

[Threat Analysis] CLOP Ransomware that Attacked Korean Distribution Giant

asec.ahnlab.com/en/19542/

January 5, 2021



In November last year, there was a case that shocked not only the security industry, but also all of the Korean industries. The system of E-Land Group, the distribution giant, was infected by the ‘CLOP Ransomware.’ According to the press report that quoted an associate of the company, over half of the brick-and-mortar stores were affected by the ransomware, leading to disruption of business. This incident showed that the ransomware attacks can occur regardless of company size, and Korean industries must now face such threats that made themselves tangible.

AhnLab, the leader of the Korean security industry, published an in-depth analysis report of CLOP Ransomware’s distribution path, whether infected PCs can be restored, course of the attack, and trend of change. This paper will briefly examine the content of the report.



Before discussing the case of attack against E-Land, the CLOP Ransomware must be analyzed as having knowledge on CLOP Ransomware's attack process and trend of change can help understand the case better.

Target of CLOP Ransomware Attack and Process

Attack Target

CLOP Ransomware targeted companies that operate Active Directory (AD). AD is more commonly used by companies than individual users as it allows companies to manage multiple Windows systems efficiently via centralized management. The attacker abused this advantage to steal AD server administrator privilege and attacked various systems within companies.

AhnLab estimates that in 2019, 369 companies and 13,497 systems (PC and server) suffered damage due to CLOP Ransomware. As only the attacks against companies were taken into account, there may be many more systems that suffered damage if taking unconfirmed systems into account.

Various industries were targeted including but not limited to public institutions, education, broadcasting, finance/security/insurance, manufacturing, IT, distribution, communications, etc. Based on the first half of 2019 and in terms of percentage, most of the ransomware attacks were done against the manufacturing industry (53%), followed by finance (15%), information service (11%), and retails industry (9%).

The attacker utilized meticulously-made spear-phishing attacks to target companies. They attempted attacks after pinpointing email recipients and meticulously wrote the email content in languages their targets use. One notable thing is that the attacker targeted non-Russian countries. The attacker designed the ransomware to first check keyboard layout and character set, and if the target is Russian or that of CIS nation's, it does not run.

Ransomware Variants

Next is the change in the number of CLOP Ransomware variants that were found in the first half of 2019. In February 2019, a large number of CLOP Ransomware variants were found. Note that 'ClopReadMe.txt,' CLOP Ransomware's ransom note, was first revealed in Pastebin.com on February 8, 2019.

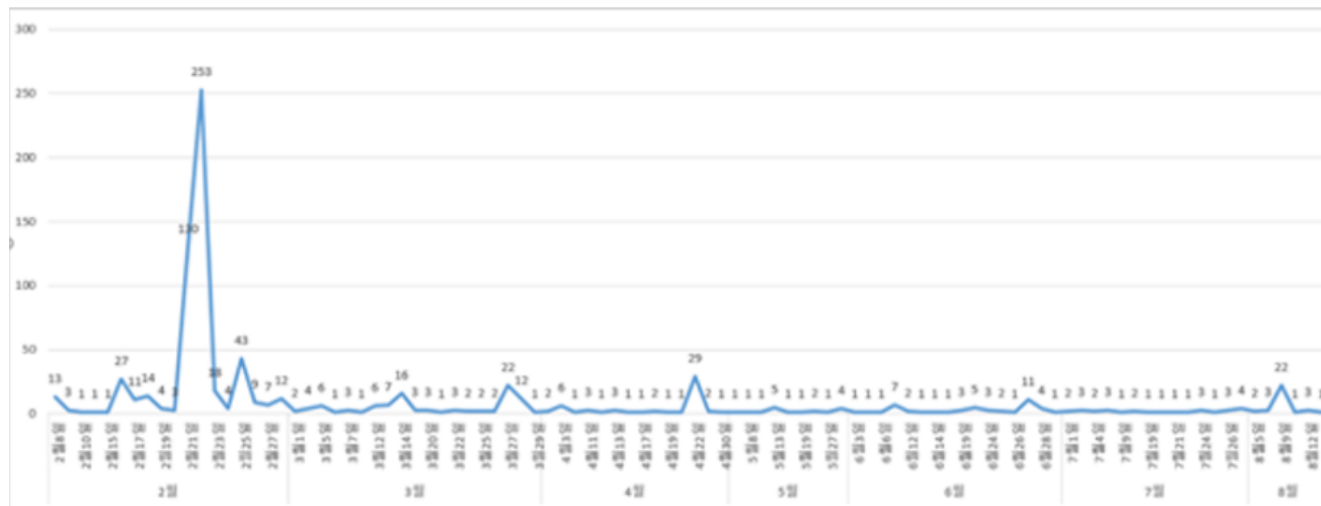


Figure 1. Change in numbers of CLOP Ransomware variants in 2019

Attack Process

The attack is carried out through preparation, domination, and execution phase. Specifically, there are 10 phases in total. The actual distribution and execution of CLOP Ransomware are the very last phase. The 3 big phases and the phases divided into 10 specific phases are as follows:

Preparation Sends malicious document attachment file via email to the first attack target and install remote control malware

- 1 User opens malicious document file (Excel, Word) attached to an email
- 2 Runs remote control malware downloader via macro inserted to a document file
- 3 If the system is added to AD (Active Directory) and operated in it,downloads remote control malware file and runs it (targeting AD environment)
- 4 Remote control malware file installs Cobalt Strike Beacon to the system

Domination Dominates system within AD using Cobalt Strike

- 5 Checks AD domain configuration info
- 6 Escalates run privilege using vulnerability
- 7 Runs Mimikatz module with escalated privilegeand obtains local administrator account or credential of AD domain administrator account
- 8 If AD domain administrator account is successfully obtained,connects to domain controller server and dominates system connected to domain

Execution	Attempts CLOP Ransomware infection on system within AD
9	Prepares malware such as CLOP Ransomware in the domain controller's shared folder
10	Distributes and runs CLOP Ransomware by using task scheduler or remote command to the system connected to AD domain

Table 1. CLOP Ransomware's attack process

CLOP Ransomware's Change Trend

Compared to the past, CLOP Ransomware did not change fundamentally in terms of encryption method and operation as a service. The difference is that it now compares after obtaining CRC instead of strings in process termination routine and encryption exception path.

Recent Changes in CLOP Ransomware

Additional change was confirmed in CLOP Ransomware collected in the second half of 2020. The past version worked by adding a symmetric-key that is encrypted with public-key along with signature to the back of the encrypted file, but the recently-confirmed CLOP Ransomware works by adding '.ClIp' extension to the same name, saving signature and encrypted key to a newly-created file.

0002A850	1E CF B5 37 93 3F CD 55 98 3F 5F 59 AF E6 9C 4B	.İµ7"?İU"? ȲæœK
0002A860	C6 73 9C 8B 5C 8D A2 E8 A6 A1 56 9F 4A 4F 89 5A	Æsœ< \.cè; ;VŸJOhZ
0002A870	B3 09 D3 D7 59 AF B1 6A ED 0C 85 C6 EA F4 3C 00	' .Ó×Ȳ±ji...Æèð<.
0002A880	08 1A 6D 8C 5C F7 4D DC 43 49 6F 70 5E 5F 2D B1	..mE\+MÜIop^±
0002A890	7C 08 3E 3D 24 B7 DF AE F1 29 77 36 85 3A 24 6A	.>=\$·Bñ)w6...: \$j
0002A8A0	54 DD 9C F6 DB E1 58 0B F0 56 6A E3 A3 9B CF 15	TŸæðŪáX.ðVjãÉ>İ.
0002A8B0	BB 73 F5 88 FC 2D 2B 98 7A 31 0A 6C D4 C4 A7 64	»sð^ù-+~zl.lôÅ\$đ
0002A8C0	0B D3 D6 DE 94 37 75 AB 01 B4 61 D4 5B 57 8C 3E	.óŌP"7u«. 'aô[WE>
0002A8D0	4E E0 00 5E 35 C8 6F 6F 41 A8 E3 DD 4D E4 3E 2C	Nà.^5ÈooA"ãÝMá>.
0002A8E0	4F CA D6 BD D7 C6 B4 AD 14 7A 54 D4 D8 DA CE 96	OÈÖ±×E' ..zTÔØŪİ-
0002A8F0	E3 4F 4D FE 52 8B 24 29 E6 5B 01 B6 99 A4 A6 A6	ãOMP<R< \$)æ[.Ÿ™H; ;
0002A900	EF 30 CF B9 8B 7E 82 40 2E 1F 30 25 47 31 2A	ı0İ²<~, @..0%G1*

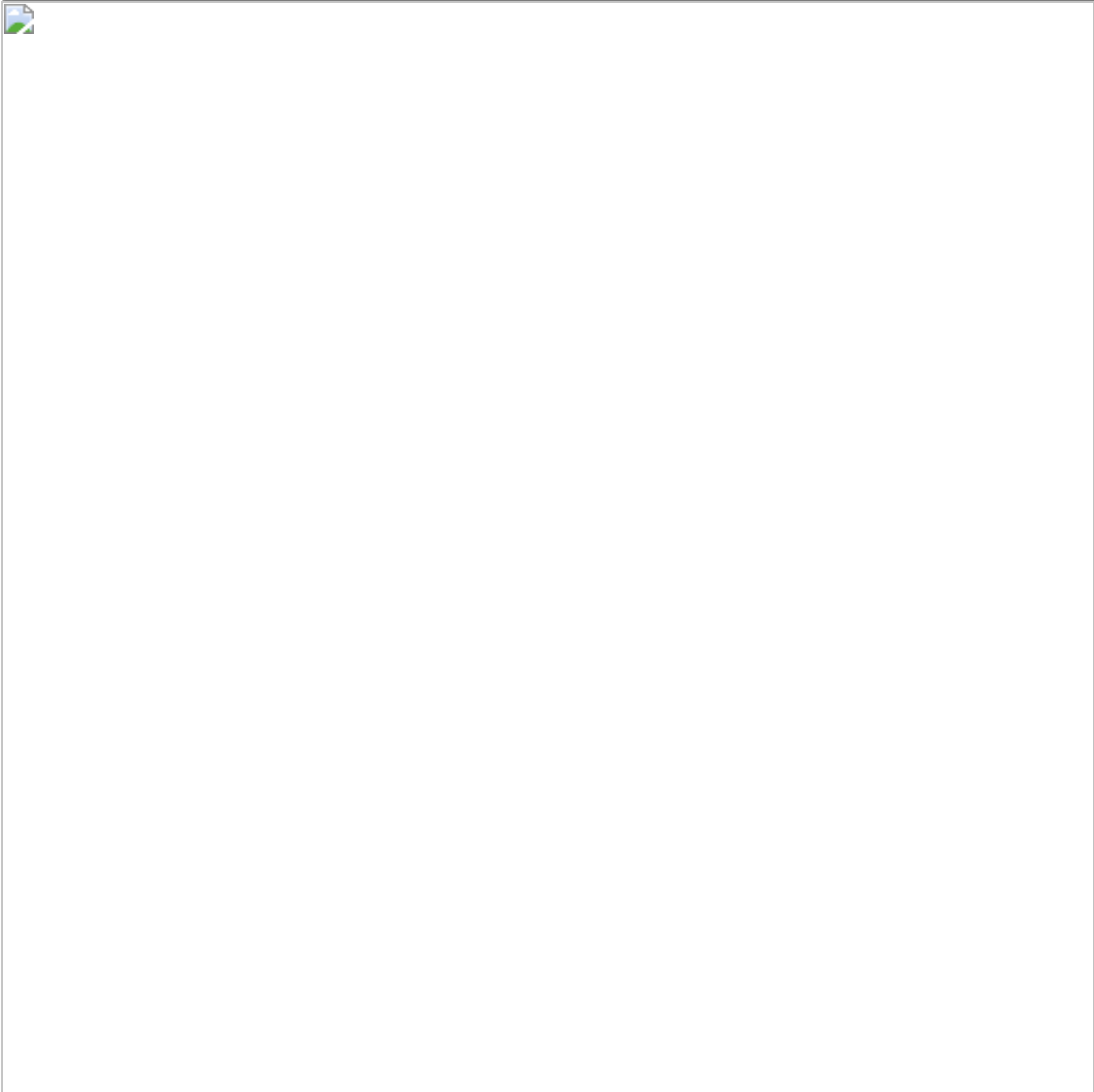


Figure 2.

Previous CLOP Ransomware – Symmetric key added to back of the encrypted file

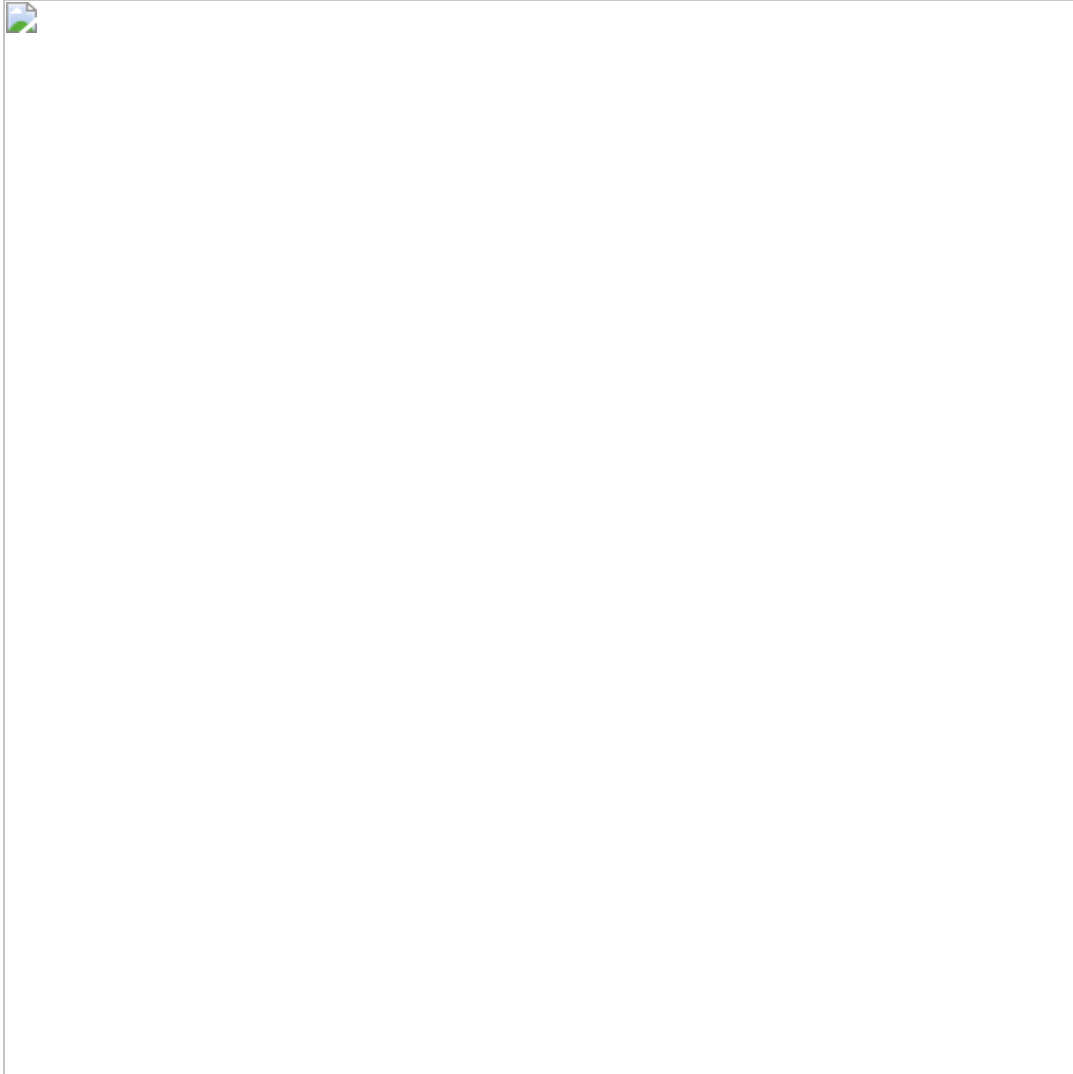
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	43	6C	6C	70	5E	5F	2D	5B	06	F0	AD	BC	59	23	E1	C5	Clip^- [.8.4Y#6A
00000010	2A	01	55	E9	67	4F	58	0C	56	AA	A8	3E	3A	24	1B	B7	*.UégOX.V^">:\$. .
00000020	84	A3	91	D0	83	24	7F	DF	C5	0E	67	D8	6A	16	34	C8	„É 'Df\$.8A.g0j.4È
00000030	38	2B	62	68	6B	42	98	60	8C	57	CF	3A	CE	85	AC	1E	8+bhkB`EWI:î...~.
00000040	2C	F0	C2	EB	E4	C5	B8	5A	34	EB	61	DA	14	F6	03	05	,8Aè8A,Z4èaÚ.8..
00000050	4E	7E	4A	05	EB	7F	00	FC	16	28	14	10	92	2F	1F	30	N~J.è...ù.(..'/0
00000060	EA	E3	C5	0A	7F	49	6C	13	B8	22	55	EF	AA	4E	60	7C	è8A..Il."UI^N`
00000070	BE	4D	82	50	DC	10	EB	1C	8A	03	07	4D	87	64	67	B7	¼M,PÜ.è.Š..M+dg-
00000080	A0	74	9E	11	F3	96	18										tž.ó-

Figure 3. Recently-found CLOP Ransomware – Saves symmetric key to .Clip file

Moreover, routine that terminates other processes and routine that deletes volume shadow copy got removed. However, the file with the identical certificate that is in charge of the process termination routine was discovered along, which can be assumed that the method of CLOP Ransomware changed. It has changed to make the additional file become capable of such a feature instead of CLOP Ransomware binary.

```
ShellExecuteA(0, 0, "cmd", "/C net stop McAfeeEngineService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbsnmp.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Symantec System Recovery\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop NetMsmqActivator /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM steam.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MExchangeMGMT /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SepMasterService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM PNTMon.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop tmlisten /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecDeviceMediaService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop ShMonitor /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbeng50.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamRESTSvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecVSSProvider /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamDeploySvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM powerpnt.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SQLAgent$PROD /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos Message Router\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop McShield /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecJobEngine /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop swi_filter /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos AutoUpdate Service\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos MCS Agent\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer100 /y", 0, 0);
```

Figure 4. Discovery of file with process termination feature



Packing method is also one of the changes. CLOP Ransomware has the appearance of a packer just like other malware such as FlawedAmmyy. This means that it keeps encoded binary to bypass file detection, and upon execution, runs the original binary decoded in memory.

Change of Ransom Note

In 2019, there were no big changes made to the content of the ransom note file of CLOP Ransomware. It mostly consists of notice that the files are encrypted, note of caution, and email address of the attacker. However, CLOP Ransomware discovered since October 2020 not only includes contact to recover encrypted files, but also a message of threat against the victim that they will publish sensitive data of the company on a deep-web. Leaked information of the company was published on a deep website mentioned in the ransom note below.

HELLO DEAR SOFTWARE AG
YOUR NETWORK IS ENCRYPTED!
ALL YOUR FILES ARE ENCRYPTED!
Also a lot of sensitive data has been downloaded from your network.
For example:

\\10.137.1.81\Finance\Private
\\10.137.1.81\Finance\Share
\\10.66.20.19\Finance
\\10.66.20.19\Contracts
\\10.21.32.57\MandAProjects

This is a small part, about 10%.

If you refuse to cooperate, all data will be published for free download on our portal:

<http://ekbgzchl6x2ias37.onion/> (use TOR browser)

mirror <http://ekbgzchl6x2ias37.onion.dog/>

To get access to your files back, contact us by email:

unlock@goldenbay.su

or

unlock@graylegion.su

AND

dromotellinghoettd@tutanota.com

or write to the chat at:

[http://geqwmtpbcicqhs7nsw5crgwtqw7mncatrz65bkrpcfpwvtv424uszsbid.onion/?](http://geqwmtpbcicqhs7nsw5crgwtqw7mncatrz65bkrpcfpwvtv424uszsbid.onion/?u=FR1GMMX2WCE4XI3Z3H38Q7CG628J7OOS5VEX71594937HCWQJ5OFI7LFFZ4SDIAO)

[u=FR1GMMX2WCE4XI3Z3H38Q7CG628J7OOS5VEX71594937HCWQJ5OFI7LFFZ4SDIAO](http://geqwmtpbcicqhs7nsw5crgwtqw7mncatrz65bkrpcfpwvtv424uszsbid.onion/?u=FR1GMMX2WCE4XI3Z3H38Q7CG628J7OOS5VEX71594937HCWQJ5OFI7LFFZ4SDIAO)
(use TOR browser)

!!! DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM !!!CI0p-_^

Figure 5. Ransom note containing information leakage threat

Analysis of Attack on Distribution Giant E-Land

This paper will now take a brief look on the attack against E-Land based on the analysis of CLOP Ransomware attack.

Like the previous CLOP Ransomware, a system infected by CLOP Ransomware used in the attack against company A cannot be restored. This ransomware uses a symmetric key algorithm to encrypt each file, and an encrypted symmetric key with a public key that exists within the binary. This means that if a private key corresponding to the public key is unknown, the encrypted files cannot be restored.

However, the previous CLOP Ransomware and the new CLOP Ransomware have different methods of saving the encrypted key. As explained in the 'CLOP Ransomware's Change Trend' section, the early version used a method of attaching encrypted keys along with specific signatures in the back of the encrypted file. However, the recently discovered CLOP Ransomware creates an additional file with an added '.Clip' extension that has the same filename (normal filename kept) as the encrypted file, and saves the relevant key to that '.Clip' file. The CLOP Ransomware used for the attack on E-Land is the latter.

Files cannot be restored as the attacker's secret key is unknown, but unlike the previous version, the ransomware does not have the command to delete volume shadow copy (a basic feature of Windows which is a saved copy of a file, folder, or a volume of a specific time). Hence, if a recovery point before ransomware affection exists, it is possible to revert the system to the uninfected state.

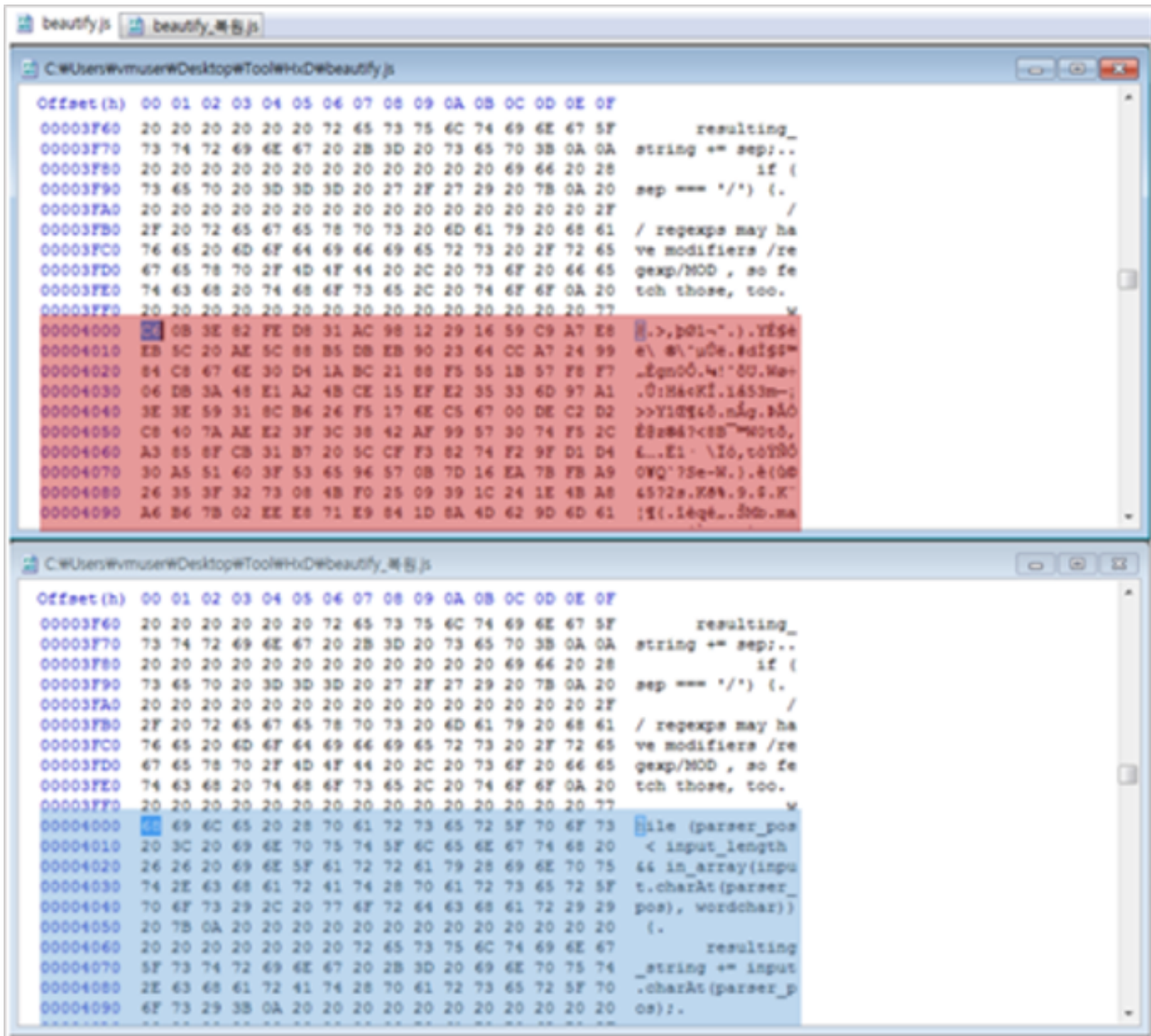
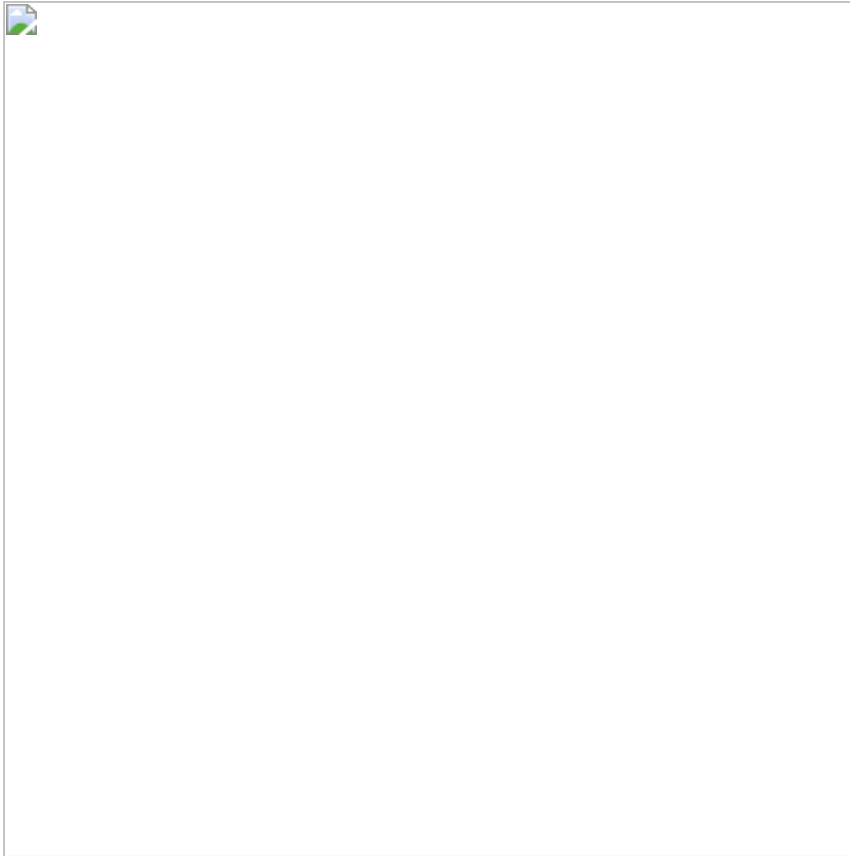


Figure 6. The infected file (upper) and the restored file (below)



Furthermore, CLOP Ransomware file used in attack against E-Land contains info of the following digital signature certificate.



Figure 7. Certificate used by CLOP Ransomware during attack against E-Land

AhnLab confirmed various files with certificates identical to CLOP Ransomware that was used to attack E-Land. According to the analysis result, other files with the certificate were distributed since October, and were created as not only ransomware, but also files to disable Windows Defender

anti-malware products. This means that the same group is developing CLOP Ransomware as well as another various ransomware using the same certificate.

In conclusion, the attacker utilized meticulous and carefully-planned strategy to attack E-Land. The attacker utilized and distributed CLOP Ransomware malware to abuse the fact that multiple systems can be controlled at once through AD. In this process, the attacker installs remote control malware and obtains system administrator privilege. The target company takes tremendous damage as their system is infected with CLOP Ransomware, their internal information is leaked, and administrator accounts are stolen. The attacker blackmails the company by threatening not only to encrypt the files, but also publish the fact that the company is infected with ransomware and stolen information to the public if they don't pay the ransom. The attacker of CLOP Ransomware is following the recent trend of threatening companies with two hostages: file encryption and internal information leakage.

CLOP Ransomware attack that occurred since 2019 is still on-going in 2020. The attacker is evolving by changing the method of malware distribution and attack. There are also reported cases of the attacker taking control of a company's AD server and letting it stay dormant, not running the ransomware immediately. Because of the time disruption factor, it is even harder to reverse track the attack when the ransomware attack occurs.

Both individuals and companies must work together to defend against CLOP Ransomware attacks. Above all, it is crucial for individuals to improve their security awareness. Adequate user education must be provided to prevent falling victim to spear-phishing, and also frequently check whether software is updated to the latest version and whether they are functioning properly. Additionally, the users must backup important documents and files in case of accidents. Companies must pay extra attention to AD security and tightly manage account info. If a security product has been installed, the system must be monitored periodically so that signs of the system abnormality can be found in a timely manner.

Categories:[Malware Information](#)

Tagged as:[clon ransomware](#)