FIN8 Reemerges with New PoS Malware Badhatch

Archived: 2026-04-06 02:57:31 UTC

Security researchers found threat group FIN8 reappearing after two years with a new point-of-sale (PoS) malware named Badhatch, which is designed to steal credit card information. Researchers from Gigamon analyzed the sample and found similarities with PowerSniff, but Badhatch features new capabilities that allow it to scan for victim networks, provide attackers with remote access, install a backdoor, and deliver other modified malware payloads such as PoSlurp and ShellTea, among other features.

Badhatch begins infection much like its predecessor PowerSniff, by sending a customized phishing email via a weaponized Word document. Once the victim enables the macros, it executes PowerShells and shellcode scripts for PowerSniff, installing a backdoor in the process. Its network scan capability makes it different from PowerSniff; it is unable to check if the systems infected is in the education or healthcare sector. The researchers also noted that it lacks the sandbox detection and anti-virus analysis evasion features, as well as the long-term persistence tools that its predecessor had. However, they note that this also serves as an advantage as the attackers can execute the routine after infection and have greater control on how the malware can be used, thereby avoiding automated sandboxing features.

[Read: RawPOS: New behavior risks identity theft]

Capable of using an alternate command and control (C&C) server communication protocol, it continuously communicates every five minutes with the C&C for command instructions and tracks the completed operations.

ShellTea serves as an implant for multiple downloads and additional code execution, allowing the malware a stealthy foothold in the victim network for more payloads the attackers may decide to deploy. It also enables the malware to adapt to target environments via other HTTPS or DNS traffic.

PoSlurp scrapes credit card data processed by the PoS devices, including stored and encrypted card data prior to malware infection. Once the information is extracted from the infected system, the attackers can check and verify the validity of the data offline. PoSlurp also allows the attackers to inject other commands, access files, copy log files back to the server, and delete log files, among others.

[Read: MajikPOS combines PoS malware and RATs to pull off its malicious tricks]

As most PoS devices and systems run on embedded versions of Windows 7 and may not have applicable patches nor anti-virus products, simple malware attacks like these may still prove profitable for FIN8. Businesses and users can protect themselves from these threats with the following best practices:

- Regularly monitor financial and bank statements for fraudulent purchases. If users suspect their accounts being used for fraudulent transactions, they should contact their banks immediately.
- Be cautious of opening email attachments or clicking embedded URLs from known and unknown senders with suspicious requests. If the sender is a known contact, confirm the request via previously used communication channels.
- For legacy system users, check for virtual patches available from security vendors.
- Limit only specific software to run in the system.
- Install a multilayered protection systemproducts – especially network defense solutionsproducts – to protect all connected devices.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend
