RedEyes hackers use new malware to steal data from Windows, phones

By Bill Toulas

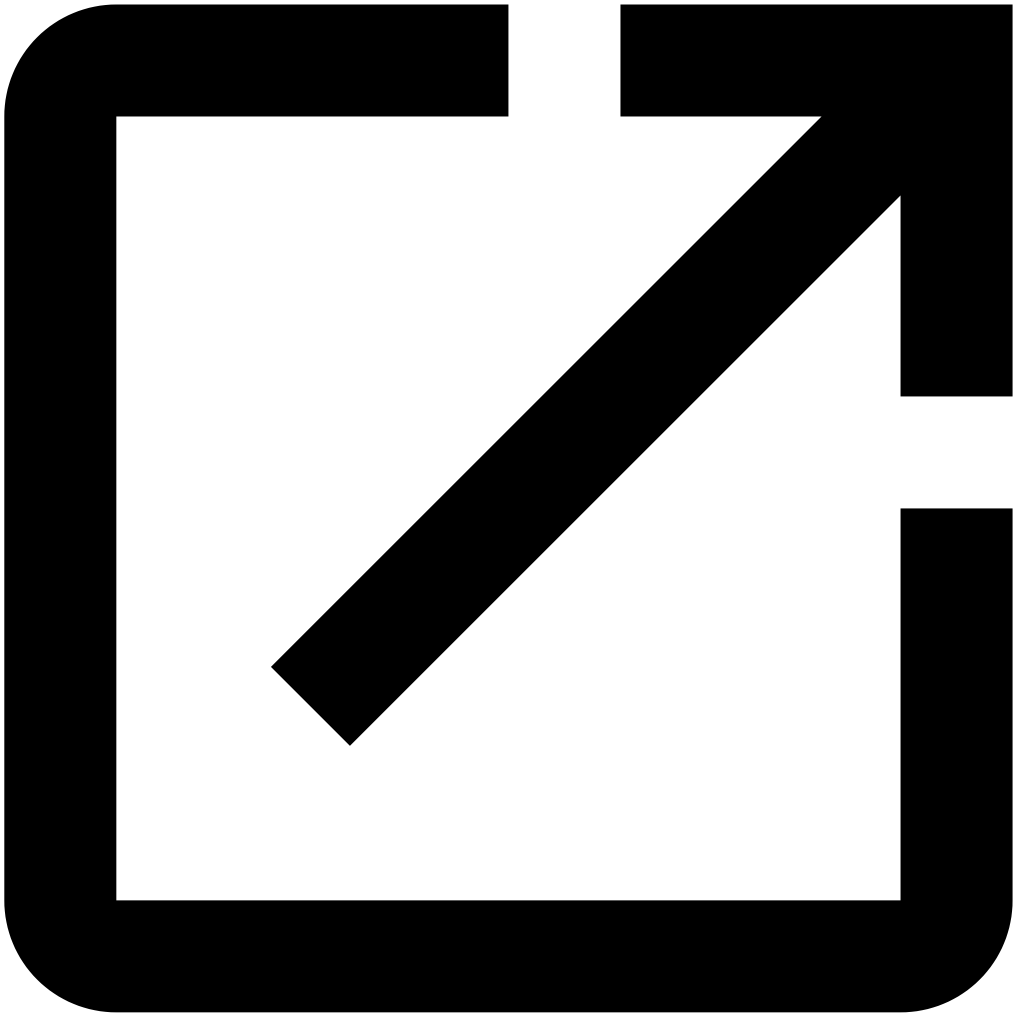
Published: 2023-02-14 · Archived: 2026-04-05 13:52:01 UTC

The APT37 threat group uses a new evasive 'M2RAT' malware and steganography to target individuals for intelligence collection.

APT37, also known as 'RedEyes' or 'ScarCruft,' is a North Korean cyber espionage hacking group believed to be state-supported.

In 2022, the hacking group was seen exploiting Internet Explorer zero-days and distributing a wide assortment of malware against targeted entities and individuals.


DIE LINKE.
0:00



For example, the threat actors targeted EU-based organizations with a new version of their mobile backdoor named 'Dolphin,' deployed a custom RAT (remote access trojan) called 'Konni,' and targeted U.S. journalists with a highly-customizable malware named 'Goldbackdoor.'

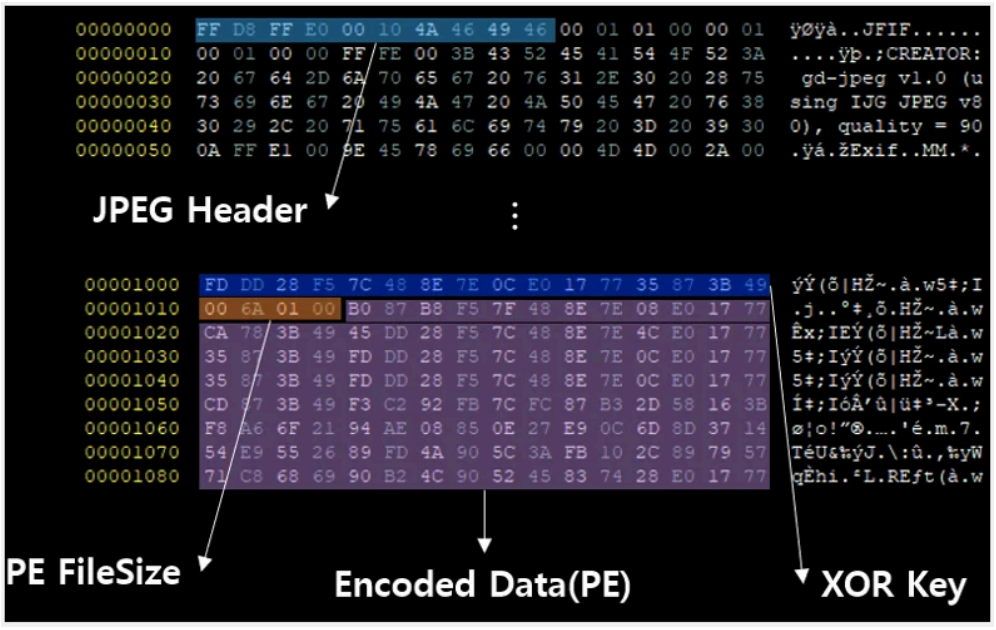
In a new report released today by AhnLab Security Emergency response Center (ASEC), researchers explain how APT37 is now using a new malware strain called 'M2RAT' that uses a shared memory section for commands and data exfiltration and leaves very few operational traces on the infected machine.

Starts with phishing

The recent attacks observed by ASEC started in January 2023, when the hacking group sent phishing emails containing a malicious attachment to their targets.

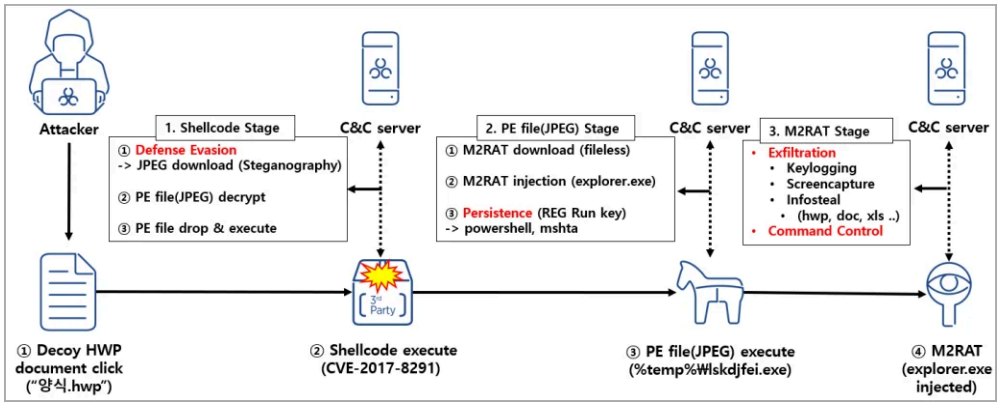
Opening the attachment triggers the exploitation of an old EPS vulnerability (CVE-2017-8291) in the Hangul word processor commonly used in South Korea. The exploit will cause shellcode to run on a victim's computer that downloads and executes a malicious executed stored within a JPEG image.

This JPG image file uses steganography, a technique that allows hiding code inside files, to stealthily introduce the M2RAT executable ("lskdjfei.exe") onto the system and inject it into "explorer.exe."



Malware code hiding in the JPEG file *(ASEC)*

For persistence on the system, the malware adds a new value ("RyPO") in the "Run" Registry key, with commands to execute a PowerShell script via "cmd.exe." This same command was also seen in a 2021 Kaspersky report about APT37.



APT37 attack flow *(ASEC)*

M2RAT steals from Windows and phones

The M2RAT backdoor acts as a basic remote access trojan that performs keylogging, data theft, command execution, and the taking of screenshots from the desktop.

The screenshot-snapping function is activated periodically and works autonomously without requiring a specific operator command.

The malware supports the following commands, which collect information from the infected device and then send it back to the C2 server for the attackers to review.

Section name	function
RegistryModuleInputMap2	Transfer of additional module run results (ex. Mobile phone data leak module)
FileInputMap2	(A:\~ Z:\) Drive file navigation, file creation/writing, file reading, file time change
CaptureInputMap2	Capture the current damage host PC screen
ProcessInputMap2	Process list verification, process creation/ending
RawInputMap2	Run the process using the ShellExectueExW API
TypingRecordInputMap2	Key logging 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)

Supported CMD commands *(ASEC)*

The malware's ability to scan for portable devices connected to the Windows computer, such as smartphones or tablets, is particularly interesting.

If a portable device is detected, it will scan the device's contents for documents and voice recording files and, if found, copy them to the PC for exfiltration to the attacker's server.

Before exfiltration, the stolen data is compressed in a password-protected RAR archive, and the local copy is wiped from memory to eliminate any traces.

Another interesting feature of M2RAT is that it uses a shared memory section for command and control (C2) communication, data exfiltration, and the direct transfer of stolen data to the C2 without storing them in the compromised system.

Using a memory section on the host for the above functions minimizes the exchange with the C2 and makes analysis harder, as security researchers have to analyze the memory of infected devices to retrieve the commands and data used by the malware.

In conclusion, APT37 continues to refresh its custom toolset with evasive malware that is challenging to detect and analyze.

This is especially true when the targets are individuals, like in the recent campaign spotted by ASEC, who lack larger organizations' sophisticated threat detection tools.

Source: https://www.bleepingcomputer.com/news/security/redeyes-hackers-use-new-malware-to-steal-data-from-windows-phones/