CHUBB®

Cyber Threat Intelligence Report Q1 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.

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 the quarter. 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 organizations.

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

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

Source: *Darktrace*

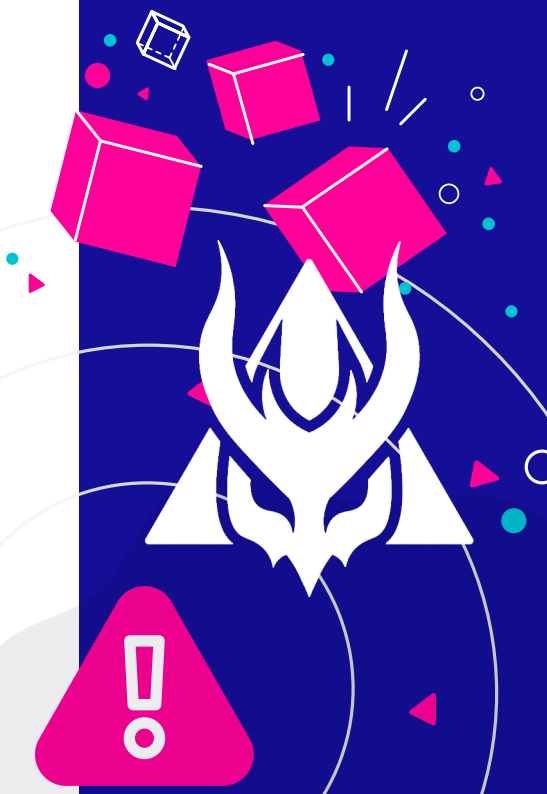
THREAT ALERT

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 organizations 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 organizations 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, organizations can better protect against the growing threat of ransomware.

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

THREAT ALERT

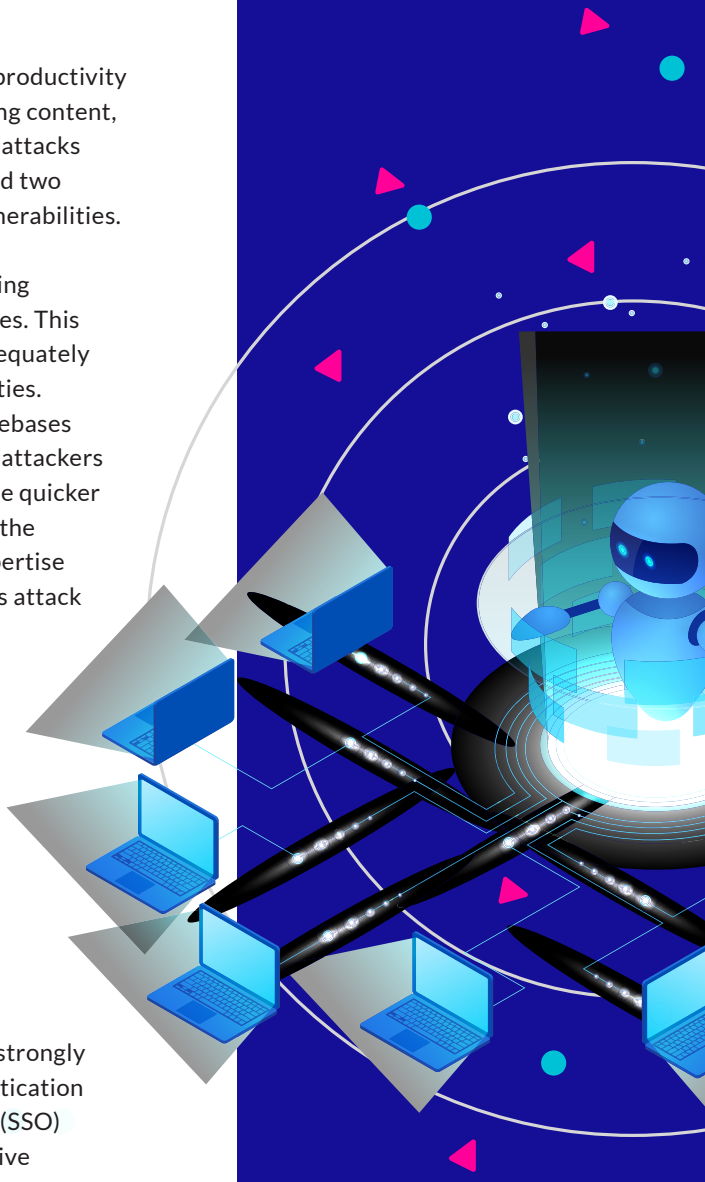
The Role of Artificial Intelligence in Evolving Cyber Threats

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 weaponized. 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 optimize 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, organizations 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, organizations 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, organizations 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 authorized by the company can also bolster security and reduce the risk of malware infections.

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

ESPIONAGE ALERT

The Escalation of State-Sponsored Espionage Activities

In 2024, threat actor groups such as Russia's APT29, China's Volt Typhoon, and North Korea's Lazarus Group have intensified attacks on critical infrastructure, government agencies, and private enterprises.

> **This new wave of advanced persistent threats (APTs) poses a critical risk to the cyber insurance market, particularly in the event of a crisis or conflict involving nations like China.**

Volt Typhoon, a Chinese state-sponsored threat actor, has launched attacks of unprecedented sophistication targeting essential services such as electrical and water distribution networks, factories, transportation systems, construction sites, and schools. These prolonged and complex attacks are designed for "prepositioning," meaning they lay the groundwork for future assaults pending political directives. A large-scale cyberattack on these facilities has the potential to paralyze entire cities or states. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has expressed growing concern over the increasing likelihood of significant cyberattacks amid heightened geopolitical tensions or military conflicts involving China.

Addressing the escalating rate and complexity of state-sponsored espionage campaigns requires a multifaceted strategy. Security professionals should tap into threat intelligence feeds and platforms to keep abreast of the current tactics, techniques, and procedures (TTPs) employed by state-sponsored actors. Honeypot technologies can help detect emerging threats, while threat-hunting programs will enhance the ability to identify APTs that may have evaded existing security measures. By taking these proactive steps, organizations can better prepare for and mitigate the substantial risks stemming from state-sponsored cyber threats.

Source: CISA

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

The information contained in this document is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither Chubb nor its employees or agents shall be liable for the use of any information or statements made or contained in any information provided herein. This document contains links to third-party Web sites solely for informational purposes and as a convenience to readers and not as an endorsement by Chubb of the entities referenced or the contents on such third-party Web sites. Chubb is not responsible for the content of linked third-party sites and does not make any representations regarding the content or accuracy of materials on such linked Web sites. The opinions and positions expressed in this report are the authors' own and not necessarily those of Chubb.

©2025 Chubb

05/2025