph MD index
1.00	0.99	------…	00402B60	sub_00402B60	00402B80	sub_00402B80		edges flowgraph MD index
1.00	0.99	------…	00402D10	sub_00402D10	00402C20	sub_00402C20		edges flowgraph MD index
1.00	0.99	------…	00403270	sub_00403270	00403180	sub_00403180		hash matching
1.00	0.99	------…	004032F0	sub_004032F0	00403200	sub_00403200		hash matching
1.00	0.99	------…	00403370	sub_00403370	00403280	sub_00403280		edges flowgraph MD index
1.00	0.99	------…	00403840	sub_00403840	00403750	sub_00403750		hash matching
1.00	0.99	------…	00403940	sub_00403940	00403850	sub_00403850		hash matching
1.00	0.99	------…	00403980	sub_00403980	00403890	sub_00403890		edges flowgraph MD index
1.00	0.99	------…	00403AB0	sub_00403AB0	004039C0	sub_004039C0		hash matching
1.00	0.99	------…	00403B4C	__security_check_cookie(x)	00403A38	__security_check_cookie(x)		name hash matching
1.00	0.99	------…	00403B8D	pre_c_initialization(void)	00403A7D	pre_c_initialization(void)		name hash matching
1.00	0.99	------…	00403C4B	__scrt_common_main_seh(void)	00403B3B	__scrt_common_main_seh(void)		name hash matching
1.00	0.99	------…	00403DB3	start	00403CA3	start		name hash matching
1.00	0.99	------…	00403DE5	___report_gsfailure	00403CD5	___report_gsfailure		name hash matching
1.00	0.99	------…	00403EE0	find_pe_section(uchar * const,uint)	00403DED	find_pe_section(uchar * const,uint)		name hash matching
1.00	0.99	------…	00403F24	___scrt_acquire_startup_lock	00403E31	___scrt_acquire_startup_lock		name hash matching
1.00	0.99	------…	00403F59	___scrt_initialize_crt	00403E66	___scrt_initialize_crt		name hash matching
1.00	0.99	------…	00403F92	___scrt_initialize_onexit_tables	00403E9F	___scrt_initialize_onexit_tables		name hash matching
1.00	0.99	------…	00404029	___scrt_is_nonwritable_in_current_image	00403F36	___scrt_is_nonwritable_in_current_image		name hash matching
1.00	0.99	------…	004040B3	___scrt_release_startup_lock	00403FC0	___scrt_release_startup_lock		name hash matching
1.00	0.99	------…	004040D0	___scrt_uninitialize_crt	00403FDD	___scrt_uninitialize_crt		name hash matching
1.00	0.99	------…	004040F8	__onexit	00404005	__onexit		name hash matching
1.00	0.99	------…	00404133	_atexit	00404040	_atexit		name hash matching
1.00	0.99	------…	00404148	___security_init_cookie	00404055	___security_init_cookie		name hash matching
1.00	0.99	------…	004041FD	__initialize_default_precision	0040410A	__initialize_default_precision		name hash matching
1.00	0.99	------…	0040422A	___scrt_initialize_default_local_stdio_optio…	00404137	___scrt_initialize_default_local_stdio_optio…		name hash matching
1.00	0.99	------…	0040425F	___scrt_fastfail	0040416C	___scrt_fastfail		name hash matching
1.00	0.99	------…	0040437A	___scrt_get_show_window_mode	00404287	___scrt_get_show_window_mode		name hash matching
1.00	0.99	------…	004043B9	__scrt_unhandled_exception_filter(x)	004042C6	__scrt_unhandled_exception_filter(x)		name hash matching
1.00	0.99	------…	0040442D	sub_0040442D	0040433A	sub_0040433A		edges flowgraph MD index
1.00	0.99	------…	00404458	j____guard_check_icall_fptr	00404365	j____guard_check_icall_fptr		name hash matching
1.00	0.99	------…	004044A6	__SEH_epilog4	004043B6	__SEH_epilog4		name hash matching
1.00	0.99	------…	004044BB	___isa_available_init	004043CB	___isa_available_init		name hash matching
1.00	0.99	------…	00404655	___scrt_is_ucrt_dll_in_use	00404565	___scrt_is_ucrt_dll_in_use		name hash matching
1.00	0.99	------…	00404670	_memmove	00404580	_memmove		name hash matching
1.00	0.99	------…	00404BF0	_memset	00404B00	_memset		name hash matching

- #02 : 8fc09cb1540a6dea87a078b92c8f2b0a Final Malware code (Left)
- #01 : 8b6c413e2539823ef8f8b85900d19724 Final Malware code (Right)

- Some functions have been added, however the key code used for the ransomware operation is the same format.



IOC

HASH

```
8b6c413e2539823ef8f8b85900d19724 14B7069B25B04EBA875F264BE4F140DA
8fc09cb1540a6dea87a078b92c8f2b0a 8b6c413e2539823ef8f8b85900d19724
9246d60c24591855bc1792aa0a672ff7 34f8228a3f12fa9542f1a4181f96edec
731d5ed57434e05c9466107052af5a6a b96f79eb633d0b2c0e79e6d889dac0da
efb886d6eaa54d666dcfde173ae02d81 e3bc953a18fe466cb008184a45c6c858
d014969ab6421bde1419cbd30d0d5ebb a98dc09226b97ddc0d959e0aaa08abe0
8274514bc52e98bb4431ef61109fb15c AC0FE3E86F9FC7E5FD08D9E618B601F3
```

ETC

ONION

```
Cl0p Ransomware leak site: ekbgzchl6x2ias37[.]onion Cl0p Ransomware
Chat site:
hxxp://cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdglsulcsid[.]onion
```

- https://www.s2wlab.com
- Facebook https://www.facebook.com/S2WLAB/
- Twitter https://twitter.com/s2wlab