KARA
Korea Anti Ransomware Alliance

2023.07.

KARA ransomware trend report

KARA ransomware trend report

■ Ransomware trends

✓ Analysis of ransomware trends

Ransomware groups are developing and testing new ransomwares to continuously carry out attacks, and are actively carrying out attacks by making tools to steal data. Among them, the Play Group developed Grixba, which scans the network and steals data, and the VSS Copying Tool, which can steal files from VSS[1], and used it for attacks. The LockBit Group, which is constantly posing threats, developed ransomware targeting the Mac OS in April, and posted a post recruiting a QA (Quality Assurance) tester through the dark web soon thereafter. Also, at the end of June, it claimed to have stolen sensitive data from TSMC, a world-class semiconductor company, but TSMC said that server settings and configuration data was leaked and that sensitive data was not leaked. The negotiated amount proposed by the LockBit Group in this case is $70 million (KRW92 billion), the highest negotiated amount of the LockBit Group that has been confirmed so far. If the claims of the LockBit group are true, significant damage is expected. Groups actively operating through collaboration with IABs were also confirmed. In particular, the Bl00dy Group, which openly recruited IABs in the first quarter, caused a lot of damage targeting the US education sector in the second quarter, followed by the BlackCat and LockBit Groups that are also carrying out continuous attacks through collaboration with IABs. Meanwhile, the activities of the Clop and Malas Groups, which find vulnerabilities in the software widely used by companies to attack multiple companies in a short period of time and exploit them to carry out large-scale attacks, continue. In particular, the Clop Group carried out a large-scale attack in December 2020, followed by two large-scale attacks in the first half of this year, causing damage to a number of companies.

[1] VSS: It is short for Volume Shadow Copy. It is a snapshot or restoration point that contains data at a specific point in time.

Activities of new ransomwares and groups

In the second quarter, a total of 15 ransomware groups, including Akira, DarkAngels (DungHill), CryptNet, CrossLock, BlackSuit, Rancoz, Ra group, MalasLocker, WiperLeak, 8base, Shadow, Rhysida, Darkrace, Lapiovra, and Noescape, operated dark webs, and began to use the double extortion strategy. Some of these groups appear to have used the source codes or builders of leaked ransomwares. It was confirmed that the CryptNet Group used the source codes and builder of the Chaos ransomware, the Shadow Group used the source codes and builder of the LockBit3.0 ransomware, the Lapiovra group used the source codes and builder of the REvil/Sodinokibi ransomware, and the Ra group used the source codes and builder of the Babuk ransomware. In addition, the BlackSuit ransomware is similar to the Royal ransomware in the codes and operation method. So it seems to be a sub-concept activity newly used by the group rather than re-branding. There are some similarities between the Rancoz ransomware and the Vicesociety ransomware, e.g., leak sites and ransom notes, but it is difficult to associate groups because there is a lack of elements that indicate a direct relationship.

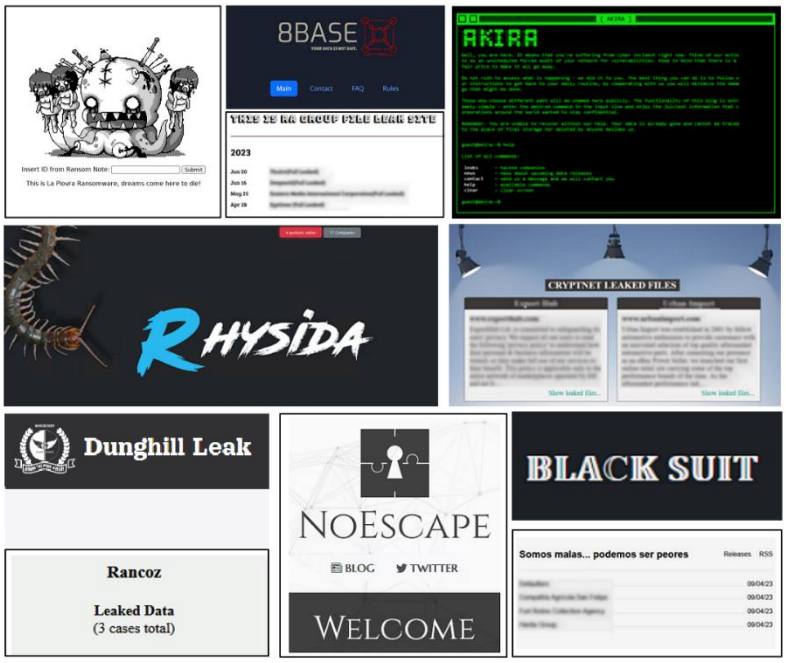


Figure 1. New ransomware dark web activities

It was also confirmed that previously active ransomware groups are operating new dark webs. The DarkAngels Group, which started its activities in May 2022, began to operate a dark web leak site DungHill around April, and the 8Base Group started operating a dark web in May of this year and posted 66 pieces of data at the same time, including the data posted since April 2022. It seems that it had been continuously active, and started a double extortion strategy in May. Meanwhile, since the dark web of the 8Base Group is similar to that of the RansomHouse Group, some speculate that it originated from RansomHouse, but the ransomware used in some attacks is one of the variants of the Phobos ransomware, and it seems that it is using the ransomwares received from various groups.

The Malas Group, discovered in May, targeted companies using the vulnerable Zimbra Collaboration Suite software, infiltrated the networks of 171 companies in a short period of time and began blackmailing multiple victims by carrying out large-scale attacks, e.g., posting on the dark web. Also, unlike general extortion methods, it is characterized by the fact that it requests donations to non-profit charities. In particular, its ransom note contains contents requesting donations to charities on grounds of hating corporations and economic inequality, not for the benefit of attack groups. It is a threat that looks like a righteous outlaw, which is quite different from simple destruction and demand for cryptocurrency, but it is not certain that the victimized site will be restored to normalcy after donations are made.

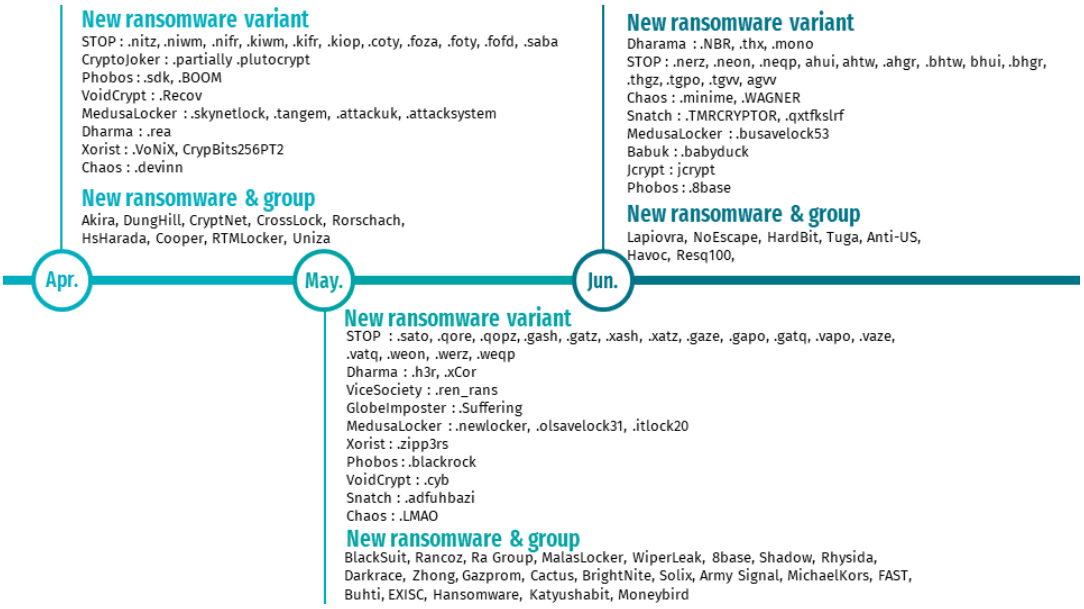


Figure 2. Activities of new/variant ransomwares

In mid-April, the LockBit Group continued its activities by developing and testing ransomware targeting the Mac OS. Meanwhile, the Rorschach ransomware was discovered at the same time, and this ransomware is also called BabLock (Babuk+LockBit) because its codes are similar to those of Babuk and LockBit2.0. In addition, it uses the fastest encryption algorithm among the ransomwares discovered so far, and is characterized by the fact that it looks like various ransomwares, e.g., the ransom notes of Yanluowang and DarkSide are generated for each variant found. Contrary to the LockBit Group, which continues public activities such as dark web operation, bug bounty, and various promotional activities, the Rorschach ransomware acts secretly, e.g., directly contacting victims and not engaging in external activities, and performing attacks targeting companies. As a result, its existence was revealed quite belatedly.

Ransomware attack group trends

In the aftermath of the ESXiArgs ransomware that targeted vulnerable ESXi servers last February, more than 3,800 servers were infected worldwide, and in the same month, 130 companies had infringement incidents due to a large-scale attack performed by the Clop Group, which exploited the vulnerability (CVE-2023-0669)[2] of the file transfer software GoAnyWhere MFT (Managed File Transfer Software). Subsequently, in the second quarter, the Malas Group, which appeared in May, posted a list of 171 companies that it infiltrated by exploiting a vulnerability (CVE-2022-24682)[3] in the e-mail and collaboration software Zimbra Collaboration Suite, and the Clop Group exploited the vulnerability (CVE-2023-34362)[4] of the file transfer software MOVEIt MFT to perform a large-scale attack once again. In particular, due to the large-scale MOVEit attack by the Clop Group, hundreds of companies suffered damage, and data posting, which was thought to stop in June, continued until July, and victims are continuously discovered. Like this, large-scale ransomware attacks continue to occur throughout the first and second quarters, and attackers and groups are exploiting the vulnerabilities of software and solutions that are frequently used by companies to carry out a wide range of attacks, resulting in a lot of damage.

Meanwhile, in Korea, there have been incidents in which data was leaked by groups such as BlackCat, BianLian, and Ra groups, and cases where some small and medium-sized businesses were infected with the Phobos ransomware were also confirmed. In particular, the attackers using the Phobos ransomware exhibit malicious behavior that is quite different from the ransomware groups that build trust by acting openly, e.g., demanding the same amount again after receiving payment from the victims.

[2] CVE-2023-0669: A remote code execution vulnerability occurring in the GoAnyWhere MTF admin panel

[3] CVE-2022-24682: A vulnerability leading to the occurrence of Cross-Site-Scripting(XSS) as validation is not done

[4] CVE-2023-34362: A vulnerability that can execute the commands of the operating system through SQL injection

Large-scale attacks

On May 27, it was confirmed that the Zero Day vulnerability (CVE-2023-34362) found in Progress's file transfer software MOVEit is actively used for attacks. The vulnerability used in the attack is the SQL injection vulnerability that can execute commands of the operating system, and it is known that the attacker exploited it to steal data from a number of companies. Soon afterwards, the Clop Group said that it was behind the attack through the dark web. It announced that it would disclose the data of companies that did not respond to the negotiations from June 14, and that it had stolen data from about 300 companies. The Clop group attacked 100 companies by exploiting the vulnerability of the Accellion FTA (File Transfer Appliance) software in December 2020, and then stole data from 130 companies through the vulnerability of the GoAnyWhere MFT software in February 2023, and from the end of May, it exploited the vulnerability of the MOVEit software to steal data from multiple companies. It continues to carry out large-scale attacks.

1. Ransomware group activities and statistics

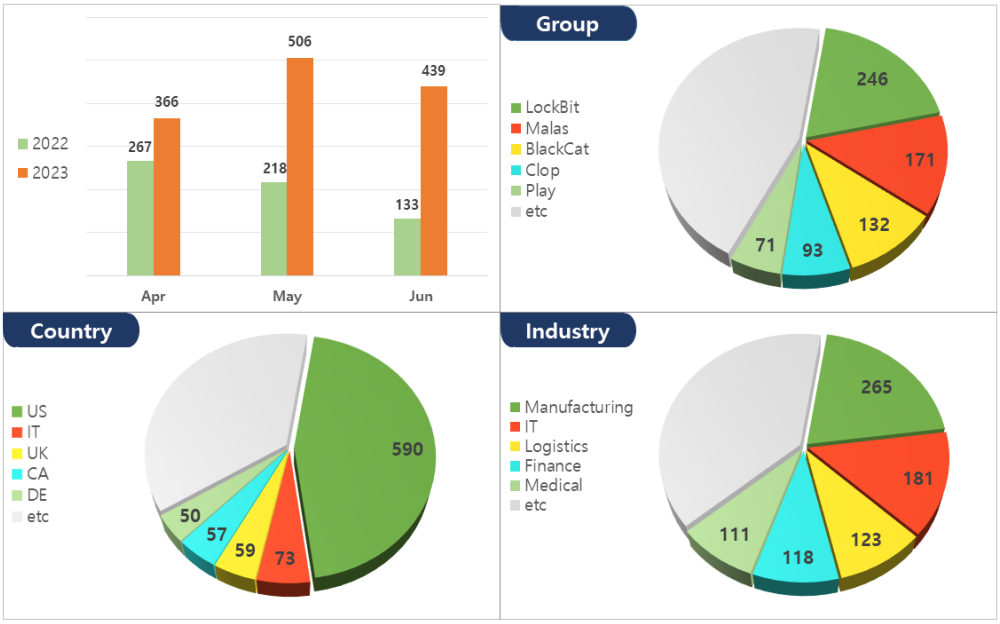


Figure 3. Ransomware group activities

It can be seen that ransomware damage has increased on average compared to last year. In particular, many attacks by new ransomware groups were discovered in May and June, and many incidents were confirmed due to large-scale attacks by the Malas Group and the Clop Group. The Malas Group started its activities from May and at the same time exploited the vulnerability of the Zimbra Collaboration Suite software to leak data stolen from 171 companies. The Clop Group, which did not show much activity in May, started posting data from companies stolen through the MOVEit vulnerability from June 14, and during the month of June, the data stolen from 89 companies was posted on the dark web. As the Clop Group announced that it had carried out attacks on about 300 companies, additional data disclosure is expected to continue. In addition, the 8Base Group, which has been operating the dark web since May, is quite active, e.g., leaking data from 47 companies during the month of June. Meanwhile, the LockBit Group showed a decrease in activity compared to the first quarter. Various inferences can be made, e.g., the intention to avoid pressure from investigative agencies, such as the arrest of some of LockBit affiliates for involvement in the distribution of ransomware, or the delay in disclosing data in awareness of the Clop group, which drew attention for a large-scale attack. Next, the BlackCat and Play Groups continue to inflict damage on companies, and the affected countries are the US, Italy and UK in that order, and the industrial groups suffer damage in the order of manufacturing, IT, and distribution industry.

2. History of Clop

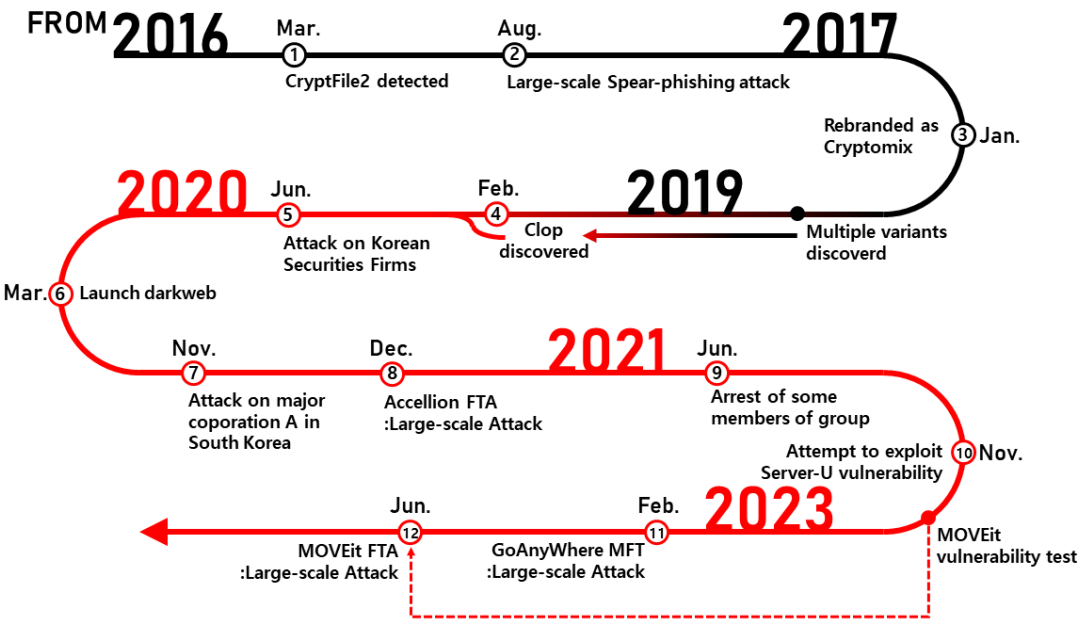


Figure 4. Clop chronology

The Clop ransomware was derived from a variant of CryptoMix and, looking at its initial starting point, it was born in 2016 through continuous rebranding from the CryptFile2 ransomware. Here, Clop (klop) is a Russian word meaning an insect that sucks the blood of humans and animals, and is known to be operated by the TA-505 hacking organization supported by the Russian government.

Unlike the existing CryptoMix ransomware, the Clop ransomware began to evolve with the addition of several functions, such as bypassing anti-virus, terminating a certain process, and including a valid digital signature, and began to be used for attacks targeting companies. Also, in March 2020, it started to use a double extortion strategy while operating the dark web, and in November of the same year, it attacked a large corporation in Korea, Company A, and leaked the stolen data through the dark web.

In November 2020, the Clop Group stayed active, e.g., exploiting the Zero Day vulnerability of the file transfer program Accellion FTA to access more than 100 companies and carry out large-scale attacks. However, as some members of the Clop Group were arrested in June 2021 with the cooperation of the police in Korea, Ukraine, and the United States, some thought that Clop activities would be disrupted, but even after the incident, the Clop Group continuously posted victims' data through the dark web, and in January 2023, it caused damage to 130 companies by exploiting the vulnerability of the GoAnyWhere MFT software, and since the end of May, it has been carrying out large-scale attacks through the MOVEit MFT vulnerability. It continues to be quite threatening.

- **Clop re-branding**

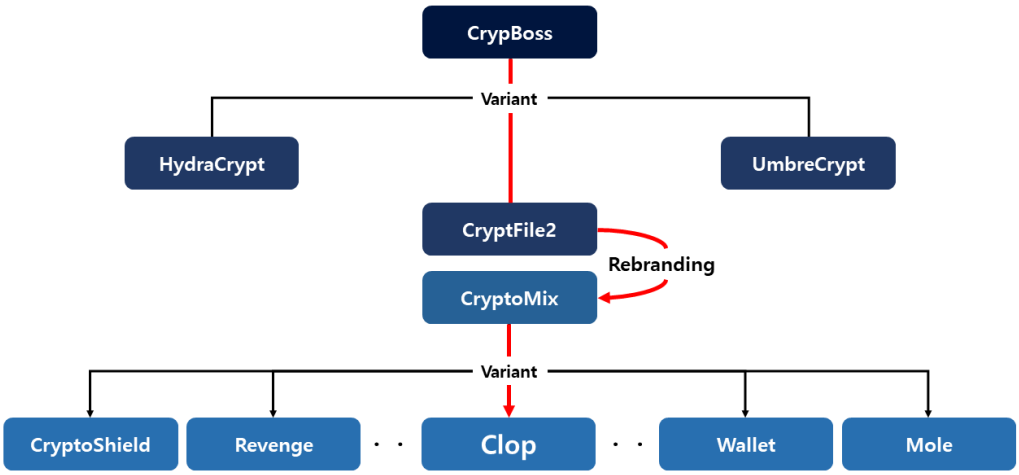


Figure 5. Clop genealogy

CryptFile2 ransomware

The CryptFile2 ransomware began to spread through Exploit Kits[5] such as Nuclear and Neutrino in March 2016, and was also used in a large-scale email attack targeting government agencies and educational institutions in the US in August 2016. CryptFile2 ransomware is presumed to be a variant of CrypBoss because its codes are similar to those of the HydraCrypt ransomware, a variant of CrypBoss, and the e-mail address used during negotiation was also used for the HydraCrypt and UmbreCrypt ransomware, which are variants of CrypBoss, and the negotiated amount is known to be 0.5 to 1.5 bitcoins (150 USD to 470 USD at the time).

CryptoMix ransomware

In January 2017, the CryptFile2 ransomware was re-branded as the CryptoMix ransomware. Here, CryptoMix is assumed to be derived from the CryptoWall and CryptXXX ransomware, because the 2 ransom notes generated when running the CryptoMix ransomware were the same as those of CryptoWall and CryptXXX, respectively. The negotiated amount was 5 bitcoins (3,100 USD at the time), and a variant named Clop was discovered in February 2019 while multiple variants such as CryptoShield, Revenge, Wallet, and Mole were discovered by April 2019.

[5] Exploit Kit: A tool that distributes malware by using the vulnerabilities of various software

- **The Clop Group opens the curtain**

In February 2019, the Clop ransomware, which was discovered as a variant of the CryptoMix ransomware, began to evolve by adding various functions such as bypassing anti-virus, terminating a certain process, and including a valid digital signature. The Clop ransomware began to be used in phishing campaigns targeting the entire world as well as domestically. It is known to be the ransomware group operated by TA-505, a hacking organization backed by Russia, in that the phishing attacks clearly specified targets and spear phishing attacks were performed with elaborately written mail in the recipient's language, and no encryption was performed when Russian is used on the PC, and RAT[6] malware SDBBot and FlawedGrace created by TA-505 organization are executed when attached files are executed.

1) Evolution of the Clop ransomware

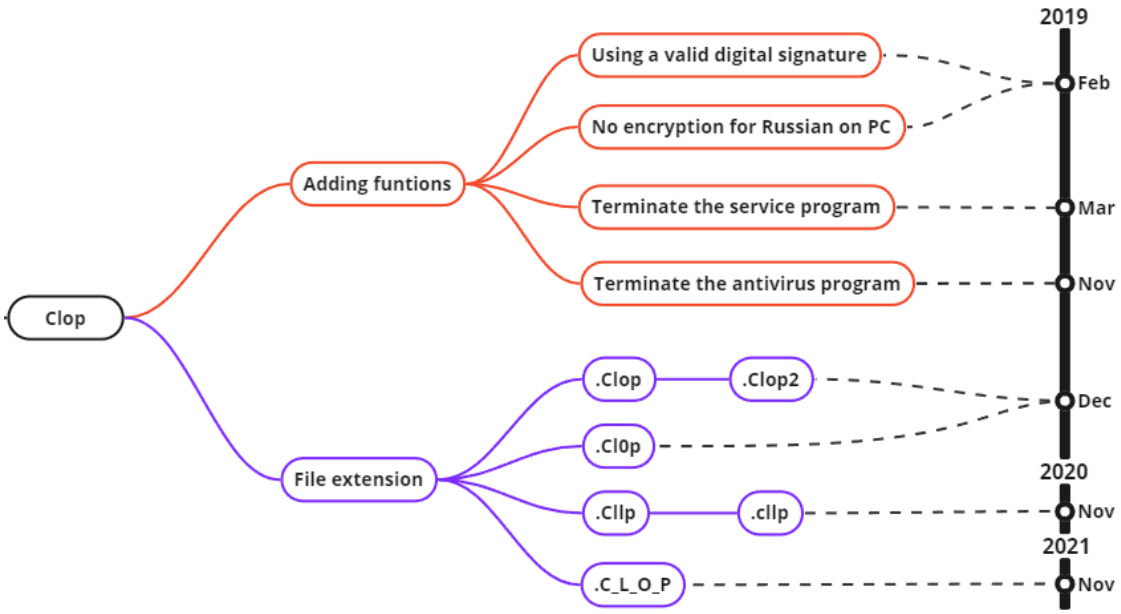


Figure 6. Evolution of the Clop ransomware

[6] RAT: It is short for Remote Access Trojan. It is a type of malware that remotely controls computers

Unlike the existing CryptoMix ransomware, the Clop ransomware began to develop by adding various functions. In particular, the routine to terminate certain service programs such as Microsoft SQL Service, MySQL, and BackupExec and anti-virus products such as Kaspersky and Window Defender was added as well as the function to check the language used in the PC and terminate without encrypting the data when Russian is used.

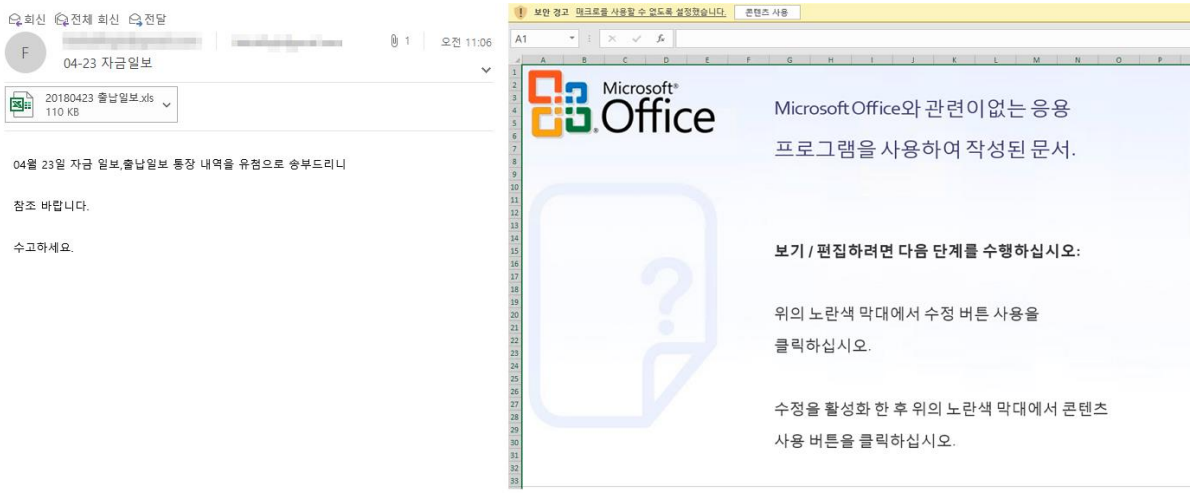


Figure 7. Spear phishing mail and malicious file

The Clop ransomware developed in this way began to be used for attacks through spear phishing in February 2019. After clearly designating attack targets, attackers carried out attacks by elaborately writing the text contents in the recipient's language. Also, during the attack process, if the system is in the Active Directory[7] (AD) environment, the DownLoader malware, which downloads additional malware, was found. AD is an environment mainly used by companies, and it can be seen that attackers prepared attacks targeting companies. A number of spear phishing attacks have been confirmed in Korea as well, and e-mails of attackers disguised as Hometax of the National Tax Service and e-tickets have also been found.

[7] Active Directory: A service that centrally manages resources such as users and computers in a corporate network environment

2) Staring activities on a full scale

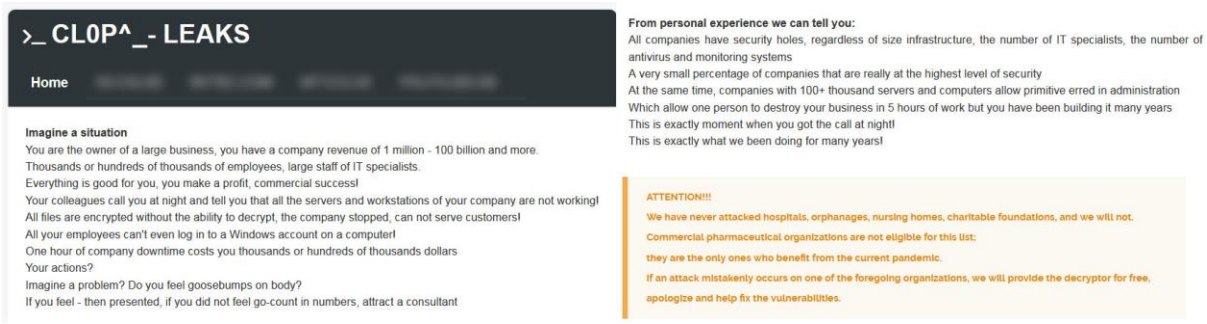


Figure 8. Clop's dark web activities

The Clop Group, which has been continuously attacking companies, started operating the dark web under the name "CL0P^_- LEAKS" in March 2020. Immediately after opening the dark web, it posted a message stating that security consulting would be provided upon payment of a certain amount, and that in case of an attack on a specific industry group such as hospitals, orphanages, nursing homes, pharmaceutical companies, etc., it would provide a decryption tool and supplement the vulnerability of the infrastructure. It set up its own rules and started using a double extortion strategy.

Meanwhile, in December of the same year, data-stealing attacks exploiting the vulnerability of the Accellion FTA software began to occur. Accellion FTA is a large-capacity file transfer program mainly used by companies, and it was confirmed that more than 100 corporate systems using this software were compromised. Later, in January 2022, as the Clop Group began double extortion via e-mail addressed to company officials, the culprit behind the incident was revealed, and the Clop Group began posting the stolen data in February.

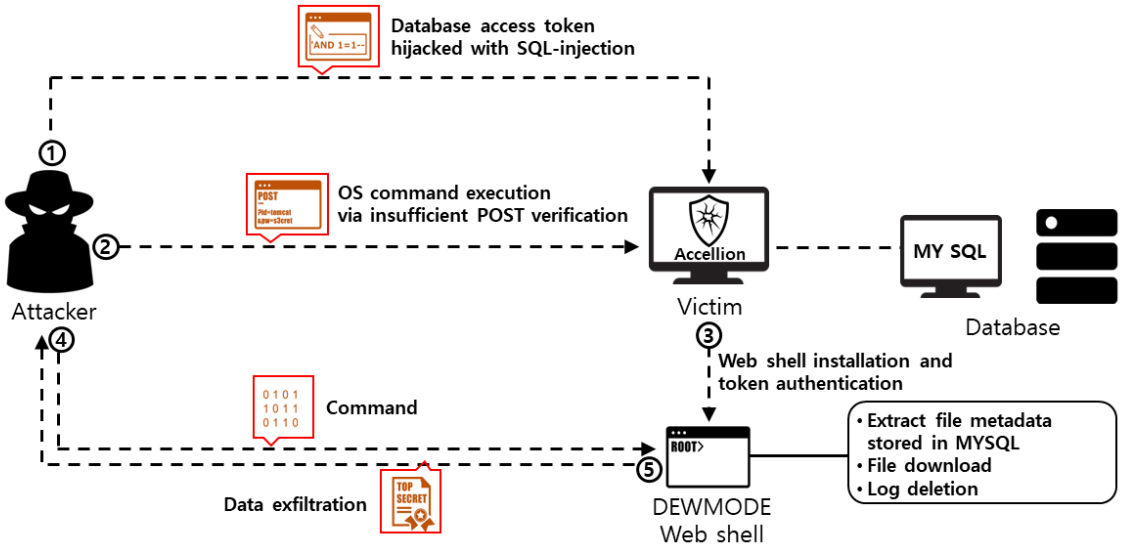


Figure 9. Accellion FTA vulnerability exploitation scenario

The Clop Group exploited the Zero Day vulnerabilities of Accellion FTA (CVE-2021-27101[8], CVE-2021-27102[9], CVE-2021-2710[10] and CVE-2021-27104[11]) that had not been discovered at the time to carry out attacks. After stealing the token that can access the database through the SQL injection vulnerability, attackers executed the OS command to download the DEWMODE Web shell using the vulnerability generated from the POST request. The DEWMODE web shell used here is a web shell developed by the Clop Group that includes functions such as searching mea-data of files in the database, downloading files, and deleting web logs. It was confirmed that they deleted web logs to steal data through this web shell and interfere with investigation of the incident.

Meanwhile, as six members involved in money laundering of the Clop Group were arrested in June 2021 with the cooperation of the Korean, Ukraine and US police, some speculated that the incident would disrupt the activities of the Clop Group, but right after that, the Clop Group posted the victim's data through the dark web and continued its activities, and in November, it looked for the vulnerability of the file transfer software Server-U and used it for an attack.

---

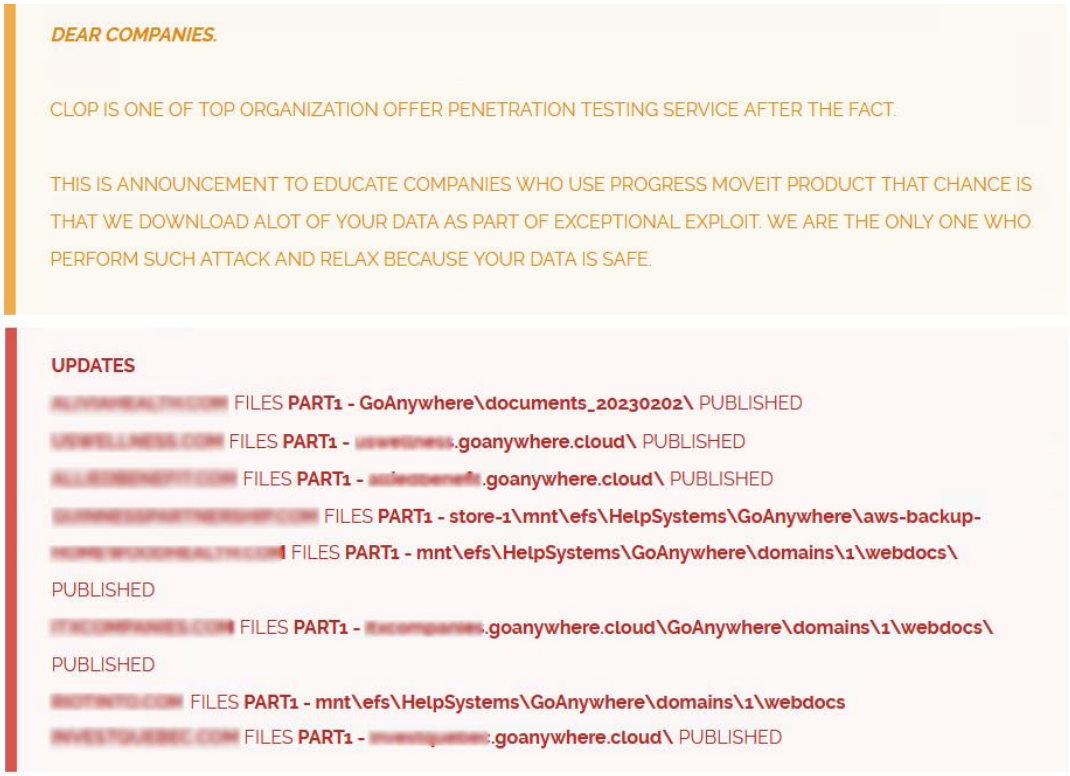
[8] CVE-2021-27101: A vulnerability that enables SQL injection as the http header is not properly validated

[9] CVE-2021-27102: A vulnerability that can execute OS commands that occur in the process of calling web service

[10] CVE-2021-27103: A vulnerability that can forge the server's request as the POST request is not properly validated

[11] CVE-2021-27104: A vulnerability that can execute OS commands as the POST request is not properly validated

3) Continuing large-scale attacks



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

UPDATES

[redacted] FILES **PART1 - GoAnywhere\documents_20230202** PUBLISHED

[redacted] FILES **PART1 - [redacted].goanywhere.cloud** PUBLISHED

[redacted] FILES **PART1 - [redacted].goanywhere.cloud** PUBLISHED

[redacted] FILES **PART1 - store-1\mnt\efs\HelpSystems\GoAnywhere\aws-backup-**

[redacted] FILES **PART1 - mnt\efs\HelpSystems\GoAnywhere\domains\1\webdocs**

PUBLISHED

[redacted] FILES **PART1 - [redacted].goanywhere.cloud\GoAnywhere\domains\1\webdocs**

PUBLISHED

[redacted] FILES **PART1 - mnt\efs\HelpSystems\GoAnywhere\domains\1\webdocs**

[redacted] FILES **PART1 - [redacted].goanywhere.cloud** PUBLISHED

Figure 10. Posting GoAnyWhere and MOVEit data.

The Clop Group exploited the Zero Day vulnerability of the Accellion FTA software to carry out large-scale attacks, followed by the attacks it performed on multiple companies by exploiting the Zero Day vulnerability of the GoAnyWhere MFT software in February 2023 and the Zero Day vulnerability of the MOVEit MFT software in May 2023. What is noteworthy here is that it infiltrated many companies by exploiting the vulnerabilities of software or solutions mainly used in companies, and that it stole only data without using ransomware.

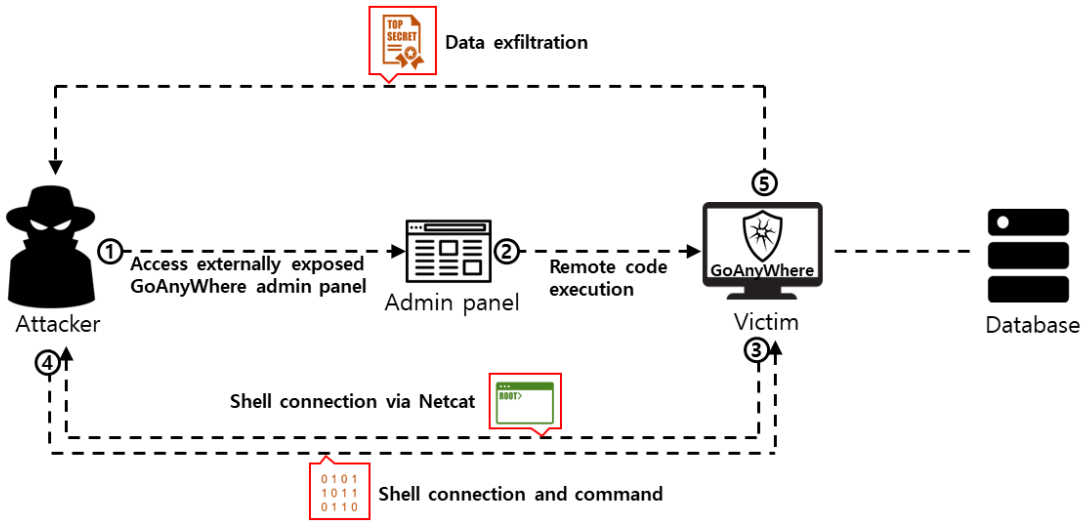


Figure 11. GoAnyWhere MFT vulnerability exploitation scenario

In February 2023, the Clop Group performed large-scale attacks once again. Attackers found and exploited the Zero Day vulnerability in the file transfer software GoAnyWhere MFT, and it is known that more than 130 locations, including institutions and companies in each country, have been damaged. They exploited the remote code execution vulnerability through the GoAnyWhere administrator panel exposed on the Internet, and executed the Netcat utility that allows data to be sent to and received from designated targets, connected the shell between the attacker and the victim, and then hijacked internal data.

In April, it was also confirmed that the Clop Group carried out attacks using the vulnerability of the print management solution PaperCut, which is often used in companies. The exploited vulnerabilities are the CVE-2023-27350[12] and CVE-2023-27351[13] vulnerabilities, which were used for attacks not only by the Clop Group but also by the LockBit and Bl00dy Groups. The Clop Group downloaded TrueBot[14] malware through remote code execution vulnerability of the PaperCut software, delivered Cobalt Strike Beacon[15] to the victim's PC through the TrueBot malware, scouted the internal network and system, and used the file sharing utility MegaSync to steal internal data.

---

[12] CVE-2023-27350: A vulnerability that can execute codes remotely through the PaperCut software

[13] CVE-2023-27351: A vulnerability that can bypass PaperCut software authentication, and extract user data

[14] TrueBot: Malware that performs the file download function made by the TA-505 organization

[15] Cobalt Strike Beacon: A tool that attackers use to remotely control the system in the software for mock access Cobalt Strike

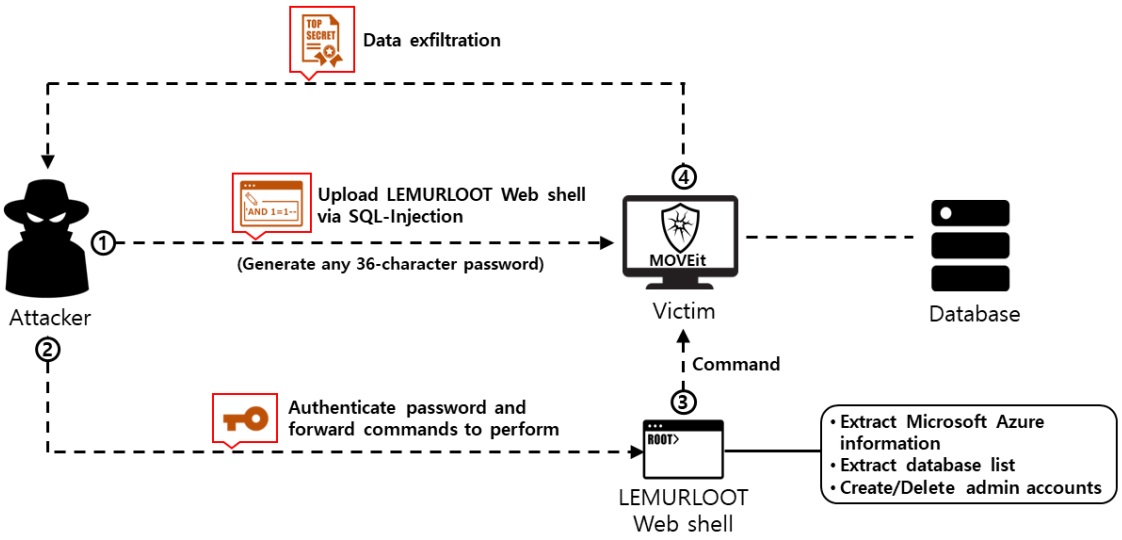


Figure 12. MOVEit MFT vulnerability exploitation scenario

At the end of May, the Clop Group carried out another large-scale attack by exploiting the vulnerability of Progress's file transfer software MOVEit. Soon after the attack, it was not known who is behind this attack, but on June 5, the Clop Group claimed that it was responsible for the large-scale attack through the MOVEit vulnerability on the dark web, and began to post the data of companies for which negotiations were not completed, and starting from June 14 until the end of June, the data stolen from 89 companies was posted. The Clop Group installed the LEMURLOOT web shell by using the SQL injection vulnerability present in the MOVEit software to carry out the attack. The web shell used here was self-produced by the Clop Group and includes a function to output MS Azure server configuration data, a file search function, and a function to create/delete administrator privilege accounts. Also, in order to access the web shell, a 36-character password must be transmitted through the HTTP header, and if the password is not entered or does not match, it displayed the 404 error page, disguising it as a non-existent page. After that, it is confirmed that the attacker stole the data in the internal database through the web shell.

Figure 13. Rewards of Justice

As the threat of the Clop Group performing large-scale attacks in a short period of time by exploiting the vulnerabilities of software frequently used by institutions and companies, such as Acellion FTA, GoAnyWhere MFT, and MOVEit MFT, increased, and the US government and some major institutions also suffered damage from the Clop Group, the Rewards of Justice (RFJ), one of the US Department of State's reward programs, started an active response by posting a message promising to pay a reward of 10 Million Dollars to those who provide information about the Clop Group. This reward program was implemented in the United States, which believed that Clop is behind these attacks, with the purpose of reducing damage to the government and major institutions, but the Clop Group denies this through the dark web, saying that they are not very interested in government data and that they are carrying out only financially motivated attacks.

Ransomware mitigations

The Clop Group has been continuously carrying out attacks targeting companies for the past 4 years. In particular, in the first half of this year, it exploited the vulnerabilities of software mainly used by companies to steal and post data from more than 260 companies so far. In this way, attackers search for vulnerabilities in various ways through the strategy established by the attacker group, infiltrate the internal infrastructure, and attempt to threaten through file encryption and data leakage. To prevent such damage, it is necessary to prepare for targeted APT attacks and prepare appropriate security elements and processes for each stage of infiltration to detect and block attacker groups before they achieve their goals.

Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST Business Group & KARA (Korea Anti Ransomware Alliance)
Producer : SK shieldus Communication Group