

Regional Report: North America

September 2025

Stephanie Schneider

Cyber Threat Intelligence Analyst



Michael Kosak

Senior Principal Intelligence Analyst

North America remains the top global target

The North America region, including the United States and Canada, faces a significant, pervasive threat from cyber espionage and high-frequency, high-impact financially motivated attacks from all over the globe—including from within the region—due to its strong economy, extensive digital infrastructure, and large consumer market. These attacks range from data collection, ransomware, social engineering attacks like business email compromise (BEC), and more. The US strategic rivalry with China and Russia drives cyberespionage activity in the region. Hacktivism is quite active and poses a moderate threat, causing temporary disruptions. Information operations present a growing threat and will likely increase during times of general civil unrest and geopolitically significant events, such as upcoming elections.

INVESTIGATIONS #2 of all global incidents

North America came in second place with 24% of all incidents investigated worldwide in 2024. The US was the most targeted country in North America with 86% of incidents, and Canada at 14%.¹

DATA BREACH 10 mil in costs

The average cost of a data breach in the United States grew 9% to \$10.22 million in 2024, compared to the global average of \$4.88 million. Costs included breach-related detection and escalation, notification, post-breach response and lost business. The average cost of a data breach in Canada was \$4.66 million.²

BEC ATTACKS \$8.5 bil lost in US over last 3 years

BEC continues to be a major source of fraud in the US. Losses reported to the FBI's Internet Crime Complaint Center (IC3) in 2024 totaled \$16.6 billion, which mostly came from fraud.³

UNITED STATES 52% of ransomware attacks

Consistent with recent activity, the US accounted for approximately half of all reported ransomware victims in Q2 2025. Canada came in second place at 23%.⁴

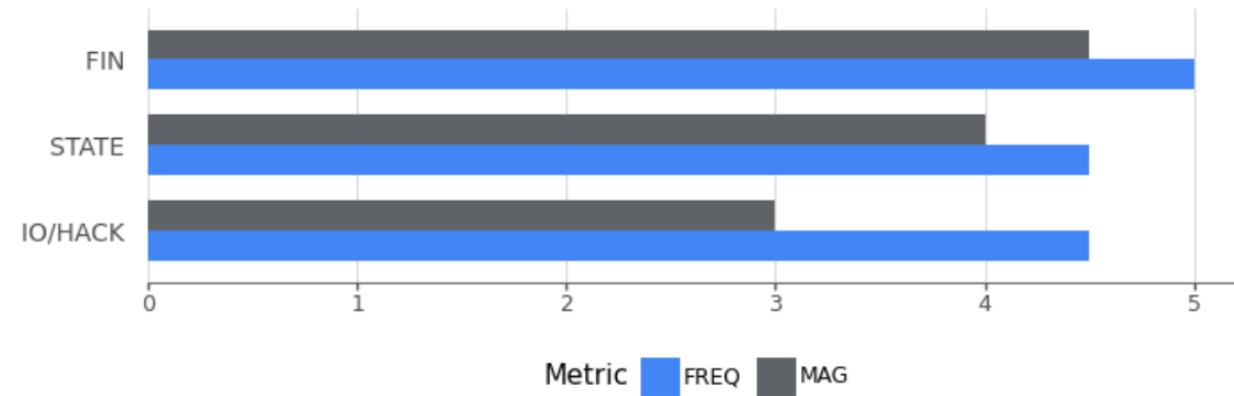
CREDENTIALS 40% of in-region incidents

Credential harvesting was prevalent, impacting 40% of reported incidents in the region, followed by data theft (30%) and espionage, extortion, and brand reputation damage (10% each).¹

Threat landscape: Drivers of regional cyber threat activity

Cyber Threat Score - North America

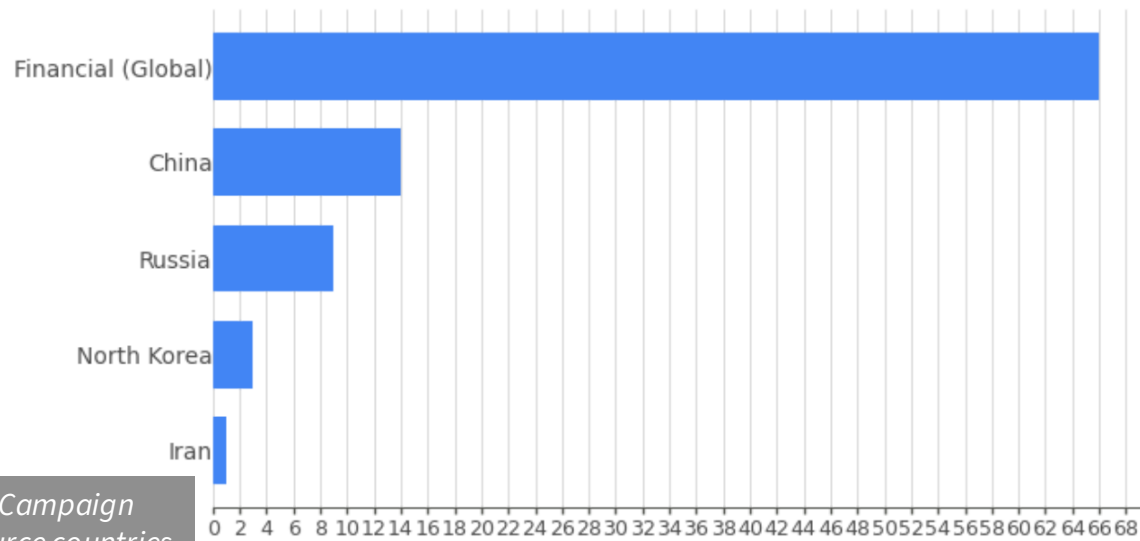
2025 CYBER THREAT SCORE



North America Cyber
Threat Score: 7.6

Campaign Source Countries

Campaigns from 2023-06-30 to 2025-07-01 impacting North America



Campaign
source countries



Top malware families targeting North America

The top malware families targeting the North American region indicate diverse attack objectives.

- **Beacon** (Reconnaissance) and **PSEXEC** (Lateral Movement) suggest post-exploitation activity, meaning attackers are already inside networks and are moving laterally or gathering intelligence.
- **ShadowLadder** and **Darkgate** indicate initial access and payload delivery, signaling attackers are actively trying to breach systems.
- **Lumma** (Infostealer) points to a focus on credential harvesting, which can lead to identity theft, account takeover, and further compromise.

STEALERS

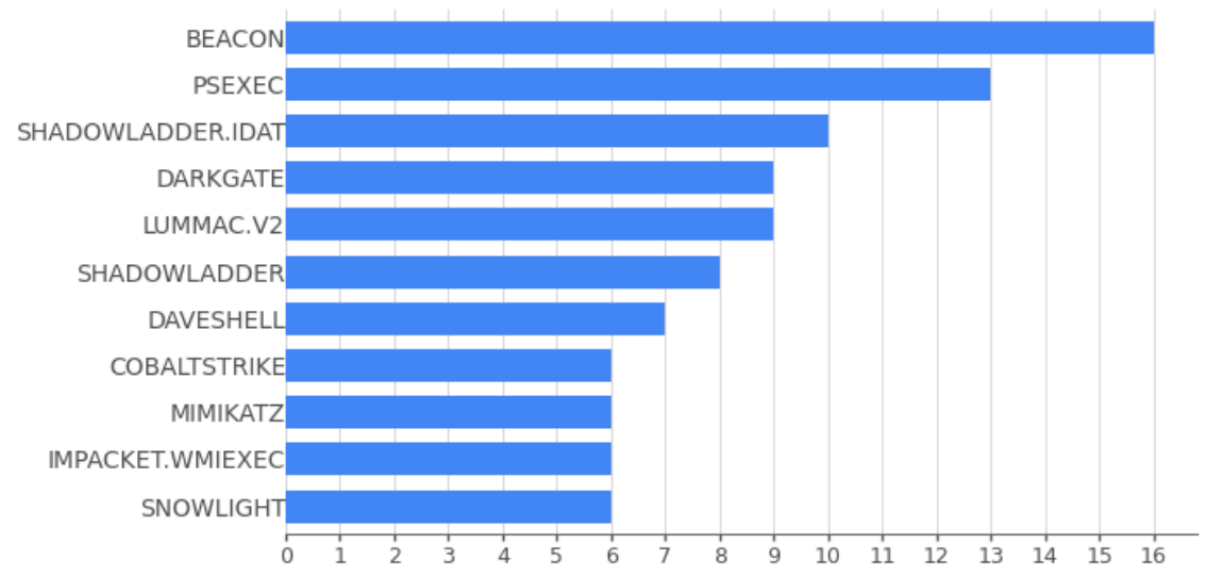
The prominence of infostealers like Lumma shows that identity theft is a major concern. Lumma demonstrated considerable resilience following a large-scale takedown operation in May 2025 and resumed its operations only two days later. Acreed, a relatively new stealer, rapidly gained market share of dumped logs while Lumma climbed back into the top rankings. Other long-standing groups like Meduza, Rhadamanthys, and Stealc have also been active. The broader infostealer market remains robust, driven by the accessibility of Malware-as-a-Service (MaaS) offerings and the constant demand for stolen data, including credentials.

Want to learn about the infostealer threat? CISA, in coordination with other agencies, released an alert about Lumma malware. The advisory details Lumma's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) from November 2023—May 2025.⁷

Top malware families targeting North America

Top Malware Families Impacting North America

Malware used in campaigns from 2023-06-30 to 2025-07-01



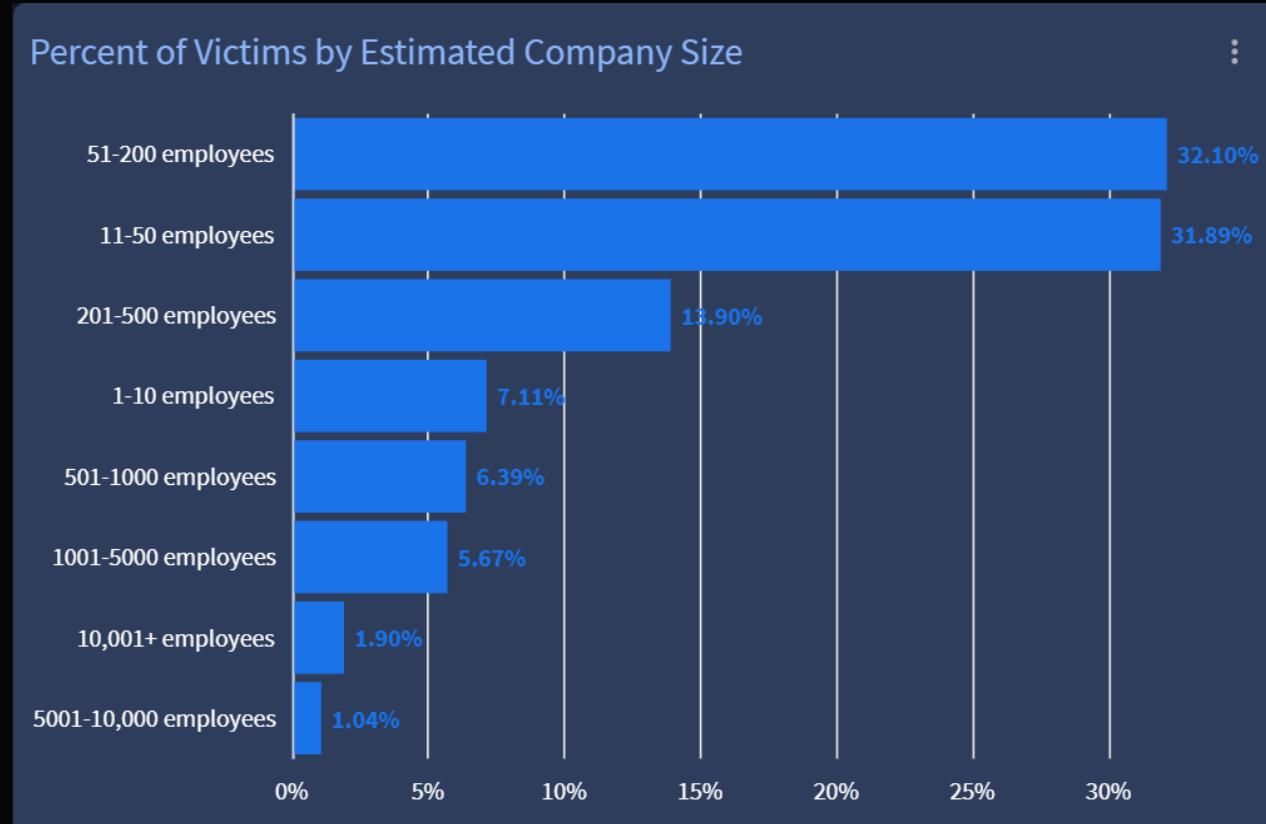
Observed malware targeting North America included Beacon (remote access trojan), PSEXEC (lateral movement/remote execution), SHADOWLADDER and DARKGATE (loaders), LUMMA (credential stealer), and more.

(Source: Google Threat Intelligence)

Ransomware targeting North America

Ransomware poses one of the most pervasive threats to entities in North America, targeting nearly all industries across both the private and public sectors.

Companies in the United States and Canada listed on ransomware data leak sites (DLS's) (January 1-September 15, 2025)
(Google Threat Intelligence)

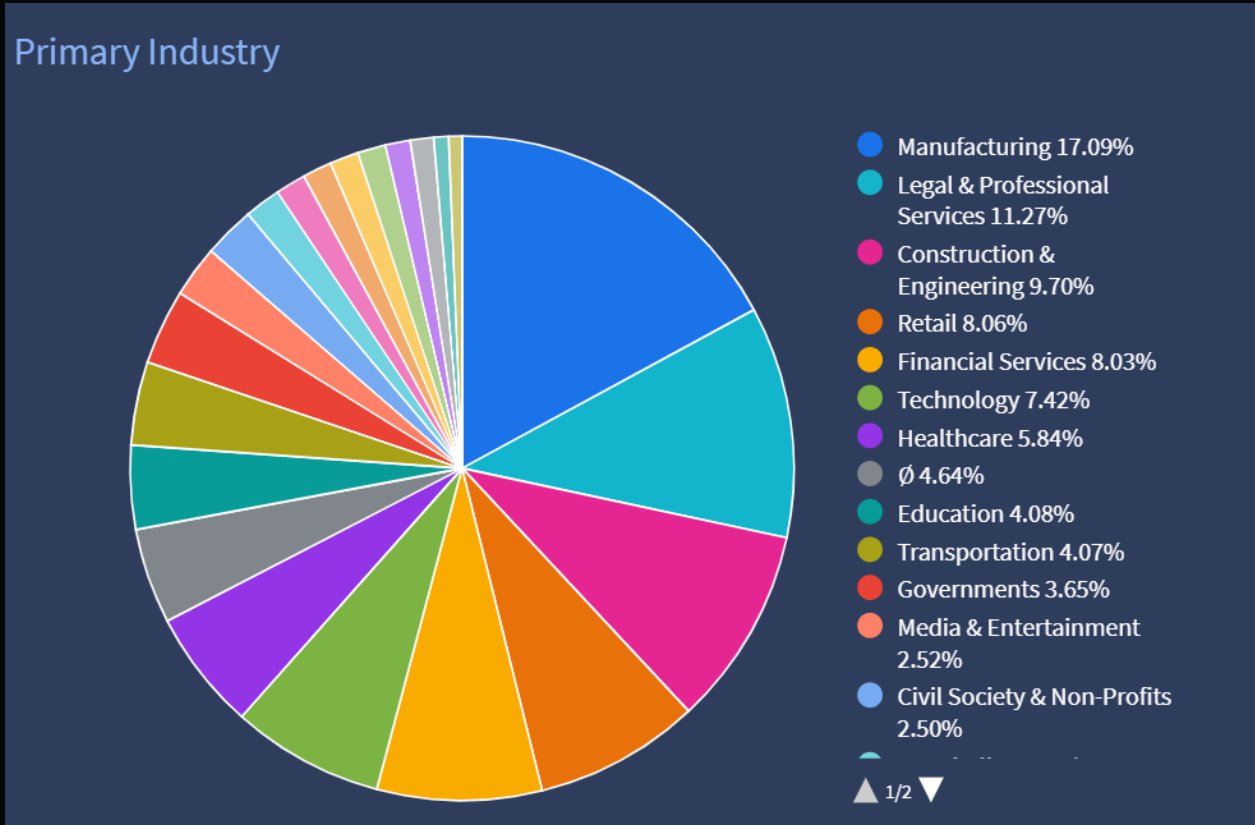


- North American victims listed on ransomware data leak sites (DLS's) were primarily small and medium sized businesses (SMBs), indicating attackers' shift from larger to smaller enterprises.
- The two most targeted entities by company size were 51-200 employees (32.1%) and 11-50 employees (31.9%).
- SMBs are typically seen as low-hanging fruit due to their historically weaker security infrastructure and lower cybersecurity budgets, compared to larger entities.

Ransomware targeting North America

Ransomware poses one of the most pervasive threats to entities in North America, targeting nearly all industries across both the private and public sectors.

Companies in the United States and Canada listed on ransomware data leak sites (DLS's) (January 1-September 15, 2025)
(Google Threat Intelligence)



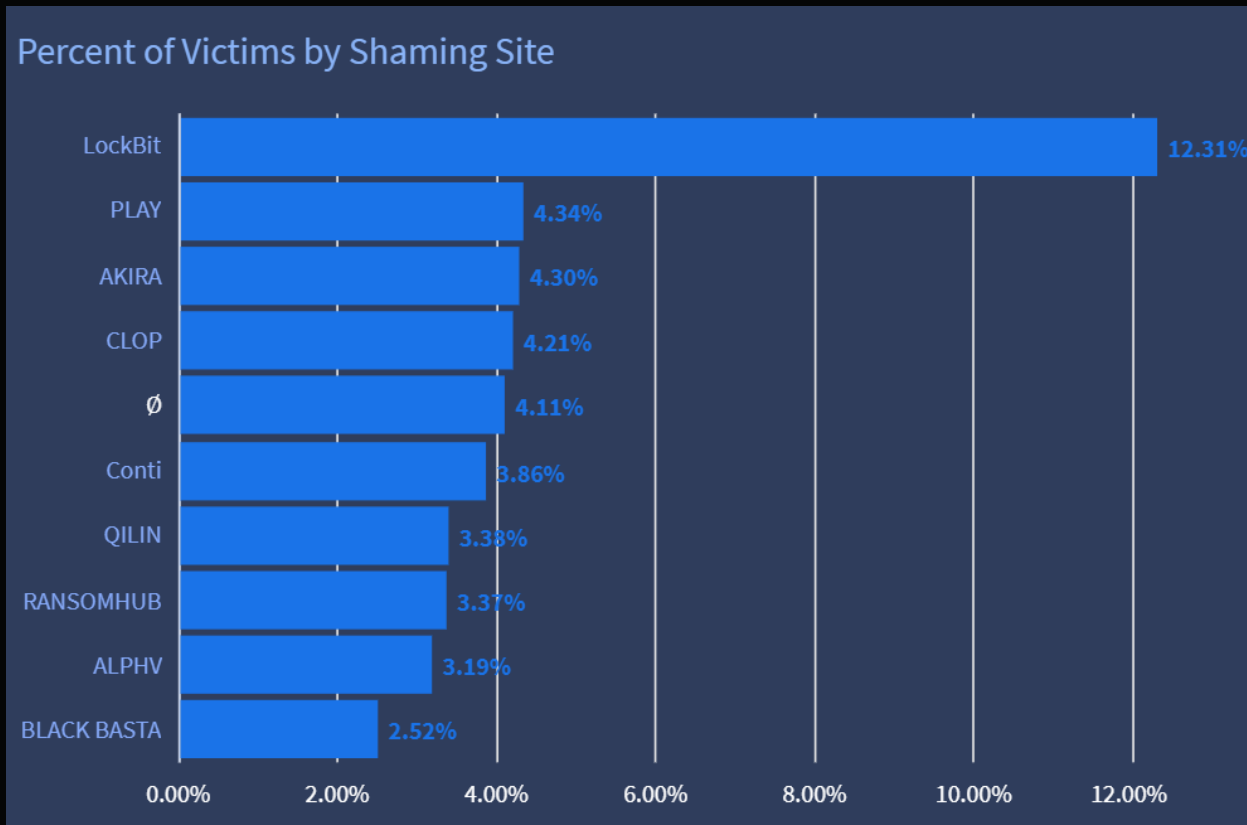
The top three industries listed across Ransomware-as-a-Service (RaaS) DLS's included:

- Manufacturing (17%) – The manufacturing sector was the most targeted industry in North America. Clop listed the greatest number of Manufacturing victims on its DLS.
- Legal & Professional Services (11.2%) – mostly Akira and Qilin.
- Construction & Engineering (9.7%) – mostly Akira, followed by Play and Qilin.

Ransomware targeting North America

Ransomware poses one of the most pervasive threats to entities in North America, targeting nearly all industries across both the private and public sectors.

Companies in the United States and Canada listed on ransomware data leak sites (DLS's) (January 1-September 15, 2025)
(Google Threat Intelligence)



- LockBit's DLS included the greatest number of North American entities (12.3%) by a wide margin.
- Victims on the LockBit DLS have spanned every region and industry, with organizations most frequently based in the US, France, UK, Canada, and more.
- In May 2025, the LockBit ransomware site was breached and its DLS was leaked online, revealing victim chat logs, user data with plaintext passwords, and insights into the group's methods.

Key regional incidents

Stolen Salesloft Drift OAuth tokens lead to widespread breaches. ^{8, 9, 10}

Salesloft Drift, an AI chatbot that can be integrated with Salesforce and other applications, announced in August a threat actor had gained access to OAuth tokens for its customers' technology integrations. The tokens were stolen from the company's AWS environment which the threat actor, called UNC6395, had moved into laterally after initially gaining access into Salesloft's GitHub account in March 2025. As of mid-September, Salesloft was still conducting remediation and fortification efforts to restore Drift.

In addition to the impact to Salesloft as the primary victim, secondary impacts include potential data exposures for hundreds of companies, including several high-profile cybersecurity companies that have already acknowledged data breaches because of the stolen OAuth tokens. In response to the ongoing campaign by UNC6395, the FBI released a FLASH advisory on September 12 warning about the campaign and sharing Indicators of Compromise and recommended mitigation measures.

Bridgestone Americas victim of cyber attack. ^{6, 7}

In September, tire company Bridgestone confirmed it was the victim of a cyber attack that impacted the operations of some of its manufacturing facilities in North America. While the exact nature of the cyber incident is not clear, threat actors associated with Scattered Spider, Lapsus\$, and Shiny Hunters have claimed the attack. Bridgestone stated it currently has no indications customer data or interfaces were impacted.

The attack on Bridgestone highlights the continued targeting of manufacturing facilities by threat actors associated with Scattered Spider. The quick response by Bridgestone is consistent with the recent IBM Cost of a Data Breach report that cited increased native incident response capabilities as a key factor in lowering data breach costs.

Chinese cyberespionage campaigns continue to target US Congress. ¹¹

On September 8, the US House Select Committee on China released a statement calling attention to an ongoing series of cyberespionage campaigns targeting and/or impersonating members of the US Congress and their staff. The report called out multiple occasions in recent weeks where the suspected Chinese nation-state hackers impersonated the chairman of the committee, John Moolenaar, in emails to "trusted counterparts" to get them to open malicious files. This followed a previous campaign in January that targeted committee staffers with a spearphishing campaign designed to steal Microsoft 365 credentials.

Chinese cyberespionage continues to grow increasingly aggressive. The attempt to steal Microsoft credentials reflects a larger trend across both nation-state actors and cybercriminals in seeking legitimate credentials to gain access to sensitive data and networks.

US sanctions cyber scammers responsible for the theft of billions of dollars. ¹²

The US Treasury Department announced sanctions against several large networks of cybercriminal scammers based in Southeast Asia. These networks were responsible for the theft of over \$10 billion from Americans in 2024. These networks leveraged forced labor, violence, and human trafficking to operate online fraud centers, forcing individuals to participate. The sanction targets are located primarily in Burma and Cambodia.

The sanctions will block these entities from the US financial system and ban them from any business with US citizens and/or companies, introducing additional legal risk to their operations and to any US citizen involved in their operations in addition to existing criminal statutes.

Deep dive of the month

LastPass Threat Intelligence, Mitigation, and Escalations (TIME) and GuidePoint Security's GRIT Threat Intelligence teams published a [joint report](#) to highlight the infostealer threat. Infostealers have been a major contributing factor driving cybercrime activity since credentials are the primary keys to accessing digital systems and data. Between stealers' high attack volume and growing sophistication, this threat will remain one of the key challenges to securing identity for the foreseeable future. Check out the full report for more in-depth analysis.^{13,14}



What are infostealers?

- Infostealers are a type of malware designed to “steal” sensitive information from infected devices.
- Modern stealers target credentials, browser and session cookies, infected operation systems, and more.



How do they work?

- Widespread adoption of the MaaS model, where developers run operations to support customers who buy the malware license to use the malware.
- Attackers sell repackaged data as logs on the dark web for as little as \$10.



How have they evolved?

- Many stealers are now capable of bypassing devices with anti-virus software, endpoint detection, and response solutions.
- Server-side stealers are one of the most recent evolutions, which are stealthier.

Deep dive of the month

HOW CAN YOU PROTECT YOURSELF?



Defenders can integrate threat feed-provided indicators to identify or prevent connection attempts to known stealer **Command-and-Control (C2) infrastructure. Indicators integrated into the proper tooling can detect or block the execution of known malware.**



Monitoring the dark web for exposed credentials is another preventative measure. If you don't know what information is out there, you're flying blind. Monitoring allows you to take control and act on exposed credentials, like revoking active sessions, resetting passwords, and enforcing MFA on all accounts.



Strong password management is essential. Password managers can help avoid password reuse, which enables brute-force attacks, and storing unencrypted credentials in browsers. This is a key target after stealers infect a system because threat actors know this is a common poor cybersecurity practice.

Trends on tap:

Supply chain attacks

NPM packages targeted as part of ongoing supply chain attacks.¹⁷

To maximize return on investments, threat actors have been targeting NPM packages and injecting malicious code, leveraging the widespread use of open-source software and corresponding dependencies to conduct massive supply chain attacks. In early September, threat actors targeted an individual responsible for maintaining several widely used NPM packages with a phishing email, gaining access to his account and injecting malicious code into NPM packages associated with 2.6 billion downloads weekly. Another attack in mid-September involved a self-replicating worm that infected nearly 200 NPM packages.

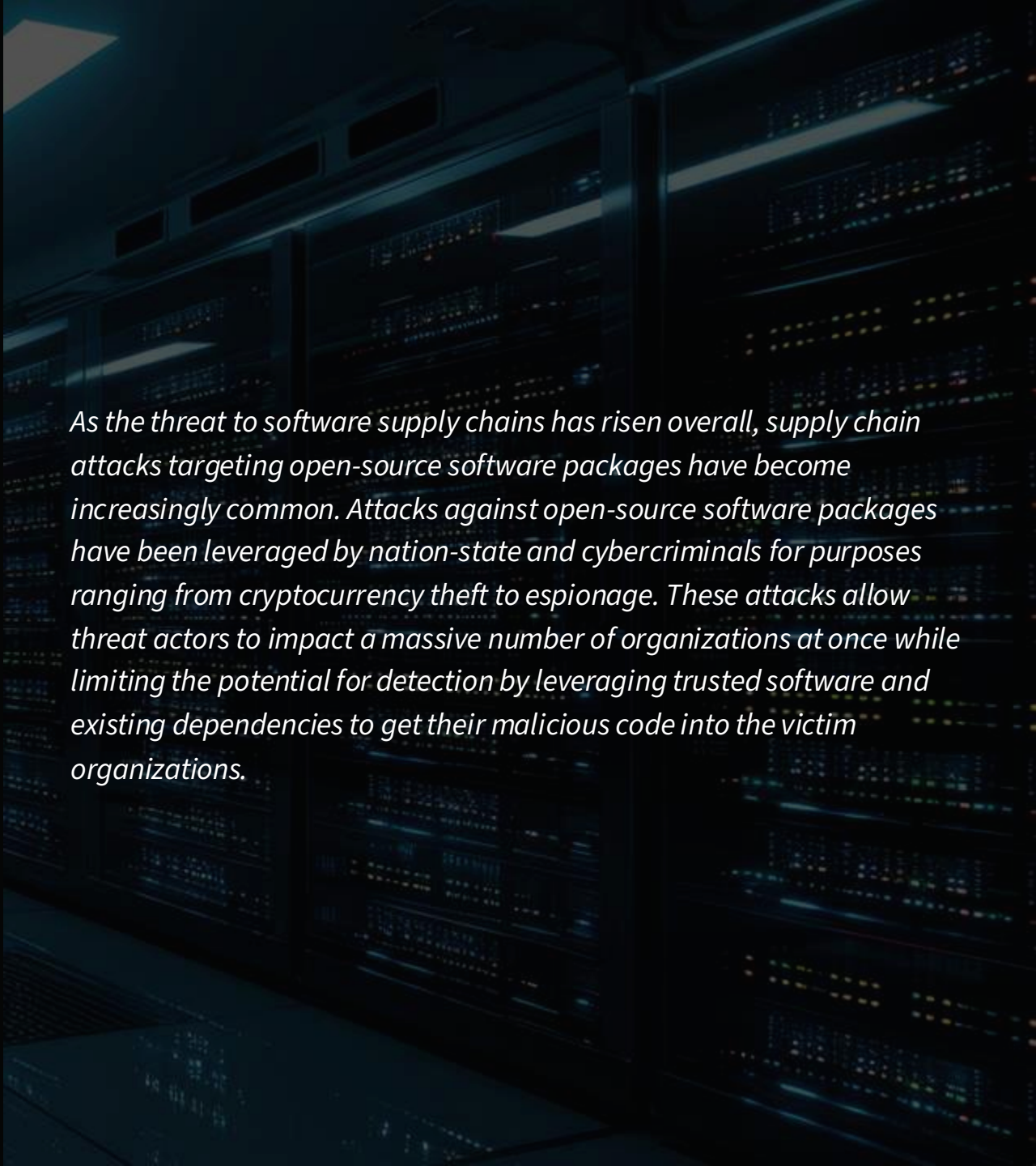
Supply chain attacks are not just impacting open-source software repositories. Two prominent examples of supply chain attacks targeting proprietary products include Russia's NotPetya wiper malware attack in 2017, which infiltrated a Ukrainian tax preparation software to deliver the malicious code that then ended up spreading globally, and Russia's SolarWinds supply chain attack that was discovered in December of 2020. In that attack, the US government estimated approximately 18,000 public and private sector customers of SolarWinds were impacted, though only a much smaller fraction of those were targeted with follow-on exploitation and attacks by Russian nation-state cyber threat actors.

Trends on tap:

China's threat to infrastructure

International cyber agencies highlight global threat to infrastructure from Chinese-backed actors.¹⁶

A recent joint advisory from a wide range of national law enforcement and cybersecurity agencies, including organizations from Canada, the UK, Australia, New Zealand, the US, Czechia, and Japan, have called attention to China's ongoing cyberespionage campaigns targeting global communications networks. These include networks within the telecommunications, government, transportation, loading and defense sectors, underscoring the breadth of the campaign. The advisory also provides extensive details on case studies; tactics, techniques, and procedures; indicators of compromise; and recommended mitigations and best practices. This advisory is the latest in a series over the last few years detailing Chinese efforts to access global critical infrastructures for cyberespionage and potentially disruptive purposes.



As the threat to software supply chains has risen overall, supply chain attacks targeting open-source software packages have become increasingly common. Attacks against open-source software packages have been leveraged by nation-state and cybercriminals for purposes ranging from cryptocurrency theft to espionage. These attacks allow threat actors to impact a massive number of organizations at once while limiting the potential for detection by leveraging trusted software and existing dependencies to get their malicious code into the victim organizations.

Want more?



Hooked on cybersecurity? Dive into *The Phish Bowl* podcast, where the LastPass TIME team's Stephanie Schneider and Mike Kosak cast a wide net on the latest on cyber threats, trends, and tales from the digital deep.

Follow **The Phish Bowl**



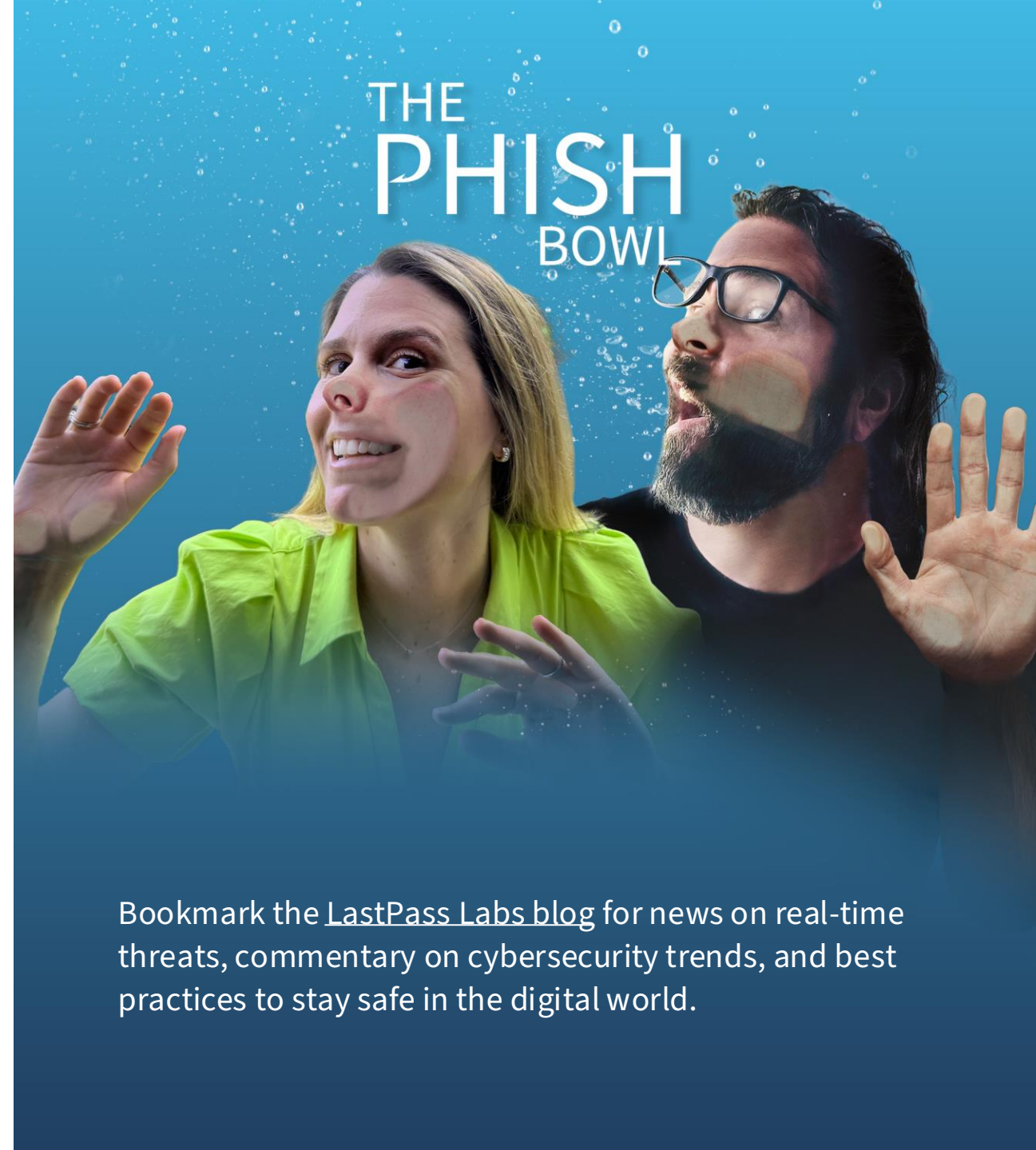
YouTube



Spotify



Apple



Bookmark the [LastPass Labs blog](#) for news on real-time threats, commentary on cybersecurity trends, and best practices to stay safe in the digital world.

Appendix – Sources & additional reading

1. [X-Force 2025 Threat Intelligence Index \(IBM\)](#)
2. [Cost of a Data Breach Report 2025 \(IBM\)](#)
3. [Internet Crime Report 2024 \(FBI\)](#)
4. [Ransomware and Cyber Threat Insights Q2 2025, April-June 2025 \(GuidePoint Security\)](#)
5. [Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations \(CISA\)](#)
6. [Bridgestone Americas continues probe as it looks to restore operations \(Cybersecurity Dive\)](#)
7. [Tire giant Bridgestone confirms cyberattack impacts manufacturing \(Bleeping Computer\)](#)
8. [Salesloft+Drift Trust Portal \(Salesloft\)](#)
9. [Widespread Data Theft Targets Salesforce Instances via Salesloft Drift \(Google\)](#)
10. [FBI FLASH: Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion \(TLP Clear\) \(FBI\)](#)
11. [Committee Statement on Ongoing PRC Cyber-Espionage Targeting U.S. Trade Policy Stakeholders \(US Congress\)](#)
12. [U.S. sanctions cyber scammers who stole billions from Americans \(Bleeping Computer\)](#)
13. [Joint Report with LastPass and GuidePoint Security Researchers: “Fighting Back Against Infostealers and How to Build Resilience in a Digital Identity Crisis” \(LastPass\)](#)
14. [The Rise of Infostealers: How Digital Identity Theft Fuels the Cybercrime Economy \(GuidePoint Security\)](#)
15. [Joint Cybersecurity Advisory: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System \(TLP Clear\)](#)
16. [Breakdown: Widespread npm Supply Chain Attack Puts Billions of Weekly Downloads at Risk \(Palo Alto Networks\)](#)