CHUBB®

Cyber Threat Intelligence Report Q4 2024

Stack up your cyber protection with Chubb.

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

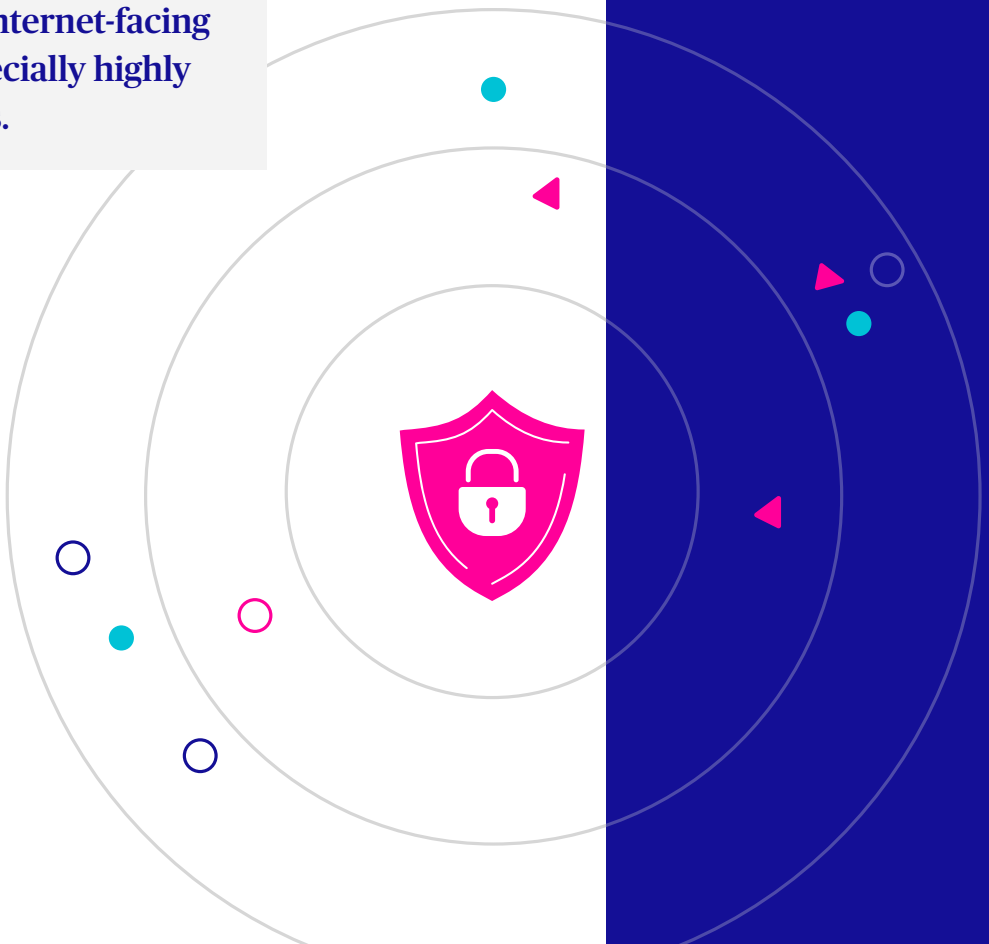
VULNERABILITY RADAR

Improper Access Control: SonicWall SonicOS

SonicWall first notified clients of a critical severity vulnerability affecting SonicOS SSLVPN and firewalls in August. Shortly after came news that the vulnerability was "potentially being exploited in the wild." CISA added the vulnerability (CVE-2024-40766) to its Known Exploited Vulnerabilities (KEV) catalog, and, via our **Vulnerability Management Outreach** program, Chubb's Threat Intelligence Team alerted affected policyholders.

According to cybersecurity firm Arctic Wolf, the vulnerability may have been exploited for initial access by Akira ransomware. Chubb's internal claims data and third-party intelligence sources pointed to continued active exploitation through Q4, particularly by Fog and Akira ransomware.

> **To mitigate this exposure, prioritize identifying and patching internet-facing devices and software, especially highly targeted VPN technologies.**



Chubb offers an array of Endpoint Protection and Vulnerability Management Solutions, including attack surface management and patch management systems, to help clients foil cybercriminals' increasingly sophisticated network infiltration efforts. **Learn more.**

VULNERABILITY ALERT

With Infostealers, Hacking Has Never Been Easier

Cybercriminals have a powerful new accomplice: **infostealers**. This information-stealing malware is increasingly being deployed to extract credentials, session cookies, and personal identity data from infected endpoints. Stolen information is then sold to ransomware operators to hijack sessions or initiate brute force attacks on externally facing services, such as VPNs. Many infostealers also load secondary payloads of malware or ransomware.

Law enforcement targeted prominent infostealers, RedLine and Meta, in Q4. Despite these efforts, Chubb expects infostealers to persist in 2025.

Infostealer

Information-stealing malware deployed to extract credentials, session cookies, and personal identity data from infected endpoints.

A common entry point:

Compromised credentials were the most common root cause of attacks against U.S. organizations in Q4, resulting in

33%
of incidents

Sources: Sophos, Spycloud

VULNERABILITY ALERT

TMChecker Infostealer Dramatically Lowers Barriers To Entry

Corporate cybersecurity faces a significant new threat with the emergence of infostealer TMChecker, an attack tool that specifically targets corporate infrastructure through VPN gateways, email servers, content management systems, and hosting panels. The tool is especially effective since it combines login verification, automated brute-force attacks, and remote access targeting. This Software-as-a-Service is an extremely cost-effective way to execute successful breaches – no advanced technical expertise needed.

TMChecker has transformed sophisticated attack methodologies into streamlined operations readily accessible to entry-level threat actors.

TMChecker is increasingly being adopted by initial access brokers and ransomware operators to validate stolen credentials against corporate VPN and email authentication systems. It is actively targeting several services regularly cited in claims, including Cisco's VPN, Citrix's VPN, Pulse Secure's VPN, FortiNet's VPN, Big-IP's VPN, WordPress, Office 365 and Outlook.

> "The emergence of TMChecker signals a notable shift in the threat landscape and lowers the technical barrier for ransomware affiliates and other threat actors. It cost-effectively automates corporate network intrusion."
>
> – **Craig Guiliano** *SVP, Head of Threat Intelligence and Policyholder Services at Chubb*

Mitigating Infostealer Risk

Mitigating infostealer risk is a multi-tiered strategy:

Password management policies and software can help prevent passwords from being stored in internet browsers – a primary target of infostealers.

Multi-Factor Authentication is critical.

Security awareness training (SAT) programs can assist employees in identifying risky behaviors which may inadvertently lead to downloading malware via phishing or compromised sites.

Mobile device policies should be strictly enforced to prevent accessing or storing credentials on personal devices or unsecure smart phones.

Monitoring infostealer logs and dark web marketplaces via threat intelligence can proactively alert information security teams of compromised credentials and other data stolen via infostealers.

Chubb offers an array of User Security and Awareness Solutions and Vulnerability Assessment Tools to help mitigate infostealer-linked risks. **Learn more.**

Sources: bankinfosecurity.com, resecurity.com

INITIAL ACCESS TRENDS

Phishing Remains Top Tactic in Q4

Continuing a trend seen over several quarters now, phishing was again the top tactic employed by threat actors to gain initial access or drop first-stage malware in Q4 2024. Most of these phishing attacks used embedded email links (75%), while a smaller percentage included a malicious attachment. VPN was the most attacked remote service (77%), continuing a trend from the previous quarter.

A content filtering solution and an email security gateway with sandboxing can effectively block most malicious email links. MFA and employee security awareness training are also critical to mitigate initial access threats.

Email security gateways with sandboxing

Conducts virtual screening of suspicious email attachments and links to identify and block malicious content before it can reach a network.

75%

of phishing attacks in Q4 used embedded email links

Source: Chubb

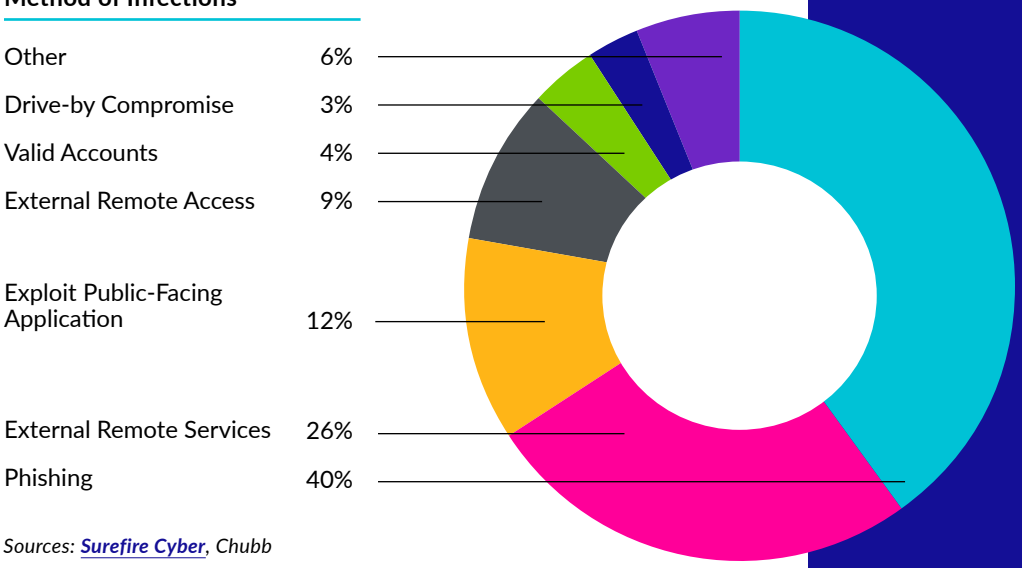
77%

of remote services attacked were VPNs

*Source: **Surefire Cyber***

To learn more about the services Chubb offers to help clients manage and mitigate cyber risk, visit **www.chubb.com/us-en/business-insurance/products/cyber-insurance/us-cyber-services**.

Method of Infections



*Sources: **Surefire Cyber**, Chubb*

CHUBB®

chubb.com