Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:55:25 UTC

Description(Kaspersky) If a Microsoft Office vulnerability is successfully exploited, the exploit creates an executable PE file on the hard drive and launches it for execution. The malicious program is a platform used to deploy extra (add-on) malicious modules, store them stealthily and thus add new capabilities for the threat actors. The attack unfolds in several stages, as described below:

1. The exploit is activated, and an appropriate (32-bit or 64-bit) version of the malicious program is installed on the victim computer, depending on the type of operating system installed on it. To do this installation, malicious code is injected into the system process ‘explorer.exe’ rather than into its memory. The malicious program has a modular structure: its main body is stored in the registry, while its add-on modules are downloaded following the instruction arriving from the C&C server. DLL hijacking (use of a modified system library) is used to ensure that the main module is launched each time the system is rebooted.
2. The main module of the malicious program receives an instruction to download and launch add-on modules, which opens new capabilities for the threat actors.
3. The malicious add-on modules provide opportunities to control the victim system, take screenshots of windows and intercept information entered from the keyboard. We have seen them in other cyber-espionage campaigns as well.
4. The threat actors use PowerSploit, a modified set of PowerShell scripts, and various utilities to steal files and passwords found on the victim computer.

The cybercriminals were primarily interested in .doc, .ppt, .xls, .docx, .pptx, .xlsx, .pdf, .txt and .rtf files on the victim computers. The harvested files were packed into a password-protected archive and sent to the threat actors’ server.

Overall, the tactics, techniques and procedures that the cybercriminals used in their attacks can hardly be considered complicated or expensive. However, there were a few things that caught our eye:

• The payload (at least one of the modules) is delivered using some simple steganography. Within traffic, it looks like a download of a regular JPEG image; however, the encrypted payload is loaded immediately after the image data. Microcin searches for a special ‘ABCD’ label in such a file; it is followed by a special structure, after which the payload comes, to be decrypted by Microcin. This way, new, platform-independent code and/or PE files can be delivered.
• If the Microcin installer detects the processes of some anti-malware programs running in the system, then, during installation, it skips the step of injecting into ‘explorer.exe’, and the modified system library used for establishing the malicious program within the system is placed into the folder %WINDIR%; to do this, the system app ‘wusa.exe’ is used with the parameter “/extract” (on operating systems with UAC).