MARCH 2026

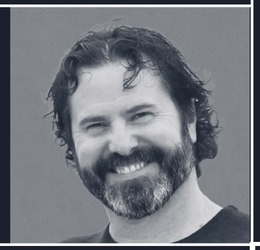
REGIONAL THREAT REPORT
AMERICAS

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

DIRECTOR OF THREAT
INTELLIGENCE



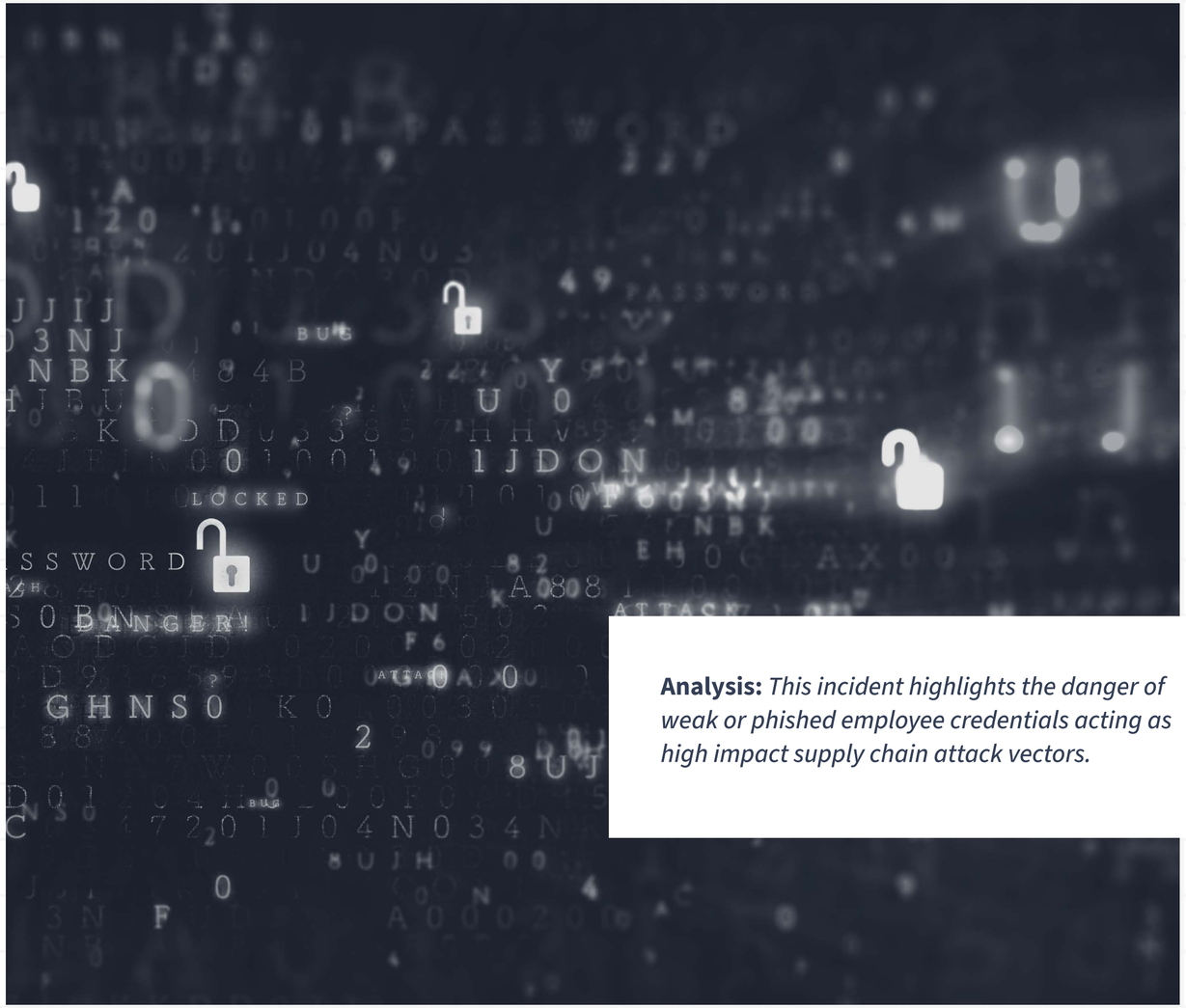
The Regional Threat Report delivers strategic insights from the LastPass Threat Intelligence, Mitigation & Escalation (TIME) Team into the evolving cyber threat landscape across key global markets. Each edition provides a concise, intelligence driven overview of the most significant threats affecting organizations within a specific region, including Europe, Asia-Pacific, and North America.

For more cybersecurity insights, visit the LastPass Threat Intel blog or listen to The Phish Bowl podcast featuring the LastPass TIME team.

TELUS DIGITAL BREACH LINKED TO UP-STREAM AND DOWN-STREAM SUPPLY CHAIN COMPROMISE ENABLED BY CREDENTIAL THEFT.

Telus Digital, a major Canadian telecommunications provider, was compromised through an upstream supply chain breach originating at Salesloft/Drift in 2025. ShinyHunters found valid Telus GCP credentials inside data previously stolen during the Salesloft Drift integration compromise, which exposed Salesforce data for over 760 organizations, including API keys, auth tokens, and embedded credentials. Using those credentials, ShinyHunters conducted largescale lateral movement across Telus infrastructure, enabling a “credential cascade,” and allegedly exfiltrated nearly 1 petabyte of data across 28+ companies serviced by Telus Digital, including call centers, support platforms, operational datasets, source code, and analytics data. Because Telus is a BPO provider for many firms, the compromise created immediate access pathways into customer environments, most notably Crunchyroll’s analytics and support systems.

SOURCE



Analysis: *This incident highlights the danger of weak or phished employee credentials acting as high impact supply chain attack vectors.*

WIDESPREAD CREDENTIAL THEFT CAMPAIGN HARVESTS VPN AND ENTERPRISE LOGIN CREDENTIALS.

In mid-January 2026, Microsoft identified a largescale credential theft operation run by Storm2561, distributing fake enterprise VPN clients through SEO poisoned search results. Users searching for trusted VPN software were redirected to malicious ZIP files where digitally signed trojans harvested VPN and enterprise login credentials. GitHub repositories hosting the malware were later removed, but not before significant exposure occurred.

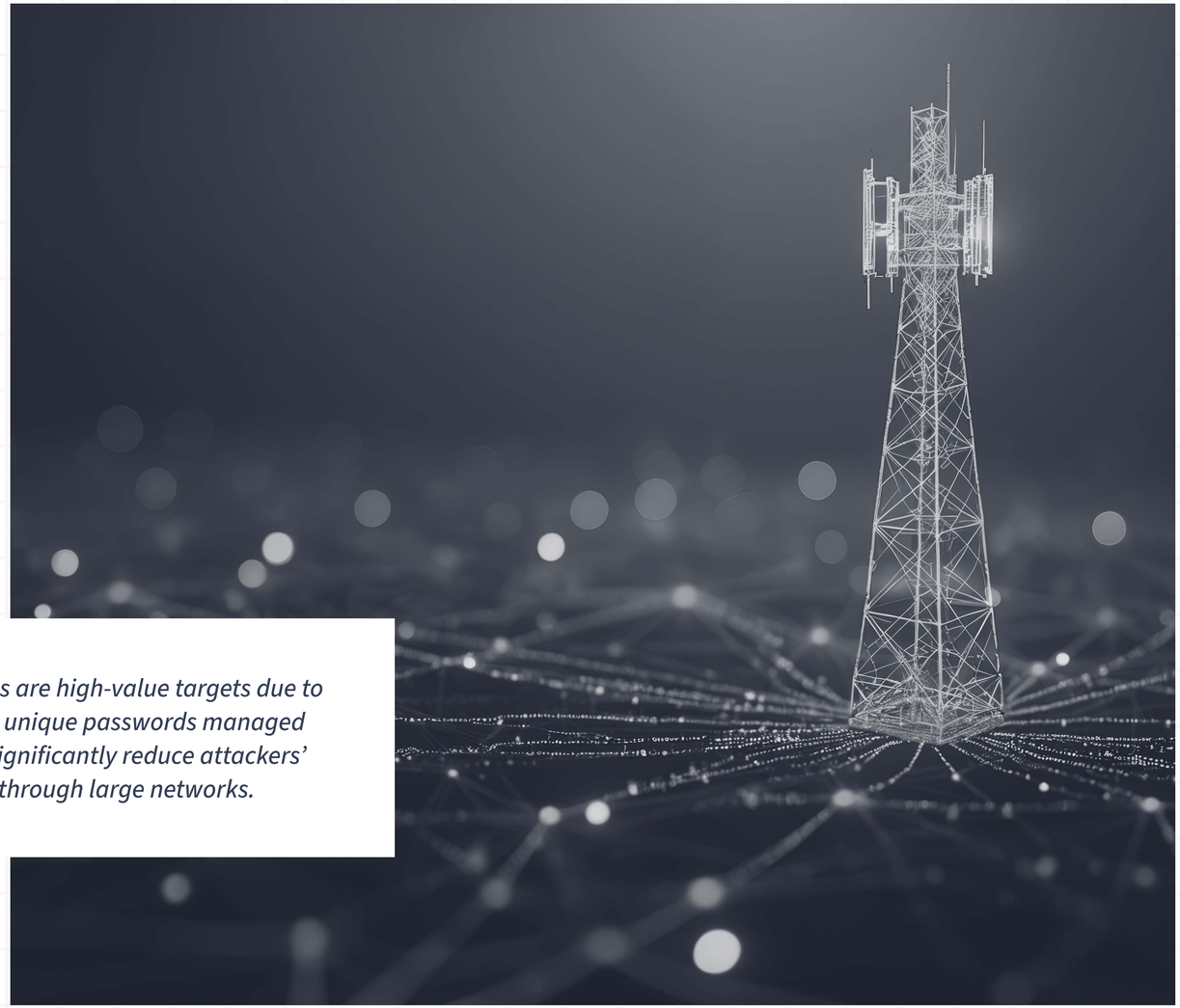
SOURCE

Analysis: *This campaign highlights the ease with which credential harvesting malware can masquerade as legitimate enterprise software and underscores the necessity of credential compartmentalization. A password manager with strong, unique secrets ensures that stolen VPN credentials do not provide broad internal access, limiting blast radius when endpoint compromise occurs.*

CHINESE STATE HACKERS TARGET SOUTH AMERICAN TELCOS WITH NEW MALWARE TOOLKIT.

A China-linked hacking group has been breaking into phone and internet companies in South America since 2024, deploying a custom toolkit designed for Windows, Linux, and telecom network equipment. The tools include a Windows backdoor, a peer-to-peer Linux implant, and an automated password-guessing utility. These attacks target telecom providers, which run the communication systems millions of people rely on every day.

SOURCE



Analysis: *Telecom systems are high-value targets due to their connectivity. Strong, unique passwords managed by a password manager significantly reduce attackers' ability to spread laterally through large networks.*

CYBERCRIMINAL GROUP SHINYHUNTERS SIMPLY LOGGED INTO CRUNCHBASE INTERNAL NETWORK AFTER TRICKING AN EMPLOYEE INTO HANDING OVER CREDENTIALS.

In January 2026, U.S.-based database company Crunchbase confirmed it was hacked after the cybercrime group ShinyHunters published files stolen from the company's internal network. ShinyHunters reportedly compromised Crunchbase by calling an employee and tricking them into giving up their Okta single-sign-on credentials through a voice phishing (vishing) operation. Attackers accessed more than 2 million internal records containing sensitive corporate intelligence and leaked the data after Crunchbase refused ransom demands.

SOURCE

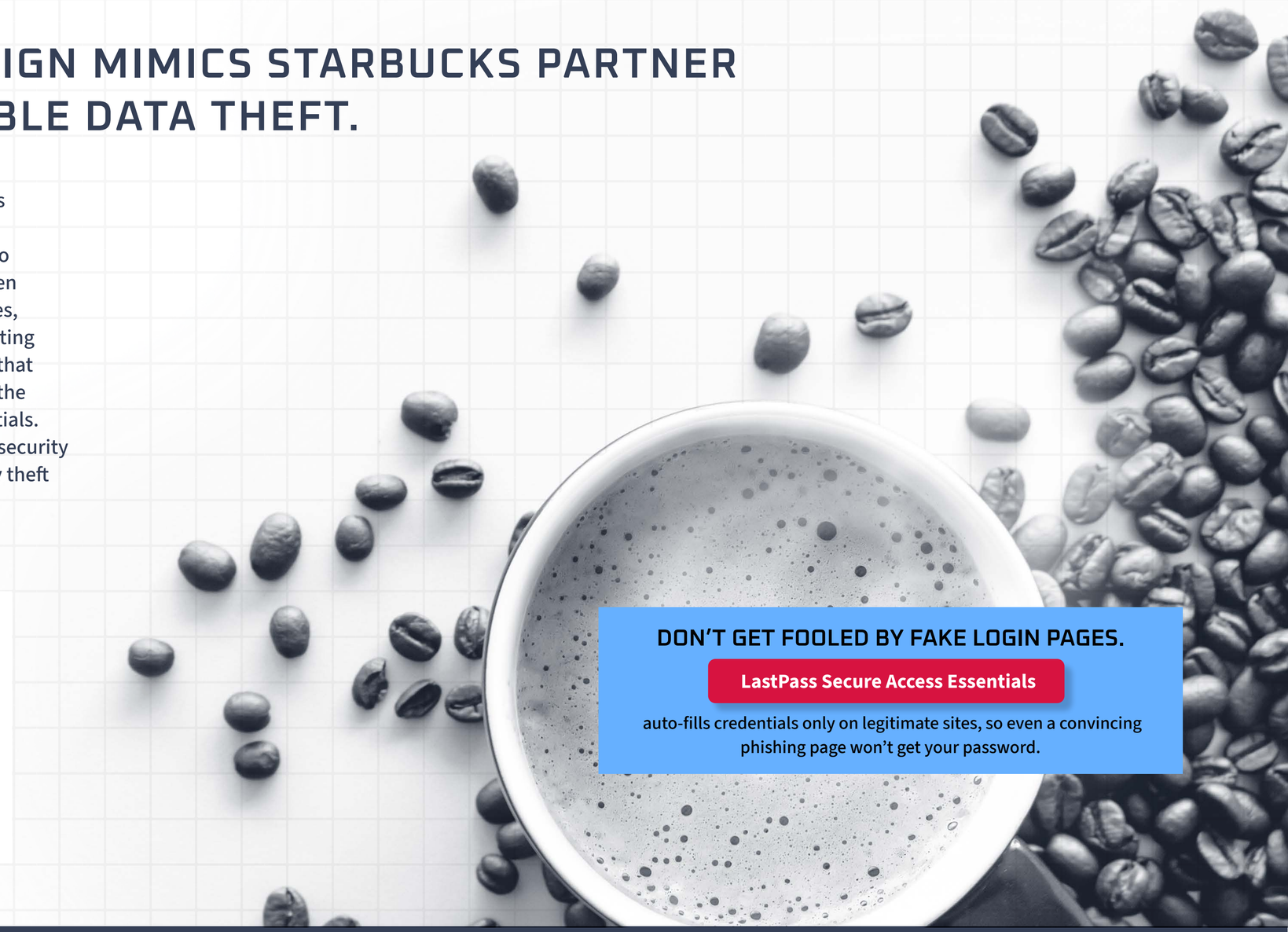
Analysis: *This breach demonstrates attackers continue to use methods like social engineering and vishing to acquire valid credentials and log in. The leaked data may now be misused for identity theft, fraud, and targeted social engineering attacks against individuals and companies connected to Crunchbase.*

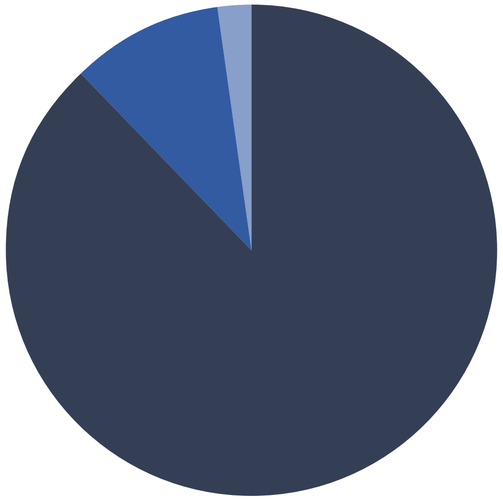
CREDENTIAL THEFT CAMPAIGN MIMICS STARBUCKS PARTNER CENTRAL WEBSITE TO ENABLE DATA THEFT.

Starbucks confirmed in February 2026 that hundreds of employees were affected by a breach of its internal Partner Central portal—used for payroll, benefits, and HR. Attackers tricked employees into entering credentials on fake websites mimicking the portal between January 19 and February 11. Attackers accessed employees' names, Social Security numbers, dates of birth, and bank account and routing numbers. Starbucks said that no customer data was involved and that the company's internal systems were not directly breached—only the employee accounts that attackers logged into using stolen credentials. The company notified law enforcement, strengthened its account security controls, and offered affected employees two years of free identity theft protection and credit monitoring.

SOURCE

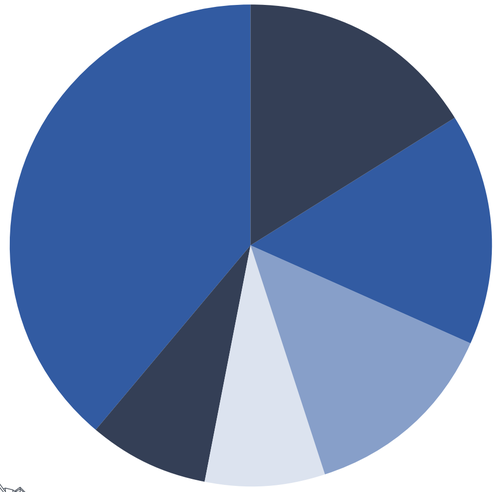
Analysis: *No malware was used; this breach relied entirely on trust exploitation and identity impersonation. A password manager protects against this type of attack by auto-filling credentials only on legitimate sites, alerting users to impostor pages and ensuring strong, unique passwords limit damage from any single compromised account.*





Most Targeted Countries:

- **88%** United States
- **10%** Canada
- **2%** Mexico



Most Targeted Industries:

- **16.3%** Legal & Professional Services
- **15.4%** Construction & Engineering
- **13.3%** Manufacturing
- **8.1%** Financial Services
- **8.1%** Healthcare
- **38.8%** Other

Most Active Ransomware Group: Qilin

Target Profile: Small and medium-sized businesses (SMBs) remain the most frequently targeted companies in North America. Companies of this size are generally attractive to attackers because they offer a balance of valuable data, ransom-paying capability, and perceived weaker defenses compared to larger enterprises.

RANSOMWARE PAYMENTS DROPPED IN 2025 AS ATTACK NUMBERS REACHED RECORD LEVELS:

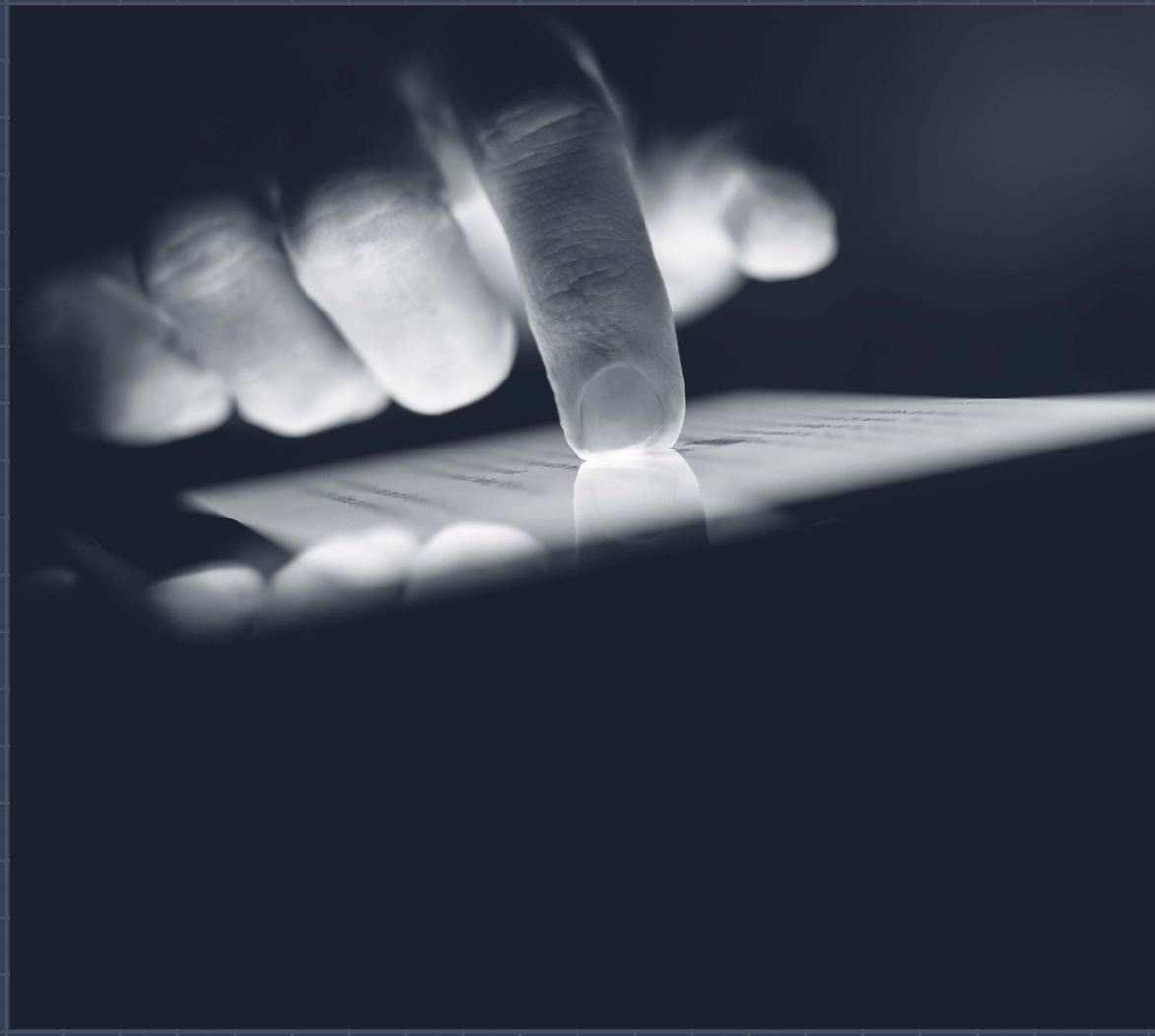
The Chainalysis 2026 Crypto Crime Report reveals some significant changes in the ransomware ecosystem observed over the last year.

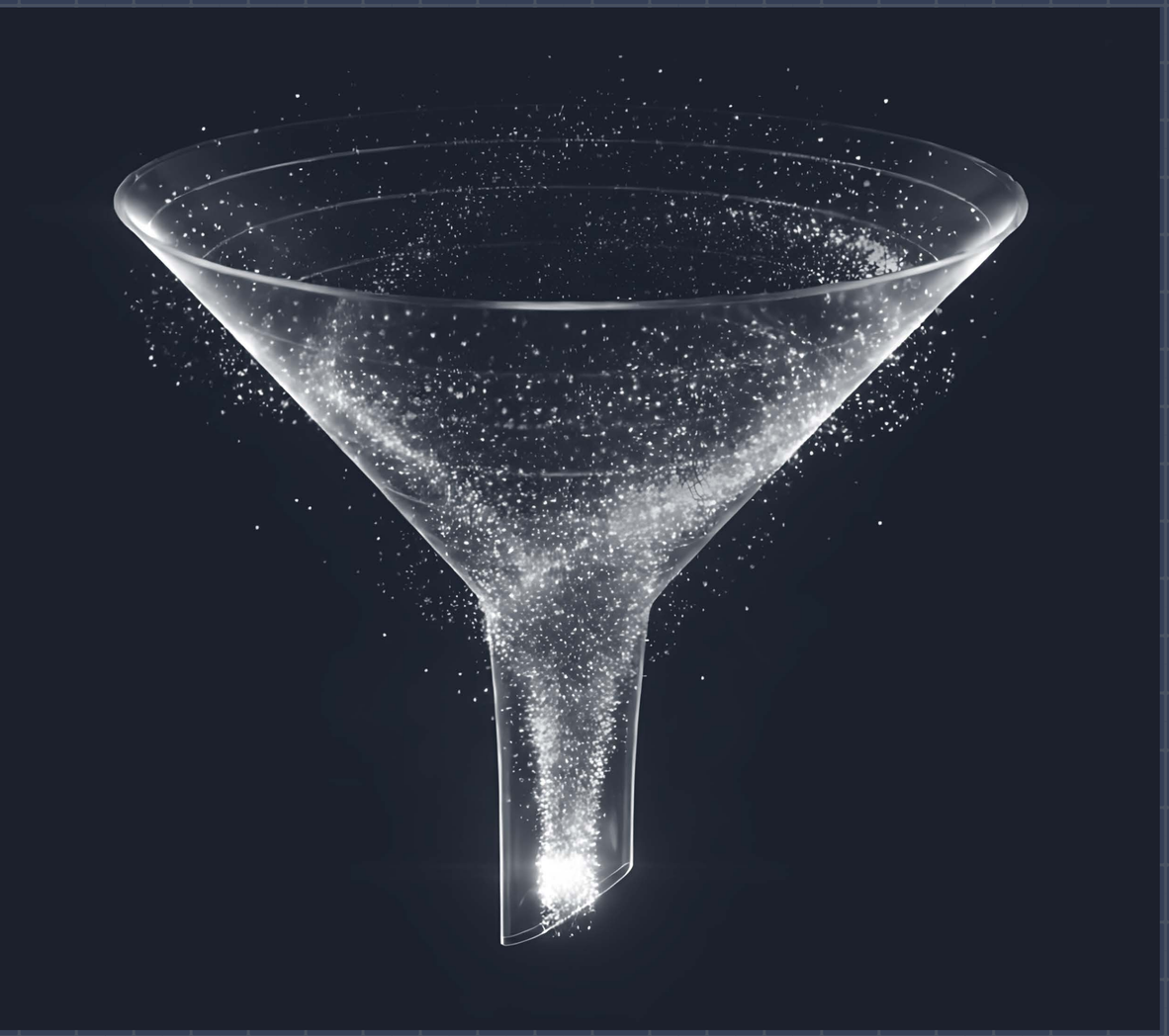
– Ransomware has shifted from Big Game Hunting to a commoditized volume-based model targeting small and medium enterprises (SMEs). However, mega breaches like Jaguar Land Rover ($2.5 billion in damage) and Marks & Spencer still occurred last year.

– This shift is driven by a 1,400% surge in AI-powered impersonation and stolen credentials sold for cheap on the dark web. This means the threat extends beyond breaches to also include the systematic abuse of legitimate credentials readily available for purchase by over 85 active extortion groups.

– The median ransom payment skyrocketed 368% to $59,556, even though only 28% of victims paid— the lowest rate on record. The company's researchers attributed the stark increase in attacks and slowdown in payments to several factors. Companies are improving incident response, and regulatory scrutiny has increased, heavily discouraging payouts. Chainalysis also said law enforcement disruption of major ransomware gangs has fragmented the ecosystem into smaller, independent operations — many using poorly designed malware that can be decrypted.

SOURCE





RANSOMWARE PAYMENTS DROPPED IN 2025 AS ATTACK NUMBERS REACHED RECORD LEVELS: SOURCE

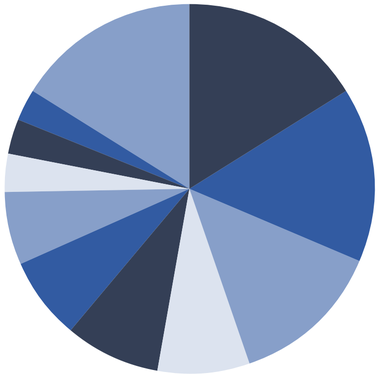
The Gateway to Extortion: How Credentials Fuel the Modern Ransomware Machine

– The “hack” often begins long before one file is encrypted. Chainalysis reported the ransomware economy has shifted to an industrialized, volume-based model where stolen credentials are the primary currency. The image of a lone hacker breaking into a server is now a sophisticated supply chain where credentials are harvested, sorted by AI, and sold in bulk.

– Here is how credentials fit into this evolving picture:

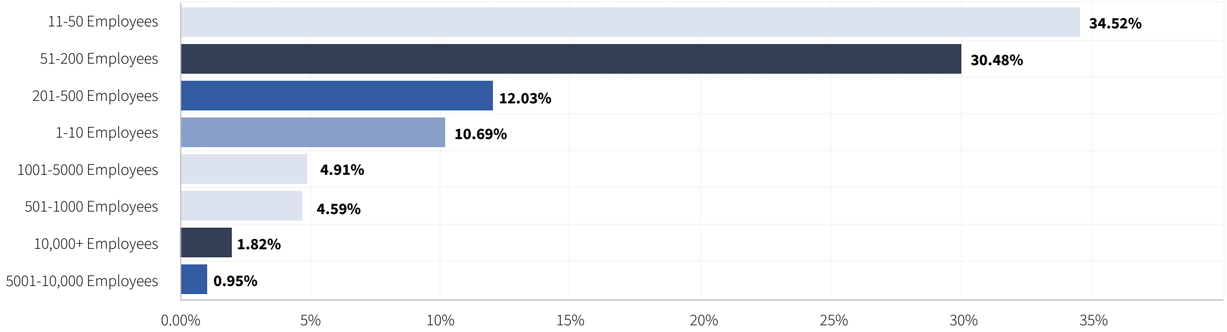
- Industrialized Access Pipelines: Initial Access Brokers (IABs) have flooded the market with infostealer logs, driving the average cost of victim access down from $1,427 to just $439 by early 2026.
- AI-Enabled Credential Harvesting: Scammers are using AI to automate the sorting of stolen credentials and to author highly persuasive phishing lures. This has led to a 4.5x increase in profitability for credential-harvesting campaigns.
- Vishing & Help Desk Exploitation: Groups like Scattered Spider have successfully used social engineering (vishing) to bypass MFA and hijack IT help desk accounts to gain administrative access.

Primary Industry

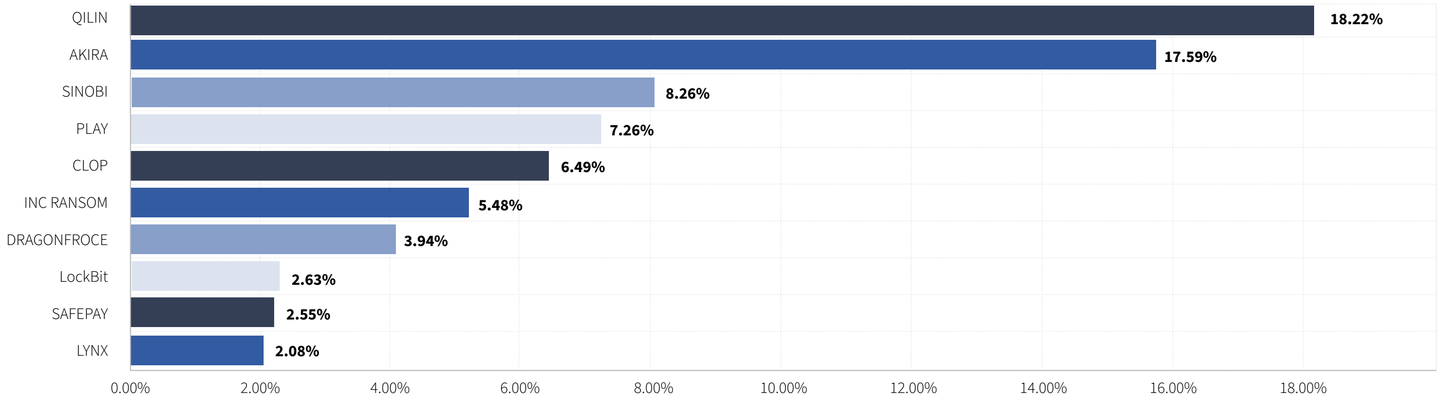


- **16.29%** Legal & Professional Services
- **15.37%** Construction & Engineering
- **13.28%** Manufacturing
- **8.11%** Financial Services
- **8.11%** Healthcare
- **7.34%** Technology
- **6.27%** Retail
- **3.47%** Civil Society & Non-Profits
- **3.14%** Transportation
- **2.78%** Governments
- **15.84%** Other

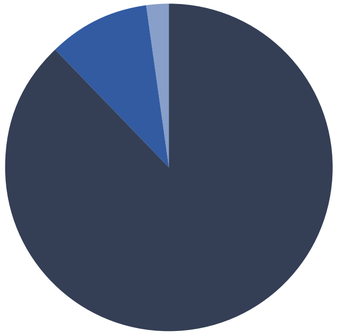
Percent of Victims by Estimated Company Size



Percent of Victims by Shaming Site



Percent of Victims by Country



- **88%** United States
- **10%** Canada
- **2%** Mexico

IRAN-U.S. CONFLICT HEIGHTENS

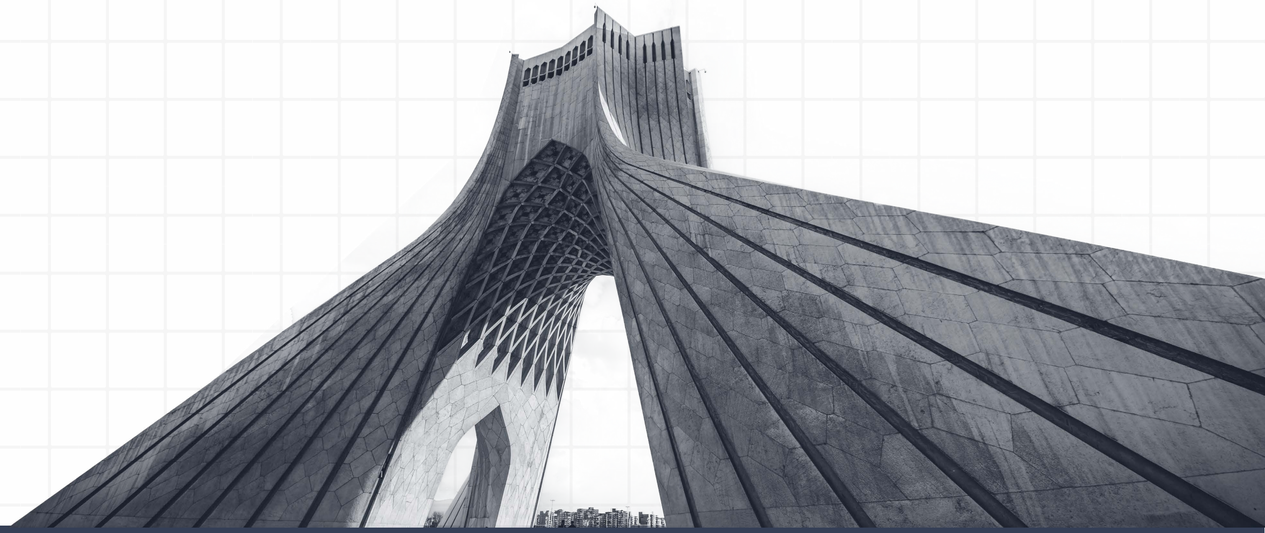
Starting in February 2026, the latest phase of the Iran–U.S. conflict (aka Operation Epic Fury) a hybrid campaign, has paired kinetic military actions with extensive cyber operations. Both sides have used digital operations to project power, disrupt adversary capabilities, and influence public perception. The U.S. launched cyber and space operations to degrade Iranian sensors, communications, and decision-making capabilities, producing internet outages that reduced Iranian connectivity to 1–4% of normal levels. These disruptions along with information operations shared anti-regime narratives, including compromising the widely used mobile app BadeSaba and hijacking state-run media websites.

Iran and Iran aligned hacking groups intensified cyber operations targeting the US and its allies. State-aligned actors—CyberAv3ngers, APT33, APT55, and MuddyWater—conducted attacks against American industrial control systems, critical infrastructure, and corporate networks. Attacks have included default password exploitation on industrial machines, password spray campaigns against energy companies, and large-scale device wiping, most notably Handala Hack's attack on U.S. medical device manufacturer Stryker.

The attackers exploited Microsoft Intune to wipe more than 200,000 devices and disrupted systems in 79 countries, marking one of the first largescale disruptive attacks on a major U.S. corporation during the conflict. In addition to these intrusions, Iran aligned hackers attempted to compromise Middle Eastern cameras to support missile targeting, probed U.S. defense contractors and water facilities, and allegedly attempted intrusion at a Polish nuclear research center.

The Islamic Revolutionary Guard Corps (IRGC) named Western companies—including technology firms—as targets, reinforcing that Tehran views tech companies as integral to Western critical infrastructure rather than neutral service providers. This aligns with longstanding Iranian targeting patterns: targeting American water plants, defense contractors, and the broader Defense Industrial Base (DIB) to degrade military capability, increase operational and energy costs, and generate economic disruption.

These activities reflect Iran's hybrid cyber strategy: espionage, sabotage, destructive attacks, and information operations carried out by a mix of state entities and aligned hacktivist groups. CISA and the FBI have repeatedly warned that Iranian actors target American critical infrastructure and political organizations using brute force attacks, credential theft, and exploiting known vulnerabilities, especially during periods of heightened geopolitical tension. As the conflict escalates, increased activity from ransomware operators and patriotic hacktivists is likely.



IRAN-U.S. CONFLICT HEIGHTENS

This conflict highlights several key lessons:

1. Kinetic operations can have unintended cyber spillover effects, including collateral damage to cloud or third-party infrastructure.
2. The attack surface now extends beyond traditional critical infrastructure, targeting sectors whose supply chain and operational roles can cause cascading effects—such as healthcare, cloud technology, and logistics.
3. Iranian aligned actors increasingly exploit “easy kill switches,” including cloud management tools and central device controllers, where a single compromised credential can trigger large-scale disruption. This is consistent with observed reliance on default credentials, common passwords, and compromised authentication material.

Given ongoing geopolitical instability, organizations—especially critical infrastructure operators, financial institutions, and supply chain adjacent enterprises—should reevaluate and prioritize their cyber hygiene. Recommended actions include:

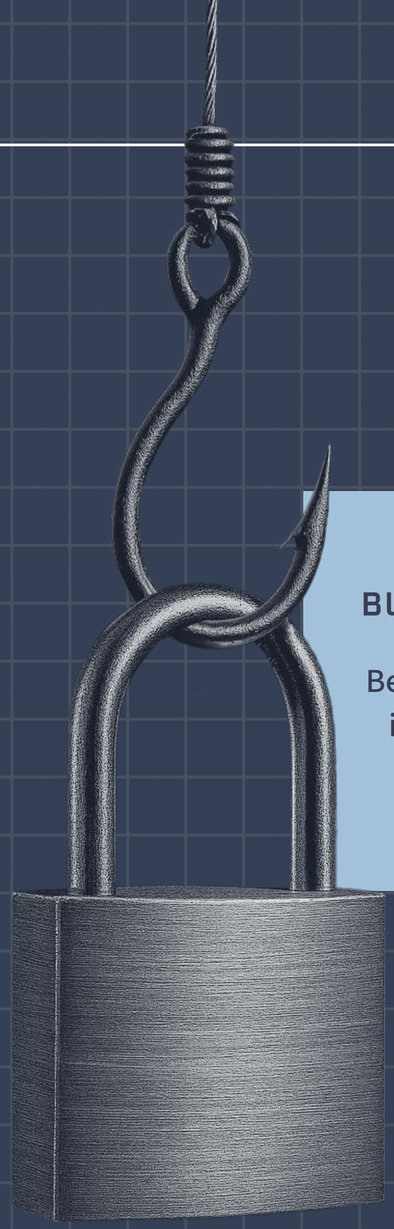
– Use strong, unique passwords across all systems.
– Implement MFA everywhere, with mandatory MFA on all administrative accounts.
– Monitor for leaked credentials, including infostealer log exposure.
– Eliminate default passwords, especially in OT and cloud management environments.
– Harden cloud and device management platforms, which have become high value targets.

LASTPASS ALERTS CUSTOMERS OF FAKE EMAIL CHAINS USED IN NEW PHISHING CAMPAIGN; NO IMPACT TO LASTPASS SYSTEMS

Beginning around March 1, 2026, LastPass's TIME team identified and moved to disrupt a phishing campaign targeting customers. Attackers spoofed LastPass's display name and sent fake security alerts—mimicking forwarded support threads about unauthorized vault exports, account recovery, or new device registrations—to create urgency and trick recipients into revealing their master password. Malicious links led to fake SSO pages designed to harvest credentials. LastPass worked with third-party partners to take down the sites and published a blog post with Indicators of Compromise to raise awareness.

The attack targeted LastPass customers using social engineering tactics but did not impact LastPass infrastructure. It highlights the need for continuous anti-phishing education, improved brand abuse monitoring, and reinforcing customer messaging around verifying support requests and never entering credentials via unsolicited prompts.

Remember that no one at LastPass will ever ask for your master password.
We are working with our third-party partners to have these sites taken down as soon as possible. In the meantime, please take the appropriate precautions, and if you are ever unsure whether a LastPass branded email is legitimate, submit it to abuse@lastpass.com. We would like to thank our customers who have submitted this email for their vigilance and commitment to keeping our community secure.



STRENGTHEN IDENTITY SECURITY ACROSS YOUR BUSINESS WITH LASTPASS SECURE ACCESS ESSENTIALS.

Beyond basic password management capabilities, you'll get visibility into SaaS and AI, strong access controls for every user, and secure access in one lightweight solution.

Learn more