Microsoft links Scattered Spider hackers to Qilin ransomware attacks

By Sergiu Gatlan

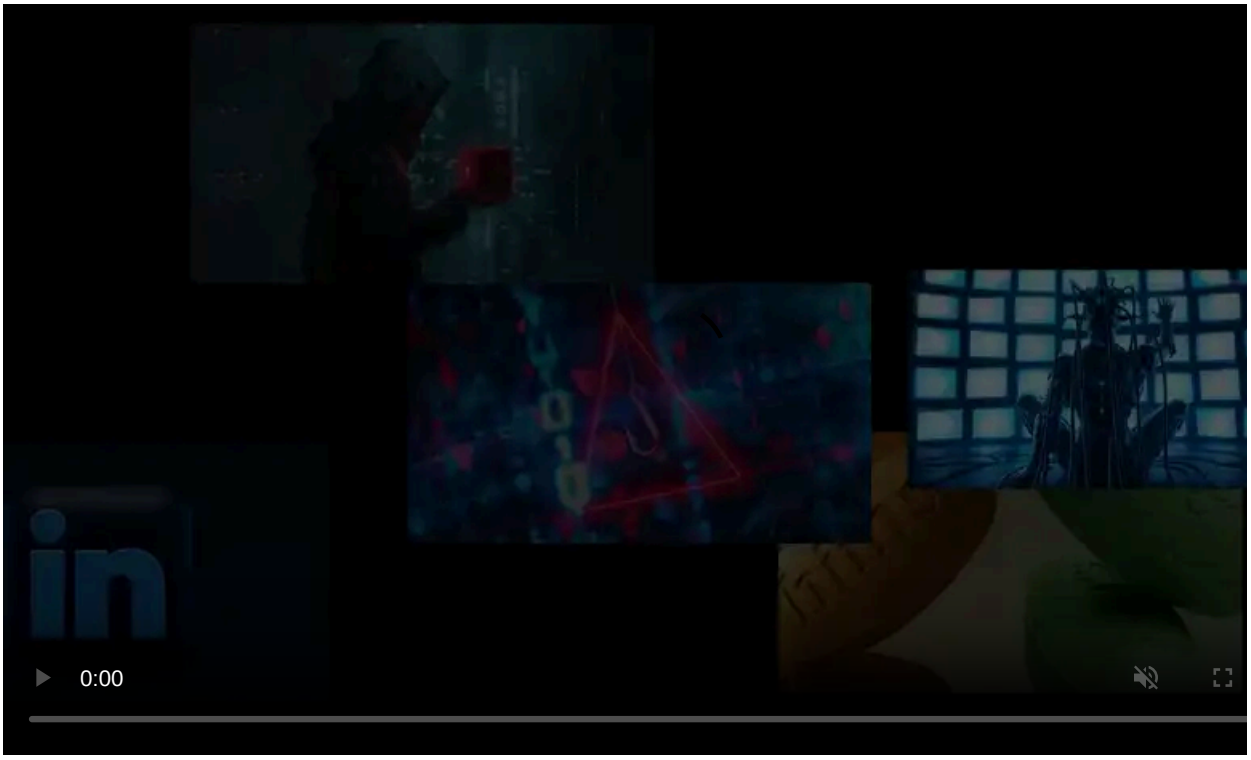
Published: 2024-07-16 · Archived: 2026-04-05 17:58:39 UTC

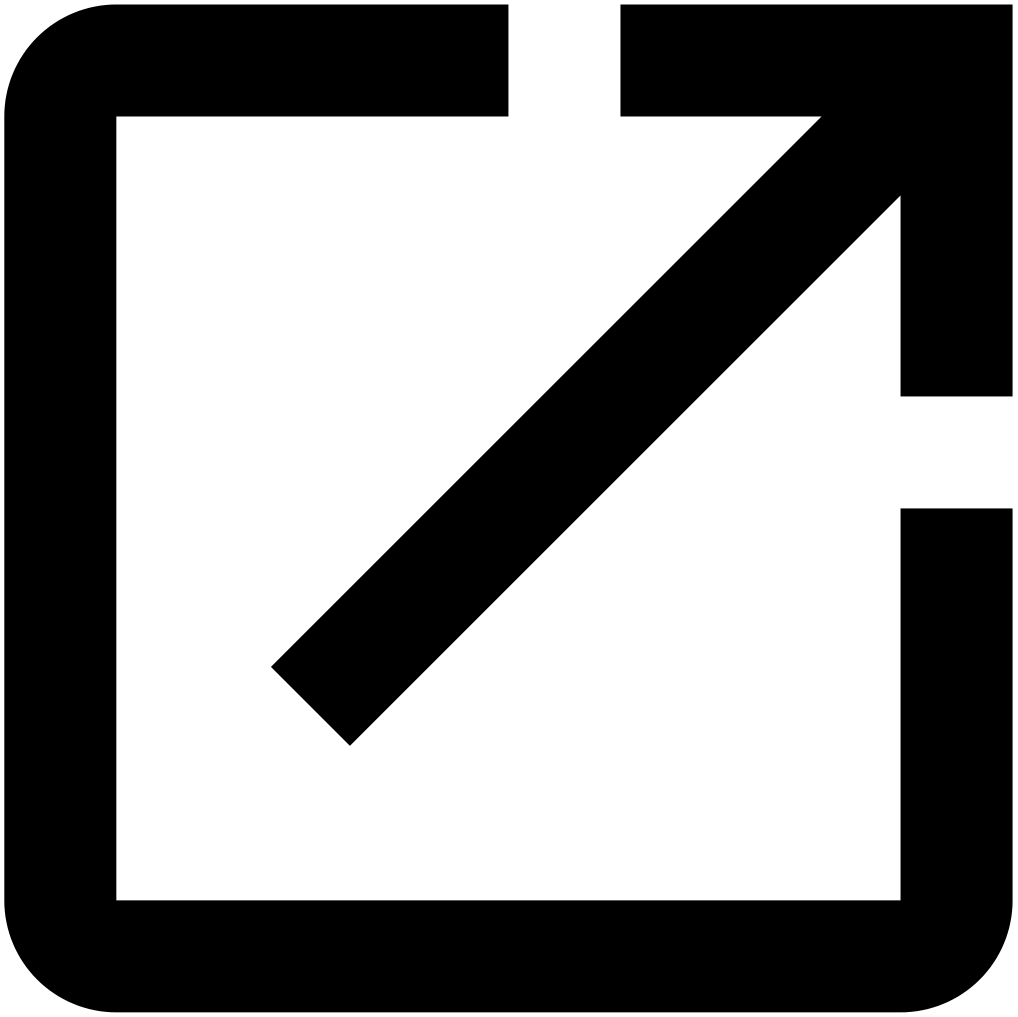
Image: Midjourney

Microsoft says the Scattered Spider cybercrime gang has added Qilin ransomware to its arsenal and is now using it in attacks.

"In the second quarter of 2024, financially motivated threat actor Octo Tempest, our most closely tracked ransomware threat actor, added RansomHub and Qilin to its ransomware payloads in campaigns," Microsoft said Monday.

After surfacing in early 2022, this threat group (also tracked as Octo Tempest, UNC3944, and 0ktapus) achieved notoriety following their 0ktapus campaign that targeted over 130 high-profile organizations, including Microsoft, Binance, CoinBase, T-Mobile, Verizon Wireless, AT&T, Slack, Twitter, Epic Games, Riot Games, and Best Buy.


0:00



The English-speaking gang has also encrypted MGM Resorts' systems after joining BlackCat/ALPHV ransomware as an affiliate in mid-2023 and was linked by Symantec to the RansomHub ransomware-as-a-service.

In November, the FBI and CISA issued an advisory highlighting Scattered Spider's tactics, techniques, and procedures (TTPs). These include impersonating IT employees to trick customer service staff into providing them with credentials or gaining persistence on targets' networks using remote access tools.

Other tactics they're known to use for initial network access include phishing, MFA bombing (aka MFA fatigue), and SIM swapping.

Scattered Spider's move to ransomware attacks (Microsoft)

The Qilin ransomware operation that Scattered Spider just joined surfaced in August 2022 under the "Agenda" name but was rebranded as Qilin just one month later.

Over the last two years, the Qilin gang has claimed over 130 companies on its dark web leak site; however, their operators weren't active until attacks picked up towards the end of 2023.

Since December 2023, Qilin has also been developing one of the most advanced and customizable Linux encryptors to target VMware ESXi virtual machines, which enterprise organizations favor for their light resource needs.

Like many other ransomware groups targeting businesses, Qilin operators infiltrate a company's networks and extract data as they move through the victim's systems.

After obtaining admin credentials and collecting all sensitive data, they deploy the ransomware payloads to encrypt all network devices and leverage the stolen data to carry out double-extortion attacks.

So far, BleepingComputer has seen Qilin ransom demands ranging from as low as $25,000 to millions of dollars, depending on the victim's size.

Last month, the CEO of the UK's National Cyber Security Centre (NCSC) linked Qilin to a ransomware attack that hit pathology services provider Synnovis in early June and impacted several major NHS hospitals in London, forcing them to cancel hundreds of operations and appointments.

Source: https://www.bleepingcomputer.com/news/security/microsoft-links-scattered-spider-hackers-to-qilin-ransomware-attacks/