Keep up with Ransomware

A double-edged sword, BitLocker

Outline

In March 2023, the number of confirmed cases of damage almost doubled over the previous month. The reason for the increase compared to the previous month is the sharp increase in the number of attacks by the Clop Group. The Clop Group has not shown any activity since January, but in February claimed to have carried out an attack using the GoAnywhere MFT (Managed File Transfer)[1] vulnerability (CVE-2023-0669), and then posted 104 cases, part of the attacks it performed, in March. The LockBit Group is quite threatening as the number of attack cases has decreased somewhat compared to the previous month, but there are still a large number of victims.

The strategies used by ransomware groups have also diversified. The Bloody Ransomware Group is seeking an IAB (Initial Access Broker), a broker that helps Initial Access with ransomware using the leaked LockBit source code, and the Medusa Group attacked a public school in the US, a space technology research institute in Pakistan, and a furniture company in the US, produced a video showing stolen data, posted it on a dark web leak site, and threatened them. In addition, the BianLian Group, which is inflicting damage worldwide, recently changed the course of its attacks from encrypting the victim's files to extracting data and stealing it, and posted 30 damaged organizations on the leak site in March. In addition to this group, some groups such as the Babuk Group and the Karakurt Group, which had been inactive since January and resumed their activities in March and posted three victims, also use a strategy to steal data without encryption and demand a ransom.

New ransomware groups called DarkPower, Abyss, and MoneyMessage were found. The DarkPower Group attacked various industries such as distribution, education, and construction, and posted a total of 10 attack cases during the month of March, and the Abyss Group posted seven cases including manufacturing and medical industries, and the MoneyMessage Group posted two attack cases in the transportation industry on dark web leak sites. Although they are new ransomware, they post many cases. So it is necessary to be alert and watch them.

[1] Used to perform secure file transfer and data exchange with software

Meanwhile, Mallox (Fargo), GlobeImposter, Nevada, LockBit 2.0 and 3.0, and BitLocker ransomware are being distributed in Korea. Mallox and GlobeImposter are ransomware that target vulnerable MS-SQL servers. GlobeImposter is ransomware used by the MedusaLocker Group for attacks and is spreading through the RDP (Remote Desktop Protocol)[2].
LockBit 2.0 mainly uses an attack method that induces attachment to be executed through e-mail, and is steadily found to be targeting small and medium-sized businesses. Recently, it is being distributed under the disguise of a resume, but it uses the icon of a Korean program to look like a Korean resume document, and puts a large space between the filename and extension to induce execution by disguising it as a non-executable file. So caution is required.

LockBit 3.0 is Ransomware-as-a-Service (RaaS) that the VenusLocker Group, known to be related to North Korea, mainly uses for attacks. On March 29, it claimed to have hacked the National Tax Service on its dark web leak site, and posted an article saying it would release information on April 1. Since then, the leaked data has not been disclosed to date, and it is possible that it was uploaded as an April Fool's joke on the grounds that the disclosure was announced earlier than the expected release time of one to two weeks on average after being uploaded to the leaked site, and that the date of data disclosure was April 1st. However, only careful speculation is possible, e.g., the possibility of negotiations without disclosing data and the possibility of disclosing data when negotiations do not go well.

The BitLocker ransomware uses BitLocker, a drive encryption technology provided by Windows, to encrypt a drive and extort money. Cases of infection of domestic medical institutions and various important infrastructures due to the BitLocker ransomware have been confirmed, and cases of damage to several domestic companies are continuously confirmed. Since the ransomware infiltrates using the vulnerabilities of MS Exchange[3] server (CVE-2021-34473[4], CVE-2021-34523[5], CVE-2021-31207[6]), it is recommended to use the patched version of the software.

[2] A protocol provided by Microsoft to remotely connect to another computer

[3] A messaging and collaboration software product developed by Microsoft

[4] It is a remote code execution vulnerability. It allows an attacker to access the Exchange Server by executing unauthenticated remote codes.

[5] It is a privilege escalation vulnerability. It can perform system privilege escalation by acquiring the remote code execute permission.

[6] It is a security feature bypass vulnerability. It allows unauthenticated remote code execution to bypass the security features of the DNS server.

■ Ransomware news

The LockBit 3.0 ransomware group claimed that it attacked the National Tax Service website.

- LockBit 3.0 claimed that it attacked the National Tax Service.
- Images, related contents, samples, etc. are not posted yet.
- There are many possibilities: e.g., it's an April Fool's Day prank or negotiations are in progress.

The FBI shut down the breached forum for fear that it is not safe.

- The administrator of the breached forum, one of the notorious forums, shut down the site after the FBI and other law enforcement agencies expressed concern that it could access the site server.
- The administrator shut down the site after hearing the news that its founder, Pompompurin, had been arrested by the FBI.
- It was mentioned that the Telegram channel would be operated for the time being and potentially he would help build a new site.

The LockBit ransomware group claims to have stolen data from tech companies related to SpaceX.

- The LockBit ransomware group claims to have stolen data from tech companies related to SpaceX.

The GlobeImposter ransomware is spreading again through the RDP. The MedusaLocker organization is distributing it.

- It infiltrates by performing a brute force or dictionary attack after scanning the RDP-enabled system.
- The e-mail address and onion address listed in the GlobeImposter ransom note are included in the list used by the MedusaLocker Group.

The Clop ransomware group began to extort GoAnywhere Zero Day victims.

- It used the Zero Day vulnerability of GoAnywhere MFT to steal data.
- It extorted money from the companies whose data it stole.

Microsoft SmartScreen Zero Day vulnerability has been exploited for distribution of the Magniber ransomware.

- Since January, it has been using the CVE-2023-24880 vulnerability that can exploit SmartScreen bypass technology to distribute malicious files.
- This vulnerability is a new variant of CVE-2022-44698.

The new DarkPower ransomware claims 10 victims in the first month.

- The new DarkPower ransomware appeared.
- It created 10 victims around the world.

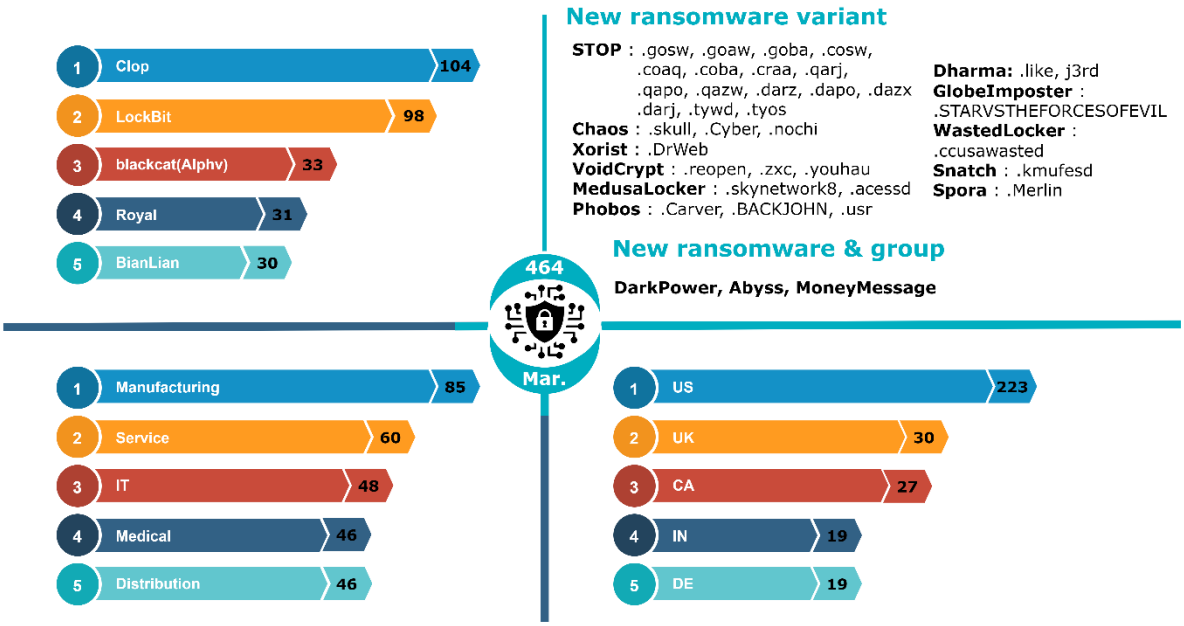
The Medusa ransomware group posted the data leaked from a Minneapolis school as a video.

- The Medusa Group threatened to post the data stolen from the Minneapolis school.
- It produced and disclosed a video showing how it accessed the stolen data.
- It can have a negative effect if it edits the video provocatively, and discloses it outside the dark web.

The BianLian ransomware group changed its line of attack to data extortion.

- The BianLian Group, which used to distribute ransomware that encrypts data, distributes ransomware that does not encrypt data.
- It changed its line of attack to stealing data and using it to extort money.

Ransomware threats



New threats

A number of variants of the Stop ransomware have been discovered, and a variant of the BlackCat (Alphv) ransomware has been found. The difference from the previous version is that ransomware can be executed only when there is a parameter that replaces the access token, and complicated obfuscation has been applied, and the Config data is not in the JSON format. In addition, the BlackCat ransomware creates and distributes polymorphic variants after the corresponding version update, which is part of a strategy to avoid detection.

Even in March, new ransomware groups are continuously discovered, and three groups called DarkPower, Abyss, and MoneyMessage have been identified. The DarkPower ransomware group is attacking organizations and companies in various countries, including the US, France, and Israel, and posted 10 victims, confirming the largest amount of damage among the three newly discovered groups. Also, it is written in the Nim[7] language that supports cross platforms[8] and its ransom note is in the pdf format. Abyss posted seven cases of victims in the construction, chemical, and distribution industries on the leak site, and the MoneyMessage Group attacked companies in Bangladesh and Hawaii, captured some of the leaked data and posted it on the dark web.

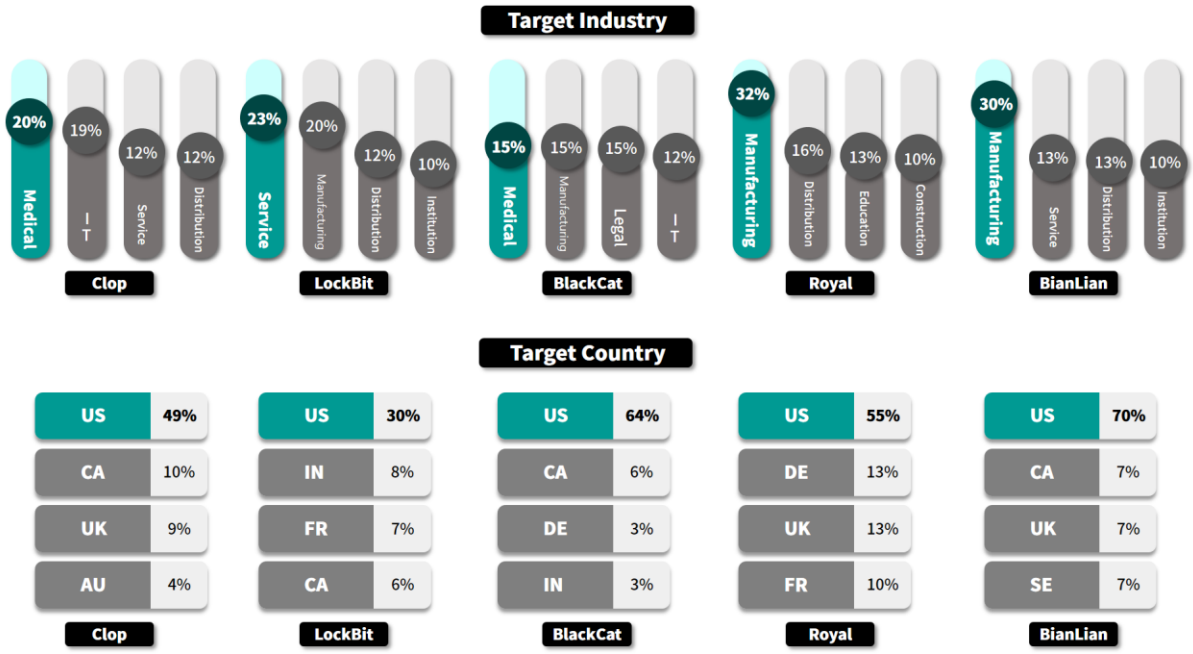
Like this, ransomware is evolving in a direction that is increasingly difficult to analyze, and after performing attacks on various countries and companies, it attempts to blackmail by posting some of the stolen information on the leak site, and if money is not paid, the stolen information is disclosed. In order to minimize damage to an organization, it is most important to prevent infection. So it is necessary to watch out for suspicious mail or files with unknown sources.

[7] Developed as an open source, it is a fast language that supports memory stability and asynchronous and parallel programming. Because it provides various functions such as memory management, generics, and concurrency processing, it is difficult to analyze compared to Clanguage. So it is also used for malware production.

[8] A language that can operate in many kinds of environments

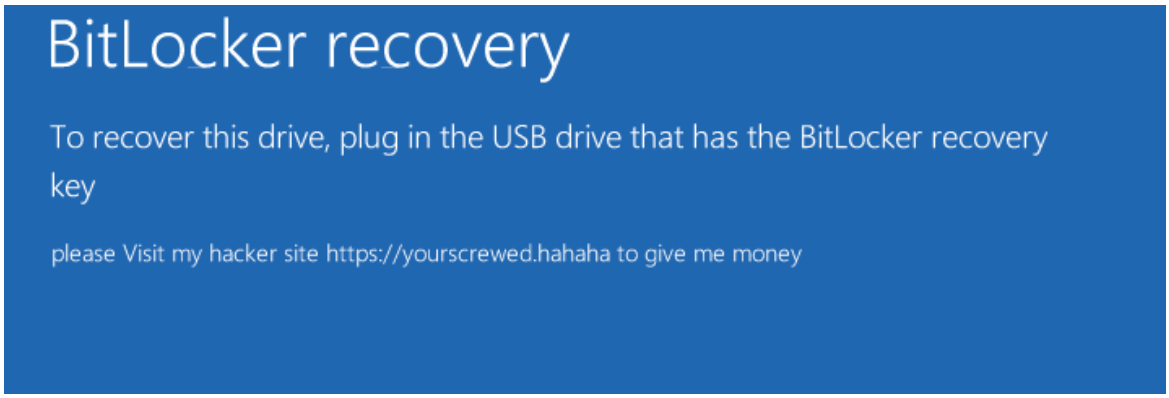
Top5 ransomware

Looking at the Top 5 ransomware, most of the attacks are made to the manufacturing and service industries, and the reason for the rapid increase in the number of damage cases compared to the previous month is the posting of attack cases using the GoAnywhere MFT vulnerability of the Clop ransomware. The Clop ransomware group has not been active since January, but in February, the data of the victim against which it claimed to have carried out an attack using the GoAnywhere MFT's vulnerability was posted on the leak site, and a number of damage cases were confirmed, and it is carrying out attacks across various industries. BlackCat also carried out attacks on various industries, while Royal and BianLian focused their attacks on the manufacturing industry. Also, the US has been targeted by ransomware most frequently in the world.



■ Ransomware focus

Ransomware exploiting BitLocker



BitLocker has an encryption function using the AES[9] algorithm and the Diffuser[10] algorithm. As it encrypts the drive, this technology is used to protect data by preventing unauthorized persons from accessing the drive.

Ransomware that exploits BitLocker is part of an attack that encrypts users' drivers for financial gain. Unlike general ransomware that directly applies encryption algorithms, this ransomware exploits BitLocker, a function that is basically built into the Windows system, for encryption.

Due to a recent ransomware attack that exploited BitLocker, damage occurred to small and medium-sized medical institutions and other important infrastructure organizations in Korea. It uses malware disguised as an open source messenger 'X-Popup', which is mainly used by small and medium-sized medical institutions, or installs files necessary for drive encryption and executes malicious commands to steal data and encrypt drives. In addition to this, several domestic companies continue to suffer damages. So caution is needed.

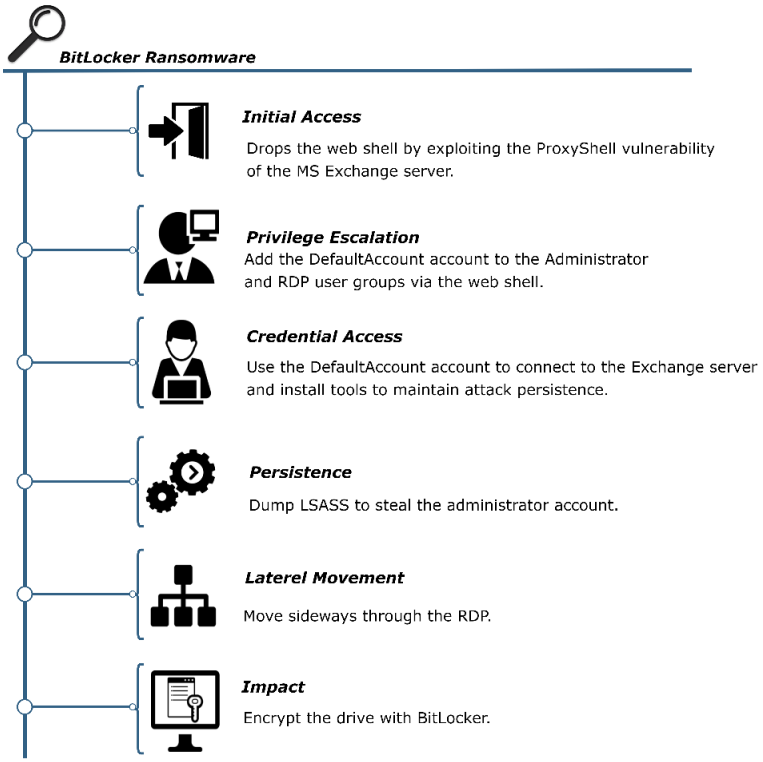
Ransomware exploiting BitLocker performs its Initial Access through the vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) of the MS Exchange[11] server. So to prevent infection, the vulnerabilities must be updated to the latest patched version. Ransomware that exploits BitLocker can cause great damage to the system if infected. So early response and prevention are important. Therefore, users must respond by continuous updating security-related information and the latest security solutions.

[9] A type of symmetric key encryption algorithms

[10] An algorithm to add a new random value to the ciphertext

[11] A messaging and collaboration software product developed by Microsoft

Scenario 1 for ransomware infection exploiting BitLocker

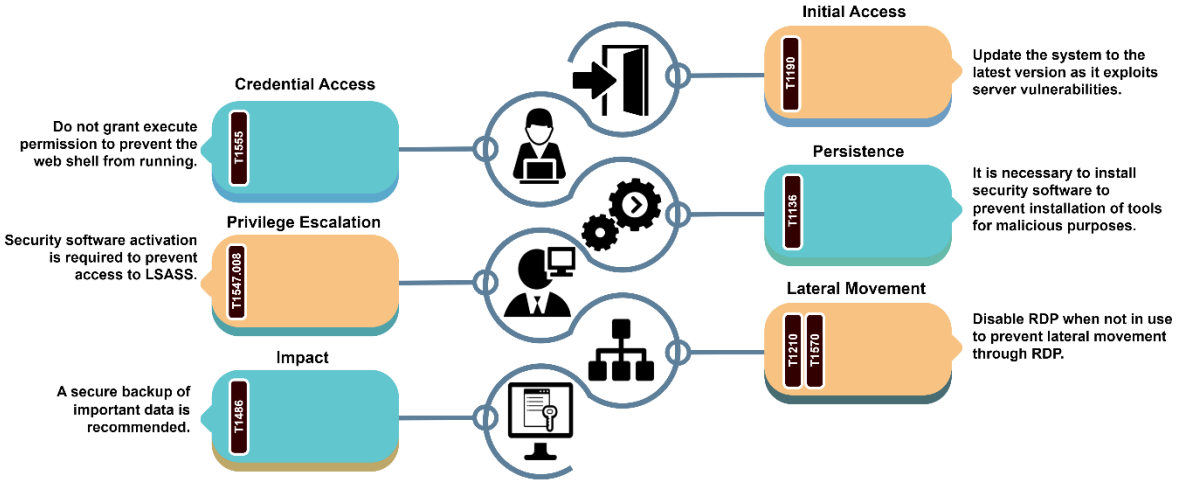


- For Initial Access, use the ProxyShell vulnerability of the MS Exchange server to get the initial access permission, and drop the web shell.
- Use the dropped web shell to execute the power shell command for the DefaultAccount account, which is an account used in the system, in the administrator group and RDP user group.
- Use the added DefaultAccount account to connect to the Exchange server and execute a batch file for maintaining the continuity of the attack to maintain the continuity of malicious behavior.
- Then, use the process monitoring tool to dump LSASS (Local Security Authority Subsystem Service)[12] to steal and decrypt the NTLM (NT LAN Manager)[13] hash for the administrator account.
- Use the stolen administrator account to move sideways through the RDP and execute BitLocker to encrypt the drive of the damaged system.

[12] A process that checks the login of Windows system users and manages password changes

[13] A hash function used in the Windows system. It is used to encrypt, store and authenticate the user's password.

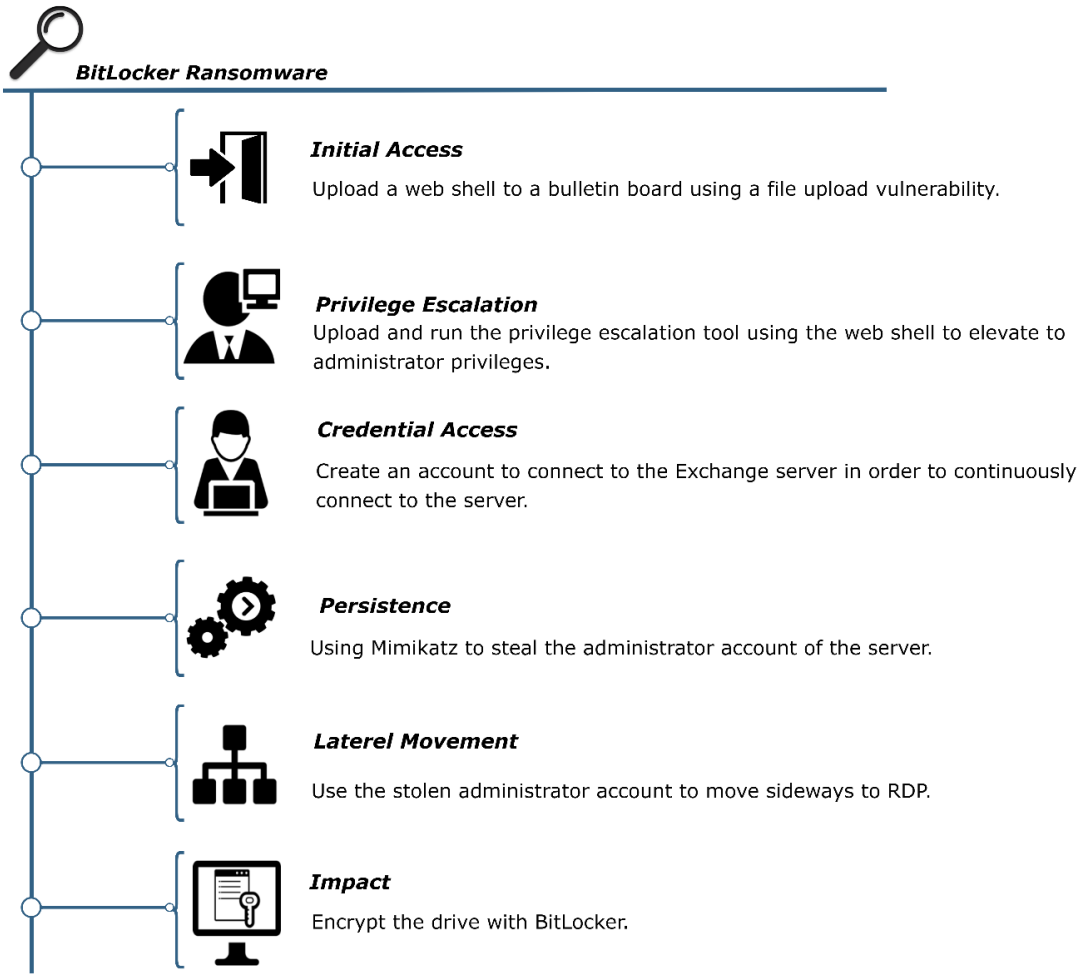
Scenario 1 - Response plan by stage



- Since the vulnerability of the server is used, the system update must be performed with the version in which the vulnerability is patched. If you access the Microsoft catalog page (https://www.catalog.update.microsoft.com) and search for the version you are using, you can check the update list. You must download and apply the version in which the vulnerability is patched.
- Execute permission should not be granted to the upload path so that the uploaded web shell cannot be executed, and measures such as file extension filtering are required.
- In addition, it is necessary to install security software to prevent installation of tools for malicious purposes, and in order to prevent LSASS dump, it is recommended enable ASR (Attack Surface Reduction)[14] rules that block access to LSASS or security software to which behavior-based rules that can block the access are applied.
- Lastly, in case the file is encrypted, important data must be protected through security backup, and backup data must be protected in a format different from the original for backup data protection, data copies must be isolated from each other, and backup data must be encrypted. These backup files should be restricted so that only permitted users can access them.

[14] Technology to block the attack path of malware

Scenario 2 for ransomware infection exploiting BitLocker



- Upload a web shell to a bulletin board using a file upload vulnerability like verification of improper extensions.
- Through the web shell uploaded in this way, upload and run privilege escalation tools such as Sweet Potato and Juicy Potato to elevate to administrator privileges.
- Create an account to connect to the Exchange server in order to continuously connect to the server.
- Use Mimikatz[15] to steal and decrypt the NTLM has of the administrator account of the server, and use the stolen administrator account to move sideways to the RDP, and execute BitLocker in the system to encrypt the drive.

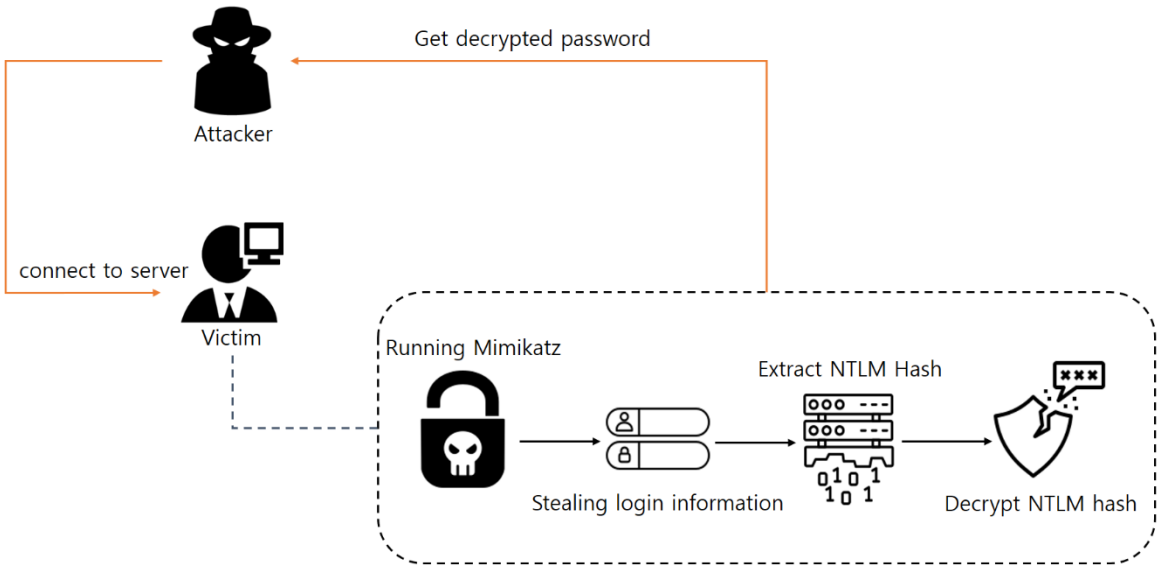
[15] A tool used to steal Windows credentials and gain administrator privileges

Scenario 2 – Exploring Mimikatz

Mimikatz is a tool that collects credentials (NTLM hash, Kerberos[16] ticket, etc.) information from Windows system. Mimikatz provides various functions such as lsadump to extract local system account information and password hash, sekurlsa to steal login information and Kerberos tickets, and a token to duplicate a process token or change it to another account. Functions frequently used in malware include lsadump, sekurlsa, and kerberos.

lsadump	It copies the contents of the LSASS memory that stores login information in an encrypted form. Malware steals login information through this function.
sekurlsa	It steals user credentials in an unencrypted form. Malware steals the personal information of the currently logged in user through this function.
kerberos	Malware steals the credentials of Kerberos protocol through this function.

The function of Mimikatz used in scenario 2 is the NTLM hash steal function. The process of stealing the NTLM hash of the server administrator account in this scenario is as follows:



[16] A protocol for maintaining security when a user is identified and authenticated on a computer network

Step 1) Steal login information

Execute Mimikatz and enter the "sekurlsa::logonpasswords" command to steal the login information of the user currently logged into the system.

Step 2) Extract the NTLM hash

Among the contents resulting from the command executed above, extract the NTLM hash corresponding to the administrator account.

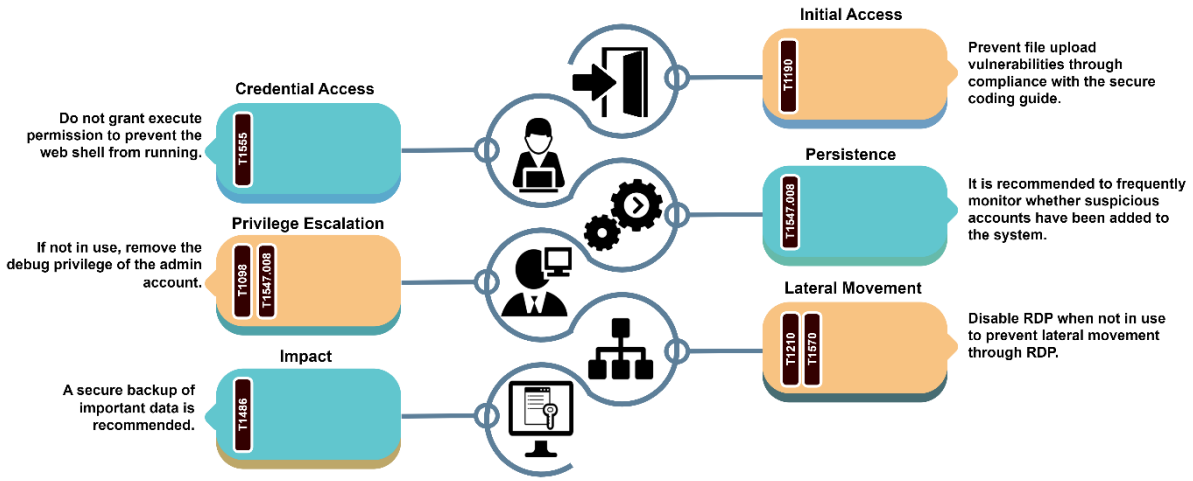
Step 3) Decrypt the NTLM hash

Decrypt the extracted NTLM hash using tools such as John the Ripper, Cain & Abel, and Hashcat. These tools use Brute Force[17] or Rainbow Table[18] methods to decrypt the hash value.

[17] An attack technique that tries all possible cases to find passwords or encrypted data

[18] An attack technique that uses a hash function to calculate the stored password in advance and make it into a table, and uses this to quickly reverse the hash value to find the password.

Scenario 2 – Response plan by stage



- In order to prevent exploitation of file upload vulnerabilities, perform an extension test based on the white list, and remove the execute permission of the path where the file is saved to prevent execution if it is uploaded.
- And to prevent the privilege escalation tool and Mimikatz from being installed, a policy restricting access to the upper directory must be set, and security software that detects these tools must be installed.
- If Mimikatz is installed, the NTLM hash can be stolen. So remove the debug permission of the administrator account to prevent Mimikatz from acquiring debug permission, and disable the RDP when not in use to prevent lateral movement. Also, it is necessary to periodically monitor whether suspicious files or accounts have been added.
- Lastly, in case the file is encrypted, important data must be protected through security backup, and backup data must be protected in a format different from the original for backup data protection, data copies must be isolated from each other, and backup data must be encrypted. These backup files should be restricted so that only permitted users can access them.

■ Reference sites

URL : https://www.swascan.com/bitlocker-ransomware-malware-analysis/

URL :http://idchowto.com/%EC%9C%88%EB%8F%84%EC%9A%B0-%EB%B9%84%ED%8A%B8%EB%9D%BC%EC%BB%A4-bitlocker-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-%EC%82%AC%EA%B3%A0%EC%82%AC%EB%A1%80-%EB%B6%84%EC%84%9D/

URL : https://thestack.technology/ransomware-attack-bitlocker/

URL : https://iboysoft.com/wiki/bitlocker-virus.html

URL : https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/

URL : https://www.securityweek.com/microsoft-smartscreen-zero-day-exploited-to-deliver-magniber-ransomware/

URL : https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/

URL : https://www.boannews.com/media/view.asp?idx=114832

URL : https://www.bleepingcomputer.com/news/security/BianLian-ransomware-gang-shifts-focus-to-pure-data-extortion/

URL : https://www.securityweek.com/ransomware-group-claims-theft-of-valuable-spacex-data-from-contractor/

URL : https://www.scmagazine.com/analysis/ransomware/north-korea-using-healthcare-ransomware-attacks-to-fund-further-cybercrime-feds-say

URL : http://www.datanet.co.kr/news/articleView.html?idxno=154612

URL : https://www.boannews.com/media/view.asp?idx=116717

URL : https://thehackernews.com/2023/02/north-korean-hackers-targeting.html