US charges five linked to Scattered Spider cybercrime gang

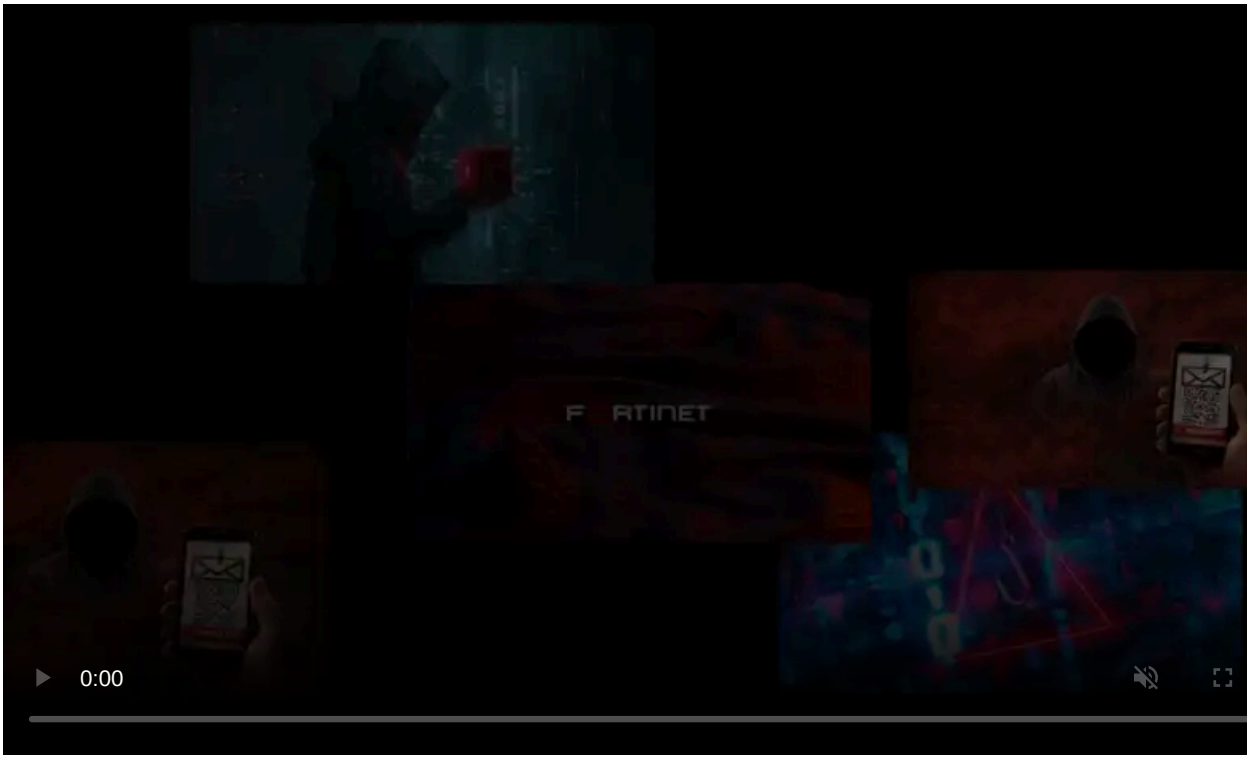
By Sergiu Gatlan

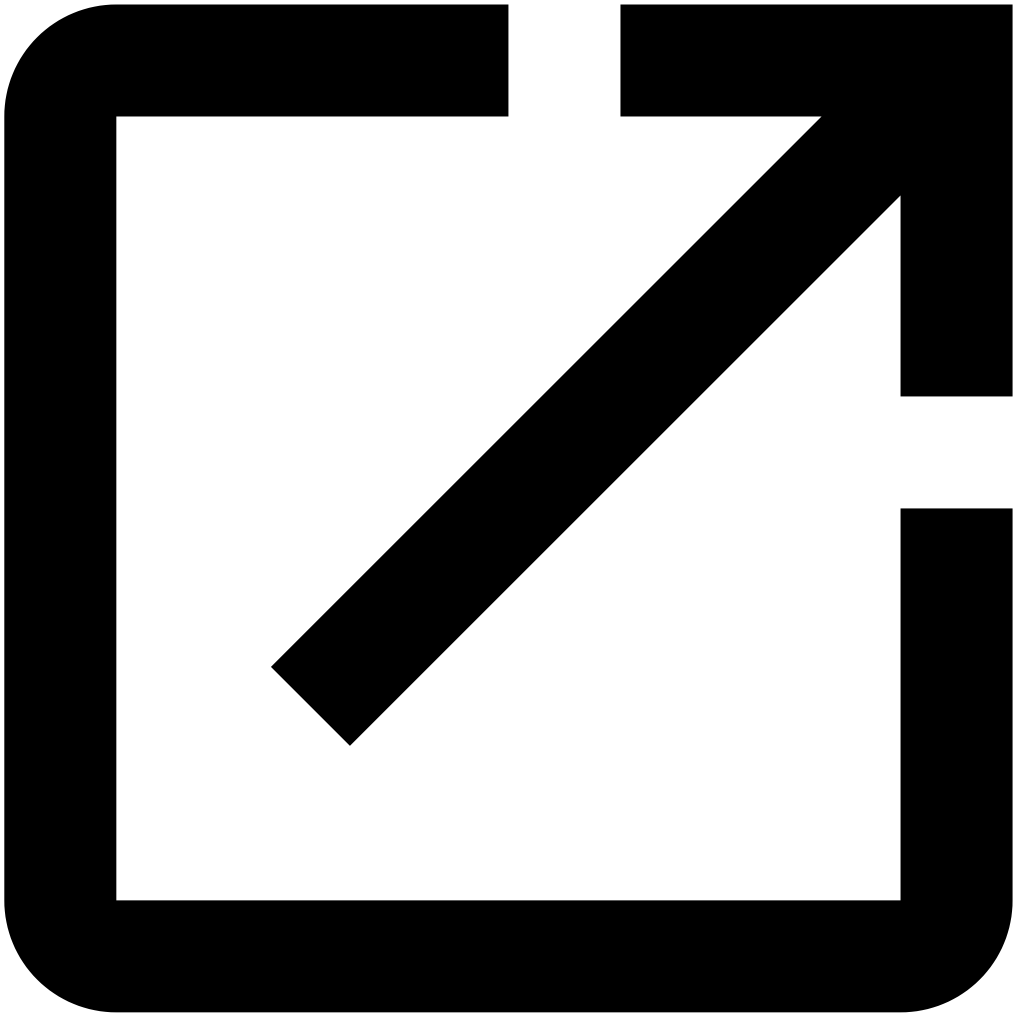
Published: 2024-11-20 · Archived: 2026-04-05 20:35:54 UTC

The U.S. Justice Department has charged five suspects believed to be part of the financially motivated Scattered Spider cybercrime gang with conspiracy to commit wire fraud.

Between September 2021 and April 2023, they were able to steal millions from cryptocurrency wallets using victims' credentials stolen in SMS phishing attacks targeting dozens of targets, including both individuals and companies.

Scattered Spider specializes in social engineering attacks, impersonating help desk technicians, and using phishing/smishing attacks to steal credentials from targeted companies' employees. In an attack on an interactive entertainment products and software company, the threat actors sent phishing messages that warned employees their VPN was being deactivated and to visit a site to reactivate it.


F RTINET
0:00



"WARNING!! Your [Victim Company 1] VPN is being deactivated, to keep your VPN active, please head over to [Victim Company 1]-vpn.net," the phishing message said. Other phishing campaigns pretended to be password change notifications, prompting recipients to click a link if they did not change their password.

According to court documents, they also used credentials stolen from hacked companies' employees to exfiltrate confidential data, including databases, "confidential work product, intellectual property, and personal identifying information" from their systems.

This information was later used to hijack their victims' email accounts in SIM swap attacks that allowed them to gain control over their phone numbers and virtual currency wallets to transfer millions to wallets under their control.

These five suspects now face charges of wire fraud, wire fraud conspiracy, and aggravated identity theft:

- Ahmed Hossam Eldin Elbadawy, 23, a.k.a. “AD,” of College Station, Texas;
- Noah Michael Urban, 20, a.k.a. "Sosa" and "Elijah," of Palm Coast, Florida;
- Evans Onyeaka Osiebo, 20, of Dallas, Texas;
- Joel Martin Evans, 25, a.k.a. "joeleoli," of Jacksonville, North Carolina;
- Tyler Robert Buchanan, 22, of the United Kingdom.

"We allege that this group of cybercriminals perpetrated a sophisticated scheme to steal intellectual property and proprietary information worth tens of millions of dollars and steal personal information belonging to hundreds of thousands of individuals," said United States Attorney Martin Estrada in a Wednesday press release.

If convicted, each defendant faces up to 20 years in prison for conspiracy to commit wire fraud, five years for the conspiracy charge, and a mandatory two-year consecutive sentence for aggravated identity theft. Buchanan also faces up to 20 years for the wire fraud charge.

What is Scattered Spider?

Security vendors and organizations also track scattered Spider as 0ktapus, Scatter Swine, Octo Tempest, Starfraud, UNC3944, and Muddled Libra.

However, even though most think of it as a cohesive group, Scattered Spider is a loose-knit group of English-speaking threat actors, some as young as 16, with varied skill sets. They orchestrate various types of attacks and communicate using the same Telegram channels, Discord servers, and hacker forums.

Some Scattered Spider members are also believed to be part of "the Com," another hacking collective linked to cyberattacks and violent incidents. This fluid organizational structure makes it challenging for law enforcement to monitor their activities and to attribute specific attacks to a particular cybercrime gang or threat actor.

In a 2023 advisory, the FBI said they're known for using various tactics to breach corporate networks, including social engineering, phishing, multi-factor authentication (MFA) bombing (targeted MFA fatigue), and SIM swapping.

Since the start of 2023, Scattered Spider has also partnered with several Russian ransomware gangs, including BlackCat/AlphV, Qilin, and RansomHub.

In July, UK police also arrested a 17-year-old suspect, believed to be a Scattered Spider hacking collective member who was involved in the 2023 MGM Resorts ransomware attack. Other high-profile attacks linked to this cybercrime gang include those on Caesars, DoorDash, MailChimp, Twilio, Riot Games, and Reddit.

Source: https://www.bleepingcomputer.com/news/security/us-charges-five-linked-to-scattered-spider-cybercrime-gang/