US arrests Scattered Spider suspect linked to telecom hacks

By Sergiu Gatlan

Published: 2024-12-05 · Archived: 2026-04-05 13:10:31 UTC

U.S. authorities have arrested a 19-year-old teenager linked to the notorious Scattered Spider cybercrime gang who is now charged with breaching a U.S. financial institution and two unnamed telecommunications firms.

Remington Goy Ogletree (also known online as "remi") breached the three companies' networks using credentials stolen in text and voice phishing messages targeting their employees.

He also impersonated the victims' IT support departments in calls designed to pressure the employees into accessing phishing sites where they were asked to enter their user names and passwords.


DIE LINKE.
0:00

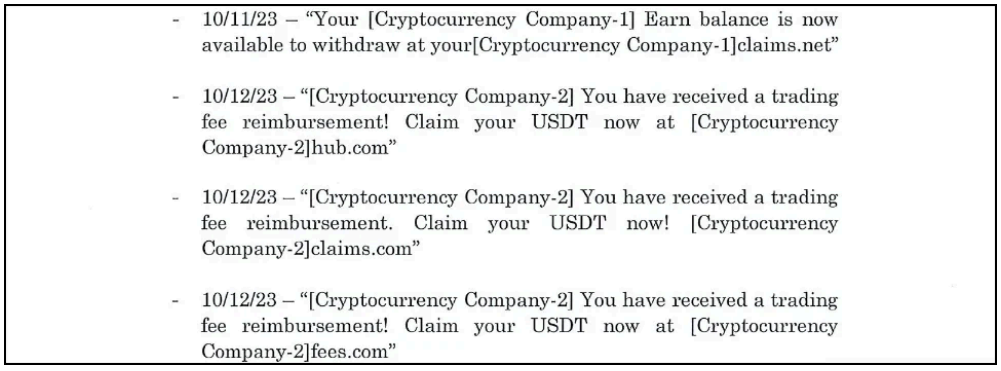
The U.S. financial institution allegedly hacked by Ogletree told the FBI that roughly 149 of its employees were targeted in a phishing campaign (between late October 2023 and mid-November 2023) that redirected them to phishing landing pages impersonating the company.

These phishing websites were designed to ask the targeted employees to enter credentials they used to access the financial institution's systems.

"A review of screenshots of the phishing messages revealed statements intended to mislead the employees into providing their credentials, including fraudulent messages claiming their 'employee benefits package [was] updated' and 'your employee schedule has been modified'," the complaint reads.

"Some of the phishing messages told employees that they had 'an inquiry from HR' or that their 'VPN profile was updated'."

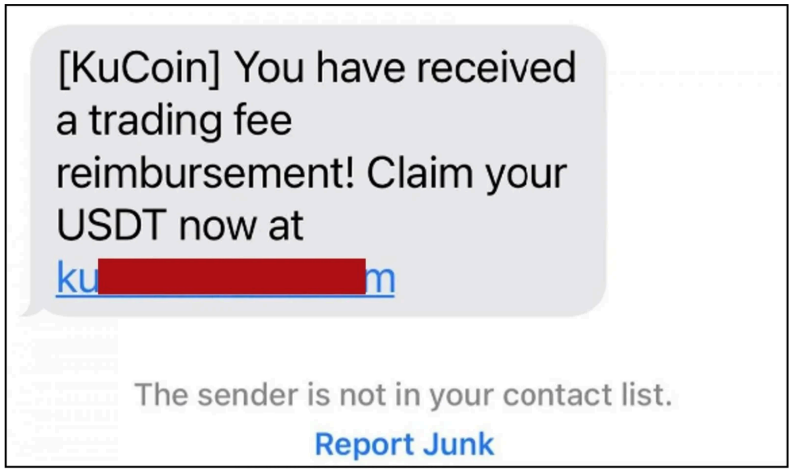
Also, between October 2023 and May 2024, Ogletree used his access to the telecoms' systems to send over 8.6 million phishing text messages to phone numbers across the United States designed to help steal recipients' cryptocurrency.



- 10/11/23 – "Your [Cryptocurrency Company-1] Earn balance is now available to withdraw at your[Cryptocurrency Company-1]claims.net"
- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement! Claim your USDT now at [Cryptocurrency Company-2]hub.com"
- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement. Claim your USDT now! [Cryptocurrency Company-2]claims.com"
- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement! Claim your USDT now at [Cryptocurrency Company-2]fees.com"

Crypto-themed phishing messages sent by Ogletree (US DOJ)

As Trend Micro reported in October 2023, some of these attacks targeted the customers of legitimate crypto platforms Gemini and KuCoin using the yourgeminiclaims[.]net and kucoinclaims[.]com domains.



KuCoin phishing text message (Trend Micro)

In February, while searching his residence in Forth Worth, Texas, the FBI found extensive proof of Ogletree's criminal activity on his seized iPhone, including screenshots of phishing texts impersonating a tech company, screenshots of credential harvesting phishing pages, and screenshots of crypto wallets with tens of thousands of dollars in cryptocurrency.

During his subsequent interview with the FBI, Ogletree said he knew "people who commit all sorts of crimes" and "key Scattered Spider members," adding that the hacking group targets business process outsourcing (BPO) companies because "they have less security" than the companies they work for.

Previous Scattered Spider arrests

Last month, the U.S. Justice Department arrested and charged five other suspects linked to the cybercrime gang who allegedly stole millions in cryptocurrency using SMS phishing attacks targeting dozens of targets.

These five suspects face charges of wire fraud, wire fraud conspiracy, and aggravated identity theft, each facing at least 20 years in prison:

- 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.

UK police also arrested a 17-year-old suspect in July, believed to be part of the Scattered Spider hacking collective who was involved in the 2023 MGM Resorts ransomware attack.

Other high-profile attacks linked to this hacking group include those on Caesars, MailChimp, Twilio, DoorDash, Riot Games, and Reddit.

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

What is Scattered Spider?

Security vendors also track the financially motivated Scattered Spider cybercrime gang as 0ktapus, UNC3944, Scatter Swine, Octo Tempest, and Muddled Libra.

This group of English-speaking threat actors, some as young as 16, has a fluid organizational structure and communicates via the same Telegram channels, Discord servers, and hacker forums to coordinate and orchestrate various attacks.

Some of its members are also believed to be part of "the Com," another hacking collective previously linked to violent incidents and cyberattacks.

The groups' loose-knit organization makes it harder for law enforcement to keep track of their criminal activity and attribute specific attacks to a specific gang member.

The FBI says they're using various tactics to breach corporate networks, including phishing, social engineering, SIM swapping, and multi-factor authentication (MFA) bombing (targeted MFA fatigue).

Source: https://www.bleepingcomputer.com/news/security/us-arrests-scattered-spider-suspect-linked-to-telecom-hacks/