Microsoft: Notorious FIN7 hackers return in Clop ransomware attacks

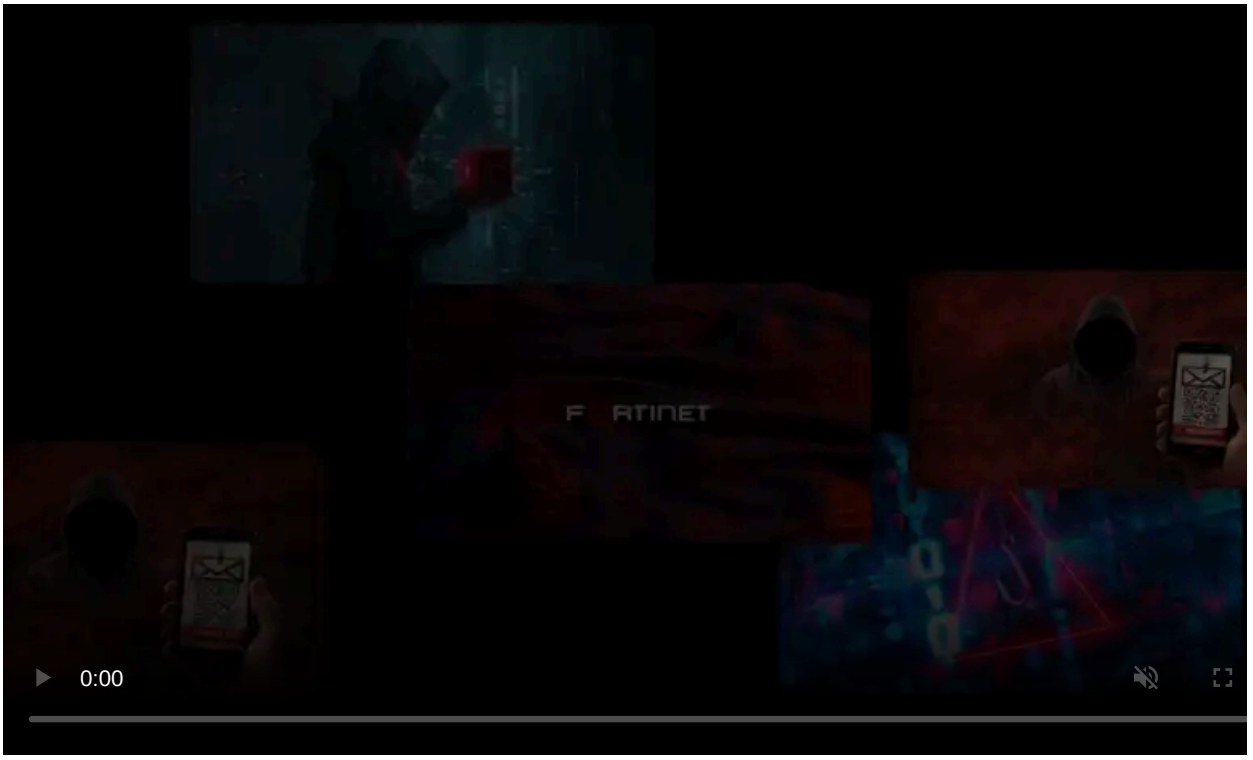
By Sergiu Gatlan

Published: 2023-05-19 · Archived: 2026-04-05 21:13:34 UTC

A cybercrime gang known as FIN7 resurfaced last month, with Microsoft threat analysts linking it to attacks where the end goal was the deployment of Clop ransomware payloads on victims' networks.

"Financially motivated cybercriminal group Sangria Tempest (ELBRUS, FIN7) has come out of a long period of inactivity," the company said in a series of tweets from the Microsoft Security Intelligence Twitter account.

"The group was observed deploying the Clop ransomware in opportunistic attacks in April 2023, its first ransomware campaign since late 2021."


F RTINET
0:00

In these recent attacks, FIN7 attackers utilized the PowerShell-based POWERTRASH in-memory malware dropper to deploy the Lizar post-exploitation tool on compromised devices.

This allowed the threat actors to gain a foothold within the targeted network and move laterally to deploy Clop ransomware using OpenSSH and Impacket. This legitimate Python toolkit can also be used for remote service execution and relay attacks.

According to Microsoft, Clop ransomware is just the newest strain the cybercrime gang has used to target victims.

The group has been previously linked to REvil and Maze ransomware before their involvement in the now-defunct BlackMatter and DarkSide ransomware-as-a-service (Raas) operations.

FIN7 tools used in PaperCut attacks

According to a private Microsoft threat analytics report seen by BleepingComputer, FIN7 was also linked to attacks targeting PaperCut printing servers with Clop, Bl00dy, and LockBit ransomware.

Microsoft saw the FIN11 financial crime group it tracks as Lace Tempest was seen employing new tooling, including the inv.ps1 PowerShell script the company connected to FIN7.

The script was used to deploy FIN7's Lizar post-exploitation kit, likely that the two threat groups' operators have recently started teaming up or sharing their tools in attacks.

Arrests, teddy bears, and ransomware

Since it started operating a decade ago, in 2013, the FIN7 financially-motivated hacking group has been linked to attacks mainly targeting banks and the point-of-sale (PoS) terminals of companies from various industry sectors (predominantly restaurants, gambling, and hospitality) in Europe and the United States.

The FBI has warned U.S. companies of USB drive-by attacks coordinated by FIN7, targeting the U.S. defense industry with packages containing malicious USB devices designed to deploy ransomware.

FIN7 operators have also impersonated Best Buy in similar attacks with malicious flash drives via USPS to hotels, restaurants, and retail businesses, packages that also bundled teddy bears to trick the targets into lowering their guard.

Although some FIN7 members have been arrested over the years, the hacking group is still active and going strong, as evidenced by this new round of attacks reported by Microsoft.

In April 2022, FIN7 "pen tester" Denys Iarmak was sentenced to 5 years in prison for network breaches and credit card theft attacks spanning at least two years.

Iarmak was the third FIN7 member sentenced in the U.S. after Andrii Kolpakov (another "pen tester") was sent to prison for seven years in June 2021, and Fedir Hladyr (a high-level manager) received a ten years sentence in April 2021.

Update: Added info on FIN7 tools adopted by FIN11.
