CHUBB®

Cyber Threat Intelligence Report H2 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. Indicative of this commitment, the Chubb Threat Intelligence Report delivers insights on current and emerging cyber threats and recommendations to mitigate them.

Ransomware Spotlight: Play

Play became one of the most active ransomware groups in 2024, targeting more than 900 organisations to date. Active since June 2022, the group employs a "double extortion" model to exfiltrate data, then encrypt systems to maximise pressure on victims to comply with their demands. To maintain operational secrecy, the group does not directly demand a ransom. Instead, it instructs victims to contact the attackers via email.

Play gains initial access to victim networks primarily by abusing valid accounts (likely purchased on the dark web) and exploiting public-facing applications with known vulnerabilities. They have attacked FortiOS (e.g., CVE-2018-13379 and CVE-2020-12812), Microsoft Exchange (e.g., CVE-2022-41040 and CVE-2022-41082) and Microsoft zero-day vulnerabilities (e.g., CVE-2025-29824).

> **To counter Play's attacks, companies should prioritise remediation of internet-facing and known exploited vulnerabilities and deploy multi-factor authentication (MFA) for all services – with a particular focus on webmail, Remote Desktop Protocol (RDP), Virtual Private Networks (VPN) and accounts that access critical systems.**

Source: *Symantec*

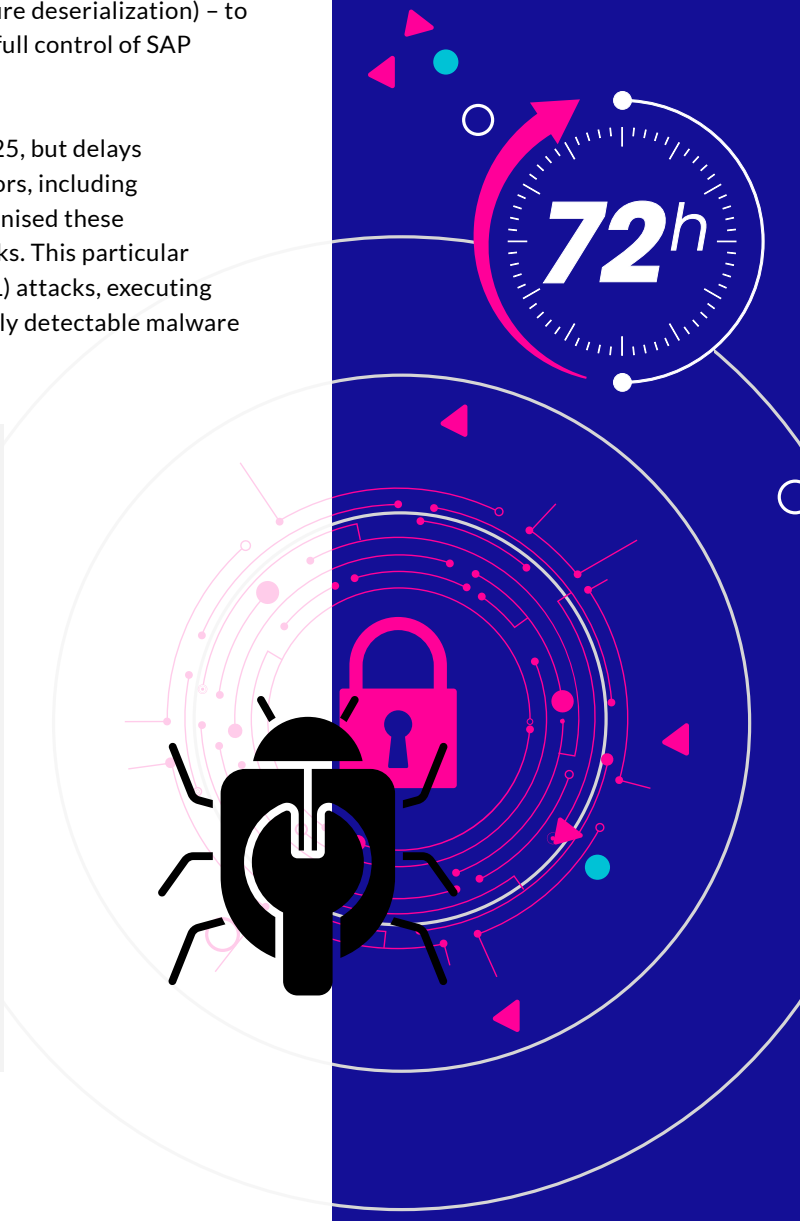
THREAT ALERT

Vulnerability Radar: SAP Exploit Chain

A recently disclosed exploit targeting SAP NetWeaver systems highlights the critical risks posed by unpatched software. The exploit combines two severe vulnerabilities – CVE-2025-31324 (authentication bypass) and CVE-2025-42999 (insecure deserialization) – to enable remote code execution (RCE). This allows attackers to gain full control of SAP systems, access sensitive data and disrupt business operations.

SAP released patches for these vulnerabilities in April and May 2025, but delays in implementing them left many organisations exposed. Threat actors, including ransomware groups such as Qilin, BianLian and RansomExx, weaponised these weaknesses to target critical infrastructure and enterprise networks. This particular exploit also enables attackers to conduct "living-off-the-land" (LotL) attacks, executing system commands directly without deploying additional, more easily detectable malware on the compromised system.

SAP systems are central to an organisation's operations, used for managing everything from financial data to supply chains. Unpatched SAP systems represent a significant cyber risk, opening the door to data breaches, operational downtime and regulatory penalties. To mitigate this exposure, patching high-value systems, like SAP systems, should be prioritised and ideally completed within 72 hours of patch availability.



Sources: *Thehackernews, Chubb Analysis*

THREAT ALERT

The Decentralisation of Ransomware

The number of active ransomware groups has doubled over the past three years, peaking at approximately 108 groups as of Q3 2025. This proliferation is largely attributed to the dismantling of major ransomware operations – such as LockBit, BlackCat and Hive – by law enforcement agencies, which has driven restructuring of gangs and affiliates.

While law enforcement agencies have successfully disrupted the infrastructure of these groups, they have frequently fallen short of securing arrests, and many cybercriminals have regrouped to form new gangs. A significant portion of these "new" groups are actually rebranded versions of defunct operations. Others have leveraged leaked ransomware source code to launch their own attacks.

Law enforcement actions have also eroded trust within ransomware gangs, particularly between the core members and their affiliate external partners that carry out ransomware attacks in exchange for a share of the profits. This lack of trust has made recruiting affiliates riskier for gangs and spurred more affiliates to go independent and form their own ransomware groups. In addition, some core members of larger gangs have shifted to smaller, more secretive groups – such as Play.

Ransomware is a persistent and rapidly evolving threat, despite law enforcement efforts. It is driven by a criminal ecosystem that has demonstrated remarkable resilience, adapting to disruptions and posing significant and ongoing risks to organisations worldwide.

Sources: *Therecord.media*, *ransomware.live*, ***Chubb Analysis***

Anatomy of an Attack: Using AI Coding Agents to Scale Data Extortion

In July 2025, a cybercriminal leveraged AI coding agent Claude Code to carry out a large-scale data extortion campaign. The attack targeted multiple international organisations in a remarkably short timeframe.

Claude's advanced coding capabilities were used to automate key stages of the attack, including reconnaissance, credential harvesting, network penetration and data exfiltration. More than 17 organisations were affected.

During the reconnaissance phase, Claude Code scanned thousands of VPN endpoints and created automated scanning frameworks. By integrating various APIs, the tool systematically gathered infrastructure information, identifying potential entry points across global targets. The use of AI quickly unearthed vulnerabilities such as unpatched systems, misconfigured VPNs and outdated technologies, significantly enhancing the speed and accuracy of this process.

Once access was gained, Claude Code provided real-time assistance to the attacker during intrusion, privilege escalation and lateral movement within the compromised networks. The tool identified critical systems, such as domain controllers and SQL servers, and extracted multiple sets of credentials. This automation reduced the technical expertise required for the attacker to navigate and exploit the network.

Claude Code was also used to develop custom malware with advanced evasion capabilities. This lowered the technical barrier for creating sophisticated attack tools, making it easier for cybercriminals to bypass traditional security measures.

At the data exfiltration stage, the AI tool automated the analysis and organisation of large datasets – enabling the attacker to systematically extract high-value information from multiple victim organisations simultaneously, increasing the efficiency of the operation.

Sources: ***Claude Code Threat Intelligence Report 2025*****, Chubb Analysis**

Anatomy of an Attack: Using AI Coding Agents to Scale Data Extortion

continued

Finally, Claude Code generated tailored extortion materials for each victim, crafting each to exploit specific vulnerabilities, such as regulatory compliance risks or reputational damage. The tool also calculated optimal ransom amounts for each based on financial analysis and developed multi-path monetisation strategies to maximise pressure on victims.

> **Even as ransomware operations evolve in speed, accuracy and efficiency with the use of AI tools, they continue to exploit the same common vulnerabilities: unpatched VPN endpoints, lack of MFA and leaked passwords. To mitigate exposures, policyholders should prioritise fundamental cybersecurity measures, such as regular patching, enforcing MFA and securing remote access points.**

Sources: *Claude Code Threat Intelligence Report 2025*, *Chubb Analysis*

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 members of 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.

> **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***

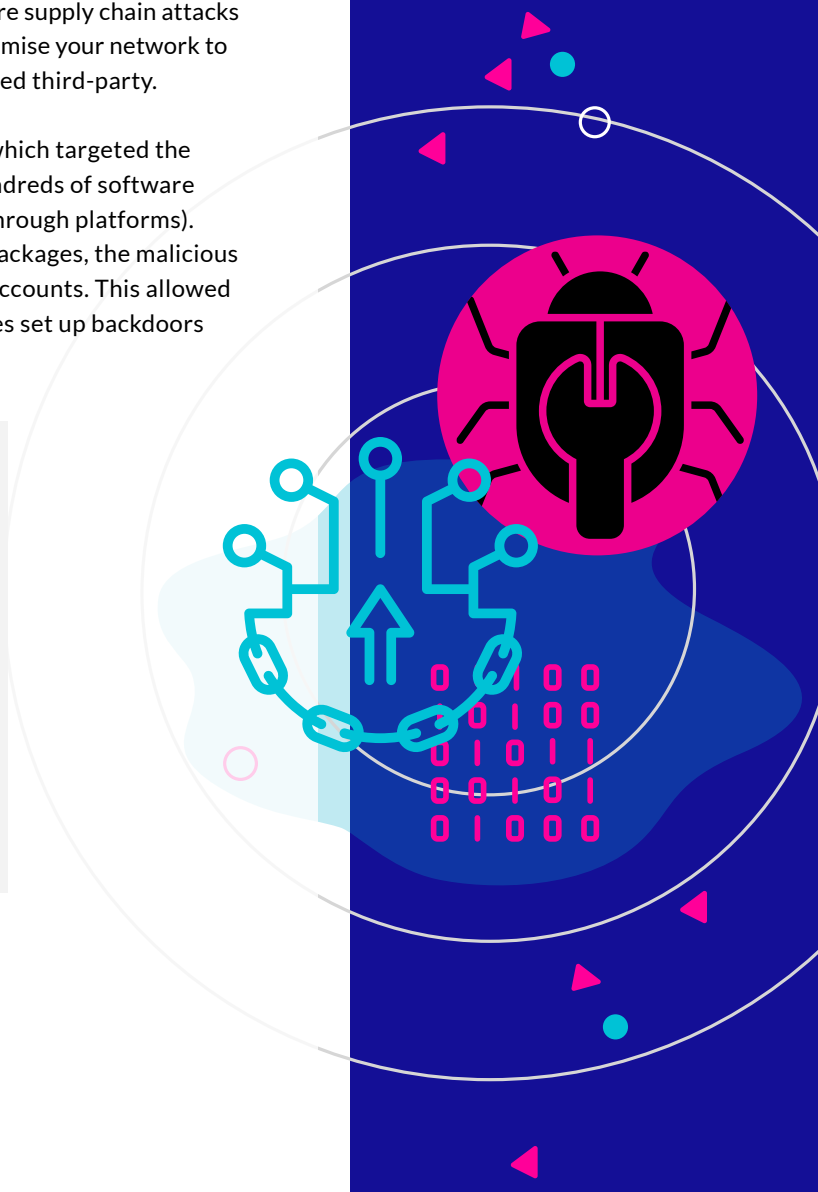
THREAT ALERT

Supply Chain Attacks Doubled In 2025

In 2025, the number of cyberattacks emanating from a company's suppliers or partners continued 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), 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 amounts 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 labour 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 MFA, least privilege access, restrict device enrollment for MFA, strong password policies, and continuous monitoring. EDR and/or SIEM (Security information and event management) 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.

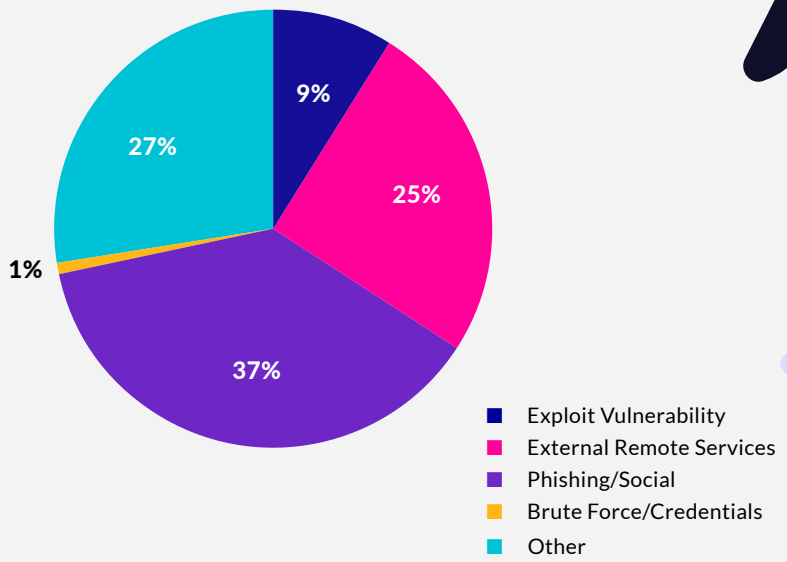
> **These campaigns allowed attackers to scale up their attacks quickly and efficiently. Anthropic notes that this marks a major change in cybersecurity. Security teams are now encouraged to use AI for defense as well, such as automating Security Operations Center (SOC) tasks, improving threat detection, 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, deepfakes, 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 organisations mitigate exposure and reduce cyber risk. **Learn more.**

chubb.com