Blurring Lines Between Scattered Spider & Russian Cybercrime

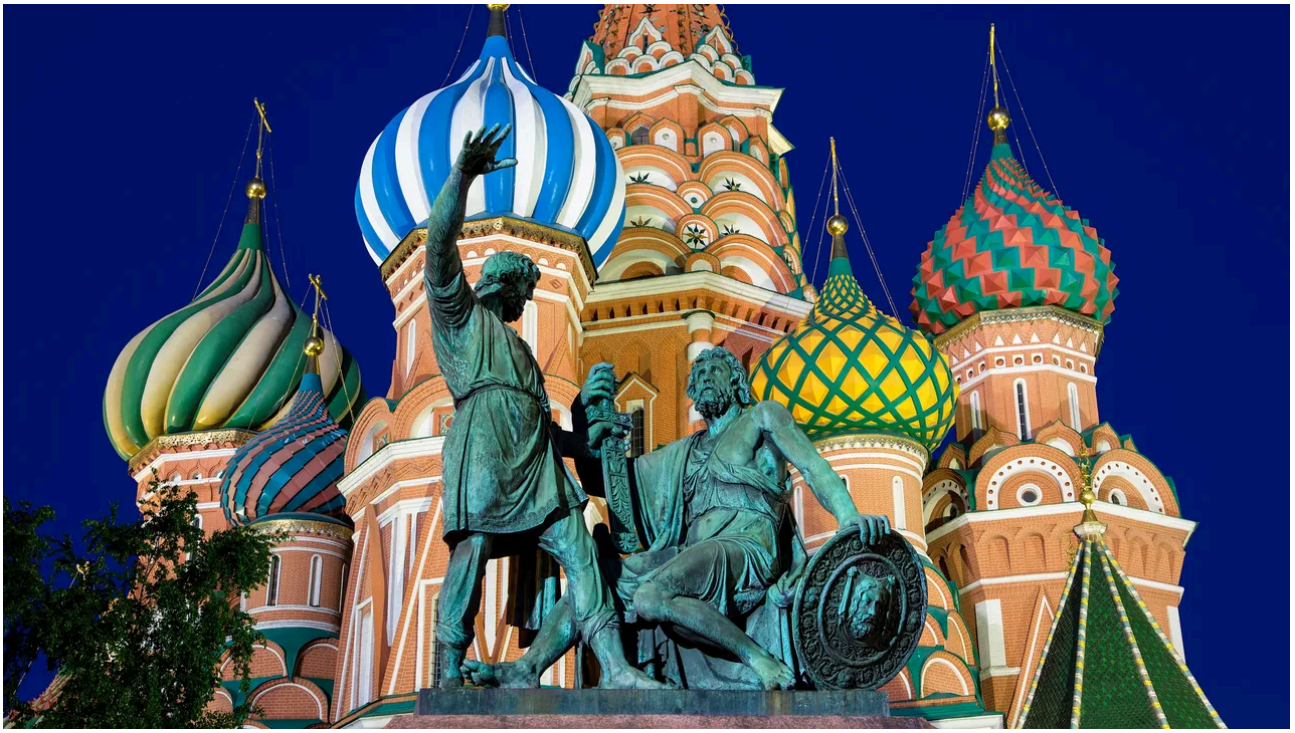
By Rob Wright

Published: 2025-05-22 · Archived: 2026-04-05 16:18:10 UTC

Rob Wright,Senior News Director,Dark Reading

May 22, 2025

6 Min Read



Jonathan Kellerman, Alamy

Law enforcement actions in 2024 were supposed to disrupt Scattered Spider. Instead, the notorious cybercrime group re-emerged this year and is trending in a direction that has alarmed some infosec experts.

The arrests of several alleged members of Scattered Spider last year, including the group's supposed ringleader, may have led to a temporary dip in malicious activity. But not only have Scattered Spider's high-profile attacks continued this year, but the group has seemingly shifted further into the Russian ransomware ecosystem.

Scattered Spider, also known as UNC3944 and Octo Tempest, first emerged in 2022 and is primarily composed of native English-speaking individuals, many of whom are under the age of 25. That distinction set the group apart from other notorious cybercrime outfits, many of which are based in Eastern Europe and include Russian-speaking actors.

It also made Scattered Spider formidable, as members of the group displayed a knack for elaborate social engineering schemes such as SIM-swapping, or phishing or vishing attacks, where they pose as IT help desk staff. In 2023, Scattered Spider achieved notoriety after two high-profile cyberattacks on Las Vegas casino giants MGM Resorts and Caesars Entertainment.

Related:Not Toying Around: Hasbro Attack May Take 'Weeks' to Remediate

The two attacks were notable not only because the group of "Advanced Persistent Teenagers" had graduated to full-fledged ransomware attacks, using a variant offered by the ALPHV/BlackCat ransomware-as-a-service (RaaS) group. It was also notable because, as Check Point Software's Cyberint noted in a recent report, the RaaS gang had previously declared that it only works with Russian-speaking affiliates.

Scattered Spider was also tied to the formerly prolific but now-defunct RansomHub group. More recently, the cybercriminal collective delved even further into the ransomware ecosystem by partnering with the emerging DragonForce RaaS operation, which reportedly assumed control of RansomHub's operations.

The deepening ties with the Russian cybercrime scene has sparked concern among threat analysts and raised questions about the composition of the group and the individuals that may be influencing it.

Scattered Spider Spins a New Web?

The recent cyberattacks on three UK retailers – Marks & Spencer, Harrods and Co-Op Group – served as a wakeup call for some when it comes to Scattered Spider. While DragonForce claimed responsibility for the attacks, some security researchers suspect Scattered Spider members were involved.

Cyberint's report noted that it is "increasingly likely" that members of the group were involved in early-stage intrusions of the UK retailers, and warned that Scattered Spider members are also targeting US retail organizations. "Known for its cloud-first, identity-centric intrusion methods, Scattered Spider is emerging as a likely access broker or collaborator within the DragonForce affiliate model," wrote Adi Bleih, security researcher, external risk management at Check Point Software Technologies.

Related:Bank Trojan 'Casbaneiro' Worms Through Latin America

Bleih tells Dark Reading that Scattered Spider has continued to align with Russian-speaking ransomware groups. "This transition indicates an ongoing strategy of collaboration with Russian-speaking entities to leverage their ransomware capabilities," he says.

The deeper collaboration with ransomware gangs, especially DragonForce, is concerning, according to Zach Edwards, senior threat researcher at Silent Push. Scattered Spider actors had previously used off-the-shelf malware, such as the Vidar and Raccoon infostealers, that displayed some level of customization, he says.

But using such publicly available tools carries risk for threat actors because it may not perform as well as custom-built malware, and could increase the chances of detection in high-profile intrusions. DragonForce, however, offers a customizable affiliate model with white-label ransomware kits that allow members to compile their own binaries and take advantage of exclusive tools and infrastructure to support attacks.

Related:AI-Powered 'DeepLoad' Malware Steals Credentials, Evades Detection

This, Edwards says, shows Scattered Spider has shifted toward "triple A"-level tools and tactics this year, which makes the group more dangerous.

"Now that they're partnering with a much more serious ransomware group and getting access to malware that's not for sale publicly, that's exactly the evolution that a lot of us were hoping wouldn't happen," he says. "But it really seems to be occurring."

It also raises questions about why major ransomware operations would choose to work with affiliate hackers that are native English speakers, especially in the wake of increased law enforcement actions.

Potential Russian Influences Within Scattered Spider

Security researchers have different theories about why secretive ransomware operators, which typically favor Russian speaking individuals, would work closely with members of a loosely-affiliated hacker group, which itself is part of a larger collective known as "The Com" that is made up of mostly younger US and UK citizens.

Bleih says the close collaboration with Russian-speaking ransomware groups raises three possibilities: they are straightforward affiliate partnerships; the groups have some kind of shared operational infrastructure; or there's "a blurring of boundaries between groups, possibly involving multilingual intermediaries."

"While their use of platforms like Telegram and Discord, along with fluent English during extortion communications, points to a primarily Western-based group, the nature of today's interconnected cybercriminal ecosystem — especially on dark web forums — allows threat actors to easily recruit collaborators who speak Russian or other languages as needed," Bleih says.

Edwards says the mystery around Scattered Spider's ransomware alliances speaks to a bigger problem for the infosec community – a lack of awareness about how Scattered Spider operates, if it even does function as an actual group, and how it recruits new members. Existing members don't typically discuss operations or sensitive matters on public Telegram chats like other cybercriminal groups, so visibility is limited.

Additionally, Edwards said that despite the arrests of alleged members in 2024, including accused ringleader Tyler Buchanan, other budding cybercriminals in the US and UK that are seemingly eager to join Scattered Spider. But the affiliate alliance with DragonForce suggests there may other, older individuals within both Scattered Spider and The Com.

"The Com is mostly younger people, 13 to 25 years old, but there were always rumblings that there were older people in their 30s and 40s who were the orchestrators," Edwards says. "There are potentially older people within this group who don't have Western ties, who are absolutely English-speaking individuals but have ties to the Russian cybercriminal underworld."

Is Scattered Spider being influenced by Russian-speaking ransomware figures? Push Security researcher Dan Green says it's an interesting question but one that's difficult to answer. Based on attack trends, he says, the group has shown a consistent pattern of identity-based intrusions, specifically takeovers of highly privileged accounts on

identity platforms like Okta and Microsoft's Entra. These techniques have been used to great success, including the casino attacks in 2023.

"I think that Scattered Spider has been influenced generally by the evolution in identity-based techniques we've seen in the past few years," Green says, the successes of which likely made a huge impact on the group and the larger Com collective.

But he says the affiliation with DragonForce shows Scattered Spider is adaptable and "willing to use anything at their disposal to achieve their goals," including Russian ransomware groups.

On thing that threat analysts appear to agree on with Scattered Spider is that the law enforcement actions had little to no effect. And they urge organizations to be vigilant not just about the group's trademark social engineering tactics, such as MFA bombing and attacker-in-the-middle phishing schemes, but other newer techniques like the use of dynamic DNS providers to generate spoofed domains of popular brands.

"They're trying new things," Edwards says, "and they're just as aggressive as ever before."

Don't miss the latest Dark Reading Confidential podcast, The Day I Found an APT Group in the Most Unlikely Place, where threat hunters Ismael Valenzuela and Vitor Ventura share stories about the tricks they used to track down advanced persistent threats, and the surprises they discovered along the way. Listen now!

About the Author

Senior News Director, Dark Reading

Rob Wright is a longtime reporter with more than 25 years of experience as a technology journalist. Prior to joining Dark Reading as senior news director, he spent more than a decade at TechTarget's SearchSecurity in various roles, including senior news director, executive editor and editorial director. Before that, he worked for several years at CRN, Tom's Hardware Guide, and VARBusiness Magazine covering a variety of technology beats and trends. Prior to becoming a technology journalist in 2000, he worked as a weekly and daily newspaper reporter in Virginia, where he won three Virginia Press Association awards in 1998 and 1999. He graduated from the University of Richmond in 1997 with a degree in journalism and English. A native of Massachusetts, he lives in the Boston area.
