Hackers switch to targeting U.S. insurance companies

By Ionut Ilascu

Published: 2025-06-16 · Archived: 2026-04-05 13:29:11 UTC

Threat intelligence researchers are warning of hackers breaching multiple U.S. companies in the insurance industry using all the tactics observed with Scattered Spider activity.

Typically, the threat group has a sector-by-sector focus. Previously, they targeted retail organizations in the United Kingdom and then switched to targets in the same sector in the United States.

“Google Threat Intelligence Group is now aware of multiple intrusions in the US which bear all the hallmarks of Scattered Spider activity. We are now seeing incidents in the insurance industry,” John Hultquist, Chief Analyst at Google Threat Intelligence Group (GTIG), told BleepingComputer.


DIE LINKE.
0:00

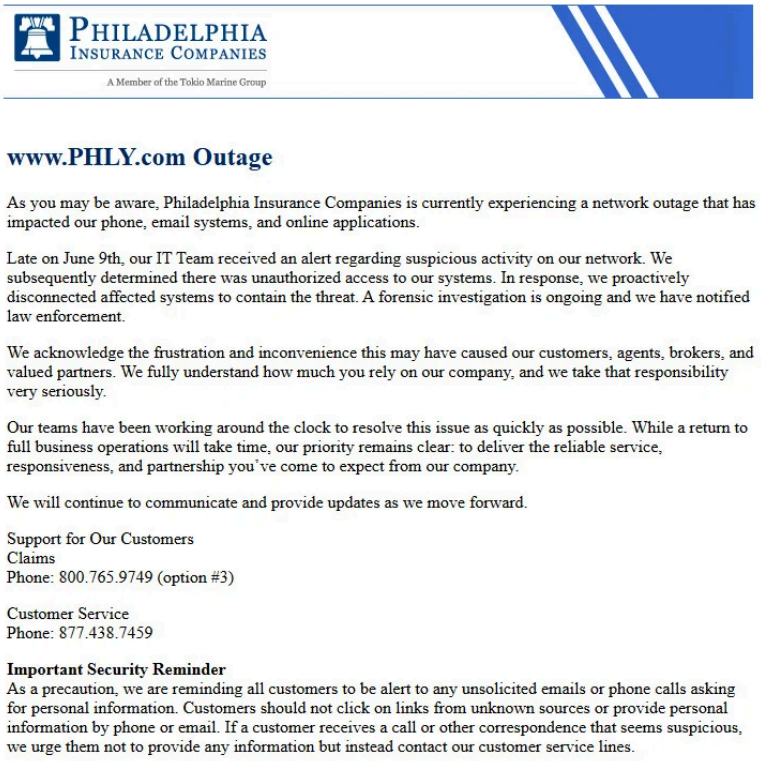
Hultquist warns that because the group approaches one sector at a time, “the insurance industry should be on high alert.”

GTIG’s chief researcher says that companies should pay particular attention to potential social engineering attempts on help desk and call centers.

Just this month, two insurance companies disclosed that their systems were impacted by cyberattacks.

Philadelphia Insurance Companies (PHLY) announced that on June 9 it discovered unauthorized access on its network and disconnected the affected systems to stop the attack from spreading.

The outage continues as the company's website still shows the outage notification.


PHILADELPHIA INSURANCE COMPANIES
A Member of the Tokio Marine Group

www.PHLY.com Outage

As you may be aware, Philadelphia Insurance Companies is currently experiencing a network outage that has impacted our phone, email systems, and online applications.

Late on June 9th, our IT Team received an alert regarding suspicious activity on our network. We subsequently determined there was unauthorized access to our systems. In response, we proactively disconnected affected systems to contain the threat. A forensic investigation is ongoing and we have notified law enforcement.

We acknowledge the frustration and inconvenience this may have caused our customers, agents, brokers, and valued partners. We fully understand how much you rely on our company, and we take that responsibility very seriously.

Our teams have been working around the clock to resolve this issue as quickly as possible. While a return to full business operations will take time, our priority remains clear: to deliver the reliable service, responsiveness, and partnership you've come to expect from our company.

We will continue to communicate and provide updates as we move forward.

Support for Our Customers
Claims
Phone: 800.765.9749 (option #3)

Customer Service
Phone: 877.438.7459

Important Security Reminder
As a precaution, we are reminding all customers to be alert to any unsolicited emails or phone calls asking for personal information. Customers should not click on links from unknown sources or provide personal information by phone or email. If a customer receives a call or other correspondence that seems suspicious, we urge them not to provide any information but instead contact our customer service lines.

Philadelphia Insurance Companies (PHLY) alerts of outage caused by unauthorized access

Erie Insurance also suffered business disruptions that started on June 7. A few days later, the company reported in a filing wiht the U.S. Securities and Exchange Commission that the outage was caused "unusual network activity," which prompted an immediate protection response for systems and data.

Scattered Spider tactics

Scattered Spider is the name given to a fluid coalition of threat actors that employ sophisticated social engineering attacks to bypass mature security programs.

The group is also tracked as 0ktapus, UNC3944, Scatter Swine, Starfraud, and Muddled Libra, and has been linked to breaches at multiple high-profile organizations that mixed phishing, SIM-swapping, and MFA fatigue/MFA bombing for initial access.

In a later stage of the attack, the group has been observed dropping ransomware like RansomHub, Qilin, and DragonForce.

Defending against Scattered Spider attacks

Organizations defending against this type of threat actor should start with gaining complete visibility across the entire infrastructure, identity systems, and critical management services.

GTIG recommends segregating identities and using strong authentication criteria along with rigorous identity controls for password resets and MFA registration.

Since Scattered Spider relies on social engineering, organizations should educate employees and internal security teams on impersonation attempts via various channels (SMS, phone calls, messaging platforms) that may sometimes include aggressive language to scare the target into compliance.

After hackers breached Marks & Spencer, Co-op, and Harrods retailers in the U.K. this year, the country's National Cyber Security Centre (NCSC) shared tips for organizations to improve their cybersecurity defenses.

In all three attacks, the threat actor used the same social engineering tactics associated with Scattered Spired and dropped DragonForce ransomware in the final stage.

NCSC's recommendations include activating two-factor or multi-factor authentication, monitoring for unauthorized logins, and checking if access to Domain Admin, Enterprise Admin, and Cloud Admin accounts is legitimate.

Additionally, the U.K. agency advises that organizations review how the helpdesk service authenticates credentials before resetting them, especially for employees with elevated privileges.

The ability to identify logins from unusual sources (e.g. VPN services from residential ranges) could also help identify a potential attack.

Update [June 17]: *Added information about cyberattacks on two insurance companies in the United States.*
