CHUBB®

Cyber Threat Intelligence Report Edition 3

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.

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*

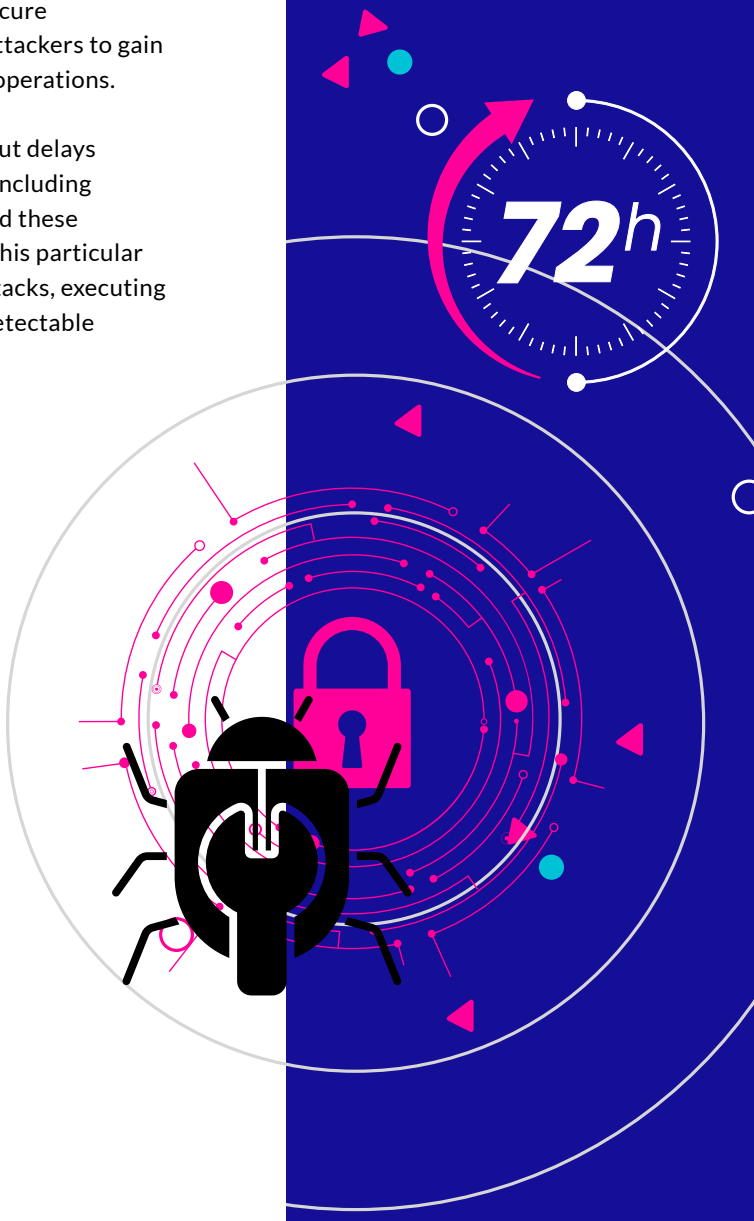
THREAT ALERT

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 deserialisation) – 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***

Microsoft Exchange 2019 and Prior Reaches End of Life

Microsoft, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a joint advisory and guidance concerning End-of-Life Microsoft Exchange Servers. The advisory warns users of Microsoft Exchange 2019 or older, in either on-premises or hybrid network environments, to decommission the servers after transitioning to Microsoft 365, Exchange Subscription Edition (SE) or similar cloud-based services. Organisations with a business justification for retaining an on-prem Exchange server due to regulatory compliance or operational technology constraints are urged to take additional steps to harden end-of-life servers. These steps include maintaining security updates via Microsoft's Extended Security Update program, and applying Zero Trust security baselines like Multi-Factor Authentication (MFA), anti-virus, anti-malware and Endpoint Detection and Response (EDR). Administrative access to Exchange Servers should be restricted and systems should be actively monitored for indicators of compromise.

Chubb Analysis: Chubb recommends moving to Exchange Online or upgrading to Microsoft Exchange SE for hybrid environments as soon as possible. In the interim, follow Microsoft's guidance for hardening Microsoft Exchange 2019 and prior deployments via the Extended Security Update, which only covers 6 months for limited security upgrades. Microsoft Exchange-related vulnerabilities have been heavily targeted by ransomware groups and other threat actors and Chubb assesses this trend will continue.

Sources: ***Microsoft, CISA, Chubb Analysis***

THREAT ALERT

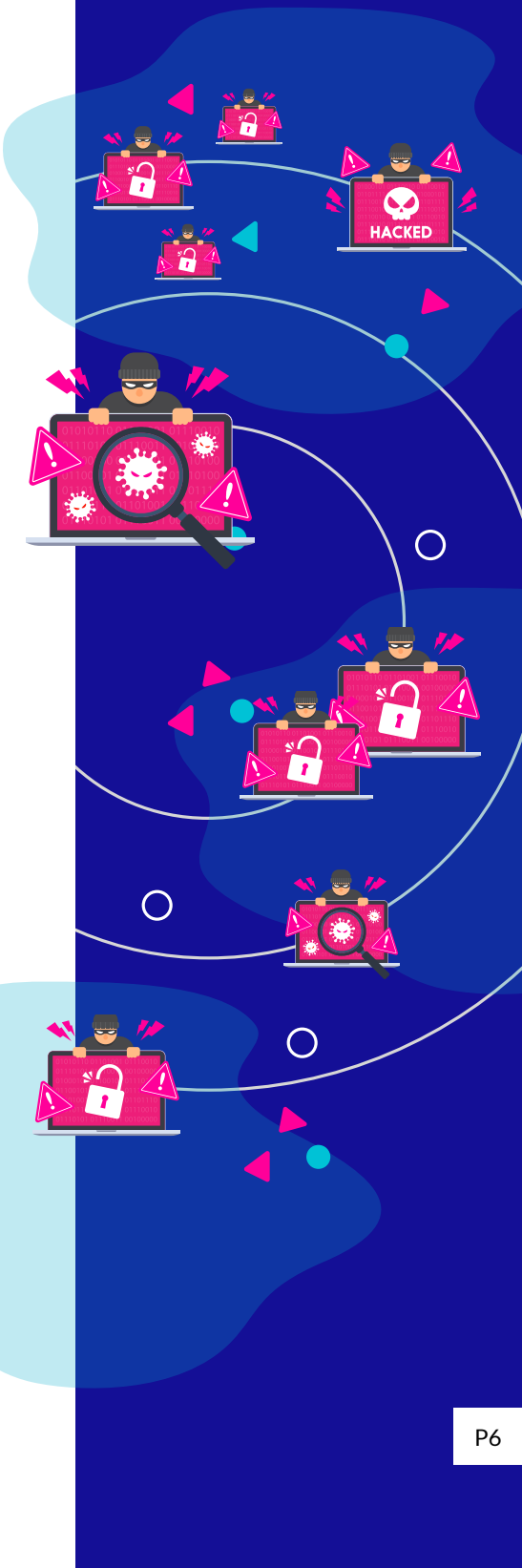
The Decentralisation of Ransomware

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, 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.

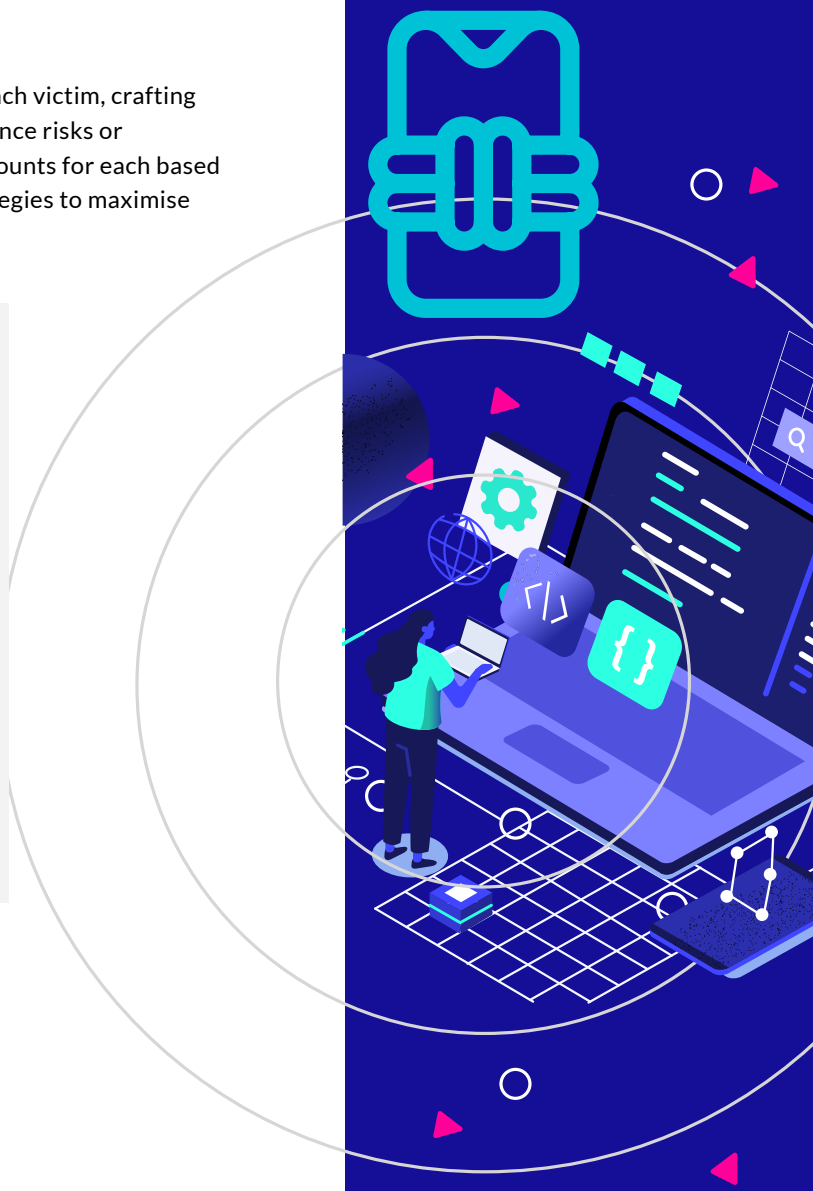
Sources: ***Claude Code Threat Intelligence Report 2025*****, Chubb Analysis**

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**

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.

chubb.com

ENG9067-MD 11/25