CHUBB®

Cyber Threat Intelligence Report Q2 2025

Stack up your cyber
protection with Chubb.

As cyber threats evolve, Chubb is committed to keeping you well informed and help keep our mutual clients protected. Indicative of this commitment, the Chubb Threat Intelligence Report delivers quarterly insights on emergent cyber threats and recommendations to mitigate them.

Ivanti Exploit Chain

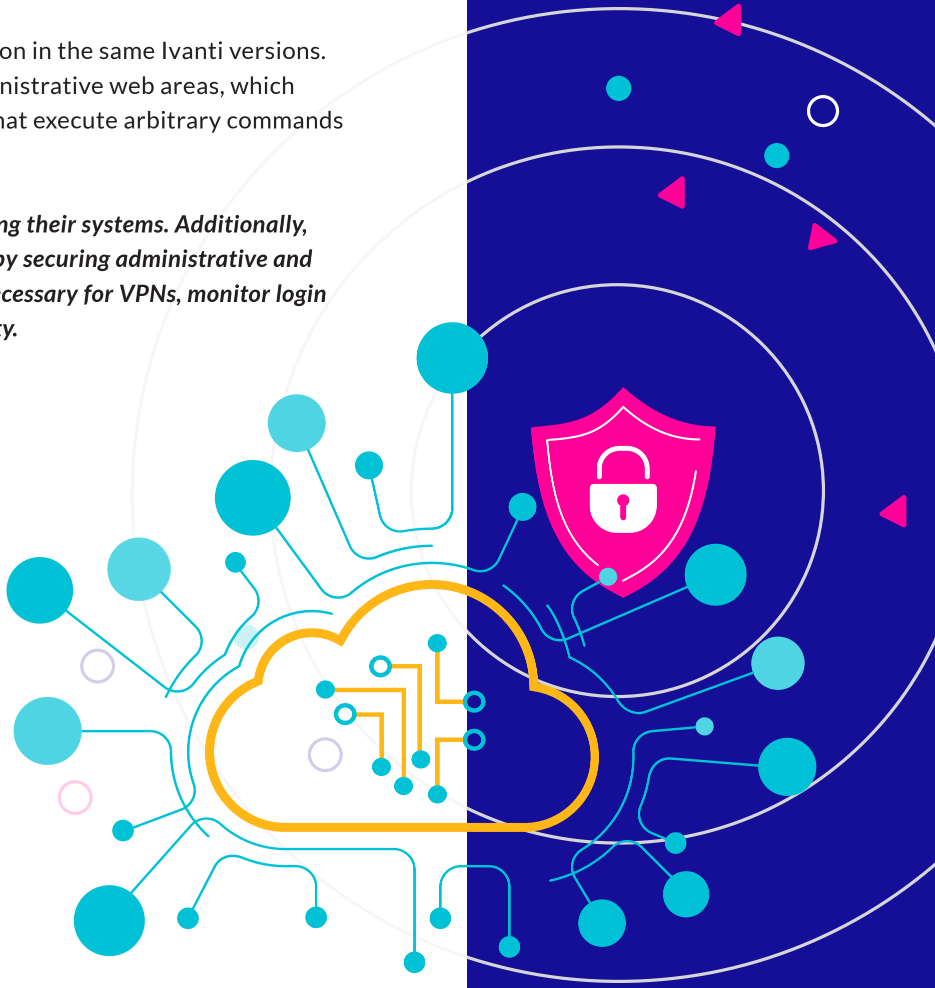
Two critical vulnerabilities in Ivanti software are currently being exploited through an exploit chain – a sequence of multiple exploits used to bypass a system's security measures that is commonly used by threat actors.

> **Exploit chains are a sequence of multiple exploits used to bypass a system's security measures.**

CVE-2023-46805 (CVSS 8.2) allows attackers to bypass authentication in the web-based components of Ivanti Connect Secure and Policy Secure, versions 9.x and 22.x. Improper URL handling enables unauthorized access to restricted systems and sensitive administrative areas without valid credentials.

CVE-2024-21887 (CVSS 9.1) permits command injection in the same Ivanti versions. It results from unsafe handling of input in certain administrative web areas, which allows an attacker to send specially crafted requests that execute arbitrary commands as a system administrator.

Companies using Ivanti software should prioritize patching their systems. Additionally, policyholders should strengthen their VPN technologies by securing administrative and service accounts. If internet-accessible login pages are necessary for VPNs, monitor login attempts closely and set lockout limits to enhance security.



Sources: *CISA*, *Ivanti*, *NVD*, *NVD*, *Vicarius*, *WIZ*

THREAT ALERT

Akira Ransomware Attacks - and How To Thwart Them

Akira has emerged as the most active cybercrime gang in 2025. A recent notable exploit compromised a victim's webcam and deployed ransomware via Server Message Block (SMB), a standard protocol for file sharing.[1]

Typical Akira attacks, however, tend to be more straightforward. The usual targets are small to medium-sized businesses with annual revenues between $10 million and $50 million. The attackers often gain network access by brute-forcing the victim's VPN technology or using compromised credentials. Akira has also been known to exploit vulnerabilities such as CVE-2023-48788, CVE-2024-2176, or CVE-2024-40766. Two of these vulnerabilities target management interfaces for populate VPNs. Once inside, they typically move laterally using Remote Desktop Protocol (RDP) and deploy ransomware within about six hours of initial network access.

It became apparent in many Akira-related claims that Multi-Factor Authentication (MFA) was not implemented for all VPN accounts, including default administrative and local accounts and weak service account security. In addition, most claims involved policyholders who expected to be protected by Microsoft Defender XDR.

> **In many Akira-related claims, MFA was not implemented for all VPN accounts, including default admin and local accounts.**

A typical Akira attack can be thwarted at several stages. Implementing robust MFA and prioritizing patching and monitoring of VPN technologies can help prevent initial access. Strengthening Server Message Block (SMB) security and deploying a well-configured Endpoint Detection and Response (EDR) solution can stop lateral movement within the network.

Source: ***Surefire incident response data, Chubb analysis.***

[1] *https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypted-network-from-a-webcam-to-bypass-edr/*

THREAT ALERT

The Weak Link in Cybersecurity: Humans

In May 2025, a series of attacks targeted major US and UK retail giants.[2] While direct evidence is scarce, all indications point to a campaign orchestrated by the group known as "Scattered Spider." This group was initially known for SIM-swapping attacks where unauthorized SIM changes bypassed phone authentication. It has now evolved into a global threat by leveraging social engineering techniques primarily targeting IT help desks.

Scattered Spider gains access through well-crafted phone calls to technical support employees or urgent requests seemingly from C-suite executives. AI voice-generation technologies are sometimes used to mimic the voice and cadence of an employee's speech. Phishing frameworks and typo-squatting are also used to capture credentials and session tokens and effectively to bypass MFA.

Social engineering and phishing – attacks that exploit human vulnerabilities – account for 37% of attacks in claims and incident response data. According to IBM, 79% of credential thefts arise from social engineering attacks.

The Best Defense

The following controls can help organizations shore up their defense against social engineering attacks targeting help desk staff:

- **Train all employees, including help desk staff, to recognize attacks.**
- **Enforce strict identity controls for password resets and MFA registration. For instance, restrict help desks from registering new devices for MFA. When resetting passwords, split new passwords between managers and the requesting employees.**
- **Require that new devices be connected to the internal network when registering. Strengthen authentication criteria by removing SMS, phone calls, and email authentication methods.**
- **Limit the hours during which the help desk performs password resets; consider restricting this to business hours.**
- **Implement additional security controls to prevent threat actors from fraudulently obtaining employment verification through human resources.**

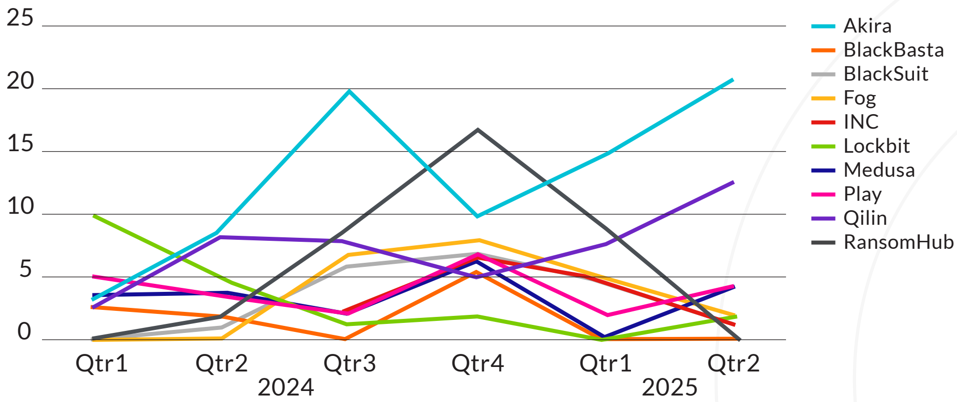
> Social engineering and phishing - attacks that exploit human vulnerabilities - account for 37% of attacks in claims and incident response data.

Sources: *KnowBe4 "Cyber Insurance and Security: Meeting the Rising Threat", IBM Cost of a Data Breach 2024, Chubb Analysis*

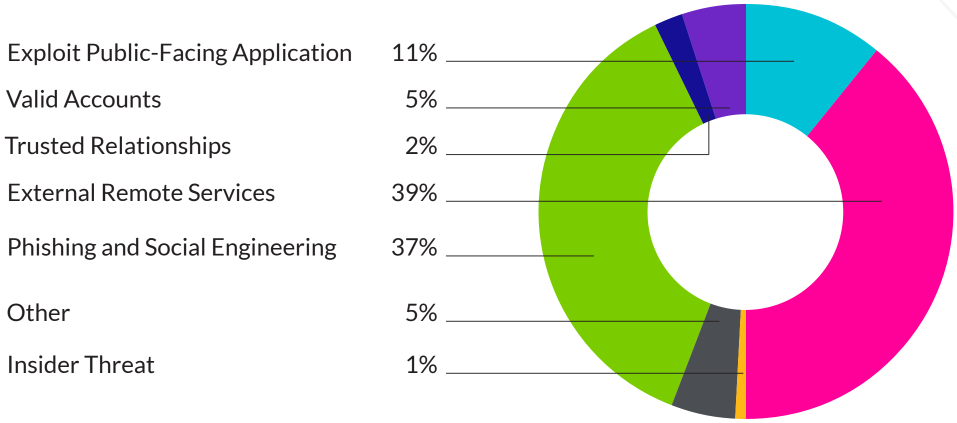
[2] *https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations?hl=en*

Claims Data and Statistics

Akira and Qilin have dominated the ransomware landscape since 2024. Both groups typically target VPNs using brute force, credential stuffing, and exploiting vulnerabilities. Qilin often relies on data obtained from infostealers. Ransomhub, which had been the leading threat actor, vanished after being hacked by the DragonForce ransomware gang in April 2025.[3]



The primary methods of compromise have remained consistent since Q4 2024: External remote services, phishing, and social engineering are the main attack vectors – each accounting for nearly 40% of incidents. Use of valid accounts has increased, likely due to the rise in infostealers and abuse of trusted relationships, possibly linked to the trend in supply chain attacks.



Be aware that access to an external remote service can be gained through phishing, using a valid account, or even by an insider. While VPN attacks are typically considered "external remote services," they could also be reclassified under "valid accounts" when involving brute-forcing or credential stuffing or "exploiting public-facing applications" when vulnerabilities in VPN technologies are targeted. Hardening VPN technologies has become increasingly important as the number of incidents targeting VPN continue to rise.Policyholders should enforce MFA, secure or remove local accounts, limit the public IP space with access to VPN, lock accounts after repeated failed authentication attempts, and prioritize patching of VPN technologies.

Source: ***Surefire, Chubb incident response data***

[3] *https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/*

Harden VPN by enforcing MFA, securing or removing local accounts, limiting the public IP space with access to VPN, locking accounts after repeated failed login attempts, and prioritizng patching.

CHUBB®

Chubb offers an array of cyber services, including incident response, vulnerability management, user security awareness training, and endpoint security protection, all aimed at helping organizations mitigate exposure and reduce cyber risk. **Learn more.**

chubb.com

This document is advisory in nature and is offered as a resource to be used together with your professional IT and insurance advisors in maintaining a loss prevention program. It is an overview only, and is not intended as a substitute for consultation with your insurance broker, or for professional IT, legal, engineering or other professional advice. Chubb hereby disclaims any liability for the accuracy, completeness or applicability of the loss control information provided and disclaims any obligation to oversee or monitor any systems or insured's adherence to any guidance or practices.