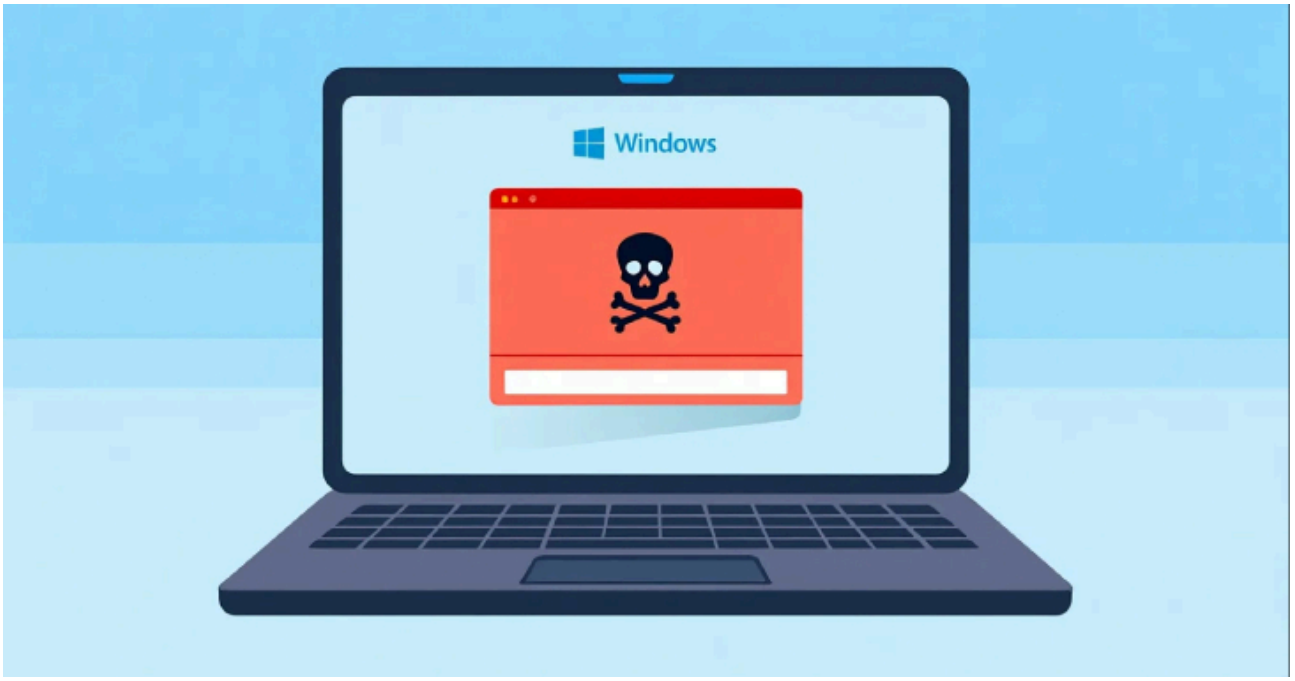
FIN7 Deploys Anubis Backdoor to Hijack Windows Systems via Compromised SharePoint Sites

By The Hacker News

Published: 2025-04-02 · Archived: 2026-04-05 21:49:53 UTC



The financially motivated threat actor known as FIN7 has been linked to a Python-based backdoor called Anubis (not to be confused with an Android banking trojan of the same name) that can grant them remote access to compromised Windows systems.

"This malware allows attackers to execute remote shell commands and other system operations, giving them full control over an infected machine," Swiss cybersecurity company PRODAFT said in a technical report of the malware.

FIN7, also called Carbon Spider, ELBRUS, Gold Niagara, Sangria Tempest, and Savage Ladybug, is a Russian cybercrime group known for its ever-evolving and expanding set of malware families for obtaining initial access and data exfiltration. In recent years, the threat actor is said to have transitioned to a ransomware affiliate.

In July 2024, the group was observed using various online aliases to advertise a tool called AuKill (aka AvNeutralizer) that's capable of terminating security tools in a likely attempt to diversify its monetization strategy.

Anubis is believed to be propagated via malspam campaigns that typically entice victims into executing the payload hosted on compromised SharePoint sites.

Delivered in the form of a ZIP archive, the entry point of the infection is a Python script that's designed to decrypt and execute the main obfuscated payload directly in memory. Once launched, the backdoor establishes communications with a remote server over a TCP socket in Base64-encoded format.

The responses from the server, also Base64-encoded, allow it to gather the IP address of the host, upload/download files, change the current working directory, grab environment variables, alter Windows Registry, load DLL files into memory using PythonMemoryModule, and terminate itself.

In an independent analysis of Anubis, German security company GDATA said the backdoor also supports the ability to run operator-provided responses as a shell command on the victim system.

"This enables attackers to perform actions such as keylogging, taking screenshots, or stealing passwords without directly storing these capabilities on the infected system," PRODAFT said. "By keeping the backdoor as lightweight as possible, they reduce the risk of detection while maintaining flexibility for executing further malicious activities."

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

Source: https://thehackernews.com/2025/04/fin7-deploys-anubis-backdoor-to-hijack.html