[Threat Analysis] CLOP Ransomware that Attacked Korean Distribution Giant - ASEC

By ATCP

Published: 2021-01-04 · Archived: 2026-04-05 14:24:16 UTC

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.

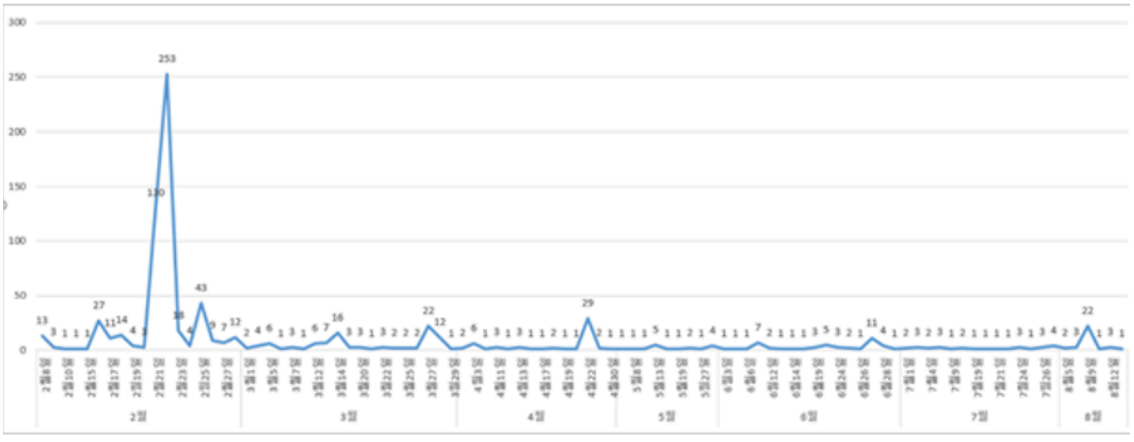

Figure 1. Change in numbers of CLOP Ransomware variants in 2019

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 ‘.Cllp’ extension to the same name, saving signature and encrypted key to a newly-created file.

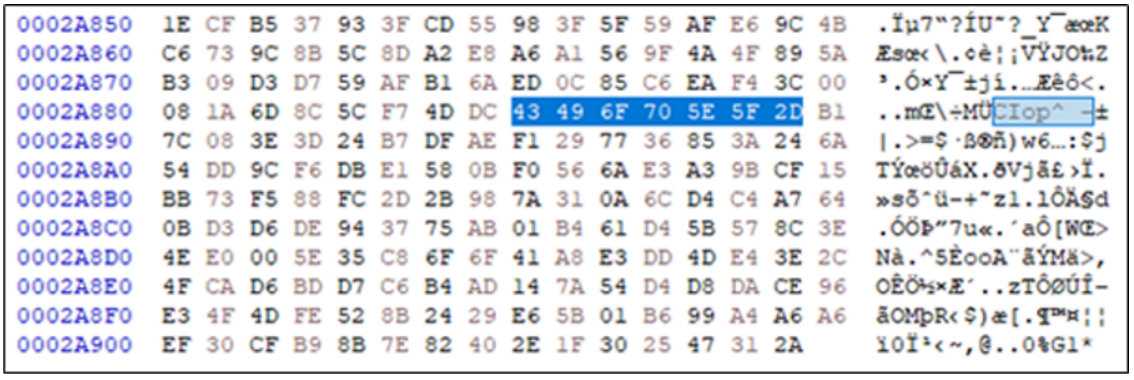

Figure 2. Previous CLOP Ransomware – Symmetric key added to back of the encrypted file

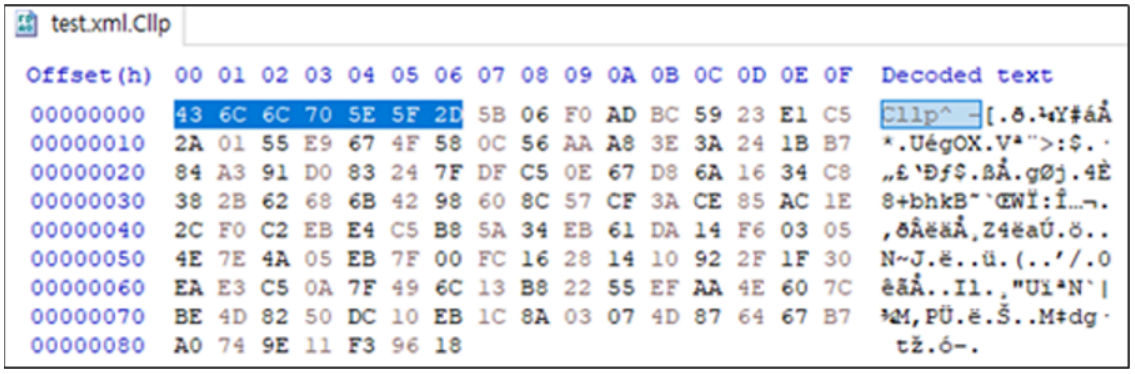

Figure 3. Recently-found CLOP Ransomware – Saves symmetric key to .Clip file

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 MSExchangeMGMT /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.

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.

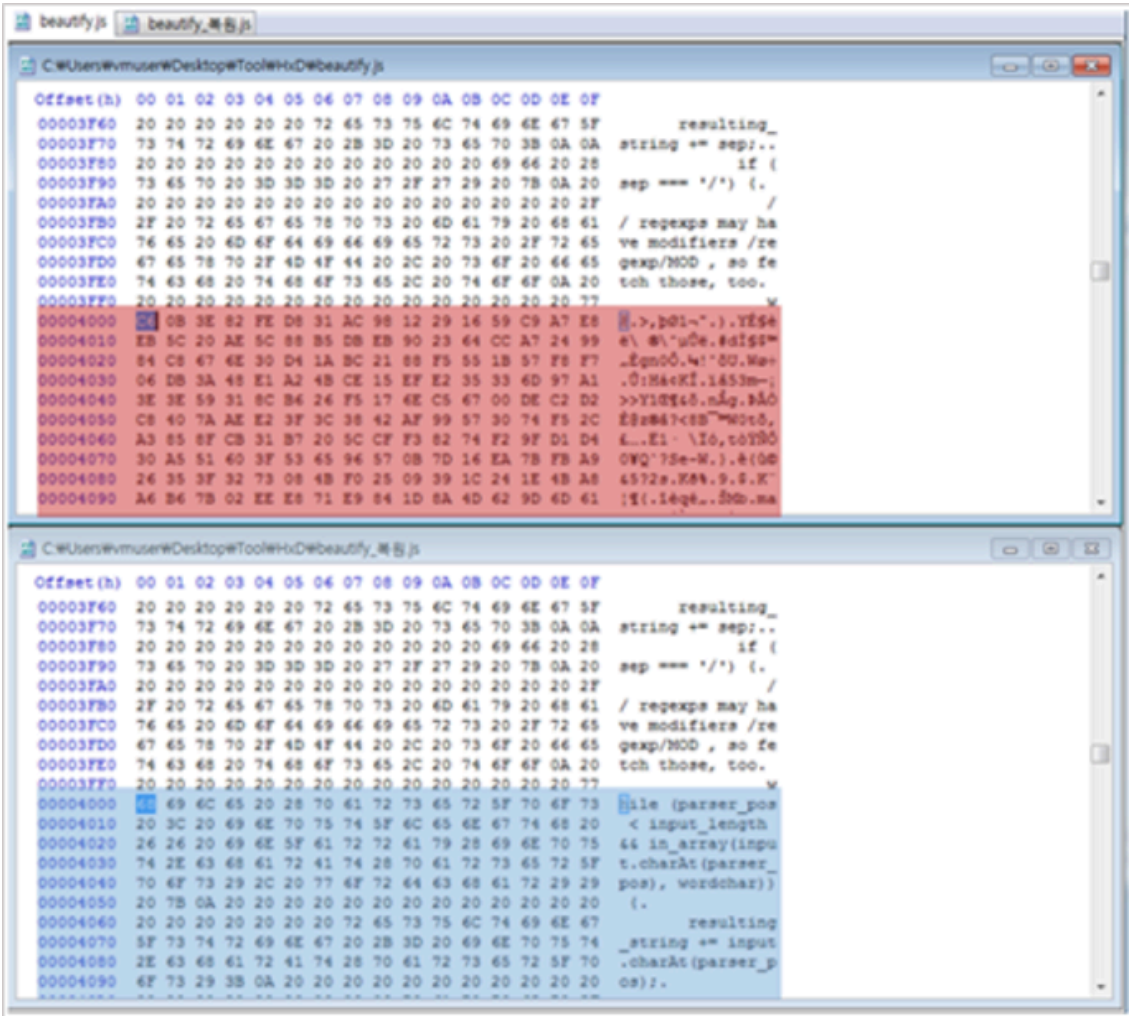

Figure 6. The infected file (upper) and the restored file (below)

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

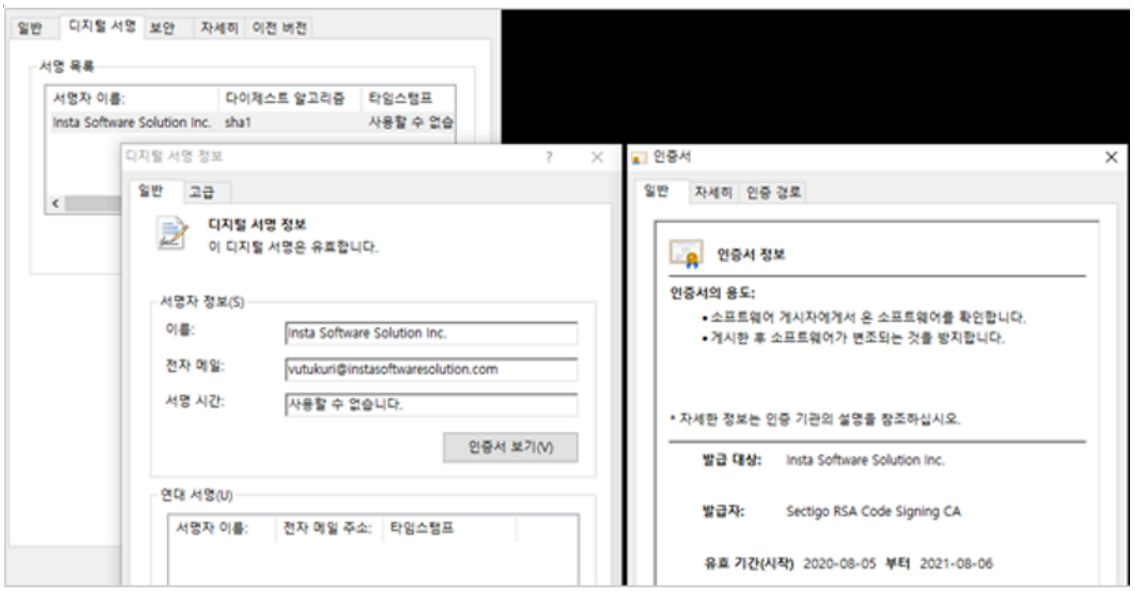

Figure 7. Certificate used by CLOP Ransomware during attack against E-Land

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.

MD5

0c155dbf2691b5dd6df2195b57bf39d5

25e11a9ebde8d2cc26084e3c739273a7

329c1d463532c33cc5627755dededcd49

34f8228a3f12fa9542f1a4181f96edec

47fe8452d486cd3822cb48f170744756

Additional IOCs are available on AhnLab TIP.

URL

http[:]//89[.]144[.]25[.]172/Ny2c

http[:]//89[.]144[.]25[.]172/a

Additional IOCs are available on AhnLab TIP.

IP

105[.]201[.]1[.]186

105[.]201[.]1[.]249

185[.]17[.]121[.]188

194[.]165[.]16[.]228

194[.]68[.]27[.]18

Additional IOCs are available on AhnLab TIP.
