JUNE 2026

REGIONAL THREAT REPORT
NORTH AMERICA

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

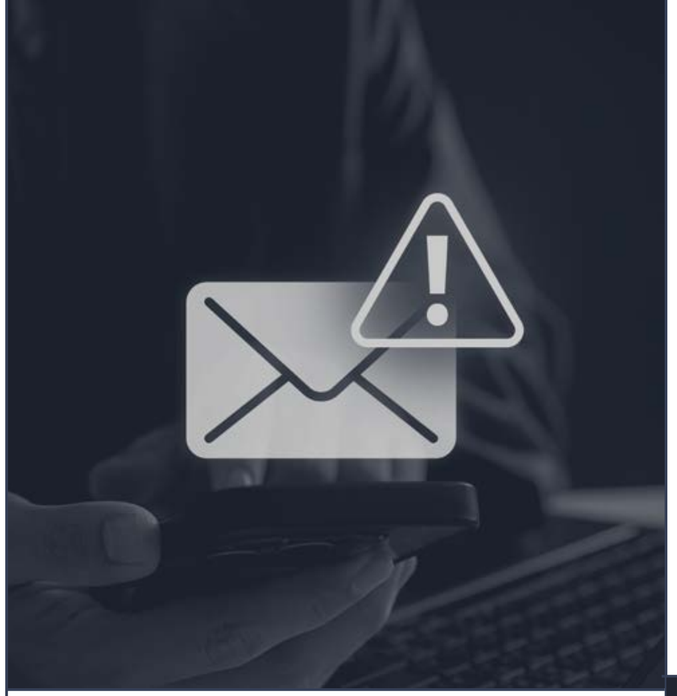
DIRECTOR OF THREAT
INTELLIGENCE

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.

WHAT'S ON TAP THIS MONTH?

Organizations operating across North America face a threat environment shaped by interconnected digital supply chains, heavy reliance on cloud productivity tools, and a patchwork of federal, state, and provincial regulations. When one supplier, platform, or service provider is compromised, the ripple effects quickly spread, affecting businesses of every size.



For small and medium-sized businesses, this shift matters enormously. Many SMBs invest in antivirus software and firewalls but have not updated how they think about identity: who has access to what, which apps connect to employee accounts, and whether staff can recognize a login page designed to steal their credentials. As attackers increasingly use AI-powered tools to make phishing emails look legitimate and automate credential theft at scale, the gap between organizations with strong identity hygiene and those without is growing fast.

Over the last few months, the most consistent pattern across North American cyber incidents was not hackers "breaking in," but rather hackers logging in. Across breaches affecting telecommunications companies, universities, healthcare systems, and technology platforms, attackers repeatedly entered through stolen credentials, piggybacked on trusted app connections, or tricked employees into handing over access. In the most notable cases, no firewall was defeated and no vulnerability was exploited. A phishing email, a reused password, or a third-party app permission was all it took.

For North American organizations, incidents involving credential theft, third-party app abuse, or data exfiltration may trigger notification obligations under HIPAA, state breach laws, Canada's PIPEDA, or Mexico's LFPDPPP, even when core operations remain online and no ransomware is deployed.

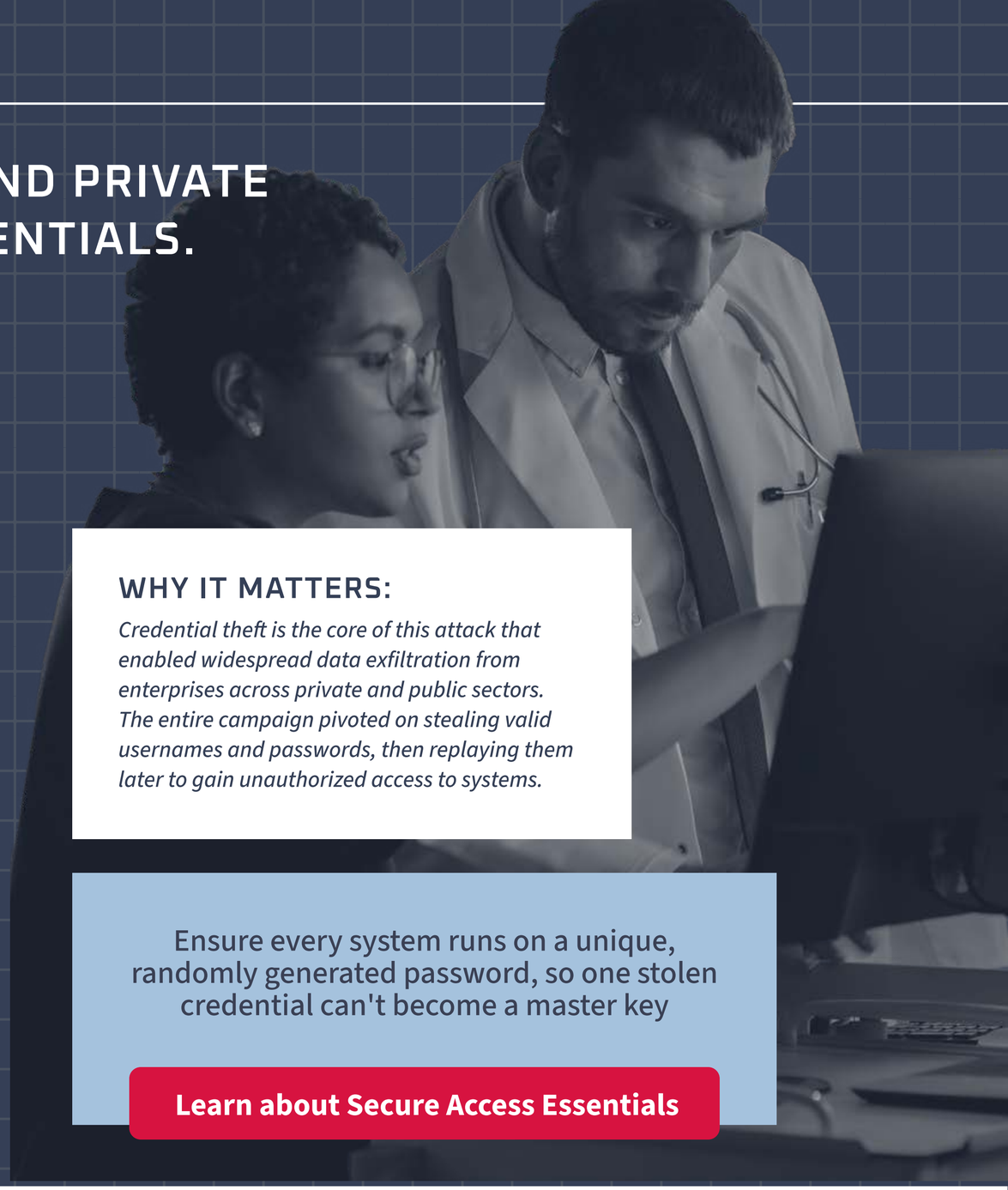
CHINESE HACKERS TARGETING US PUBLIC AND PRIVATE MEDICAL COMMUNITY USING STOLEN CREDENTIALS.

Google's Threat Intelligence Group (GTIG) just published research on a sophisticated, long-running espionage campaign tied to a Chinese state-sponsored threat actor called UNC6508.

KEY TAKEAWAYS:

- The campaign ran undetected for over a year from September 2023 through at least early 2026.
- Targets included entities involved in everything from pandemic response to military readiness, such as North American academic medical centers, military health institutions, government health bodies, and defense-adjacent research organizations.
- UNC6508 started by exploiting externally facing REDCap servers, a popular web-based research data platform, and then deployed custom malware called INFINITERED, which quietly harvested login credentials in the background. The malware cleverly survived software updates by injecting itself into the upgrade process itself.
- After sitting on the systems for over 14 months, they used those stolen credentials to log in as an administrator.
- From there, they used a built-in enterprise email feature (content compliance rules) to silently BCC-forward matching emails to a Gmail account they controlled to effectively wiretap the organization's inbox.

SOURCE



WHY IT MATTERS:

Credential theft is the core of this attack that enabled widespread data exfiltration from enterprises across private and public sectors. The entire campaign pivoted on stealing valid usernames and passwords, then replaying them later to gain unauthorized access to systems.

Ensure every system runs on a unique, randomly generated password, so one stolen credential can't become a master key

Learn about Secure Access Essentials

HACKERS HIT A LEARNING PLATFORM USED BY 41% OF NORTH AMERICAN UNIVERSITIES DURING FINAL EXAMS.

ShinyHunters breached Canvas, a widely used learning management platform in North American higher education, in reportedly the largest education-sector breach on record. The attack disrupted finals week for hundreds of institutions across the US and exposed personal data belonging to a wide age range of students.

KEY TAKEAWAYS:

- *In late April, ShinyHunters gained access by exploiting a vulnerability in a free account program that allowed educators to sign up without institutional verification, enabling the attackers to secure a low-security side door into the platform.*
- *The group claimed to have stolen 3.65 terabytes of data from approximately 275 million users, including private messages between students and teachers, names, email addresses, and student ID numbers.*
- *On May 7, ShinyHunters defaced Canvas login portals at roughly 330 institutions, including Harvard, Princeton, and the University of Pennsylvania, with ransom demands. This secondary attack forced Instructure's platform offline during final exam periods.*
- *Instructure, Canvas's parent company, paid a ransom on May 11 and stated it received confirmation of data destruction. The attack affected 8,809 educational institutions worldwide, with North America bearing the heaviest impact given that Canvas is used by 41% of higher education institutions in the region.*

SOURCE

WHY IT MATTERS:

Schools, colleges, and universities hold enormous amounts of personal data for students, as well as faculty, staff, and contractors. If your organization does business with or employs people affiliated with affected institutions, some of that data may now be in criminal hands. More broadly, any organization that relies on a third-party platform for critical operations like payment processors, HR systems, or collaboration tools should consider their plan if that platform goes down or is compromised. Having your own backups and a business continuity plan is no longer optional.

SOCIAL ENGINEERING ATTACK AGAINST CARNIVAL EXPOSES PERSONAL DATA OF NEARLY 6 MILLION PEOPLE.

ShinyHunters cybercriminal group breached cruise operator Carnival in April 2026 and stole personal information, including passport and driver's license details.

KEY TAKEAWAYS:

- The threat actor reportedly gained access to a limited portion of Carnival's IT environment after using social engineering tactics to compromise an employee account and copied personal information from its systems.
- The stolen data varies by individual. It includes names, addresses, email addresses, phone numbers, dates of birth, driver's license numbers and passport numbers.
- According to the notification shared with the Maine Attorney General's Office, the total number of individuals affected is just under 6 million.

SOURCE

WHY IT MATTERS:

This breach underscores the continued effectiveness of social engineering-driven credential compromise as an initial access vector, particularly by groups like ShinyHunters, which consistently leverages account takeovers to access and exfiltrate large datasets of personally identifiable information (PII). The scale and sensitivity of the stolen identity data increase downstream risk of credential stuffing, identity fraud, and highly targeted phishing, reinforcing the need for phishing-resistant MFA and strong credential hygiene to prevent a single compromised account from exposing high-value identity repositories.

FBI WARNS ABOUT HACKERS USING PHAAS PLATFORM TO BYPASS MFA AND ACCESS MICROSOFT 365 ENVIRONMENTS.

The FBI recently issued a warning about the Kali365 phishing-as-a-service (PhaaS) platform, which facilitates Microsoft 365 account hijacking by abusing OAuth device code authentication and adversary-in-the-middle (AitM) proxying.

KEY TAKEAWAYS:

- These methods bypass multi-factor authentication (MFA) to steal session tokens, granting unauthorized access to cloud environments, enabling data theft, and allowing the persistence of malicious inbox rules and device registrations.
- The campaigns primarily targeted Microsoft 365 environments using phishing emails impersonating trusted cloud productivity and document sharing services that directed victims to Microsoft's device code login portal, where they unknowingly authorized attackers to access their Microsoft 365 accounts and various services, including Teams, Outlook and OneDrive.

SOURCE

WHY IT MATTERS:

The Kali365 platform subscription serves as an entry point for less sophisticated attackers. The FBI warning comes about a month after a report by Arctic Wolf on an operation that used the Kali365 platform. Other recent reports have found criminal actors using device-code phishing to gain access to Microsoft 365 accounts.

IRAN-LINKED HACKERS TARGET KEY US, ALLIED SECTORS WITH SOPHISTICATED SPEAR-PHISHING MESSAGES.

Palo Alto Networks recently reported that Iranian government-backed hackers are using spear-phishing attacks and remote access Trojans (RATs) to spy on “high-value sectors” in the U.S. and the Middle East as part of Tehran’s response to the U.S.-Israeli war.

KEY TAKEAWAYS:

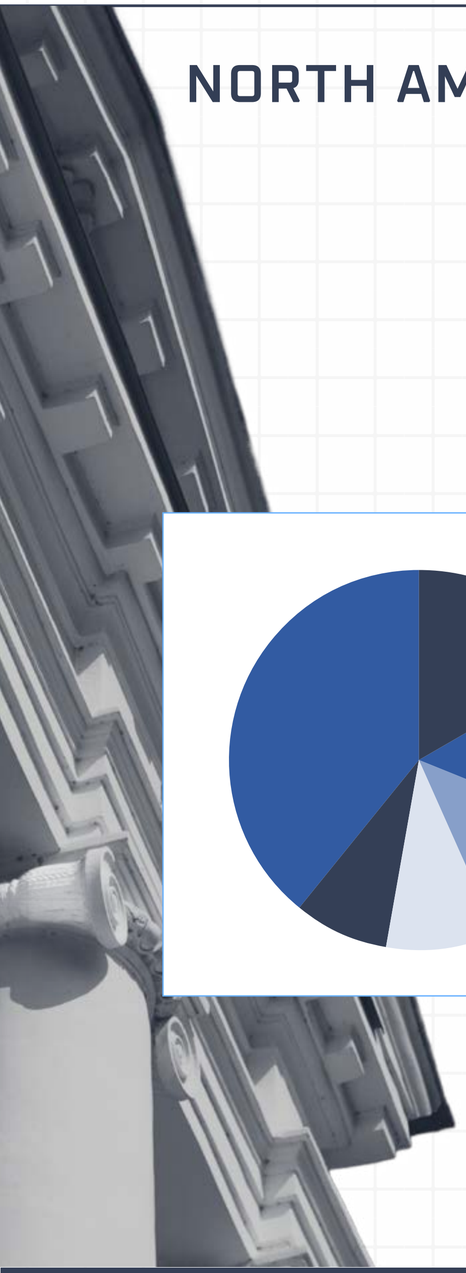
- The company’s Unit 42 researchers recently discovered six new RATs used for espionage purposes and used by an Iran-linked group dubbed Screening Serpens (aka UNC1549, Smoke Sandstorm, Nimbus Manticore).
- Screening Serpens consistently set its sights on “high-value sectors,” especially in the aerospace, defense and telecommunications industries.
- The group lures victims with convincing fake job offers and spoofed video conferencing invites, then delivers malware once the target downloads what looks like a legitimate file.
- Once a device is compromised, attackers have broad remote control, including the ability to steal files and load additional malicious modules, which could expose any sensitive data on the machine.

SOURCE

WHY IT MATTERS:

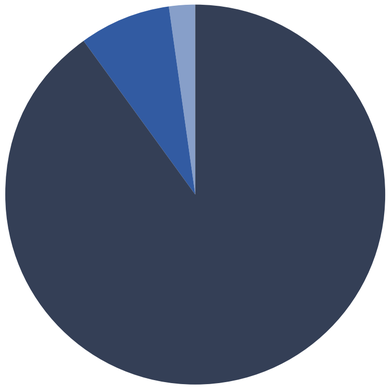
Iranian government-backed hackers continue to conduct espionage operations against strategically relevant sectors to collect intelligence and harden its posture amid the ongoing conflict with the United States. Tehran-aligned actors have previously targeted municipal governments in the Middle East and U.S. critical infrastructure operators. These campaigns demonstrate how private sector industries, especially those tied to the Defense Industrial Base (DIB), can be at greater risk of being targeted by nation-state actors, especially during conflicts.

NORTH AMERICA RANSOMWARE TRENDS



Most targeted industries:

- **16.7%** Legal & Professional Services
- **14.5%** Construction & Engineering
- **12.2%** Manufacturing
- **9.4%** Healthcare
- **8.3%** Retail
- **38.9%** Other



Most targeted countries:

- **90.3%** United States
- **7.6%** Canada
- **2.2%** Mexico

The US remains far ahead in the lead for number of ransomware attacks in North America. It's not because US-based companies are uniquely vulnerable, but because of the sheer concentration of businesses, healthcare systems, and educational institutions that are appealing to hackers thanks to their ability to pay ransoms.

MOST ACTIVE GROUPS:

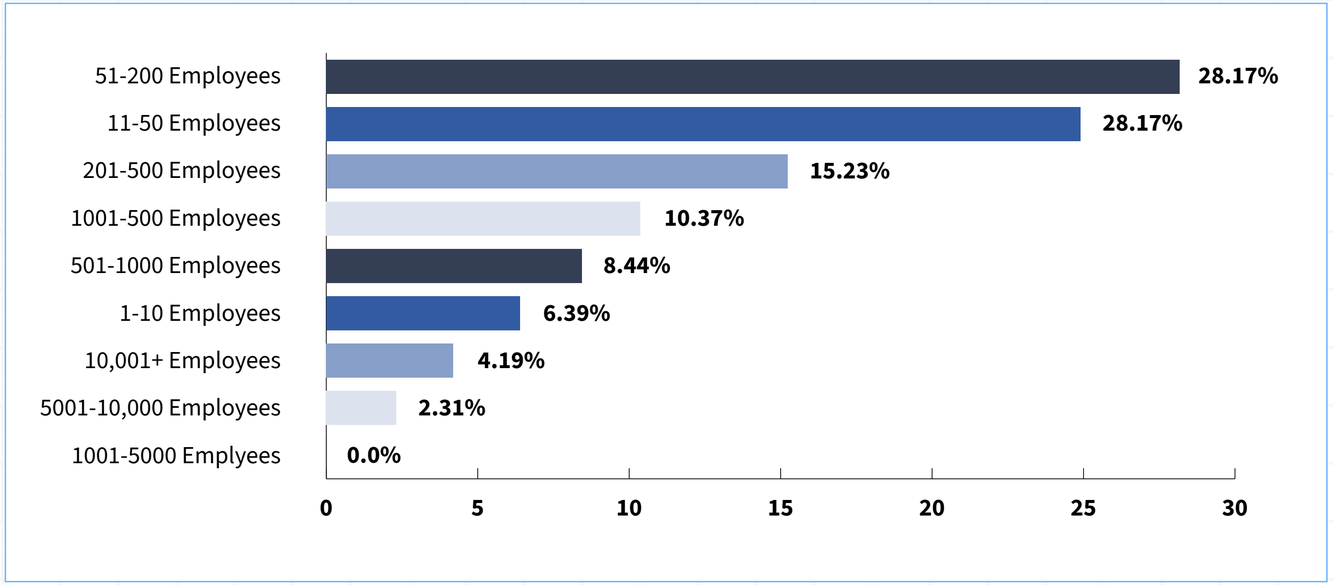
- Qilin
- AKIRA
- Dragonforce
- INC Ransom
- Play

RANSOMWARE SPOTLIGHT: AKIRA

How they get in: Akira frequently partners with Initial Access Brokers, which are criminals who specialize in selling pre-obtained VPN and network credentials. This lets them skip the initial intrusion step entirely and go straight to spreading through a victim's systems.

What they do once inside: Akira is known for rapid movement. Once credentials are secured, the group can encrypt a large network within hours. In some sectors, including financial services, Akira has shifted toward data theft and extortion rather than encryption — particularly exploiting 'Shadow AI,' where employees use unauthorized AI tools that inadvertently expose configuration data or credentials.

Who they are targeting in North America right now: Financial services, manufacturing, and technology companies, with a growing focus on mid-sized firms with less mature security programs.



Target profile

Small and medium-sized businesses remain the most frequently targeted in North America. While ransomware groups most often set their sights on smaller businesses, the impact rarely stays contained — shared vendors, platforms, and service providers mean a breach at one company can ripple across its entire network of partners and clients.

SUMMARY

A recent study by the Interisle Consulting Group titled “Malicious Registrations in the Domain Name Market” found that at least 10% of 85 million domains created in the generic top-level domain (gTLD) market in 2025 have already been blocklisted due to association with malicious activity. Interisle also states 10% is a conservative estimate, with a projection of up to 20% being blocklisted by the end of 2026. Further, the report found that five registrars account for 50% of all blocklisted domains, demonstrating a concentration of threat actor activity with a relatively small number of registrars.

KEY POINTS

- The acquisition and deployment of new domains is central to cybercriminal operations, particularly for phishing, spearphishing, and malware deployment.
- Interisle’s analysis found that approximately 92% of the domains created in 2025 and subsequently blocklisted were in gTLDs operated by just eight companies. This concentration may suggest a preference on the part of cybercriminals for certain organizations.
- The report noted that the current market incentivizes some registrars and registry operators to do business with malicious actors and tolerate abusive registrations.
  - Interisle cites sales and incentive programs designed to drive market share and growth which coincides with a general practice by threat actors of buying domains for malicious activity in bulk.

WHY THIS MATTERS:

The analysis conducted by Interisle is consistent with our own experience in dealing with phishing sites and registrars. Part of our Threat Intelligence, Mitigation, and Escalation (TIME) team’s mission is protecting our customers against phishing attacks and our own analysis finds significant concentrations within certain gTLDs and that many of the phishing sites we identify for takedown are also inordinately associated with several notable registrars. As AI further enables malicious actors to branch into cybercrime and improve their tactics, techniques, and procedures as well as grow the scale and scope of their operations, we expect to see continued growth in the registration of domains for malicious use for use in future phishing and other malicious campaigns.

RECOMMENDED ACTIONS FOR ORGANIZATIONS

- **DEVELOP A "SECURITY FIRST" CULTURE:** Prioritize patching for internet-facing systems, identity infrastructure, SaaS platforms, VPNs, cloud control planes, and critical operational technology, where newly discovered flaws are most likely to be exploited quickly.
- **HARDEN HELP DESK AND SOCIAL ENGINEERING DEFENSES:** Implement strict identity verification protocols before any credentials are issued or reset over phone or chat, and limit how much data any single customer-facing system can expose to reduce the blast radius of a successful social engineering attempt.
- **FOCUS ON IDENTITY AND CREDENTIAL HYGIENE:** Rotate CI/CD secrets, API keys, and OAuth tokens on a regular schedule and immediately after any third-party tool compromise is disclosed. Treat app permissions with the same rigor as user accounts, auditing and removing unused OAuth authorizations across SaaS platforms regularly.
- **STRENGTHEN IDENTITY AND SAAS HYGIENE:** Ensure patching and remediation efforts extend to SaaS configurations, identity providers, OAuth applications, and cloud management tools, which are often updated outside traditional IT processes.