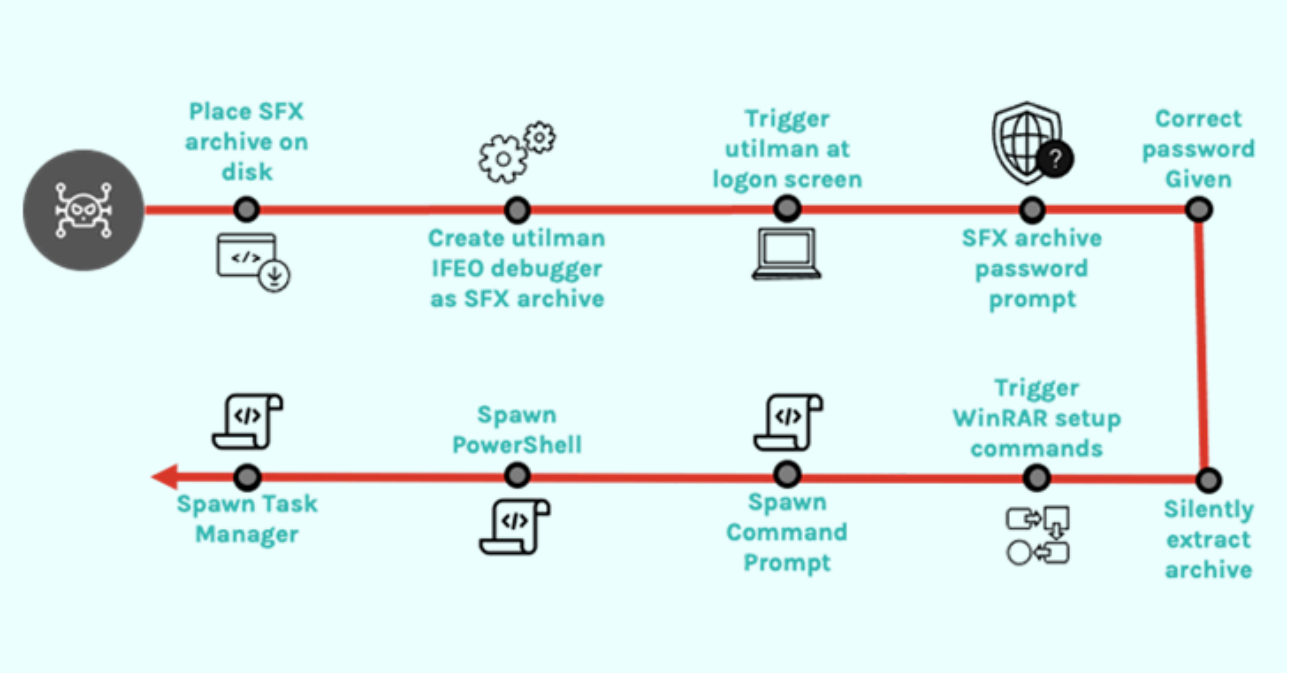
Hackers Using Self-Extracting Archives Exploit for Stealthy Backdoor Attacks

By The Hacker News

Published: 2023-04-05 · Archived: 2026-04-05 22:03:37 UTC



An unknown threat actor used a malicious self-extracting archive (SFX) file in an attempt to establish persistent backdoor access to a victim's environment, new findings from CrowdStrike show.

SFX files are capable of extracting the data contained within them without the need for dedicated software to display the file contents. It achieves this by including a decompressor stub, a piece of code that's executed to unpack the archive.

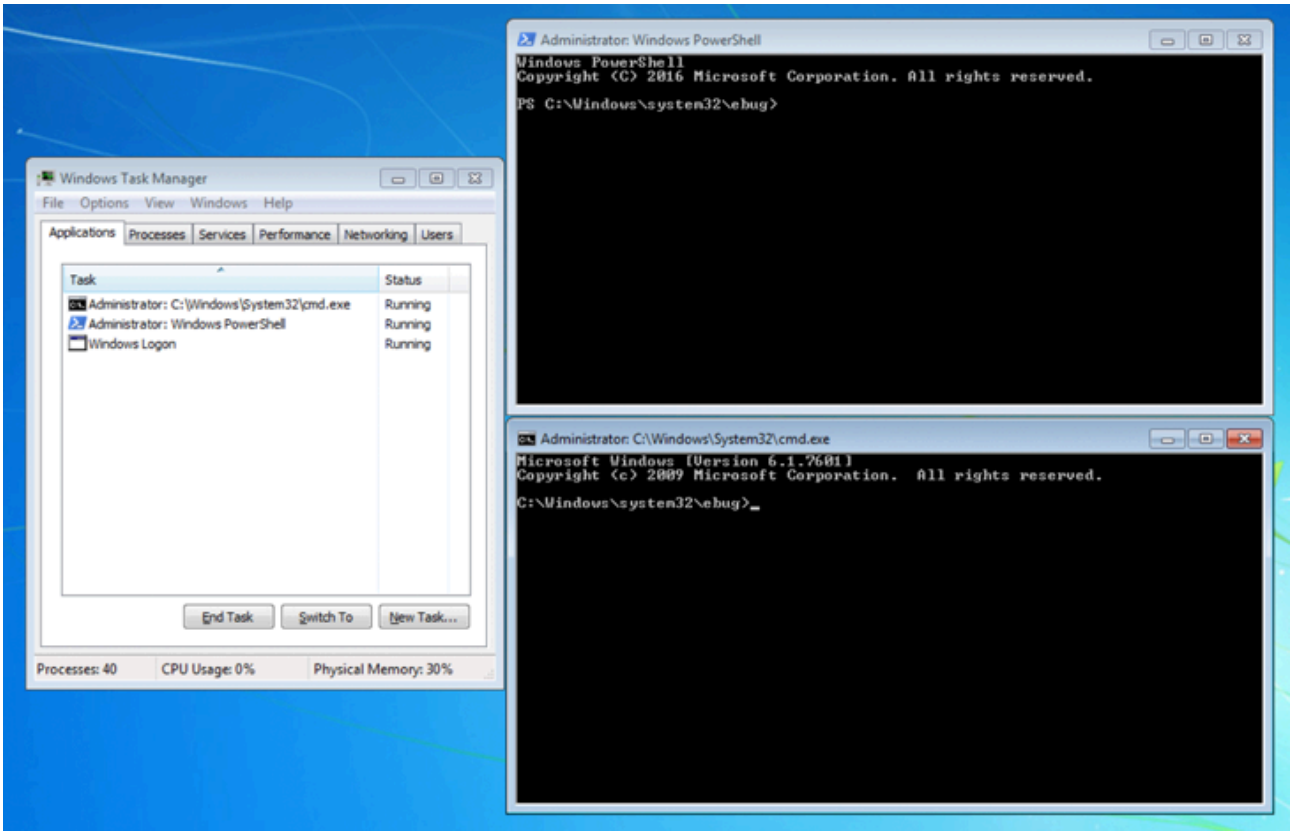
"However, SFX archive files can also contain hidden malicious functionality that may not be immediately visible to the file's recipient, and could be missed by technology-based detections alone," CrowdStrike researcher Jai Minton said.

In the case investigated by the cybersecurity firm, compromised credentials to a system were used to run a legitimate Windows accessibility application called Utility Manager (utilman.exe) and subsequently launch a password-protected SFX file.

This, in turn, is made possible by configuring a debugger (another executable) in the Windows Registry to a specific program (in this case, utilman.exe) so that the debugger is automatically started every time the program is launched.

The abuse of utilman.exe is also noteworthy as it can be launched directly from the Windows login screen by using the Windows logo key + U keyboard shortcut, potentially enabling threat actors to configure backdoors via the Image File Execution Options Registry key.

"Closer inspection of the SFX archive revealed that it functions as a password-protected backdoor by abusing WinRAR setup options rather than containing any malware," Minton explained.



Specifically, the file is engineered to run PowerShell (powershell.exe), Command Prompt (cmd.exe), and Task Manager (taskmgr.exe) with NT AUTHORITY\SYSTEM privileges by providing the right password to the archive.

"This type of attack is likely to remain undetected by traditional antivirus software that is looking for malware inside of an archive (which is often also password-protected) rather than the behavior from an SFX archive decompressor stub," Minton added.

This is not the first time SFX files have been employed in attacks as a means for attackers to stay undetected. In September 2022, Kaspersky disclosed a malware campaign that utilized links to such password-protected files to propagate RedLine Stealer.

A month later, the infamous Emotet botnet was observed sending out an SFX archive that, once opened by a user, would automatically extract a second password-protected SFX archive, enter the password, and execute its content without further user interaction using a batch script.

To mitigate threats posed by this attack vector, it's recommended that SFX archives are analyzed through unarchiving software to identify any potential scripts or binaries that are set to extract and run upon execution.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
