Keep up with Ransomware

Play ransomware attack threats on the rise

■ Overview

In March 2024, the number of damage cases caused by ransomware attacks decreased by about 3% to 405 compared to the previous month(418 cases). The LockBit ransomware group returned after seizure of its infrastructure and demonstrated explosive attack power, but it is showing some signs of slowdown in March. Meanwhile, the BlackCat(Alphv) ransomware group temporarily suspended its activities, and several situations presumed to be an exit scam[1] were detected. In other words, in March, the slight decrease in the number of ransomware attack damage cases compared to the previous month is interpreted to have been influenced by the decreased activity of the LockBit ransomware group and BlackCat(Alphv) ransomware group.

It also became an issue when a user presumed to be a 'notchy' affiliate posted a post on the Russian hacking forum RAMP claiming that he had not received commissions from BlackCat(Alphv). They attacked a healthcare company and received about 350 BTC (approx. KRW 35.2 billion), but the management of the BlackCat(Alphv) group moved all the virtual currency to another address and did not pay the commission to the affiliate. The day after the post was uploaded, the screen of the dark web data leak site was changed to indicate that it had been closed by an international investigative agency. However, it was confirmed that the website had been changed by the BlackCat(Alphv) group, not the investigative agency. Also, the BlackCat(Alphv) group made suspicious movements, e.g., changing the status message of the Tox messenger, one of its communication means, to 'GG' and 'Selling source codes 5kk'. This is a typical sign of an exit scam, and it is presumed that it has since disappeared from dark web sites and forums and has virtually ceased operation.

[1] Exit scam: A fraudulent practice of not paying commissions to affiliates or receiving money from ransomware victims and then disappearing without restoring files.

On the other hand, the Play, Medusa, and RansomHub groups increased the number of posts about damage compared to last February, showing more activity than other ransomware groups. First, the Play ransomware group has a history of attacking IT service company Xplain and stealing about 65,000 documents related to the Swiss government.

This incident occurred in May of last year, but the related investigation was completed last month, consuming a significant amount of time, i.e., about 10 months, and resources. It teaches us that damage caused by ransomware attacks is not a one-off event.

In addition, it was confirmed that the Play ransomware group attempted an attack exploiting ConnectWise's ScreenConnect vulnerabilities CVE-2024-1708[2] and CVE-2024-1709[3]. These vulnerabilities are an attack method that has been actively exploited by various ransomware groups such as the LockBit, BlackCat(Alphv), BlackBasta, and Bloody group. Specifically, a ransomware attack is carried out exploiting the 1-day vulnerability[4]. This makes it relatively easy to access an attack target after specifying it. Attack targets are selected by exploiting platforms that help search, monitor, and analyze devices accessible on the Internet, such as Shodan and Censys, to select servers where vulnerabilities exist.

In addition, there were cases of exploiting the CVE-2024-27198 authentication bypass vulnerability and the CVE-2024-27199 directory transversal vulnerability discovered in JetBrains' Teamcity. The Jasmin ransomware, created by the BianLian group and open source, exploited this to perform data takeover and file encryption. It was confirmed that through this vulnerability, it was possible to perform malicious tasks by distributing not only ransomware but also XMRig, a cryptocurrency mining malware, Cobalt Strike, a penetration test tool, and SparkRAT, a backdoor malware.

[2] CVE-2024-1708: A directory traversal vulnerability occurring in ConnectWise's ScreenConnect

[3] CVE-2024-1709: An authentication bypass vulnerability in ConnectWise's ScreenConnect

[4] 1-day vulnerability: A patch has been released for the discovered vulnerability, but it has not been applied to the vulnerability yet.

Both the ScreenConnect and Teamcity vulnerabilities mentioned earlier have CVSS[5] scores of 9.8 (CVE-2024-27198), 7.3 (CVE-2024-27199), 8.4 (CVE-2024-1708), and 10.0 (CVE-2024-1709), which are fairly high-level threats. In addition, as most of the exposed servers are operated with vulnerabilities unpatched, quick action is needed if the module and server are still in operation.

Lastly, a tool that can decrypt the Mallox (Fargo) ransomware distributed through MS-SQL database server vulnerability has been released. Although it only supports Mallox ransomware variants distributed between October 2022 and February 2024, excluding the latest version, it appears that damage can be reduced as many versions are supported.

[5] CVSS (Common Vulnerability Scoring System): A numerical value indicating the risk of vulnerability to cybersecurity

■ Ransomware news

infosec

Detection of BlackCat(Alphv) Exit Scam

- On Mar 3rd, An affiliate user posted on the RAMP forum stating the had not received fees from BlackCat(Alphv).
- Related to the Health Care company attack occurred on Feb 21st. Through this attack, BlackCat(Alphv) received 350BTC.
- BlackCat(Alphv) transferred all 350BTC to 8 different wallet addresses without paying the fees.
- BlackCat(Alphv) change their status message on the Tox. (GG → Selling source code 5kk)
- Posting FAKE page to make it appear as if the DLS has been seized by international law enforcement agencies.
- It is suspected that they have ceased operation by disappearing from dark web forums.

Ransomware groups exploiting vulnerabilities in JetBrains' TeamCity

- CVE-2024-27198, an authentication bypass vulnerability, and CVE-2024-27199, a directory traversal vulnerability.
- Access to TeamCity endpoints through URL manipulation, enabling the creation of Administrators.
- There is a possibility of exploitation as the vulnerabilities were fully disclosed and patched simultaneously on March 4th
- Detect evidence that BianLian group and Jasmin ransomware, developed as open source, exploit.
- Various malware (e.g. cryptocurrency-mining malware and backdoor etc.) also exploit Team City.

Play leaked Swiss Federal Government data through IT Service provider

- Attack occurred in May 2023, and investigations began in August 2023, continuing until March 2024.
- Approximately 65,000 Swiss Federal Government document were leaked and posted on DLS.

The aiohttp Python library is suspected to be utilized in ransomware attacks

- The aiohttp library, asynchronous HTTP client/server framework, has a directory traversal vulnerability (CVE-2024-23334).
- ShadowSyndicate ransomware attackers were observed scanning vulnerable servers from February to March.
- Patched Version 3.9.2 released on January 28, and PoC exploit code* was disclosed on GitHub* on February 27.

* PoC (Proof of Concept) exploit code: Demonstration source code showing attack using a vulnerability is possible.
* GitHub : Web-based source code version management and collaboration platform.

Mallox ransomware decryption tool updated

- The decryption method involves key generation, allowing decryption of variants from October 2022 to February.
- Mallox group posted a forum thread urging the creation of a decryption tool for the latest variants.

Distribution of CryptoWire including the decryption key

- An open-source-based ransomware that was trending in 2018, primarily distributed through phishing emails.
- Autoit-script-based. Embedding the decryption key within the script or transmitting key to the attacker's server.

Qillin ransomware group hits Big Issue, UK-based publishing and social enterprise

- 550GB of data stolen, including contracts, partner data, financial statements and investment information.
- Big Issue promptly took measures to restrict system access and initiated system recovery procedures.
- They announced that the magazine's publishing and distribution were not affected.

Rust based variant of the Qillin ransomware has been discovered

- Rust variant of Qillin is distributed to VMware Center* and ESXi servers using a PowerShell script.
- Utilizing various tools and systems including RMM, Cobalt Strike, PsExec, SecureShell. SYS driver.

* VMware Center: A service that centrally manages and monitors multiple ESXi hosts and virtual systems.

KillSec ransomware group launches a new dark web leak site

- Operating on Telegram since October 2023, the ransomware group targeted Romanian police in November 2023.
- In March 2024, they began posting victims on a DLS.

BlackByte and RA Group ransomware groups resume their operations

- BlackByte resumes activity after 5 months with a renewed DLS and posts a new leak.
- RA Group rebrands to RA World and resumes activity by posting 7 new leaks after 3 months.

A new ransomware called DoNex emerges from the DarkRace lineage

- The DarkRace ransomware is developed based on the leaked LockBit builder.
- Utilizing ransomware from the DarkRace discovered in May 2023, they post 5 new leaks.

Medusa hits US #1364 Federal Credit Union

- A financial institution in the U.S offering a variety of financial services. (e.g. loads, investments, savings and cards)
- Suspected to be related to the service disruption on February 21st.
- Posted on a dark web leak site on March 7th.

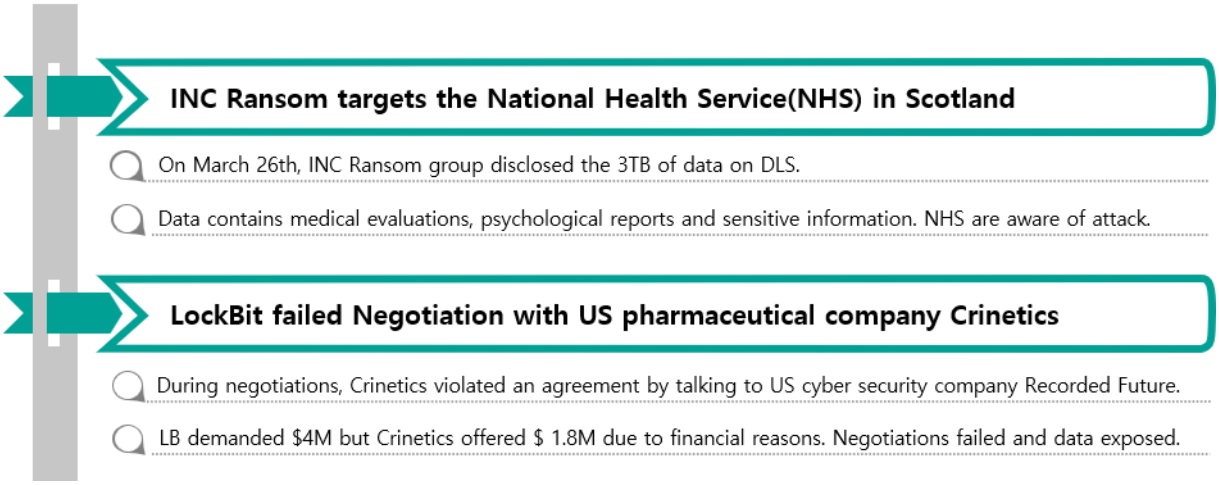


Figure 1. Ransomware trends

■ Ransomware threats

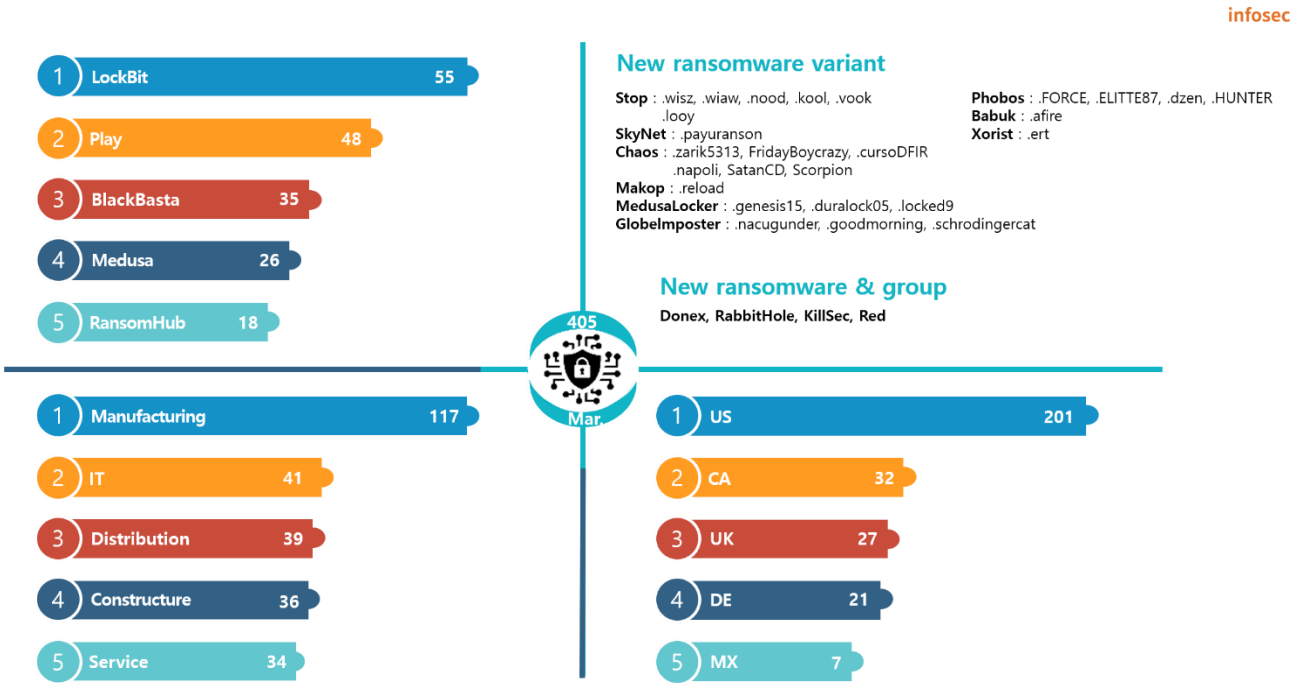


Figure 2. Ransomware threats status as of March 2024

New threats

In March, many groups resuming their activities were discovered. IntelBroker, a seller who had been active on BreachForums, a notorious hacking crime forum, restored its account in March and continued its activities, and the BlackByte ransomware group reorganized its data leak site after about five months and posted new leaked data. Lastly, RA Group resumed its activities three months after December 2023 by posting seven pieces of data under the name RA World.

The Donex group is using the DarkRace-based ransomware discovered in May 2023, and has leaked data on five organizations to date. It is believed that the DarkRace ransomware was developed based on the leaked LockBit builder codes by integrating the technologies of the LockBit ransomware, such as the ransom note format, changing file icons, and changing extensions.

The dark web data leak site of the Rabbit Hole group was discovered. However, since no damage has been posted yet, it appears that they are building infrastructure or preparing for attacks. The KillSec group appears to have started its activities through Telegram in October 2023, and recently opened a data leak site on the dark web and began posting victims. Looking at its leak history on Telegram, it is claimed that it posted 200,000 pieces of data in November 2023 and the Rumanian police paid EUR 1,500 (approx. KRW 2.2 million), but it has not been confirmed whether it actually happened or not.

The Red group posted 12 cases of damage leaks in total upon its appearance. In the early days after its discovery, there were suspicions of scams, as all sample file download links in the leaked data did not work properly or some of the leak targets had already suspended business. However, as it was confirmed that all download links were working normally as of April 1, it seems that it remains to be seen whether they are a scam group or not.

Top 5 ransomwares

Figure 3. Major ransomware attacks by industry/country

After resuming its activities, the LockBit ransomware group is actively carrying out attacks and producing the largest number of victims. It used a unique strategy of 'not compromising on the financial aspect'.

On March 18, it posted Crinetics, a US startup pharmaceutical company, on a dark web data leak site. The disclosure was that Crinetics violated confidentiality and shared the breach with Recorded Future, a US security company. In addition, the LockBit ransomware group notified Crinetics that it would disclose the data unless it paid USD 4 million (approx. KRW 5.5 billion), but Crinetics said it offered USD 1.8 million (approx. KRW 2.5 billion) due to its financial situation. In the end, LockBit did not accept this offer, notified that it would disclose the data, and ended the conversation. This move is interpreted as sending a warning message to other companies that they will not compromise on the negotiated amount.

The Play ransomware group has been steadily operating since 2022. It showed a brief slowdown early this year, but the number of attack cases has recently been on the rise again. They are carrying out attacks that exploit vulnerabilities consistent with recent ransomware trends, but unlike other groups that mostly operate RaaS[6], they are known as a closed group that does not operate Ransomware-as-a-Service (RaaS).

While the BlackCat (Alphv) ransomware group stopped its activities and other ransomware groups that were strong began to falter, the Medusa, BlackBasta, and RansomHub groups performed many ransomware attacks and quickly emerged as the top 5 ransomwares. The BlackBasta group's activity slowed down last January when the dark web leak site was taken offline for about 10 days, but it is understood that it has been steadily posting victims as it performed the ScreenConnect vulnerability attacks, which is continuously exploited recently.

The Medusa ransomware group recently attacked the Tarrant Appraisal District (TAD), a Texas government agency, demanding a ransom of USD 700,000 (approx. KRW 960 million), but negotiations appear to have failed. Additionally, it attacked US #1364 Federal Credit Union, a financial institution, and caused service disruption.

[6] RaaS (Ransomware-as-a-Service): A form in which ransomware groups provide ransomware to affiliates or attackers in exchange for compensation

The RansomHub group stated that it will not attempt attacks against CIS[7], Cuba, North Korea, China, Romania countries and non-profit organizations. However, according to the information disclosed on the dark web leak site, it can be seen that Rumania is excluded from the attack exclusion list. Additionally, rules were set to prevent reinfection with ransomware. Also, they are promoting the RaaS affiliate program by posting it on RAMP, a Russian hacking forum. This ransomware protects symmetric keys using the x25519 algorithm and supports fast encryption speed by encrypting files with AES256, chach20, and xchacha20 symmetric key algorithms depending on the hardware. It is written in the Go language[8] and supports various platforms such as Windows, Linux, ESXi[9], and ARM/MIPS[10]. It uses an affiliate's virtual currency wallet for negotiation and uses a strategy of providing only a 10% commission once payment is confirmed. This appears to be a strategy to prevent financial loss due to the BlackCat (Alphv) group's exit scam.

[7] CIS (Commonwealth of Independent States): An international organization of countries that gained independence after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc.

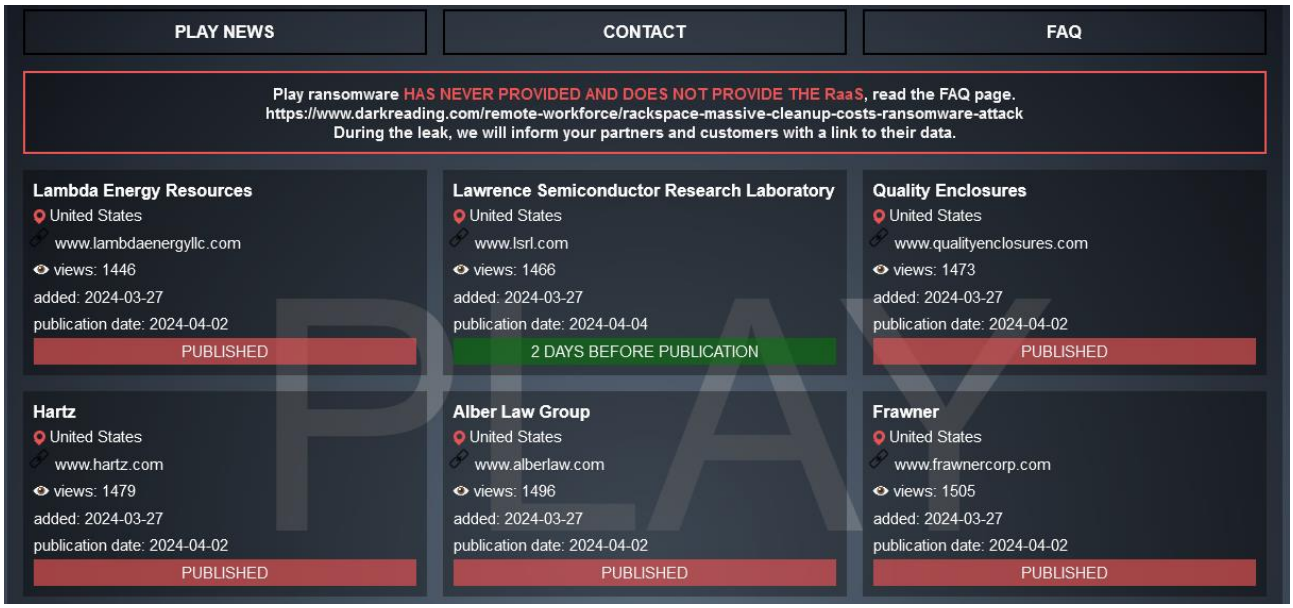
[8] Go language: An open source programming language developed by Google to increase productivity

[9] ESXi: VMware A UNIX-based logical platform, developed by VMware, that can run multiple operating systems simultaneously on a host computer

[10] ARM/MIPS: A type of CPU architecture. ARM is mainly used in Macs and mobile devices, while MIPS is mainly used in embedded systems

■ Ransomware in focus

Outline of the Play ransomware



Source: Play ransomware group data leak site

The Play ransomware group began its activities in June 2022 and has posted about 410 victims on the dark web data leak site to date. In particular, the Play group is characterized by posting multiple victims simultaneously at certain intervals, and posted 48 victims in March alone. Caution is needed as the number of attack cases has been steadily increasing since January when its activity slowed down somewhat.

It was confirmed that the same strategy was recently used in a number of ransomware attacks, and a report was released stating that the Play group provides RaaS. However, the Play group announced on the dark web leak site that unlike other ransomware groups, it does not provide RaaS. We cannot be 100% certain about the Play Group's announcement. The reason they stated that they do not provide RaaS is that they actually do not use it, or it can be seen as a strategy to prevent investigative agencies from closing in on them.

The Play ransomware uses strategies quite similar to those of the Hive and Nokoyawa ransomware. As they use ▲Nekto, PriviCMD, and WinPEAS for privilege escalation, ▲download attack tools through Cobalt Strike, ▲use the Coroxy and SystemBC malware that can be controlled remotely, ▲use PsExec, a tool that helps execute programs remotely, some correlations have already been confirmed. In addition, they are implementing differentiated strategies, e.g., using the independently developed Grixba data takeover tool and AdFind, a tool that collects Active Directory information on the network.

The Play group also uses a strategy to protect victims from being identified for a certain period of time by hiding their names using the '?' character when posting leaked data on dark web leak sites. In this case, it is possible to quietly make financial gains without reporting the damage. However, this strategy appears to be used only for companies that have room for negotiation, not for all victims.

As a result of the analysis, it has been found that the Play ransomware's penetration method is to use the exposed RDP[11] server, stolen accounts, Fortinet VPN[12] server vulnerabilities (CVE-2018-13379[13]and CVE-2020-12812[14]), MS Exchange Server[15] ProxyNotShell vulnerabilities (CVE-2022-41040[16]and CVE-2022-41082[17]), and ConnectWise's ScreenConnect vulnerabilities CVE-2024-1708 and CVE-2024-1709, etc. Also, it was found that the RMM[18] tool is mainly exploited as one of the evasion strategies to prevent detection of penetration and ransomware attacks. This strategy is used not only by Play but also by many ransomware groups.

[11] RDP (Remote Desktop Protocol): A protocol that allows you to remotely control another computer

[12] VPN (Virtual Private Network): A virtual security network used to protect personal information and bypass geo-restrictions on the Internet

[13] CVE-2018-13379: A web path exploration vulnerability that can download FortiOS system files

[14] CVE-2020-12812: An inappropriate authentication vulnerability that allows you to log in without being prompted to enter the authentication factor FortiToken

[15] MS Exchange Server: A message and collaboration software product developed by Microsoft

[16] CVE-2022-41040: Server-Side Request Forgery (SSRF) attack vulnerability

[17] CVE-2022-41082: A remote code execution vulnerability

[18] RMM (Remote Monitoring and Management): A commercial program providing remote monitoring and management

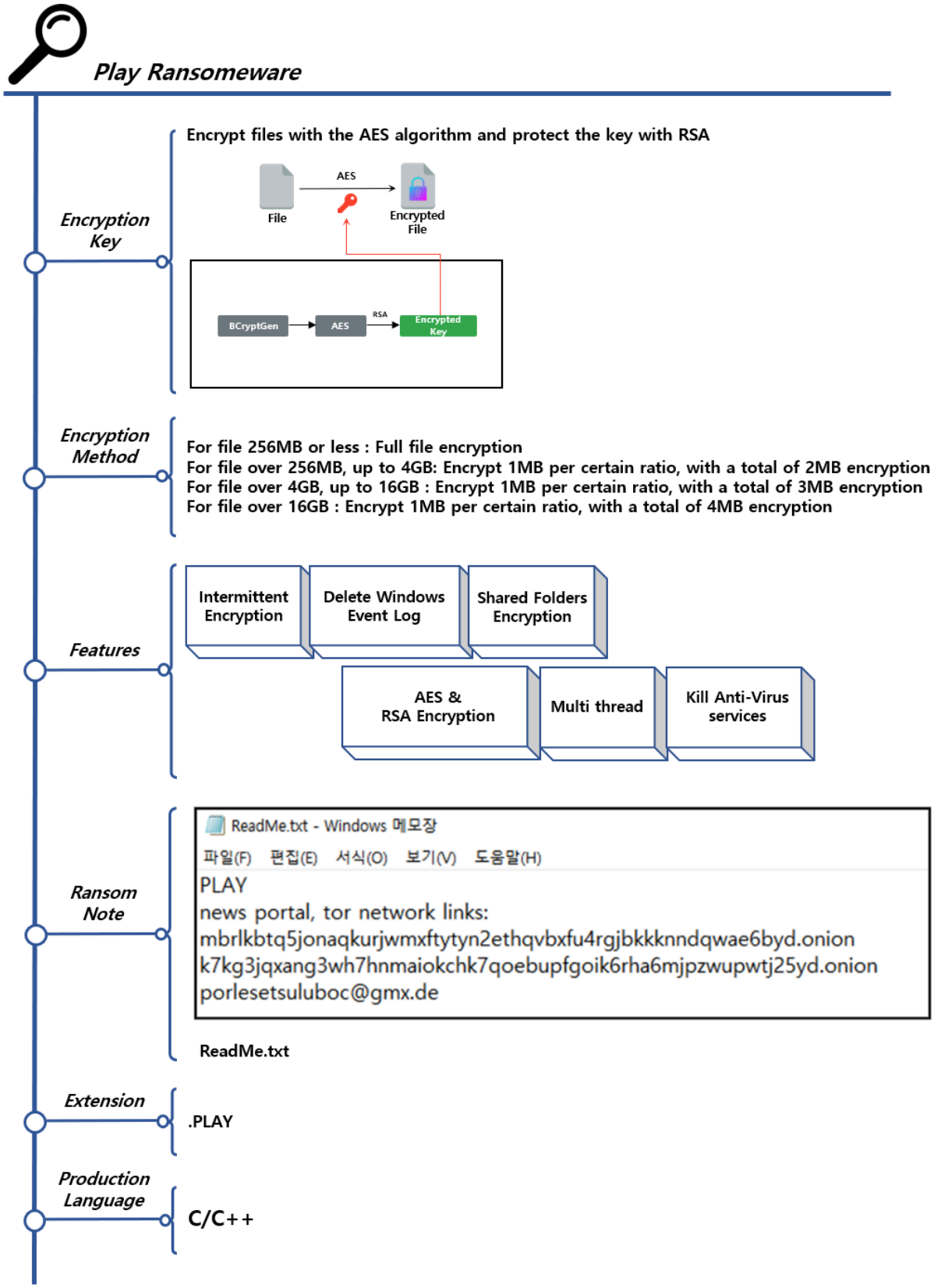


Figure 4. Play ransomware Outline

Play ransomware strategy

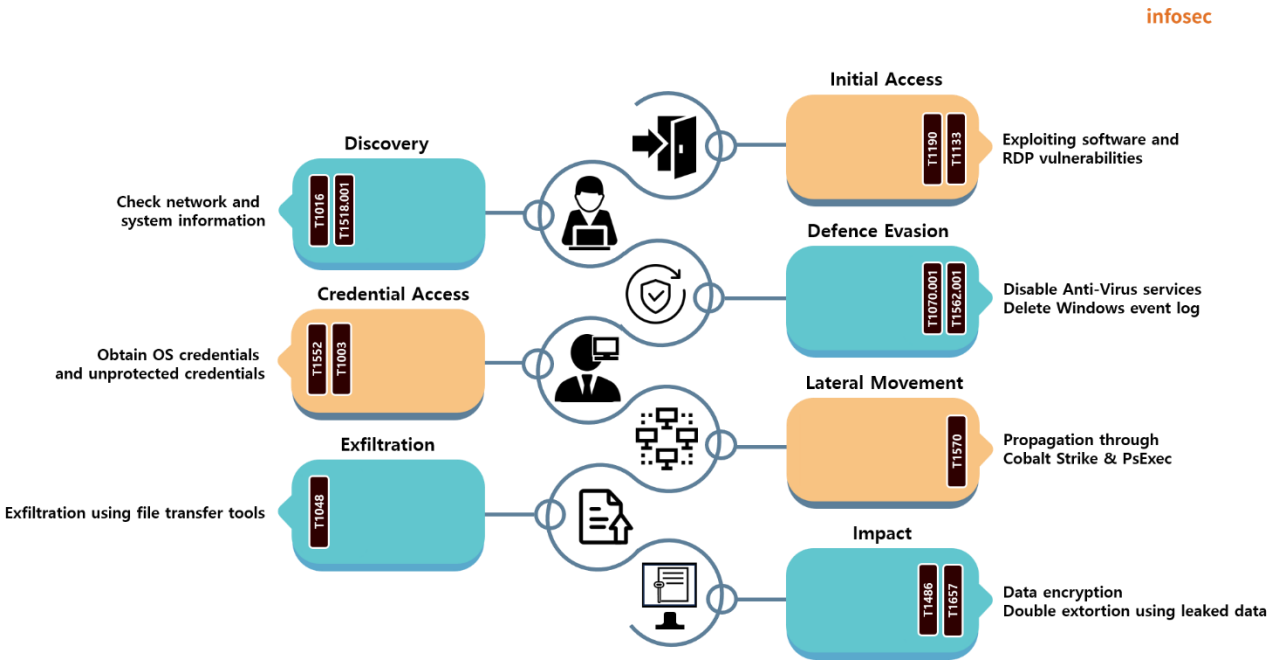


Figure 5. Play ransomware attack strategy

The Play ransomware attempts initial access by utilizing the exposed Remote Desktop Protocol (RDP) or software vulnerabilities. RMM vulnerabilities such as the Fortinet VPN server vulnerability, the MS Exchange Server ProxyNotShell vulnerability, and the ConnectWise's ScreenConnect vulnerability were mainly utilized. In addition, there is a history of initial access attempts using stolen account information.

If initial access is successful, tools for credential takeover, system data collection, internal propagation, remote connection, and data leakage are downloaded and used. For privilege escalation, ▲Nekto, ▲PriviCMD and ▲WinPEAS are used, and for internal propagation, Cobalt Strike and PsExec are downloaded. In addition, to leak data, various tools such as Grixba, a self-developed data takeover tool, or WinRAR, a compression tool, and WinSCP, a file transfer program, are used.

Because the Play ransomware uses a variety of tools like this, the ransomware file itself only has file encryption and ransom note creation functions. Instead, to make it difficult to analyze ransomware files, character strings are obfuscated before storage, and garbage codes that are completely unrelated to the program execution flow are used. Also, the API required for program execution is dynamically loaded, and the address of the API is checked through xxHash32, one of the hash algorithms.

For file encryption, not only the target PC's drive but also shared folders are encrypted. Files are encrypted using a randomly generated AES key for each file, and the key used for encryption is protected using RSA and added to the end of the file. The Play ransomware uses multi-threading and partial encryption for fast encryption. If the file size is smaller than 256MB, the entire file is encrypted, but if it exceeds 256MB, only 1MB per certain percentage of the file is encrypted.

infosec

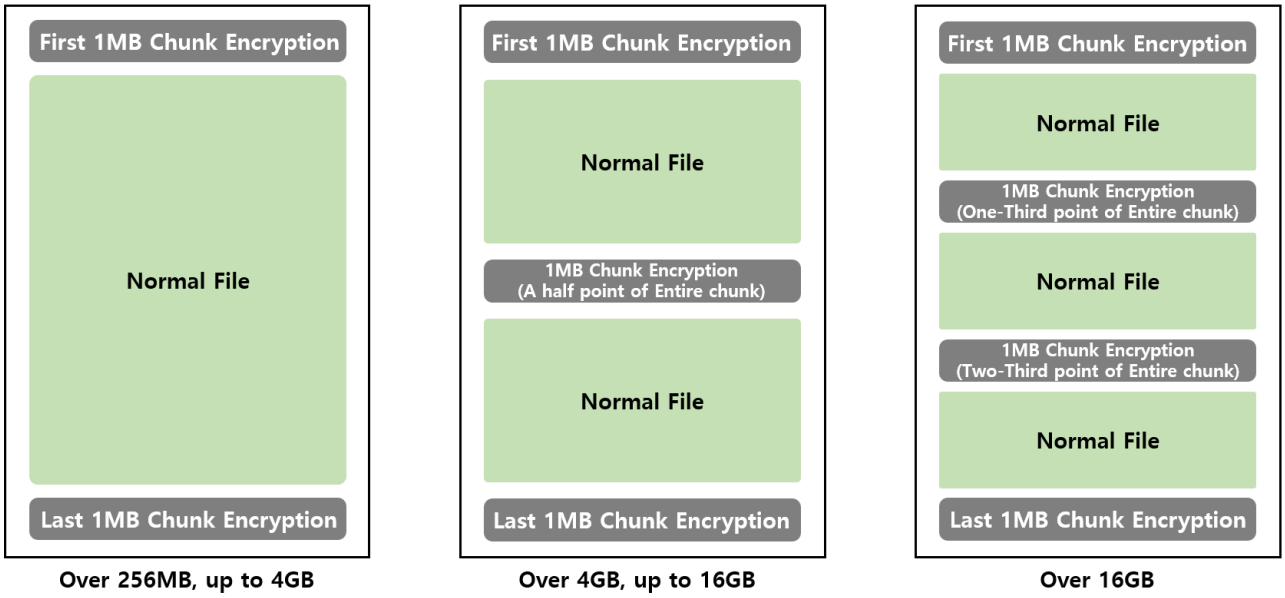


Figure 6. Play ransomware's partial encryption method

The Play ransomware divides files into chunks of 1 MB in size for encryption, and in the case of large files, it encrypts only a small portion of the entire chunks of the file.

For files over 256 MB and under 4 GB, only the first and last chunk are encrypted, and for files over 4 GB and under 16 GB, not only the first and last chunks, but also the chunk located at 1/2 point are encrypted. Lastly, for files over 16 GB, the first and last chunks are encrypted, and the chunks located at the 1/3 and 2/3 points are also encrypted. If the file consists of 6,000 chunks, the first and last chunks are encrypted, and the 3,000th chunk, which is 1/2 the point, is also encrypted.

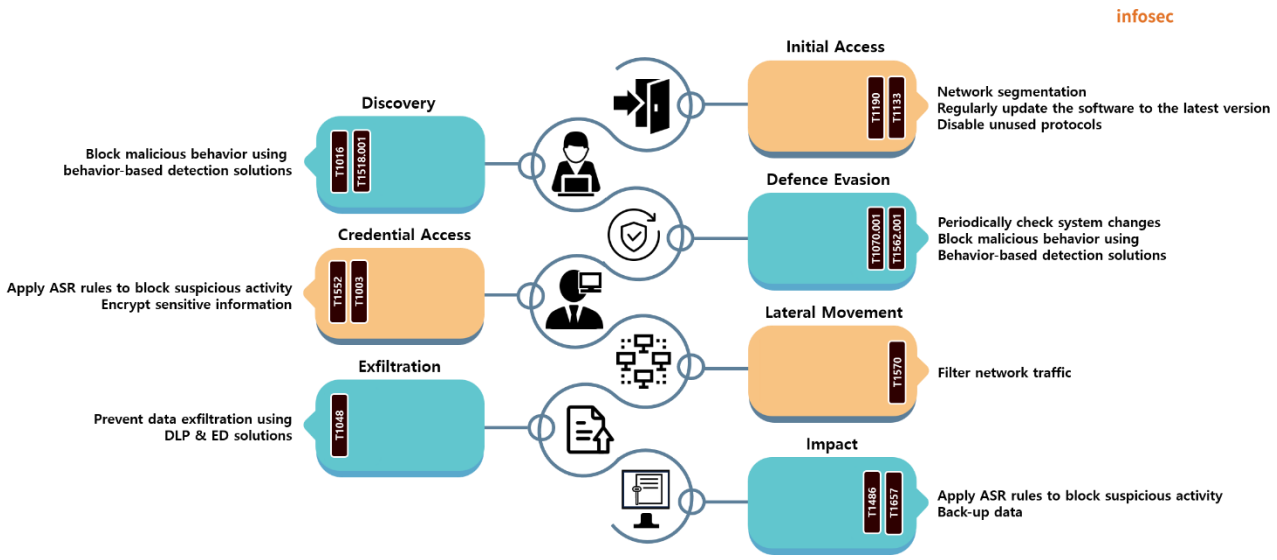


Figure 7. How to respond to the Play ransomware

As Play mainly distributes directly using software vulnerabilities or protocol vulnerabilities, it is important to periodically update the software or operating system to a non-vulnerable version. Also, unused protocols and services should be disabled or removed to prevent exploitation. In addition, damage can be minimized through network separation, e.g., segmenting the network or using a virtual private network.

The following are the vulnerabilities confirmed to have been exploited by the Play ransomware group. If you are using an affected server or solution, you need to update it to the version with the vulnerability patched.

CVE	Description	Affected version	Patch version
CVE-2018-13379	A file path exploration vulnerability that can download system files when using SSL VPN on Fortinet's secure OS FortiOS	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 or higher 6.0.5 or higher
CVE-2020-12812	An inappropriate authentication vulnerability where two-factor authentication (2FA) is not performed properly when using SSL VPN on Fortinet's secure OS, FortiOS	6.0.9 or lower 6.2.0 ~ 6.2.3 6.4.0	6.0.10 or higher 6.2.4 or higher 6.4.1 or higher
CVE-2022-41040	A server-side request forgery (SSRF) attack vulnerability occurring in the MS Exchange Server	Exchange Server 2013, 2016, and 2019 before the update	KB5019758 Update
CVE-2022-41082	A remote code execution vulnerability occurring in the MS Exchange Server	Exchange Server 2013, 2016, and 2019 before the update	KB5019758 Update
CVE-2024-1708	A remote desktop solution ScreenConnect vulnerability. It is a path exploration vulnerability which allows path exploration to access random files or directories	23.9.7 or lower	23.9.8 or higher
CVE-2024-1709	A remote desktop solution ScreenConnect vulnerability. It is an authentication bypass vulnerability that could allow a system administrator account to be created on a remote desktop	23.9.7 or lower	23.9.8 or higher

Table 1. Software vulnerabilities exploited by the Play ransomware

After initial access, the Anti-Virus service is terminated for malicious activities such as data collection and ransomware distribution. Also, OS authentication information and various unprotected credentials are obtained and used additionally in attacks. Therefore, malicious actions must be blocked by activating the ASR rules, or sensitive information such as account information must be encrypted and stored safely.

The ransomware is spread and executed remotely using Cobalt Strike and PsExec. Therefore, to prevent this, you must continuously control traffic flow and access through network monitoring tools and filter network traffic to prevent unknown or untrusted sources from accessing internal systems.

It is also necessary to prepare for data takeover and file encryption. Data leakage can be prevented by using the DLP[19] solution or the EDR[20] solution. In some cases, normal tools are used during the data leak process. So measures need to be taken to recognize it in advance.

Caution is required especially for large files. In addition, regular backups must be created and managed for file recovery, and since data in NAS[21] and backup storage may be deleted, it is recommended to manage data by performing vaulting backup[22] on a separate network or storage. In the case of the Play ransomware, as the ability to delete backup copies has not been confirmed, some files can be restored by creating a separate restore point.

[19] DLP (Data Loss Prevention): A data leak prevention solution that monitors the flow of data and monitors/blocks important information leaks

[20] EDR (Endpoint Detection and Response): A solution that prevents the spread of damage by detecting, analyzing, and responding to malicious actions occurring on terminals such as computers, mobile devices, and servers in real time

[21] NAS (Network Attached Storage): A storage device connected to a network that allows multiple users to share and access data

[22] Vaulting backup: A method of separately storing backed-up data at a certain distance away.

Indicator Of Compromise

Play : SHA256

5a0a4e5379e1f0bc9bdd42f5c638c601a0068da4b19b063e5276a01494ae116e
2d01ddc075b48db3ba69b036f9f5977f3607edba5dec6799e4fae7ccd4f1ba75
50d72707eb0a9b7f4ecaa8e0242675e3349b9d67901ac020635ae2ec0eb328e4
64087027f0c727a807c8b6ccf602398adc9d346fe518cbd3b589348702dc39ed

File Name

LkToXG.exe
Thimble pulverization
P137.exe

■ Reference site

• Official Symantec website (https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy)

• Official BleepingComputer website (https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/#google_vignette)

• CISA Security Advisory (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a)

• The Register newsletter (https://www.theregister.com/2024/03/08/swiss_government_files_ransomware/)

• Official SOCRadar website (https://socradar.io/dark-web-profile-play-ransomware/)

• Official Trend Micro website (https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play)

• Official Malwarebytes website (https://www.malwarebytes.com/blog/news/2023/12/fbi-issues-advisory-over-play-ransomware)

• Joint CISA advisory (https://www.cisa.gov/news-events/alerts/2023/12/18/fbi-cisa-and-asds-acsc-release-advisory-play-ransomware)

• DarkReading newsletter (https://www.darkreading.com/cloud-security/-play-ransomware-group-targeting-msps-worldwide-in-new-campaign)

• MS Security Response Center (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082)

• MS Security Response Center (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040)

• NIST national vulnerability database (https://nvd.nist.gov/vuln/detail/CVE-2018-13379)

• NIST national vulnerability database (https://nvd.nist.gov/vuln/detail/CVE-2024-12812)

• NIST national vulnerability database (https://nvd.nist.gov/vuln/detail/CVE-2024-1708)

• NIST national vulnerability database (https://nvd.nist.gov/vuln/detail/CVE-2024-1709)