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

Archived: 2026-04-05 18:44:14 UTC

Author: TALON (BLKSMTH, HOTSAUCE)

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).

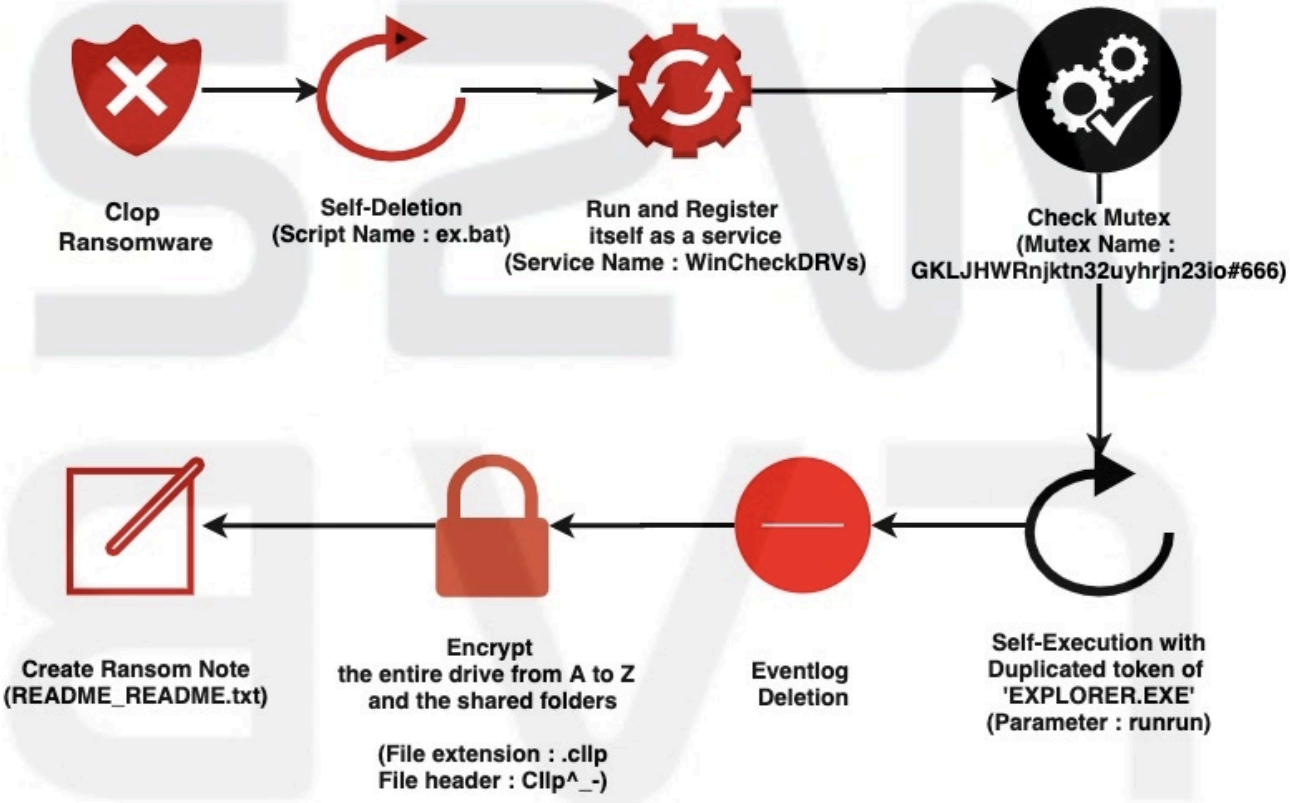
We have yet finalized the deploying patterns but we can assume the intrusion technique by referring to previous incidents.

Network intrusion using SMB exploit.

A massive deployment by compromised administrator account of an Active Directory.

Malicious document files distributed as attachments via spear phishing emails.

> 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



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

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);
}
```

MD5 : 14B7069B25B04EBA875F264BE4F140DA

Build Time : 2020-11-20 14:35:08

Run and register itself as a service

Service name : WinCheckDRVs

Uses mutex to check if another instance is running (duplication check)

Mutex name : GKLJHWRnjktn32uyhrjn23io#666

Tours around remote shared folders and attempts to encrypt

Gets token of 'EXPLORER.EXE'

Collects primary access token of user is logged on to the active RDP session

Collects RDP session token of the same account as the username of the collected EXPLORER.EXE token

Collects token of active session if username is 5 or less

Executes itself on winsta0\default with "runrun" as a parameter

Tours around remote shared folders and attempts to encrypt

Run event log deletion command

> Loading PowerShell code…

Attempts to encrypt the entire drive from A to Z except Floppy Disk, CD-ROM.

The new version of the clop ransomware attempts to encrypt files in use by forcing an application or service to restart using the Restart Manager API.

RSA Public Key hard coded inside the malware.

> Loading Plain Text code…

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)

.INI : Initialization file

.CHM : Compiled HTML help file

.LNG : Language pack 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)

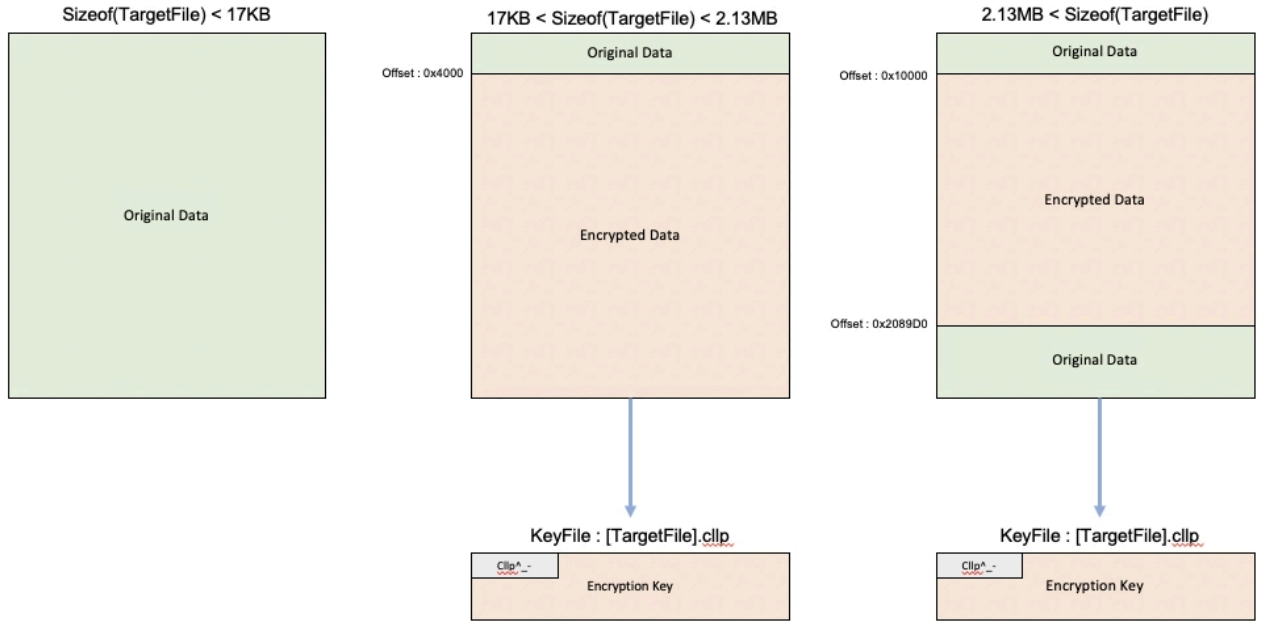
Uses general file input/output method

2.13MB < sizeof(TargetFile) : 0x10000~0x2089D0 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



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

> Loading Plain Text code…

117byte default key is used when creation fails

> Loading Plain Text code…

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 encrypted by RSA public Key → 128byte

Tours around shared folders and attempts to encrypt

Identical encrypting schemes is used to encrypt afterwards

Attempts to encrypt files from the C Drive

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

> Loading Plain Text code…

Do not delete the shadow volume unlike before

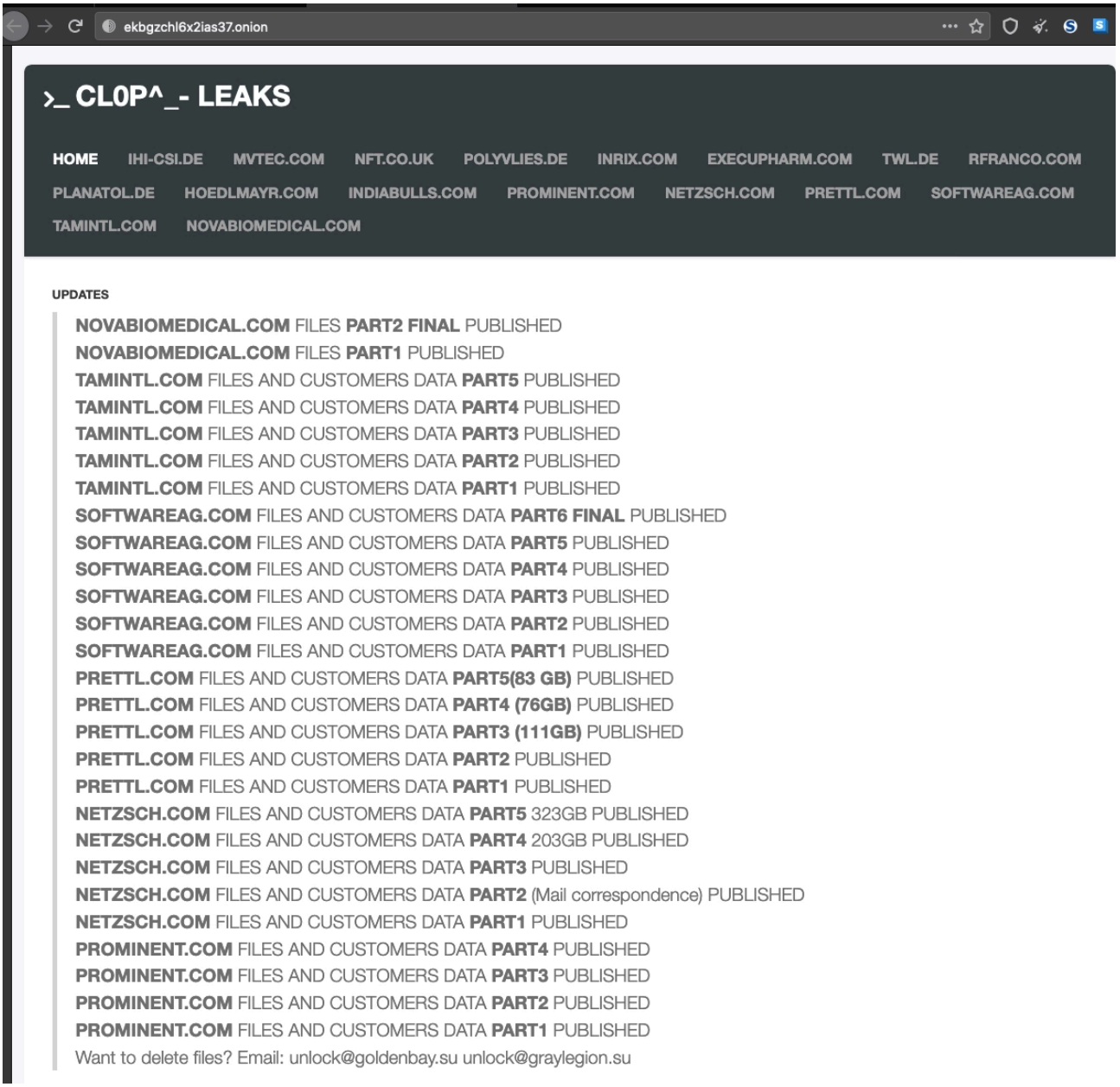
When Command line parameter = temp.dat

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

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

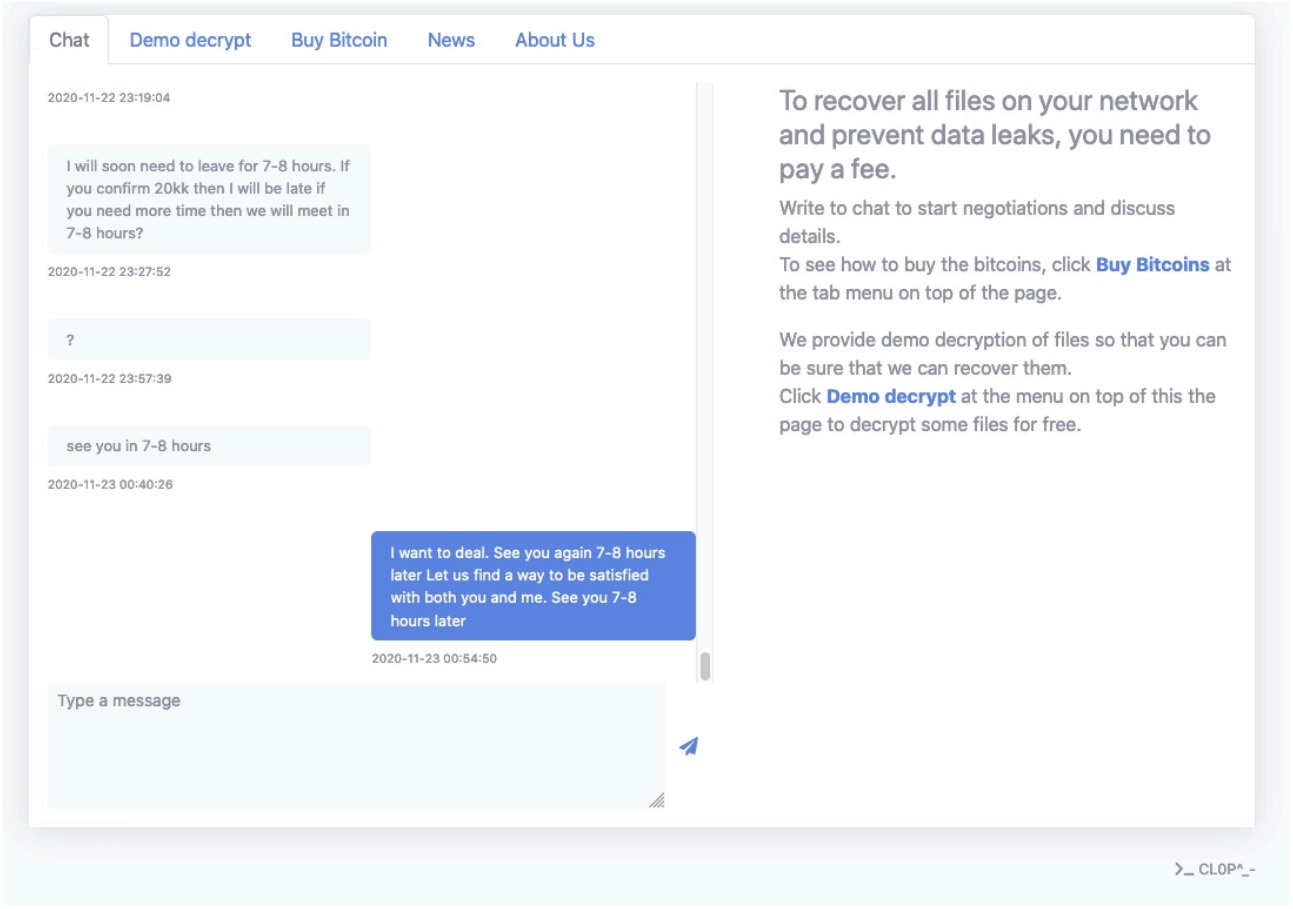
Contact (E-mail addresses) information is identical with the information from the Darkweb website that list-up the Clop ransomware victims (Leaks Website*).

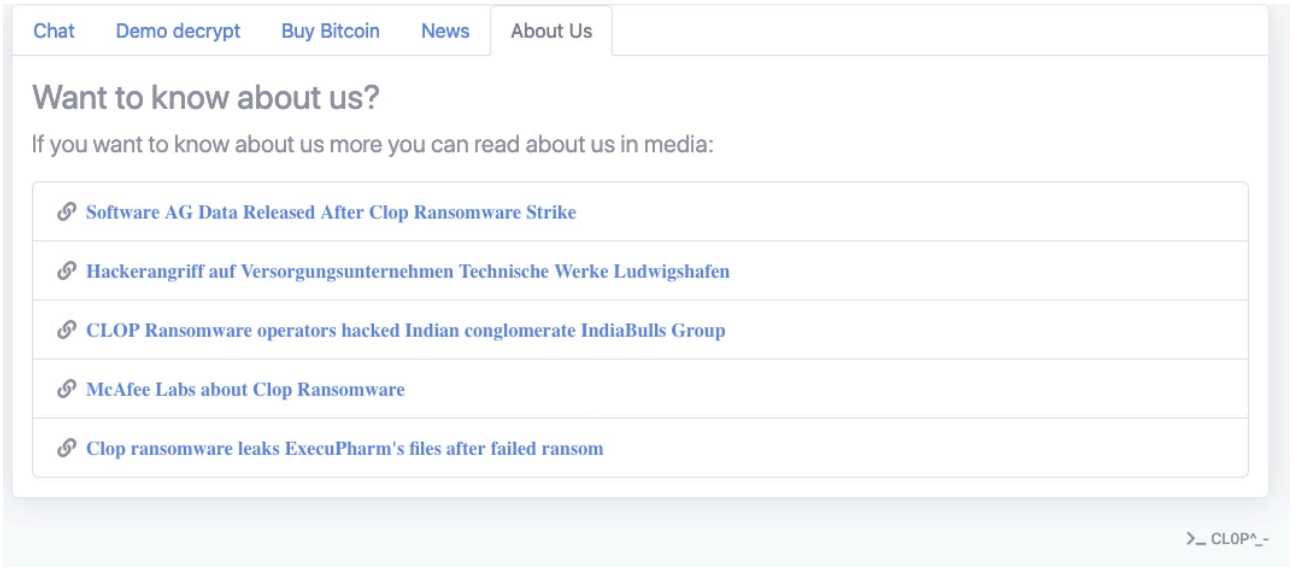


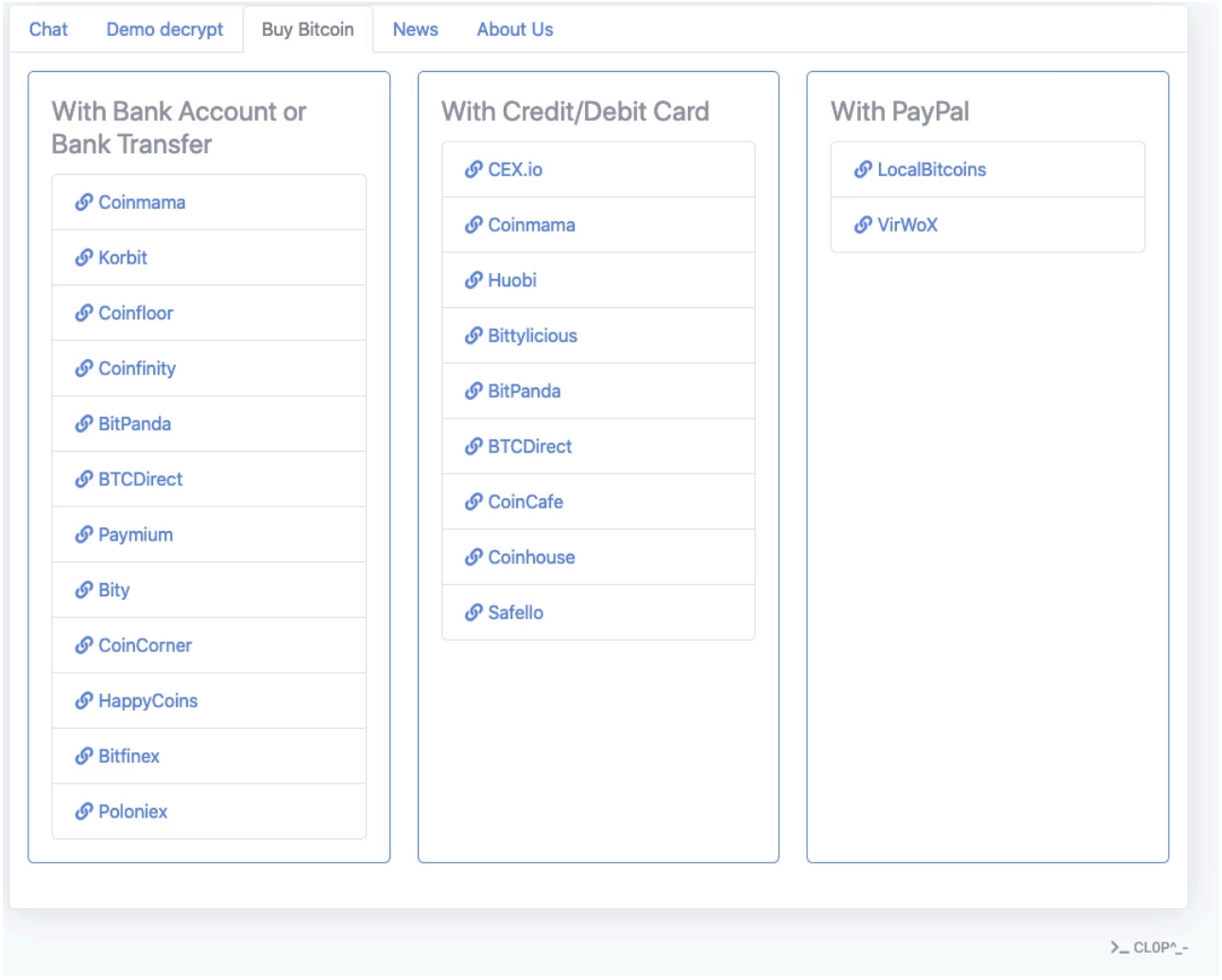
Number of Clop Ransomware Victims on the Darkweb: 17

Data uploading cycle for negotiated firm: Approximately 7 days – 1 month

Accounting related information


Chat
Demo decrypt
Buy Bitcoin
News
About Us
2020-11-22 23:19:04
I will soon need to leave for 7-8 hours. If you confirm 20kk then I will be late if you need more time then we will meet in 7-8 hours?
2020-11-22 23:27:52
?
2020-11-22 23:57:39
see you in 7-8 hours
2020-11-23 00:40:26
I want to deal. See you again 7-8 hours later Let us find a way to be satisfied with both you and me. See you 7-8 hours later
2020-11-23 00:54:50
Type a message
To recover all files on your network and prevent data leaks, you need to pay a fee.
Write to chat to start negotiations and discuss details.
To see how to buy the bitcoins, click Buy Bitcoins at the tab menu on top of the page.
We provide demo decryption of files so that you can be sure that we can recover them.
Click Demo decrypt at the menu on top of this the page to decrypt some files for free.
>_ CLOP^_-


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^_-


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
>_ CL0P^_-

	'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+/EYRGu9HUFkplCAgJ e3MeraGTOS8wa6lZfirCt0oRPARUcF1aNVupKfLeqc02BX+MAn3n15EJpoe1SRya iESj5Z+dJl2WBFaYoV/SBg5EQWganz32HN3dhH037t3vrDP7jsQa2lziD32hLd3y 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	JLKHFVIjewhyur3ikjfldskfkl23j3iuhdnfklqhrjjio2ljkeosfjh7823763647823hrfuweg56t7r6t73824y78Clop	JKHfg34789t6y8f9JLKHFUEWir3289457yfnKLSFEj2jk34y57823fjvsdiogh23funrjtubh287yutihfgvdfkjrgb34hj
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

> Loading Plain Text code…

of other malware similar to recent sample

11 different malware code MD5 lists that share identical signature information

> 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)

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

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

Source: https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-English-088056baf01242409a6e9f844f0c5f2e