Keep up with Ransomware

Clop, exploits vulnerabilities to threaten large-scale attacks

■ Overview

In June 2023, there were 439 cases of ransomware damage. The number slightly declined by 69 cases compared to the previous month (508 cases). The reason why many cases of ransomware damage appeared last May is that Malas exploited the vulnerability (CVE-2022-24682[1]) on the e-mail platform Zimbra Collaboration Suite to successfully launch 171 large-scale attacks.

A noteworthy issue of this month is that Clop carried out another massive attack. It was confirmed that Clop carried out a large-scale attack again in June following last February and April. Clop exploited the vulnerability (CVE-2023-34362[2]) of Progress MOVEit Transfer to post victims' data on a dark web leak site and demand money. In July 2021, it seems that Clop had been preparing for this attack for a long time, e.g., conducting an attack test that abused CVE-2023-34362. In the future, there is a possibility that victims' data due to this incident will be continuously posted on the leak site. So we need to keep an eye on it. Due to Clop's successive large-scale attacks, the US government announced that it would offer a $10 million reward to those who provide information about Clop, and the attention of investigative agencies is focused on Clop.

In addition, the activities of LockBit have slowed down compared to last May, but it threatened to disclose sensitive data of TSMC (Taiwan Semiconductor Manufacturing Co.), a Taiwanese semiconductor manufacturing company, on the dark web, and demanded a ransom of $70 million (KRW90. 5 billion). However, it is doubtful whether LockBit's negotiation request will be accepted considering that the company has earned $91 million in revenue only from US companies so far.

[1] CVE-2022-24682: Cross Site Scripting vulnerability that allows script codes to be executed in the security context of the victim's browser

[2] CVE-2023-34362: SQL Injection vulnerability that allows web shell upload

The BlackCat (Alphv) Group has also been consistent. BlackCat said in February that it attacked Reddit, an American discussion site. Later, in April and June, it sent an e-mail to Reddit asking for money, but Reddit did not respond. So BlackCat expressed its intention to leak 80GB of compressed and confidential data to the leak site. However, the truth battle continues as Reddit revealed that the BlackCat Group acquired an employee's credentials through phishing and obtained only some internal documents, codes, and access privileges to some internal dashboards and business systems.

What Clop's MOVEit attack exploiting vulnerabilities and BlackCat's Reddit attack have in common is that they focus on data theft without using ransomware for the attack. Similar cases existed before. Last January, the BianLian Group switched from data encryption through ransomware to pure data theft after Avast, a Czech security company, unveiled a ransomware decryption tool. It can be seen that ransomware groups are also requesting ransom by posting data to leak sites through data theft excluding encryption. However, the actual use of ransomware has not decreased significantly, and it is widely used in cybercrime. It is also worth noting that the attack methods of the RaaS groups are changing. Ransomware groups look organized, e.g., cooperating with professional manpower such as IABs[3] (Initial Access Broker) and hiring professional manpower within the group.

In addition to this, a ransomware group called 8Base carried out many activities in June. The leak site of 8Base was disclosed in May, but as leaked data that is estimated to have been stolen since April 2022 was posted on the leak site, it is believed that it has been quietly active for about 1 year. 8Base posted a total of 115 pieces of leaked data, 44 in June alone. Also, the possibility that 8Base is a group originating from RansomHouse has been raised due to the similarity of the leak sites and the virtually identical ransom note and service terms. However, since the customized Phobos ransomware loaded through SmokeLoader[4] used by 8Base is ransomware as a service (RaaS), it is difficult to view the use of the said ransomware as an indicator of its affiliation. Therefore, it is still difficult to determine which group 8Base originated from.

One notable ransomware among the ransomware variants newly discovered in June is the Linux target BlackSuit based on the Royal ransomware. The BlackSuit ransomware has versatility targeting both Windows and Linux systems. It adopted the double extortion method, applied the AES method to file encryption, and protected the encryption key with RSA. In addition, it improved the speed of the encryption process through intermittent encryption.

[3] IAB: An individual or group selling initial access path

[4] SmokeLoader: Malware used to download other malware to the infected system

Also, new ransomware groups, Lapiovra and NoEscape, were discovered. The Lapiovra Group started its activity by posting leaked data from an American nanotechnology research firm. The ransomware used by the Lapiovra Group is similar to that of the REvil (Sodinokibi) Group, e.g., config data, user's keyboard language identification, and C&C URL creation routine. So it is assumed that it was created based on the latter. The NoEscape Group was discovered this month, but has been active, posting seven cases of leaked data from various industries, including finance, education, and manufacturing. The NoEscape ransomware operates as RaaS and is similar to the Avaddon ransomware in that it adds random character strings to files and has a similar ransom note. NoEscape has not only ransomware targeting Windows, but also variants targeting Linux and ESXi systems. In particular, ransomware targeting Windows is characterized by the fact that it uses the Reflective DLL Injection[5] technique.

Meanwhile, in Korea, the Mallox ransomware targeting MS-SQL firmware, which is still vulnerable, is being distributed. What is unusual is that not only EXE files but also BAT file extensions are used. The BAT file is a script file used in Windows and is mainly used when a series of tasks are automated. As it is possible to deliver the malware payload by executing the Powershell script through this, it is used to bypass detection from the attacker's point of view. Mallox ransomware uses this to perform initial access by performing a Brute Force Attack[6] or a Dictionary Attack[7] on the credentials managed by the vulnerable system.

In addition, it was confirmed that groups using the Crysis ransomware distributed the Venus ransomware by obtaining account information with the Brute Force Attack or Dictionary Attack through vulnerable RDP. They caused network diffusion by installing tools like port scanners and Mimikatz, including the Venus ransomware. Therefore, in case of damage due to the Crysis ransomware, it is necessary to check how it was spread to the internal system, and it is important to follow the correct password policy and keep the system up to date.

[5] Reflective DLL Injection: A technique that directly maps and executes DLL data after inserting it into the memory of the running process

[6] Brute Force Attack: A technique that enters all possible values to crack a password

[7] Dictionary Attack: A technique that finds a password by entering words in a dictionary

■ Ransomware news

infosec

Clop, a zero-day vulnerability in MOVEit Transfer, is being exploited for large-scale data exfiltration.

- Clop group exploits vulnerability CVE-2023-34362 in MOVEit Transfer.
- They exploit the vulnerability to deploy a web shell, ensuring persistence and performing authentication.
- More than 1400 hosts are exposed to the risk.
- They demand ransom without performing encryption.

Evidence confirms that Clop has been testing vulnerabilities in MOVEit Transfer since 2021.

- While analyzing the logs from the affected system, evidence confirms testing activities dating back to 2021.
- Further evidence confirms similar activities in July 2021 as well.
- It is estimated that hundreds of companies have been affected.

Akira ransomware, developing free decryption tools.

- Avast company develops and distributes free Akira decryption tools.
- Development of decryption tools for both 32-bit and 64-bit Windows systems.

BlackCat (Alphv) poses a threat of Reddit data breach.

- BlackCat threatens to publicly release approximately 80GB of compressed data stolen from Reddit.
- It stems from a phishing attack conducted in February.

Rhysida, leaking documents stolen from the Chilean military.

- A Chilean Army corporal is implicated in the attack.
- They allege posting 360,000 Chilean Army documents, revealing only 30% of their stolen data.
- Using tools like CobaltStrike, they spread across the network and then deploy ransomware payloads.

* CobaltStrike : Commercial penetration testing tools, cracked versions of which have been released, are being exploited.

Suspect accused in the United States for being associated with the LockBit group.

- The third prosecution of a LockBit affiliate in the United States since November of last year.
- Directly carried out at least five attacks.

US government offers $10M reward for Clop ransomware information.

- The US Department of State announces a reward for individuals providing information on the Clop group.
- Setting up servers for submitting information on attackers, including Clop.

LockBit demands $70 million (approx. ₩9.05billion) after attacking TSMC subcontractor.

- LockBit group accesses the internal systems of TSMC subcontractor Kinmax, exfiltrates data, and demands a ransom of $70 million.
- TSMC unaffected, terminates collaboration with subcontractor.

Attacking Russian game users by impersonating the WannaCry ransomware.

- Attacking Russian FPS game users by impersonating the WannaCry ransomware.
- Since the game is free, it can be downloaded, malicious payload inserted, and distributed.
- Impersonating WannaCry, it utilized the open-source "Crypter" encryption tool for malicious purposes.
- Imitating WannaCry to intimidate victims and increase the burden of ransom payment.

Ransomware attackers utilize cloud mining services for cryptocurrency laundering.

- North Korea's APT43 uses cloud mining services for cryptocurrency laundering and anti-forensic activities.
- Cloud mining is a service that allows remote cryptocurrency mining.
- It creates ambiguity in the source of funds and makes the origin of funds appear legitimate.

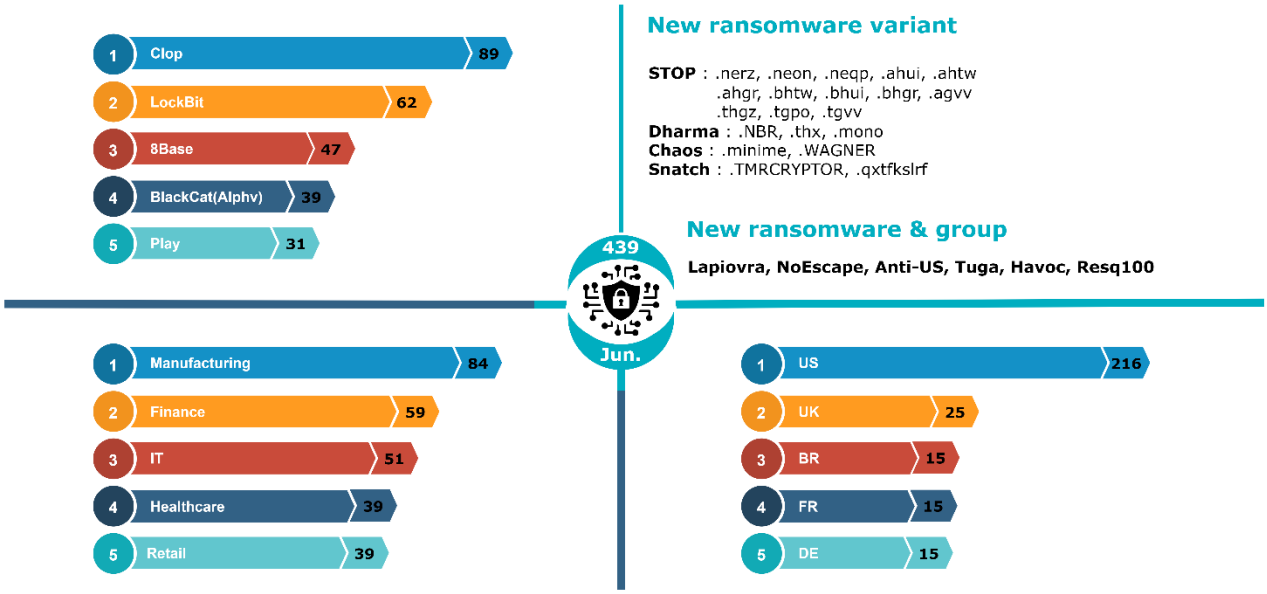
The Cyclops ransomware group sells Go-based infostealer malware on forums.

- Cyclops sells information-stealing malware designed to capture critical data from infected systems.
- Designed to target both Windows and Linux, it enables the theft of desired data.

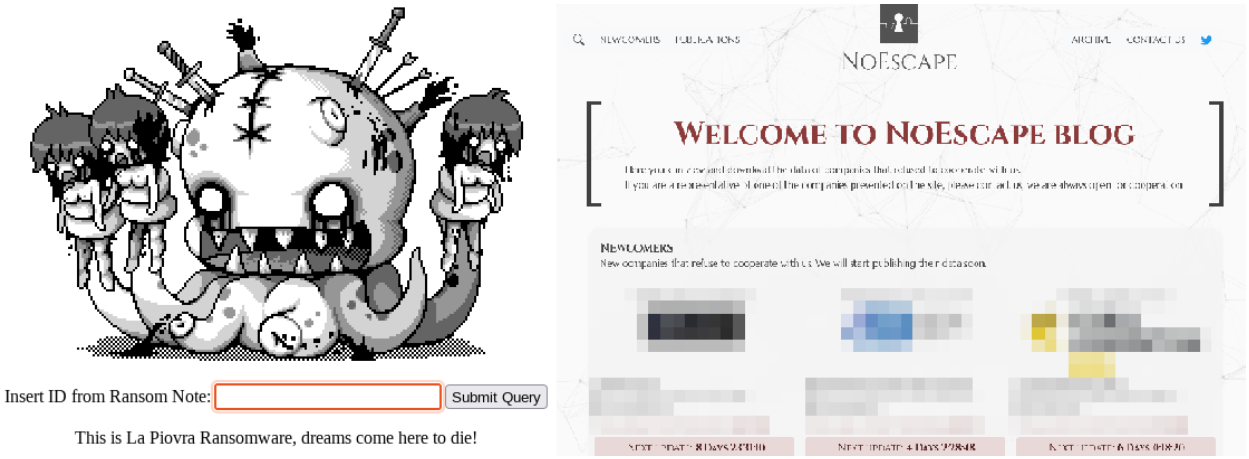
The TargetCompany ransomware group operates with the Xollam variant of the Mallox malware.

- Xollam spreads through spam emails with malicious MS OneNote files attached as attachments.
- The TargetCompany ransomware group establishes Telegram channels for double-extortion purposes.

■ Ransomware threat



New threats



* Source: Lapiovra, NoEscape ransomware Group site image

In June 2023, there were 439 cases of ransomware damage, a relatively small number compared to the 508 cases of last May, but it is still a dangerous situation as new and variant ransomware are steadily appearing. Furthermore, ransomware groups invested a lot of time and resources in the initial access process for ransomware attacks in the past, but today, as the ransomware ecosystem is organized, the difference is that this trend has begun to change.

In particular, the RaaS Group, which appeared recently, recruits affiliates or attackers to delegate privileges, and they access the victim's network by paying a certain amount to IABs to obtain an initial access path. After that, they steal and encrypt file, perform double extortion and extort money under the pretext of file decryption and data leakage. If it conducts an attack through an affiliate, it collects a certain amount from the affiliate and distributes a certain percentage to the general manager. If an attacker performs an attack, the general manager collects money and distributes a certain percentage to the attacker, and launders money through the mixing service. Due to the invigoration of the IAB market, ransomware groups can easily and quickly succeed in initial access, and through this, they can carry out massive attacks in a short period of time, thereby increasing risks.

A notable variant ransomware discovered in June is the Linux-based BlackSuit ransomware. This ransomware is operated by the Royal Ransomware Group and is known as ransomware that targets both Windows and Linux. It is also developing a way to use IcedID[8] and Emotet[9] as loaders for distribution. The BlackSuit ransomware has a very high level of similarity with the Royal Ransomware Group to the extent that it shows a similarity of about 98% or more as a result of checking it through a binary file comparison tool. BlackSuit is not yet as active as the Royal ransomware, but as it is continuously tested, it remains to be seen whether it will be re-branded as BlackSuit in the future or whether it will be used only for targets that meet certain conditions.

New ransomware groups discovered this month are Lapiovra and NoEscape. In particular, Lapiovra shows considerable similarity with REvil (Sodinokibi) codes. In particular, it was confirmed that users avoid the C&C URL creation routine and encryption using a specific language, and that the structure of the config data is also similar. Through this, it is guessed that it is ransomware produced by purchasing or receiving the codes of the REvil (Sodinokibi) ransomware.

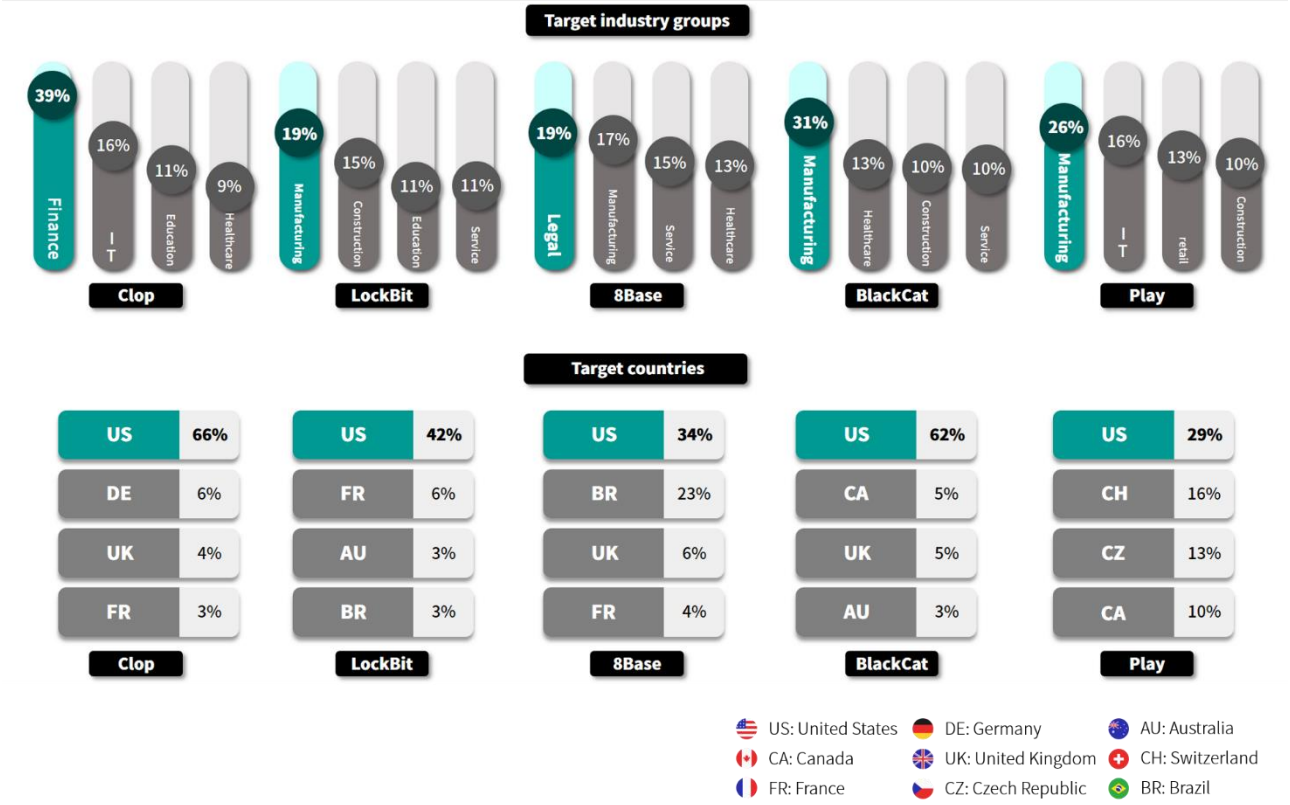
The NoEscape Group is continuously publicizing the recruitment of affiliates through RaaS. Instead of using codes from other groups, it is using ransomware developed in-house in C++ language, and it adopted a hybrid encryption method that mixes ChaCha20 and RSA algorithms. In addition, it is characterized by the fact that it supports Windows, Linux and VMWare ESXi attacks. It also provides a service that can perform DDoS if affiliates pay an additional fee, which is highly likely to increase the burden of ransom payment to the victim by making additional threats through DDoS attacks on top of the existing double extortion. Meanwhile, as they have a condition not to carry out an attack against companies in CIS countries[10], it can be assumed that the attacker may be related to CIS countries.

---

[8] IcedID: A malware that mainly targets companies to steal payment information and delivers other malware or downloads additional modules.

[9] Emotet: A Trojan horse used to download and install other malware

[10] CIS countries: An international organization of countries that became independent after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc.



In June, many ransomware attacks were still concentrated on the manufacturing industry too. Looking at the attacks by country, it can be confirmed that all of the top 5 ransomwares have performed the most attacks targeting the United States. The number of damage cases decreased slightly compared to last month, but Clop performed a large-scale attack by exploiting the MOVEit Transfer vulnerability, and continues to post victim data.

LockBit is a ransomware group that has shown considerable influence, extorting a total of $91 million from US companies so far. Hearing the news of the recent arrests of those who participated in the LockBit Group attack in the US and Russia, it can be seen that the attention of investigative agencies has been focused on this ransomware group. It is guessed that the size of Clop's attacks has decreased due to the pressure from investigative agencies, and it is showing signs of slowing down for various reasons, e.g., delaying the disclosure of leaked data as attention has been focused on its large-scale attack issues.

Nevertheless, LockBit still generates a large number of victims. Around the end of June, LockBit demanded $70 million ransom (approximately KRW90.5 billion) while threatening to disclose sensitive data from TSMC, a Taiwanese semiconductor manufacturer, on the dark web. However, when Kinmax checked facts, it found that the specific environment of the network was vulnerable, and the leaked information was mainly about the installation of systems provided by the company as a default configuration to the customer. In addition, TSMC stated that there is no impact on business operations, and customer information is also safe. The outcome of the negotiations has not yet been disclosed, but if LockBit Group's claim is true, it is expected that a significant amount of damage will occur.

8Base, which newly appeared on the list of top 5 ransomwares this month, has been quietly active without disclosing its victims for a year. It is necessary to keep an eye on what it will do in the future. 8Base's ransom note shares many similarities with the leaked Babuk's variant ransom note addressed to ESXi, and its contents are more detailed than other ransom notes. Looking at the contents, it contains prohibition of third-party intervention, guarantees that stolen data will not be disclosed to the outside, and it said that ransom should be paid only in bitcoin.

BlackCat (Alphv) posted a message on Reddit on June 17 on the dark web leak site. In this message, it claimed that it attacked Reddit and stole data last February, and revealed its plan to leak data because Reddit did not agree to a negotiation. BlackCat claims to have a significant amount of compressed files containing confidential data, and Reddit claims that only some data and access privileges have been infringed. So it is still too early to figure out what the situation is like. The Play Ransomware Group is also active, posting a total of 27 victims' data, including construction, manufacturing, and IT fields, on the leak site this month alone.

■ Focus of ransomware

Clop's MOVEit Transfer

Clop ransomware is operated by a group identified as TA505, which evolved from the CryptoMix ransomware discovered in March 2016. This group has been steadily engaging in large-scale attacks through vulnerabilities. Starting with the attack by exploiting the vulnerability (CVE-2023-0669[11]) of GoAnywhere MFT, a file transfer solution, last February, it conducted an attack through the vulnerability of PaperCut (CVE-2023-27350[12]), a printer solution, and in June, it is gradually posting damage cases of attacks it performed by exploiting the vulnerabilities of MOVEit Transfer of Progress, a file transfer solution, on the leak site.

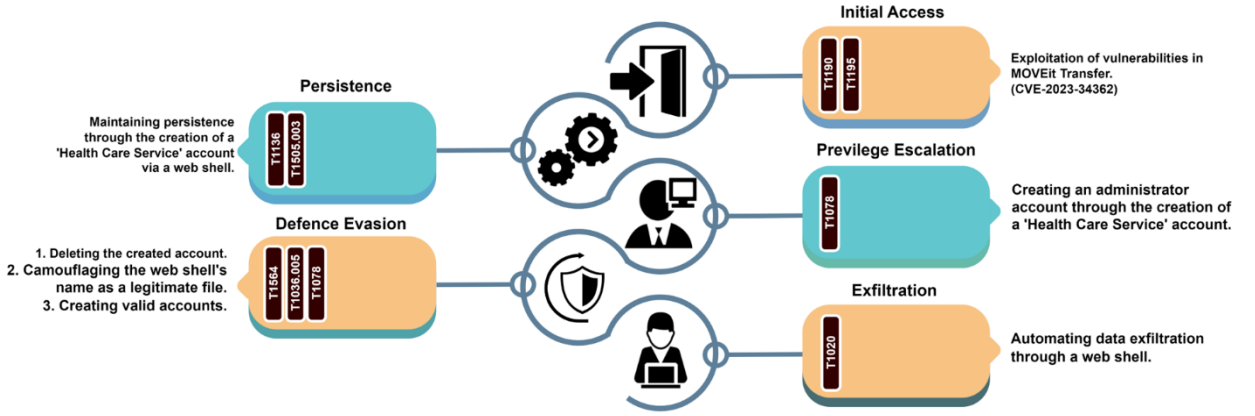
The peculiarity of this MOVEit Transfer attack is that it does not use an encryption strategy using ransomware. Clop, who chose the strategy of stealing data instead of encrypting data, said in an interview with Bleeping Computer that it prefers stealing data to encrypting data.

---

[11] CVE-2023-0669: A remote code execution vulnerability likely to occur in GoAnywhere MFT

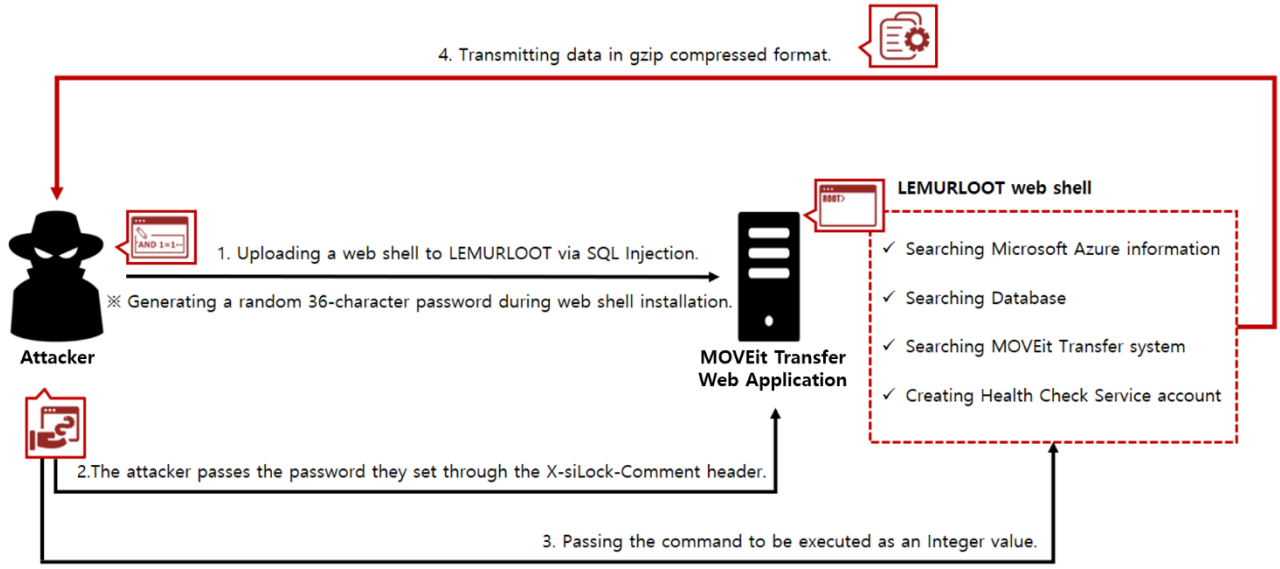
[12] CVE-2023-27350: A remote code execution vulnerability likely to occur in PaperCut

Clop's MOVEit Transfer attack strategy



Clop exploited the vulnerability (CVE-2023-34362) of MOVEit Transfer to perform a supply chain attack by uploading a web shell. The web shell used at this time was uploaded under the name human2.aspx, disguised as human.aspx, a component of MOVEit Transfer. This web shell maintained continuity and created an administrator account through the creation of an account called Health Care Service, and after privilege elevation, Clop stole specific data and files stored in Azure. In addition, it meticulously deleted the account it created to hinder infringement incident analysis later on.

Clop's MOVEit Transfer attack scenario



Clop installed a web shell called LEMURLOOT, which acts as a backdoor in a MOVEit Transfer attack, into the firmware through the SQL Injection[13] attack. This web shell performs the function of stealing the data uploaded by MOVEit Transfer users and credentials including Azure Storage Blob[14] information. The backdoor command is delivered as an HTTP request, and the attacker performs authentication through the X-siLock-Comment header.

In order for an attack to succeed, the X-siLock-Comment header must be sent along with the specific password specified by the attacker to perform authentication in the web shell. If the command value is delivered after password authentication, the web shell performs the following actions:

① Search Microsoft Azure system settings, Azure Blob Storage, Azure Blob Storage account, Azure Blob key and Azure Blob Container, and list the fields within the DB.
② Search the MOVEit Transfer system for a file whose name is a character string that matches the character string transmitted by the attacker.
③ Use the randomly generated user name, and the LoginName and Real Name value set to "Health Care Service" to create a new administrator privilege account.
④ Delete the account whose LoginName and RealName value is set to "Health Care Service"

[13] SQL Injection: An attack in which an attacker enters malicious SQL codes to acquire unauthorized access to the database

[14] Azure Storage Blob: A platform for storing and managing large amounts of data in the Azure cloud environment

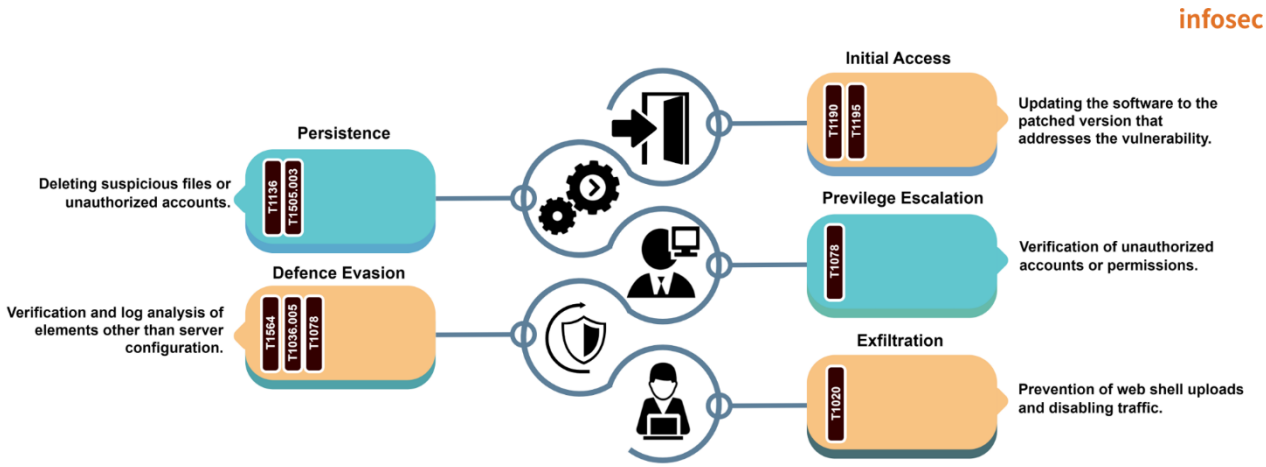
Clop not only steals desired files through the web shell that executes these commands, but also maintained continuity by creating an account called Health Care Service to access the system again at any time. For that matter, it meticulously stole Azure Storage Blob information to access the data stored in the Azure cloud. Stolen data is compressed in the gizp format, and the attacker obtains it through download.

If the password transmitted along with the X-siLock-Comment header is not valid, it returns the 404 status code[15] to pretend that the backdoor does not exist. After that, the connection to the database and the web shell is terminated. At this time, since the password is different for each web shell file, various IoCs[16] (Indicator of Compromise) exist.

[15] 404 status code: An error code indicating that the web server cannot find the relevant resources for the client's request.

[16] IoC: An indicator used to analyze infringement incidents in a computer system or network. It includes hash, IP, filename, etc.

Step-by-step countermeasure against Clop's MOVEit Transfer attack



In order to prevent initial access through the vulnerabilities of MOVEit Transfer, it is effective to install a patched version or update it to a patched version. However, in situations where immediate action is difficult, it is necessary to disable HTTP traffic for the MOVEit Transfer environment or delete suspicious files or unauthorized accounts that are not included in the components of the firmware. In addition, removel of enabled sessions or review of logs will also be helpful in preventing infringement incidents. It should be emphasized again and again. The most important thing is to use the software with vulnerabilities patched. Check the version of the software you are using and if the patch has not been applied, it is recommended to install a new version from a reliable official website.

Vulnerable version	Patched version
MOVEit Transfer 2023.0.0(15.0)	MOVEit Transfer 2023.0.2(15.0.2)
MOVEit Transfer 2022.1.x(14.1)	MOVEit Transfer 2022.1.6(14.1.6)
MOVEit Transfer 2022.0x(14.0)	MOVEit Transfer 2022.0.5(14.0.5)
MOVEit Transfer 2021.1.x(13.1)	MOVEit Transfer 2021.1.5(13.1.5)
MOVEit Transfer 2021.0.x(13.0)	MOVEit Transfer 2021.0.7(13.0.7)
MOVEit Transfer 2020.1.x(12.1)	It is possible to use a special patch.
MOVEit Transfer 2020.0.x(12.0) 이상	It needs to be upgraded to a supported version.

Indicator Of Compromise

human2.aspx : SHA256

0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e90ea05169d11141
5903a1098110c34cdbbd390c23016cd4e179dd9ef507104495110e301d3b5019177728010202c8
096824829c0b11bb0dc0bff55547ead182861826268249e1ea58275328102a5a8d158d36b4fd31
2009e4a2526f0bfbc30de22413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f
31acbc52ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59348e4351
96dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d387cee566aedbafa8c114e
d1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a38e69f4a6d2e81f28ed2dc6df0daf31e73ea
365bd2cfc90ebc31441404cca2643a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d
3c2a74545725b

File Name

human2.aspx : An malicious web shell disguised as human.aspx, which is one of the components of MOVEit Transfer

■ Reference sites

URL: https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/

URL: https://thehackernews.com/2023/06/new-linux-ransomware-strain-blacksuit.html

URL: https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/

URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

URL: https://thehackernews.com/2023/06/clop-ransomware-gang-likely-exploiting.html

URL: https://www.bleepingcomputer.com/news/security/royal-ransomware-gang-adds-blacksuit-encryptor-to-their-arsenal/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-exploiting-moveit-zero-day-since-2021/

URL: https://www.malwarebytes.com/blog/news/2023/06/more-moveit-vulnerabilities-found-while-the-first-one-still-resonates

URL: https://www.securityweek.com/new-moveit-vulnerabilities-found-as-more-zero-day-attack-victims-come-forward/

URL: https://www.bleepingcomputer.com/news/security/cisa-lockbit-ransomware-extorted-91-million-in-1-700-us-attacks/

URL: https://www.bleepingcomputer.com/news/security/suspected-lockbit-ransomware-affiliate-arrested-charged-in-us/

URL: https://www.malwarebytes.com/blog/news/2023/06/moveit-discloses-yet-another-vulnerability-three-times-a-charm

URL: https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response