CHUBB®

Cyber Threat Intelligence Report Edition 4

Stack up your cyber protection with Chubb.

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

VULNERABILITY RADAR

CVE Focus: Salesforce Plugin Attacks

In late 2025, two significant cyber incidents targeted the Salesforce ecosystem through third-party software integrations: the Salesloft Drift breach in August and the Gainsight incident in November. The threat actor behind these incidents, known as "**Scattered LAPSUS$ Hunters**" – a cybercriminal group formed from several well-known hacking collectives – abused trusted cloud software integrations to bypass authentication and access data in connected Salesforce environments.

Both breaches took advantage of weaknesses in how Salesforce plugins handle OAuth tokens. OAuth is a technology that lets applications access data securely on your behalf without sharing your password. If attackers steal these tokens, they can pretend to be legitimate users and access sensitive information such as customer details and activity records, without permission. Over 200 organisations were impacted by the Gainsight breach, while the Salesloft incident affected approximately 700 organisations; however, the third-party exposure could be much greater.

> **These incidents show why it is important for large and medium-sized policyholders to carefully monitor and control their third-party software connections. Policyholders must treat OAuth integrations as Tier-0 infrastructure and maintain an inventory of OAuth apps, granted scopes, and token lifetimes.**

> **Third-party risk management procedures must include reviews of integration(s) security controls, including OAuth token inventories, storage procedures, and protection models as well as requirements and support for rapid token revocation.**

Microsoft Exchange (e.g., CVE-2022-41040 and CVE-2022-41082) and Microsoft zero-day vulnerabilities (e.g., CVE-2025-29824).

Sources: ***Google Threat Intelligence Group***, ***SocRadar***

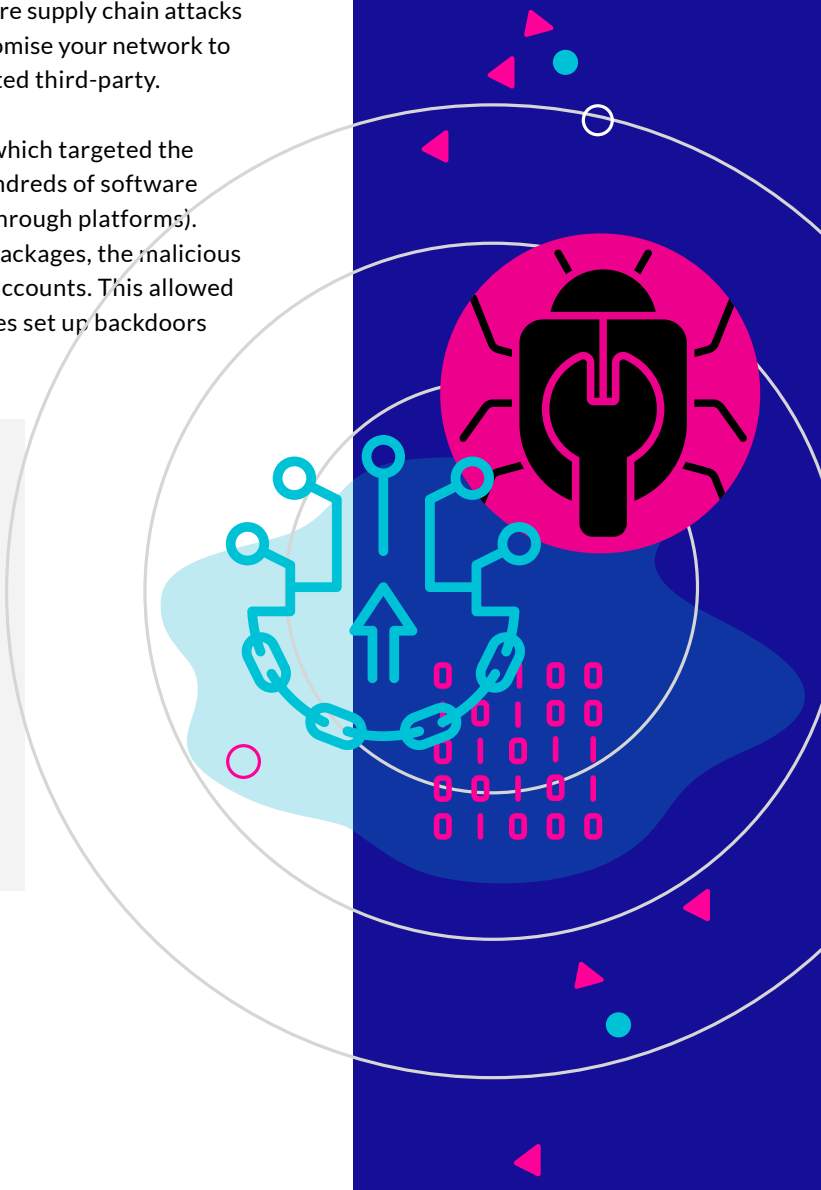
THREAT ALERT

Supply Chain Attacks Have Doubled In 2025

In 2025, the number of cyberattacks emanating from a company's suppliers or partners continues to increase year over year. This is especially true in the IT, technology, and industrial sectors, where organisations rely heavily on outside vendors and interconnected systems. Attackers often use stolen or legitimate credentials or exploit vulnerabilities or misconfigurations in partner networks to gain initial access to targeted organisations. These methods allow attackers to bypass standard security controls by using stolen legitimate credentials or by stealing data from a third-party network through file transfer protocols, often as a result of software supply chain attacks or zero-day vulnerabilities. Indeed, a threat actor need not compromise your network to gain illicit access to your data which is in the possession of a trusted third-party.

A major example from early 2025 is the "Shai Hulud 2.0" attack, which targeted the software supply chain. This attack spread rapidly by infecting hundreds of software packages (small pieces of code that developers reuse and share through platforms). When victim developers unknowingly used these compromised packages, the malicious code spread to their systems and other projects including cloud accounts. This allowed attackers to steal passwords, access sensitive data, and sometimes set up backdoors (hidden ways to access systems in the future).

> **This trend highlights the need for a robust vendor risk management program and closely working with partners to improve cybersecurity. Organisations should follow security best practices such as, ensuring appropriate segmentation between networks, continually monitoring their third-party suppliers, implementing Software Bill of Materials (SBOM) best practices, and periodic patching of software vulnerabilities.**



Sources: *Cyble*, *Checkpoint*

Insider Threat Is Growing

Three of the most notorious English-speaking cybercriminal groups (Scattered Spider, LAPSUS$, and ShinyHunters) have joined forces to form the Scattered LAPSUS$ Hunters (SLSH) collective. This new group poses a major threat because it actively recruits disgruntled employees – so called insider threats. Further, the ability to work remotely and anonymously, lowers the barrier for skilled professionals to participate in illegal activities. By offering substantial amount of monetary compensation in exchange for network access, SLSH turns insider threats from a passive risk into an initial access vector.

At the same time, the dark web is seeing a surge in illicit job postings. This creates an unregulated labor market that attracts disgruntled employees and job seekers who may be struggling to find traditional jobs. Reports show that cybercrime organisations now operate as legitimate business fronts and that up to 69% of applicants are willing to accept any position within these "businesses," with some roles offering pay as high as top Silicon Valley companies. This environment attracts people looking for high rewards with little oversight. These developments mean organisations face a growing risk, as skilled professionals are increasingly drawn to cybercrime.

In this context, policyholders should implement robust identity and access management (IAM) practices, including multi-factor authentication (MFA), least privilege access, restrict device enrollment for MFA, strong password policies, and continuous monitoring. EDR and/or SIEM tools should be set up to monitor user authentication and access events, identify unauthorised access attempts and alert on any identity policy violations.

Human resources and hiring managers must follow strict protocols for verifying applicant identities, removing separated employees from systems access, and consider implementing insider threat programs.

Sources: ***Bleepingcomputer, ETEdge Insights, SOS Ransomware, ArcticWolf***

THREAT ALERT

Disabling Defenses: The Threat of EDR Killer

Cyber attackers are increasingly leveraging readily available tools to disable or bypass security software such as antivirus and Endpoint Detection and Response (EDR) solutions. These tools, which can be purchased on dark web forums – even by less skilled criminals – make advanced attacks more accessible. For instance, in May 2023, the "Terminator" tool was sold on a Russian-language forum for $300–$3,000, claiming it could disable up to 24 security products.

A 2023 analysis by CrowdStrike showed that the Terminator tool works as a BYOVD (Bring Your Own Vulnerable Driver) tool. In a BYOVD attack, malware installs a known vulnerable driver (a piece of software that helps hardware communicate with the operating system) on a computer. Attackers then exploit this driver to gain deep system access, hide their malware, steal credentials, and disable security protections, including EDR.

Many other EDR killer tools are available on cybercriminal forums. As these attacks become more sophisticated, organisations should use multiple layers of security.

To reduce risk, organisations should: keep operating systems and applications up to date, remove outdated or unused software, enforce strong Windows security role hygiene (making sure users only have the permissions they need), maintain an up-to-date whitelist (approved list) of safe drivers and block any vulnerable drivers not in use, ensure endpoint security solutions include tamper protection (features that prevent unauthorised changes to security settings).

Sources: *Sophos, Surefire analysis*

The Rise of Agentic AI in Cybersecurity Breaches

In November, a state-sponsored hacking group demonstrated the use of artificial intelligence (AI) with "agentic" capabilities to carry out large-scale cyberattacks. Agentic AI refers to AI systems (sometimes called AI agents) that can work on their own for long periods, completing complex tasks with little human help. The operation targeted major companies and government agencies. According to Anthropic, this is the first documented case of a major cyberattack conducted mostly by autonomous AI.

To achieve this level of sophistication, the attackers built an automated framework (a set of tools that work together automatically) to compromise selected targets. This framework used Anthropic's Claude Code, an AI-powered tool that can write and run computer code, to automate many parts of the attack. To get around the system's built-in security restrictions, the attackers used a technique called "jailbreaking" (tricking an AI system into ignoring its safety controls, like divulging sensitive training or proprietary data). In this case, the attackers broke down malicious activities into smaller, harmless-looking tasks and coded the AI to act as if it were a legitimate cybersecurity employee doing defensive testing.

Once a target was chosen, the AI agent automatically gathered reconnaissance information about the target's systems and reported its findings to the human operator. In later steps, the AI found and exploited security weaknesses, wrote its own attack code, stole credentials, extracted sensitive data, identified privileged accounts, and set up backdoors. In these campaigns, AI handled 80–90% of the attack process, with humans making only a few key decisions.

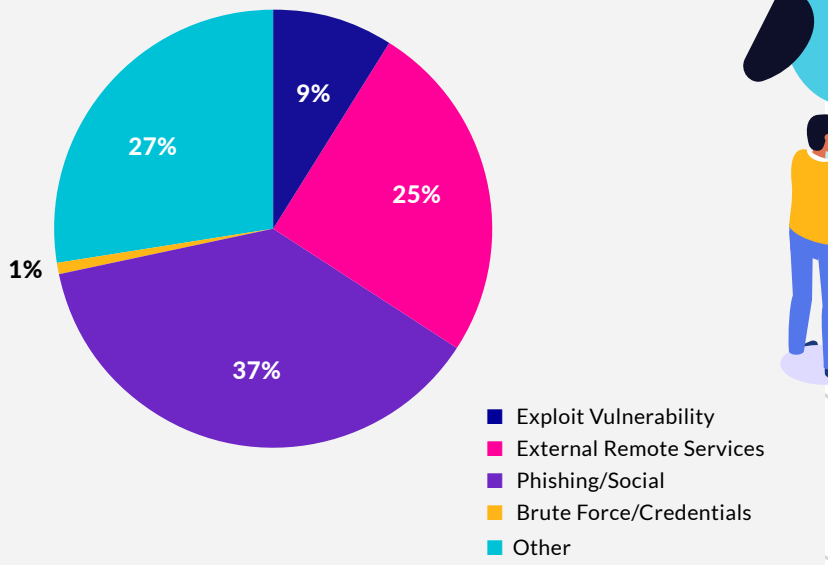
> **These campaigns allowed attackers to scale up their attacks quickly and efficiently. Anthropic notes that this marks a major change in cybersecurity. Security teams are now encouraged to use AI for defense as well, such as automating Security Operations Center (SOC) tasks, improving threat detection, running vulnerability scans, and responding to incidents faster.**

Source: *Anthropic*

Threat Actor Tactics

In reviewing 2025 initial access tactics resulting in ransomware, data breaches, business email compromises (BEC), and other adversary-led cyberattacks, phishing, social engineering, and external remote services remain highly utilised. VPN abuse remained elevated throughout 2025, frequently resulting in ransomware claims. To further highlight the risk associated with VPN, Chubb issued more vulnerability alerts in 2025 for VPN-related exposures than any other appliance or software. Critical or high-severity vulnerabilities, credential abuse, or misconfigurations or failed controls (like MFA) continue to plague VPN and merit special consideration for security professionals. Social engineering – manipulating call centers, deep fakes, and other tactics – were also up in 2025.

Initial Access Tactics



Source: ***Chubb***

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.

chubb.com

All content in this material is for general information purposes only and may not be shared externally without Chubb's consent. It does not constitute personal advice or a recommendation to any individual or business of any product or service. Please refer to the policy documentation issued for full terms and conditions of coverage.

Chubb is a world leader in insurance providing commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index.

ENG9159-MD 03/26