CIRT.GY Guyana National Computer Incident Response Team

AL2023_16 New malware used to steal data from Windows devices and phones (February 17, 2023)

Description

The APT threat group known as RedEyes is utilizing a new stealthy and evasive malware dubbed ‘M2RAT’ to steal data from Windows devices and phones.

Details

The supposedly state sponsored APT37 threat group (RedEyes) is a North Korean cyber espionage hack group that has been seen active in 2022 targeting specific entities with malware and exploiting vulnerabilities. Their last targets involved EU-based organizations, where RedEyes deployed their new version mobile backdoor called Dolphin and a custom Remote Access Trojan (RAT) called Konni. However, researchers at the AhnLab Security Emergency response Center (ASEC) recently discovered RedEyes using a new malware called ‘M2RAT’ that was seen capable of data exfiltration, command execution and evasive maneuvers to remain undetected.

ASEC stated that recent attacks began in January 2023, where RedEyes used phishing emails with malicious attachments to target victims. The phishing email contains an EPS file under the name ‘Form.hwp’, which is a file format used by Hancom Office; a Korean proprietary suite similar to Microsoft Office suite. An EPS file is a graphic file format that expresses a graphic image using the PostScript programming language, created by Adobe. High-definition vector images can be expressed through EPS, and the Hancom word processor supports a third-party module (ghostscript) that processes EPS. However, the vulnerability CVE-2017-8291 gives attackers access to the ghostscript module using a special crafted EPS file and grants them remote code execution.

RedEyes uses this exploit to gain initial access to victim’s devices, where they execute a shell code that downloads a JPEG image from the attacker’s C2 server containing malicious code. Researchers found that the RedEyes group made use of the steganography technique to hide a malicious portable executable (PE) file in the image. It is believed that this technique was used to evade network detection. The PE file is decrypted in the ‘temp’ folder as ‘lskdjfei.exe’ and the function of this file is to download the additional RAT malware M2RAT, inject the malware into the ‘explorer.exe’ process and add a ‘powershell’ and ‘mshta’ command to the registry Run key related to autorun to maintain persistence.

The M2RAT malware is executed through the explorer.exe process. This malware performs basic remote access trojan functions such as keylogging, data exfiltration, process execution/termination and screen capturing. The malware exfiltrates capture data directly to the attacker’s server and avoids making copies or storing any of the data on the victim’s device; it does this to leave no trace of data on the victim’s device. The malware receives commands from the attacker’s C2 server in the body of the POST method through specific commands.

C&C commands	**Explanation**
OKR	Commands received at the time of initial C&C communication connection
URL	Registry key value modification for C&C update
UPD	Update the C&C you are currently connected to
RES	C&C connection termination (M2RAT termination)
UNI	C&C connection termination (M2RAT termination)
CMD	Execute remote control commands (keylogging, process creation/execution, etc.)

The M2RAT malware creates a shared memory section to execute control commands received from the attacker’s C2 server. This technique is used to most likely evade network detection by concealing the command information in the POST body, similar to the steganography in the JPEG image. The CMD commands are delivered through the shared memory and the name of the memory section used are as follows:

Memory section name	**Function**
RegistryModuleInputMap2	Transmission of additional module execution results (ex. mobile phone data leakage module)
FileInputMap2	(A:\ ~ Z:\) Search drive files, create/write files, read files, change file time
CaptureInputMap2	Screen capture of current victim host PC
ProcessInputMap2	Check process list, process creation/termination

RawInputMap2	Executing a process using the ShellExectueExW API
TypingRecordInputMap2	Keylogging data leak
UsbCheckingInputMap2	USB data leak (hwp,doc,docx,xls,xlsx,ppt,pptx,cell,csv,show,hsdt,mp3,amr,3gp,m4a,txt,png,jpg,jpeg,gif,pdf,eml)

M2RAT also has the ability to scan for any portable devices connected to the infected computer, such as smartphones and tablets. It can scan the connected devices for files which can be copied and exfiltrated to the attacker's server. The copied data is then deleted once exfiltrated to remove any trace.

Indicators of Compromise

The MD5 hashes for the EPS file, JPEG image, and M2RAT malware are:

- 8b666fc04af6de45c804d973583c76e0 // (EPS) – Exploit/EPS.Generic (2023.01.16.03)
- 93c66ee424daf4c5590e21182592672e // (JPEG) – Data/BIN.Agent (2023.02.15.00)
- 7bab405fbc6af65680443ae95c30595d // (PE file - JPEG) Stage PE – Trojan/Win.Loader.C5359534 (2023.01.16.03)
- 9083c1ff01ad8fabbcd8af1b63b77e66 – Downloader/PS.Generic.SC185661 (2023.01.16.03)
- 4488c709970833b5043c0b0ea2ec9fa9 // (M2RAT) – Trojan/Win.M2RAT.C5357519 (2023.01 .14.01)
- 7f5a72be826ea2fe5f11a16da0178e54 // (Cell phone data theft) – Infostealer/Win.Phone.C5381667 (2023.02.14.03)

Remediation

To protect yourself against RAT attacks, especially the M2RAT that relies on phishing emails, we recommend being wary of suspicious emails and any attachments embedded. In this case, the attackers use a malicious document to initiate the infection, so it is always recommended to scan email attachments and disregard any attachments that seem suspicious.

If you are infected by a RAT, we recommend the following:

- Upon infection discovery, immediately disconnect the infected device from the network to prevent any malicious activities from occurring.

- Launch the device in safe mode and have a reputable anti-virus installed.
- Perform a full scan on the device and remove any threats detected.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B (2023, February 14). *RedEyes hackers use new malware to steal data from Windows, phones*. Retrieved from the BleepingComputer. https://www.bleepingcomputer.com/news/security/redeyes-hackers-use-new-malware-to-steal-data-from-windows-phones/
- M. (2023, February 14). *Hangeul (HWP) malware using steganography: RedEyes (ScarCruft)*. Retrieved from ASEC. https://asec-ahnlab-com.translate.goog/ko/47622/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp