APRIL 2026

REGIONAL THREAT REPORT

APAC

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

DIRECTOR OF THREAT
INTELLIGENCE

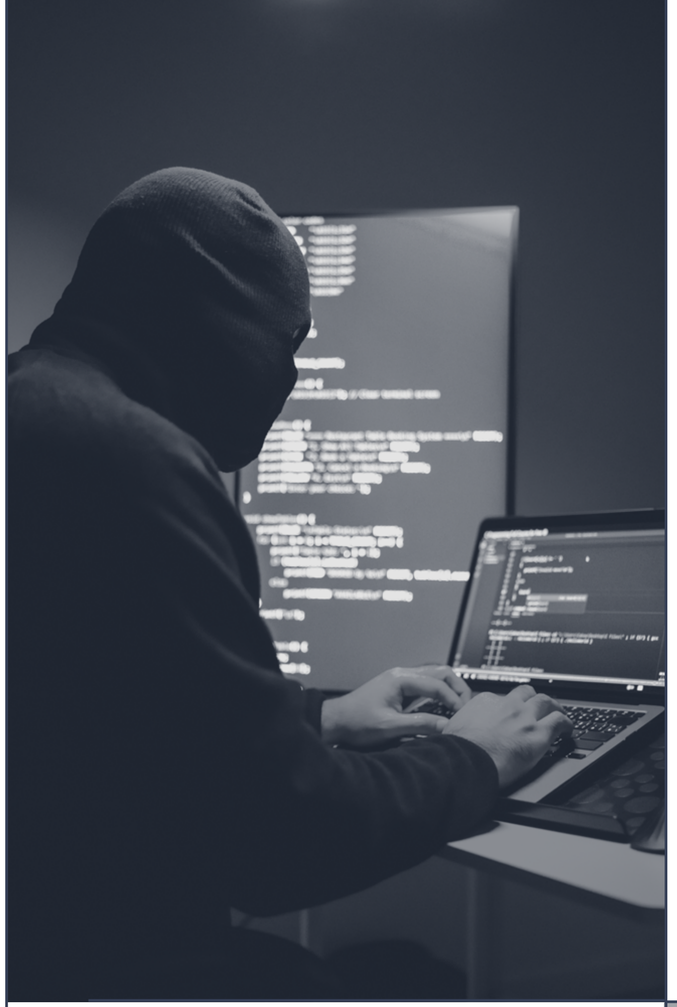
The Regional Threat Report delivers strategic insights from the LastPass Threat Intelligence, Mitigation & Escalation (TIME) Team into the evolving cyber threat landscape across key global markets. Each edition provides a concise, intelligence driven overview of the most significant threats affecting 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.

WHAT'S ON TAP THIS MONTH?

IDENTITY-DRIVEN ATTACKS CONTINUE TO ESCALATE

This month's APAC Threat Report highlights a continued escalation in identity-driven cyber activity, with attackers increasingly relying on stolen credentials, abused cloud roles, and trusted access paths rather than traditional exploits. High-impact incidents across the region—from SaaS supply chain breaches to ransomware and state-aligned intrusions—demonstrate how attackers are exploiting weaknesses in authentication, privilege management, and developer environments.



SUPPLY CHAIN COMPROMISE REMAINS A KEY RISK AREA

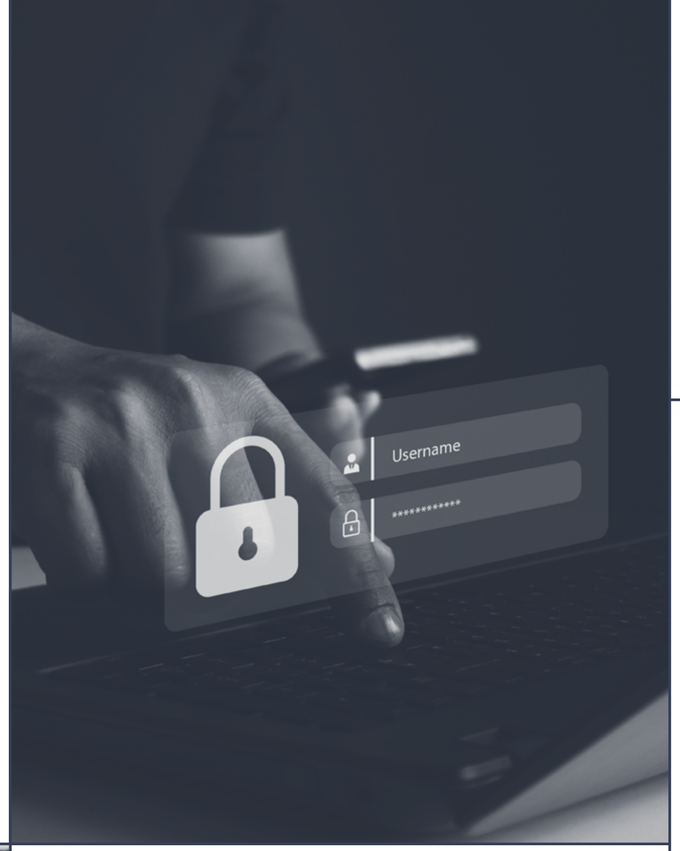
Supply chain risk remains a central concern to both the public and private sectors. Breaches involving trusted platforms and service providers, including cloud and SaaS environments, show how a single identity compromise can cascade across downstream customers, government agencies, and critical industries. Regional alerts from authorities such as Australia's ACSC further underscore the active targeting of code repositories, CI/CD pipelines, and API credentials as primary entry points.

RANSOMWARE CAMPAIGNS GROW MORE TARGETED

Ransomware activity across APAC is also becoming more targeted and patient, with several groups focusing on credential-enabled intrusions into highly connected enterprise environments, particularly in manufacturing, healthcare, and professional services. These operations increasingly emphasize privilege escalation, lateral movement, and operational disruption before encryption, reflecting a shift toward stealthier, identity-centric tradecraft.

GEOPOLITICAL ACTIVITY RAISES SPILLOVER RISK

Ongoing geopolitical tensions continue to influence the regional threat landscape. State and state-aligned actors are targeting telecommunications providers, cloud infrastructure, and enterprise management platforms, reinforcing the risk of spillover from geopolitical conflicts into commercial and private-sector environments.



WHAT THIS MEANS FOR APAC ORGANIZATIONS

For organizations across APAC, securing identities, credentials, and access pathways is now the most critical factor in reducing cyber risk across ransomware, supply chain compromise, and state-aligned activity alike.

LEXISNEXIS DATA BREACH EXPOSES VULNERABILITIES IN THE SAAS SUPPLY CHAIN, INCLUDING CREDENTIAL MANAGEMENT, ACCESS CONTROLS, AND PATCH GOVERNANCE.

A threat actor operating as FulcrumSec claimed responsibility for exfiltrating approximately 2.04 GB of structured data from LexisNexis' AWS cloud environment, with exposed data linked to Australian federal government agencies and law firms.

KEY TAKEAWAYS:

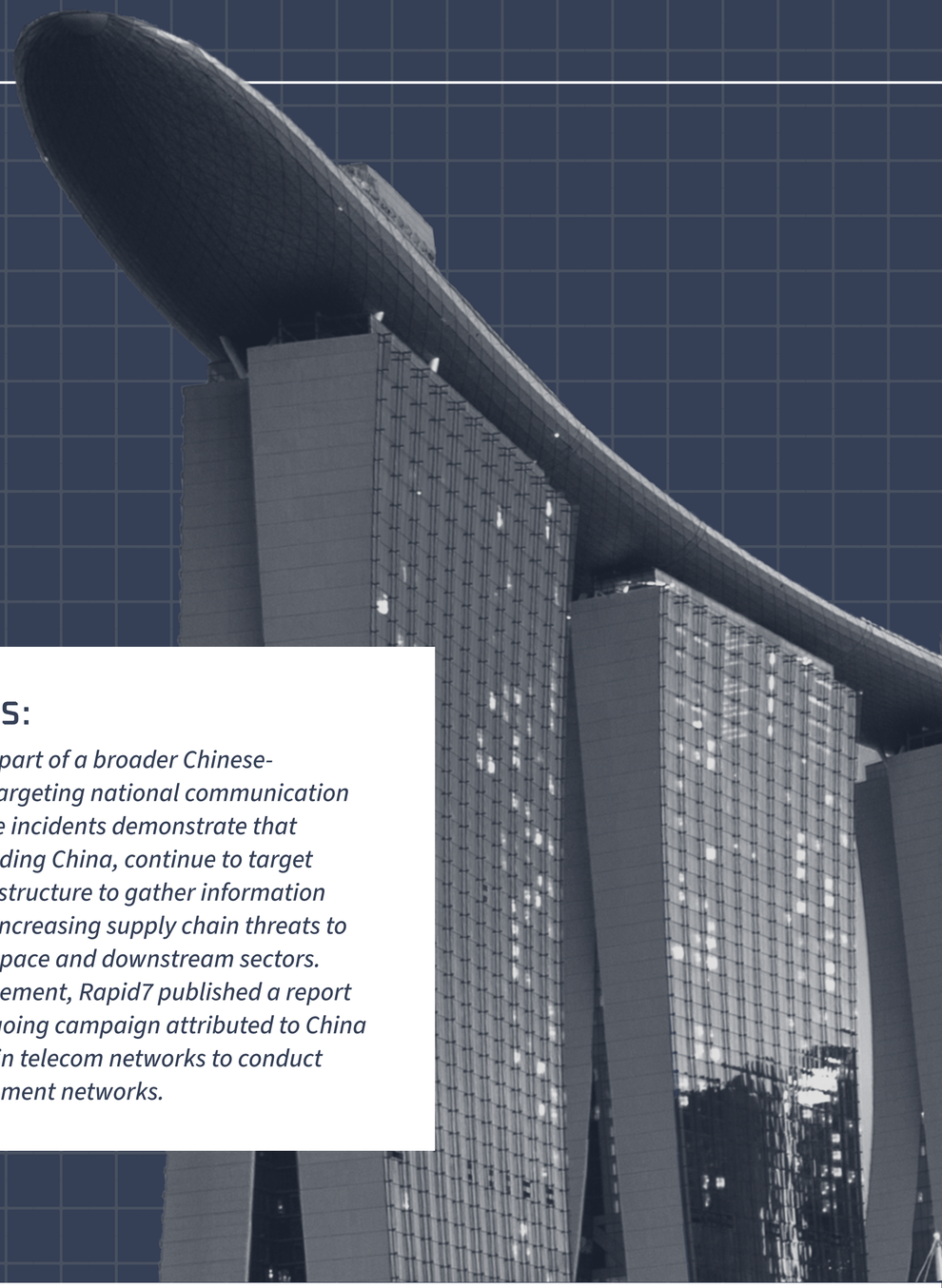
- A threat actor named FulcrumSec claimed responsibility for breaching LexisNexis Legal & Professional, part of RELX Group, and posted details on March 3 alleging the theft of 2.04 GB of structured data from the company's Amazon Web Services (AWS) cloud infrastructure.
- On February 24, the actor accessed sensitive production systems, exposing flaws in access controls, credential management, and patching, by exploiting an unpatched React2Shell vulnerability in a React frontend application.
- From there, the actor compromised an AWS Elastic Container Service (ECS) task container, "LawfirmsStoreECSTaskRole" which held broad read permissions across the AWS account, and they were able to access other data.

SOURCE

WHY IT MATTERS:

The breach underscores risks in cloud environments where over-privileged roles and weak passwords enable lateral movement. The AWS role the attacker leveraged was over-privileged, granting broad read access across the AWS account and enabling access to additional production data.

CHINESE-BACKED HACKERS BREACH SINGAPORE'S FOUR MAJOR TELECOS VIA ZERO-DAY



Singaporean government authorities disclosed in February that Beijing-linked UNC3886 targeted four of the country's major telecommunications providers (Singtel, StarHub, M1, and Simba) in a sophisticated campaign first detected in 2025.

KEY TAKEAWAYS:

- *According to the Cyber Security Agency of Singapore, attackers leveraged an unnamed zero-day exploit to bypass perimeter firewalls and deployed rootkits for persistent access and detection evasion for 11 months.*
- *Attackers focused on stealing technical network configuration data, rather than consumer records or disruptive activity, suggesting long-term intelligence gathering objectives.*
- *In response, the government launched a coordinated effort called "Operation Cyber Guardian" to contain the breach and strengthen infrastructure defenses.*

SOURCE | SOURCE

WHY IT MATTERS:

The Singapore incident is part of a broader Chinese-backed espionage effort targeting national communication backbones globally. These incidents demonstrate that state-backed actors, including China, continue to target telecommunications infrastructure to gather information straight from the source, increasing supply chain threats to entities operating in this space and downstream sectors. Shortly after this announcement, Rapid7 published a report detailing a long-term, ongoing campaign attributed to China that has embedded itself in telecom networks to conduct espionage against government networks.

RANSOMWARE GANGS USE STOLEN CREDENTIALS AND VULNERABILITIES TO TARGET AUSTRALIAN HEALTHCARE AND OTHER SECTORS.

The Australian healthcare sector remains under immense ransomware pressure, with several recent attacks highlighting the elevated threat.

KEY TAKEAWAYS:

- China-linked Storm-1175 has been aggressively targeting healthcare organizations, as well as education, professional services, and finance sectors in Australia, the United Kingdom and the United States with Medusa ransomware. Storm-1175 is weaponizing a combination of zero-day and N-day vulnerabilities to launch “high-velocity” attacks against internet-facing assets, successfully moving from initial breach to encryption in under 24 hours.
- In March, the Australian Cyber Security Centre (ACSC) warned that the INC Ransom group breached over 11 Australian organizations between July 2024 and December 2025, primarily targeting healthcare and professional services sectors. These affiliates reportedly breached networks using stolen credentials and legitimate administrative tools to blend into normal network traffic and bypass basic defenses.

WHY IT MATTERS:

The high volume of Australian healthcare ransomware targeting aligns with regional targeting as healthcare remains one of the top targeted sectors in the APAC region. The ACSC alert provides several mitigation recommendations, including implementing multi-factor authentication (MFA) as an additional layer of protection, controlling privileged access to reduce the impact of credential compromise, and restricting the use of remote management tools to authorized administrators only.

SOURCE | SOURCE

IRAN-LINKED HACKTIVISTS WEAPONIZE MICROSOFT INTUNE CREDENTIALS AT STRYKER.

Iran-aligned hacktivist group Handala used stolen Microsoft Intune administrator credentials to remotely wipe up to 200,000 devices worldwide, causing large-scale operational disruption.

KEY TAKEAWAYS:

- According to third-party reporting, the attack was likely enabled by compromised credentials that were stolen by infostealer malware prior to the attack.
- Handala stated the reason Stryker was specifically targeted was because they purchased an Israel-based subsidiary in 2019.
- Iran later also announced expanded targets and named several US tech giants, commercial entities, and financial institutions.

WHY IT MATTERS:

The attack on Stryker emphasizes the importance of not only protecting your credentials but also monitoring the dark web to proactivity identify any enterprise credentials that may have been previously compromised and need to be changed.

From a geopolitical perspective, direct Iranian attacks on technological infrastructure and companies establish a new precedent. This shift indicates that Tehran now views the private sector as targets during conflicts because Tehran views these as extensions of US state power. Ongoing Iran-related cyber activity continues to influence the regional threat landscape, with heightened risk of disruptive or retaliatory cyber operations and spillover to Western entities. Organizations can anticipate an increase in password-spraying campaigns, exploitation of unpatched vulnerabilities in public-facing applications, and targeted phishing.

SOURCE

OVER 200K AUSTRALIAN DRIVER'S LICENSES EXPOSED IN YOUX BREACH

A breach at Sydney-based financial tech firm youX exposed sensitive personal data, belonging to borrowers in Australia whose information was processed through nearly 800 mortgage brokers and lenders using the youX platform.

KEY TAKEAWAYS:

- Threat actors reportedly compromised a misconfigured cloud database, possibly leveraging the MongoDB Server Leak vulnerability (CVE-2025-14847).
- The attacker claimed they exfiltrated data belonging to 444,538 individuals. Among the compromised information were 229,226 Australian driver's license numbers, along with names, phone numbers, email addresses, residential addresses, loan applications, and financial records.
- More than 8,000 password hashes belonging to broker employees were also reportedly accessed.

SOURCE

WHY IT MATTERS:

The youX data breach underscores a recurring and preventable pattern in modern cyber incidents: poor cyber hygiene at the data layer can enable large-scale identity exposure. Whether exploitation occurred through a known vulnerability or simply due to database exposure, the outcome was equally damaging: personally identifiable information (PII) was exfiltrated at scale and can be used for extortion and downstream fraud, phishing campaigns, and identity theft.

RISING RANSOMWARE PRESSURE ON APAC'S MOST CONNECTED INDUSTRIES

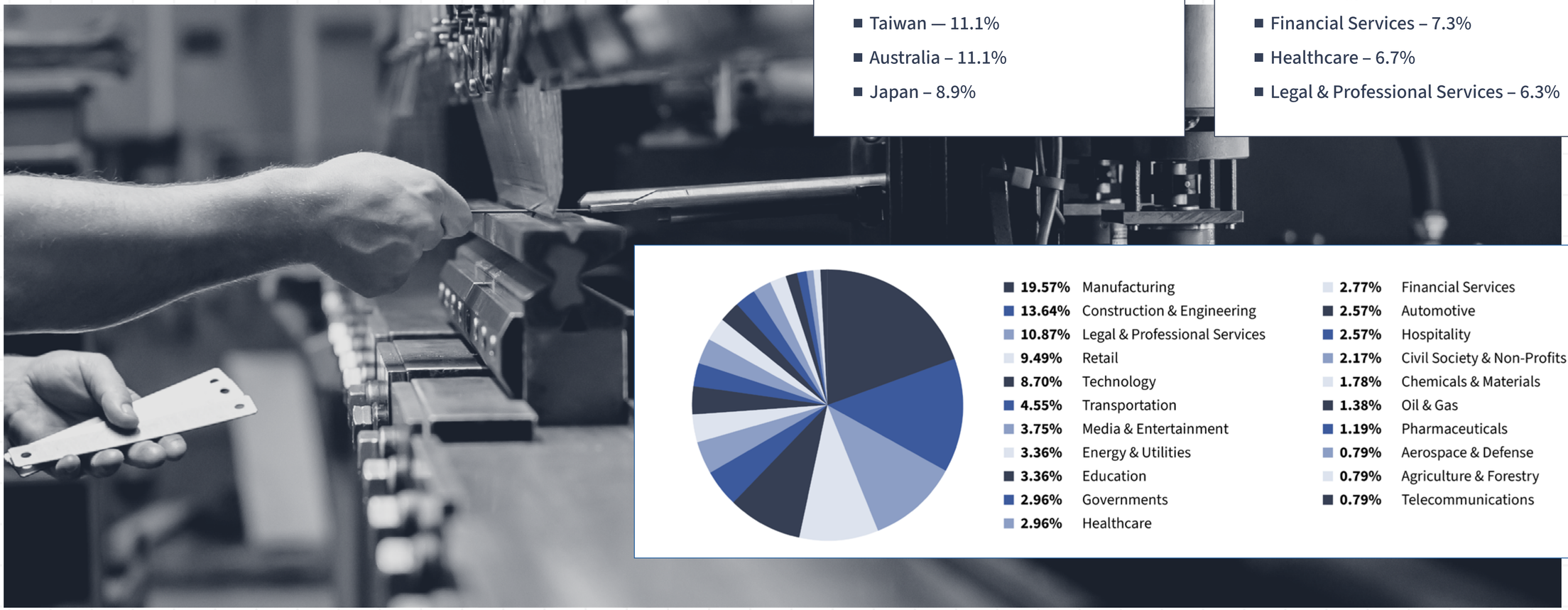
Target Profile: Small and medium-sized businesses remain the most frequently attacked.

Most targeted countries:

- India — 15.5%
- Thailand — 14%
- Taiwan — 11.1%
- Australia – 11.1%
- Japan – 8.9%

Most targeted industries:

- Manufacturing – 25%
- Technology – 10.8%
- Financial Services – 7.3%
- Healthcare – 6.7%
- Legal & Professional Services – 6.3%



19.57%	Manufacturing	**2.77%**	Financial Services
13.64%	Construction & Engineering	**2.57%**	Automotive
10.87%	Legal & Professional Services	**2.57%**	Hospitality
9.49%	Retail	**2.17%**	Civil Society & Non-Profits
8.70%	Technology	**1.78%**	Chemicals & Materials
4.55%	Transportation	**1.38%**	Oil & Gas
3.75%	Media & Entertainment	**1.19%**	Pharmaceuticals
3.36%	Energy & Utilities	**0.79%**	Aerospace & Defense
3.36%	Education	**0.79%**	Agriculture & Forestry
2.96%	Governments	**0.79%**	Telecommunications
2.96%	Healthcare		

MOST ACTIVE RANSOMWARE GROUP:
THE GENTLEMEN

Though relatively new on the scene, the Gentlemen ransomware group outpaced Qilin during this period. First observed in mid-2025, the Gentlemen is a highly capable ransomware-as-a-service (RaaS) with a focus on APAC organizations, particularly in Thailand and Southeast Asia. Unlike most other opportunistic ransomware gangs, the Gentlemen group conducts targeted intrusions against mid-to-large enterprise environments. Its targets are primarily in sectors with operational technology (OT)-heavy or domain-centric networks that have highly connected IT systems, such as manufacturing, construction, healthcare, and insurance.

Initial access is commonly achieved via compromised credentials or exposed FortiGate VPN services, followed by extensive internal reconnaissance and privilege escalation before ransomware deployment. The Gentlemen's targeting reflects a shift toward highly tailored, credential-enabled ransomware operations. The group's reliance on legitimate credentials, tools, and directory infrastructure highlights a shift toward stealthy, identity-driven ransomware, elevating the importance of privileged access controls and identity monitoring in large APAC enterprises.

KEY TAKEAWAYS:

- Ransomware in APAC is becoming more targeted and more patient.
- Identity compromise has replaced exploit-driven entry as the dominant access vector.
- Ransomware groups heavily abuse domain-wide identity controls.
- Double extortion is table stakes, while operational extortion is rising.

Recent supply chain attacks have put a spotlight on how risks introduced by trusted third parties globally can cascade across organizations globally. For SMBs, especially those operating in the Asia-Pacific region, these attacks increasingly bypass traditional defenses by abusing credentials, identities, and automated trust relationships rather than exploiting software vulnerabilities directly.

DPRK SOCIAL ENGINEERING CAUSED NPM SUPPLY CHAIN ATTACK

North Korea-linked UNC1069 compromised npm credentials of Axios' lead maintainer through a tailored social-engineering campaign. Using the stolen npm creds, attackers published malicious Axios versions directly via stolen tokens, bypassing OIDC-protected CI/CD. This incident reflects a broader evolution of UNC1069 tradecraft, expanding from crypto-focused targets to open-source maintainers, enabling large-scale supply-chain compromise through single identity takeovers.

WHY IT MATTERS:

- Social engineering remains an effective strategy to bypass security measures and, in this case, compromise the maintainer's endpoint identity.
- Personal developer identities have become strategic supply chain entry points, especially in open-source ecosystems.

TEAMPCP'S CASCADING CI/CD CREDENTIAL CAMPAIGN

In March, TeamPCP initially compromised Aqua Security's Trivy open-source vulnerability scanner and other developer security tools by stealing CI/CD credentials from GitHub Actions workflows. Stolen secrets then reused to compromise Checkmarx GitHub Actions, LiteLLM, and Telnyx packages across GitHub, npm, PyPI, Docker Hub, and CI pipelines. The hackers force-pushed malicious updates, harvesting additional credentials at every step and expanding laterally across ecosystems.

WHY IT MATTERS:

- CI/CD runners handle multiple powerful credentials at the same time, such as cloud credentials, API keys, and service accounts, which allows attackers to steal many identities from a single breach.
- Even organizations with strong perimeter controls were compromised simply by running trusted workflows.
- For SMBs, reused tokens and long-lived credentials dramatically increased blast radius once a single dependency was compromised.

REGIONAL HIGHLIGHT

On April 1, the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) issued a high-priority alert regarding active targeting of online code repositories and developer environments. Threat actors are reportedly hijacking developer access via compromised authentication tokens and social engineering, then abusing legitimate tooling to modify public packages and systematically scrape repositories for cryptographic secrets. This poses a significant supply-chain risk for SaaS platforms and FinTech companies processing critical eCommerce transactions.

KEY TAKEAWAYS:

- API tokens and service identities are now primary supply chain targets, not secondary assets.
- Valid credentials allow adversaries to blend seamlessly into normal operations, significantly delaying detection.
- SMBs using SaaS, managed services, or AI platforms often lack visibility into how deeply these identities can traverse environments once compromised.

- **HARDEN IDENTITY AND ACCESS CONTROLS:** Lock down identities and credentials across SaaS applications and your supply chain. Enforce MFA across all users and administrators and tightly restrict privileged access to limit the impact of credential compromise.
- **REDUCE CREDENTIAL EXPOSURE:** Eliminate long-lived passwords, API keys, and tokens in favor of scoped, short-lived credentials wherever possible.
- **SECURE DEVELOPER AND CI/CD ENVIRONMENTS:** Limit privileges for build systems and service accounts and monitor repositories and pipelines for unauthorized changes or leaked secrets.
- **STRENGTHEN CLOUD AND SAAS CONFIGURATIONS:** Review permissions for cloud roles and service identities, removing overly broad access that enables lateral movement.
- **ASSUME SUPPLY-CHAIN COMPROMISE AND PLAN ACCORDINGLY:** Maintain dependency visibility, monitor for leaked credentials, and be ready to rapidly rotate secrets and re-establish trust following upstream incidents.