CHUBB®

Cyber Threat Intelligence Report H1 2025

Stack up your cyber protection with Chubb.

As cyber threats evolve, Chubb is committed to keeping you informed and helping our clients and partners stay protected. This Chubb Threat Intelligence Report delivers insights on current and emerging cyber threats and recommendations to mitigate them.

Critical Vulnerabilities in File Transfer Application: Cleo file transfer (CVE-2024-50623)

File transfer applications are increasingly attractive targets for ransomware groups due to the essential role they play in business operations and the wealth of confidential information they store. Another managed file transfer vulnerability led to widespread exploitation during 2024 and into 2025 Q1. Identified as CVE-2024-50623, the critical-severity vulnerability affected Cleo file transfer software and it allowed attackers to upload and download files from these applications without restrictions, posing significant risk to organisations.

Although a patch was released in late October 2024, the Clop ransomware group managed to bypass it by late November, successfully exploiting the vulnerability in three products: Cleo Harmony, VLTrader, and LexiCom. This exploitation can lead to unrestricted file uploads and downloads, potentially resulting in remote code execution and allowing attackers to take control of affected systems.

In December 2024, Chubb's Threat Intelligence Team identified widespread exploitation of Cleo file transfer software by the Clop group and issued an urgent alert regarding CVE-2024-50623 and another associated vulnerability, CVE-2024-55956. This situation emphasises the critical need to stay informed about vulnerabilities affecting file transfer applications and implement robust security measures to protect sensitive information.

This situation emphasises the critical need to stay informed about vulnerabilities affecting file transfer applications and implement robust security measures to protect sensitive information.

Source: *Darktrace*

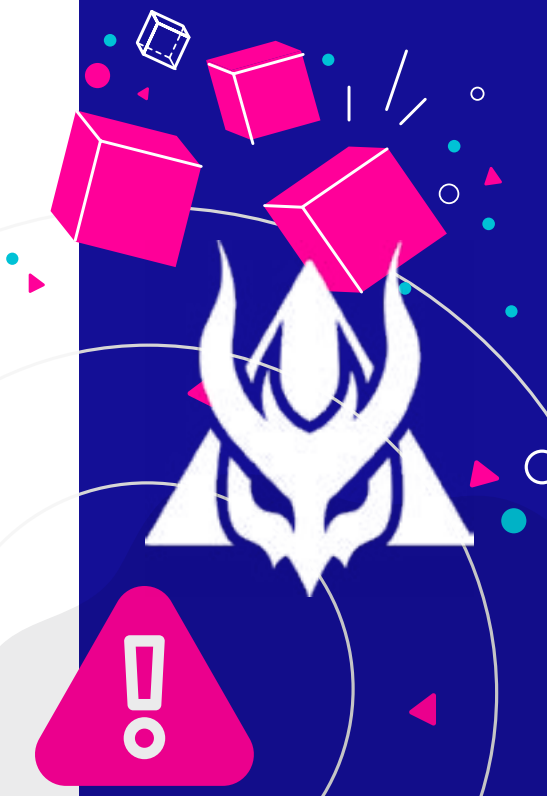
THREAT ALERT

Understanding Qilin: The Evolving Threat of Ransomware-as-a-Service

Qilin operates as a Ransomware-as-a-Service (RaaS), a cybercrime model that recruits affiliates to infiltrate networks and deploy ransomware in exchange for a share of the ransom payments. This model facilitates data encryption and employs a double extortion strategy, where attackers threaten to leak sensitive information unless a second ransom is paid.

One of the distinguishing features of Qilin is its innovative approach to targeting adjacent third parties. The group exploits credentials stored in web browsers, particularly Chrome, to gather sensitive information such as login credentials and personal details. This tactic allows them to breach third-party accounts, thereby exacerbating the impact on their primary victims. Additionally, Qilin leverages Group Policy Objects (GPOs) within Active Directory environments to execute malicious scripts during user logins. This method enables the mass collection of credentials every time users connect to their devices, significantly amplifying the scale of the attack.

Interestingly, a North Korean state-sponsored threat actor known as Moonstone Sleet has been observed deploying Qilin RaaS in both profit-driven activities and state-sponsored espionage. To gain initial access, Qilin affiliates typically exploit vulnerabilities in Virtual Private Networks (VPNs), Remote Desktop Protocol (RDP), and Microsoft Exchange.



> **Qilin's tactics underscore the growing prevalence of credential theft in ransomware attacks and the urgent need for organisations to implement stringent security measures, especially for internet-facing devices and services, like VPN technologies.**

Qilin's tactics underscore the growing prevalence of credential theft in ransomware attacks and the urgent need for organisations to implement stringent security measures. It is essential to adopt Multi-Factor Authentication (MFA) across all systems and applications, particularly for VPN access. User education is crucial; employees must be made aware of the risks associated with browser-stored credentials and encouraged to use secure password managers instead. Implementing Privileged Access Management (PAM) solutions is also advisable to securely monitor and manage privileged accounts and access. By understanding Qilin's tactics and adopting these security measures, organisations can better protect against the growing threat of ransomware.

Source: ***Sophos, Bleeping Computer,*** **Surefire Cyber**

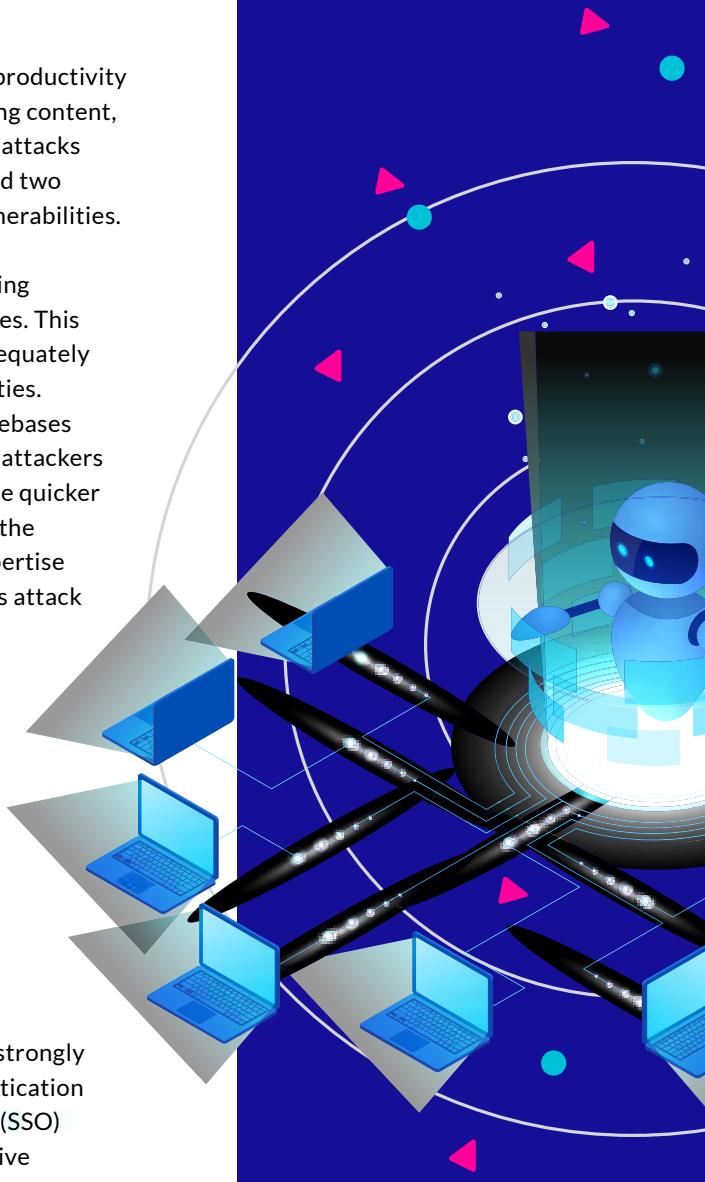
THREAT ALERT

The Role of Artificial Intelligence in Evolving Cyber Threats

Cybercriminals are increasingly using artificial intelligence (AI) to increase productivity and efficiency in areas like research, code debugging, and creation of phishing content, as opposed to as a "doomsday weapon." While no groundbreaking AI-driven attacks have emerged thus far, our incident response partner, Surefire, has identified two notable trends: a rise in brute-force attacks and an increase in zero-day vulnerabilities.

AI significantly amplifies the threat posed by brute-force attacks by employing advanced algorithms that enable faster and more efficient guessing processes. This capability can render even complex passwords vulnerable if they are not adequately secured. AI is also accelerating the discovery and exploitation of vulnerabilities. Cybercriminals can leverage machine learning to rapidly scan extensive codebases and identify weaknesses more efficiently than humans. This speed provides attackers with a considerable advantage; the sooner vulnerabilities are discovered, the quicker they can be weaponised. Once a vulnerability is identified, AI can automate the generation of exploit code, dramatically reducing the time and technical expertise required to execute an attack. Furthermore, AI systems can simulate various attack scenarios pre-deployment and optimise exploits to bypass security.

Once a vulnerability is identified, AI can automate the generation of exploit code, dramatically reducing the time and technical expertise required to execute an attack.



To mitigate the risks associated with brute-force attacks, organisations are strongly encouraged to implement MFA. Additionally, adopting passwordless authentication methods — such as biometric logins, hardware security keys, Single Sign-On (SSO) systems, or Passkeys — can further enhance security. By taking these proactive measures, organisations can better protect themselves against evolving, AI-fueled cyber threats.

Source: Picus RedReport 2025, *Gcore*, Surefire Cyber

ClickFix Technique Makes a Comeback

ClickFix is a social engineering technique employed by the Lazarus Group that uses fake browser alerts to deceive users into downloading malware. This method exploits people's tendency to want to resolve issues quickly and independently, leading users to act without consulting their IT departments — thus circumventing security measures.

Attackers craft counterfeit error messages that appear on users' screens, simulating problems with software or websites. These messages typically include seemingly legitimate instructions, encouraging users to copy and paste commands into PowerShell, a command-line tool in Windows. When users execute these commands, they inadvertently run malicious scripts that can install malware on their systems.

To enhance its credibility and increase the likelihood of success, ClickFix often masquerades as well-known applications such as Word or Chrome. Additionally, it can be delivered through various channels, including compromised websites, documents, emails, and notifications from platforms like GitHub.

To mitigate the risks associated with ClickFix and similar social engineering tactics, organisations should conduct regular training sessions to educate employees about these threats. It is also wise to limit the use of PowerShell to those whose job requires it. Implementing a whitelist to restrict the use of any software not specifically authorised by the company can also bolster security and reduce the risk of malware infections.

Source: ***Proofpoint, Thehackernews, US Department of Health and Human Services***

Ivanti Exploit Chain

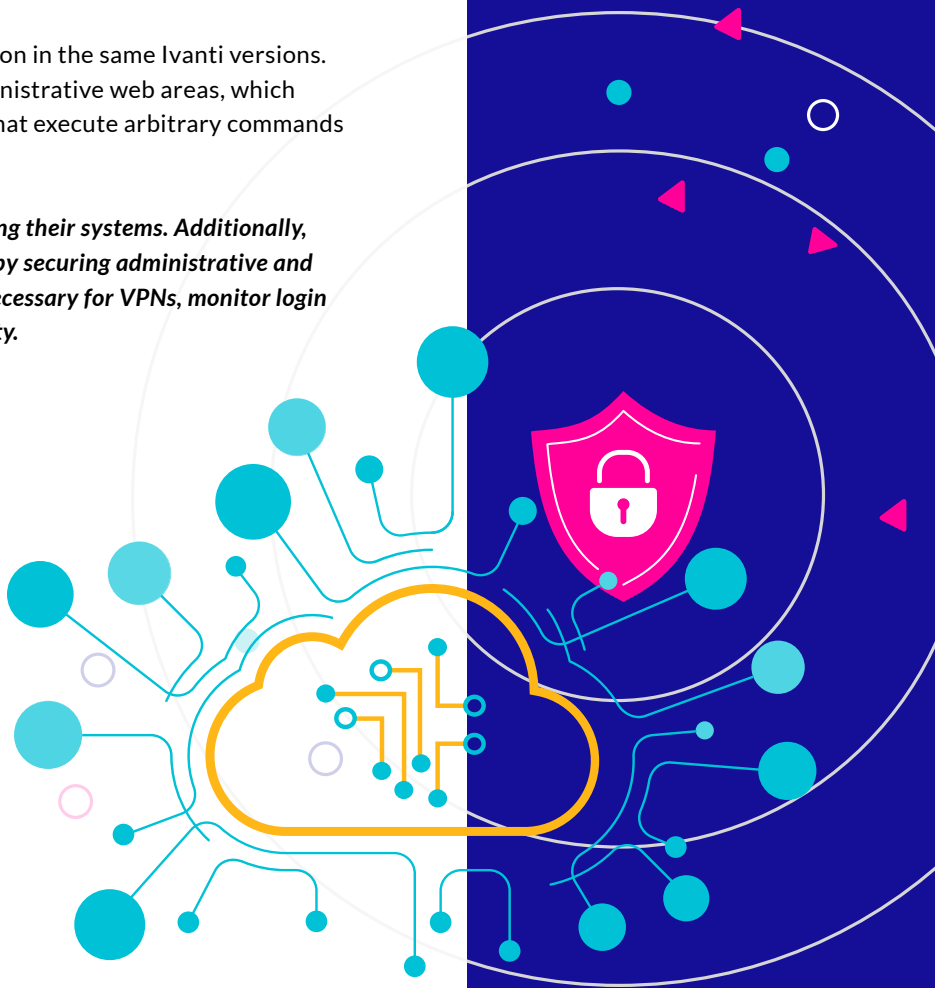
Two critical vulnerabilities in Ivanti software are currently being exploited through an exploit chain – a sequence of multiple exploits used to bypass a system's security measures that is commonly used by threat actors.

> **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 unauthorised 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 prioritise 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,

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 popular 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 prioritising 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 unauthorised 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 Defence

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

- **Train all employees, including help desk staff, to recognise 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.**

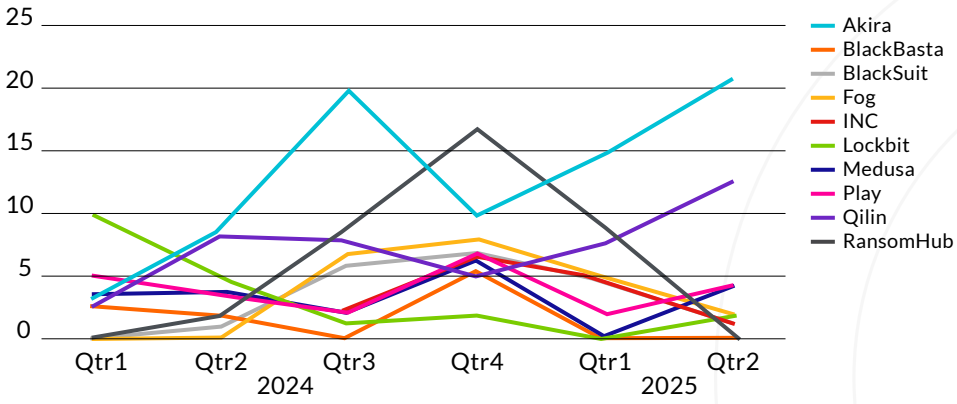
> **Social engineering and phishing - attacks that exploit human vulnerabilities - account for 37% of attacks in claims and incident response data.**

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

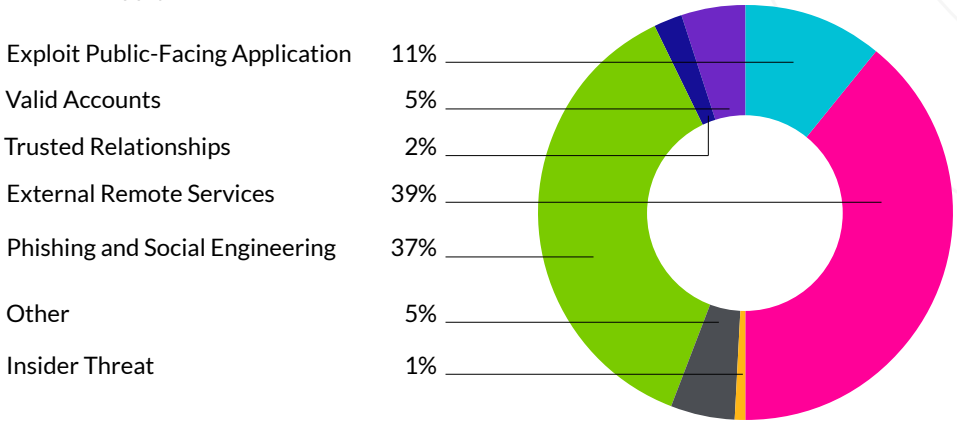
[2] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations?hl=en

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 and phishing/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 prioritise 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 prioritising 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 organisations mitigate exposure and reduce cyber risk. Learn more.

chubb.com