



APAC 2025 Q1 Regional Report

Stephanie Schneider
Cyber Threat Intelligence Analyst



Michael Kosak
Senior Principal Intelligence Analyst

Regional snapshot

The Asia-Pacific region (APAC) experienced high-frequency cyber espionage and financially motivated attacks involving phishing, data theft, ransomware, and network access sales. Campaigns involved credential harvesting, malware distribution via fake installers, cryptomining, and exploiting vulnerabilities in Palo Alto and FortiManager products. Additionally, AI-driven attacks and deepfake scams are emerging as new threats.

MOST TARGETED

34%
of incidents

APAC experienced the largest number of incidents globally in 2024 (34%), representing a 13% increase in attacks.¹

MANUFACTURING

56%
of attacks

Manufacturing was the most targeted industry regionally, followed by finance & insurance (16%) and transportation (11%).¹

JAPAN

66%
of incidents

Japan was the most targeted country regionally last year. The Philippines, Indonesia, South Korea, and Thailand each represented 5% of cases.¹

CREDENTIALS

55%
of breach victims

Stolen credentials were reported by 55% of breach victims in APAC, indicating their frequent use in initial intrusions.² Nearly one in four incidents in 2024 involved stolen data or credentials.³

AUSTRALIA

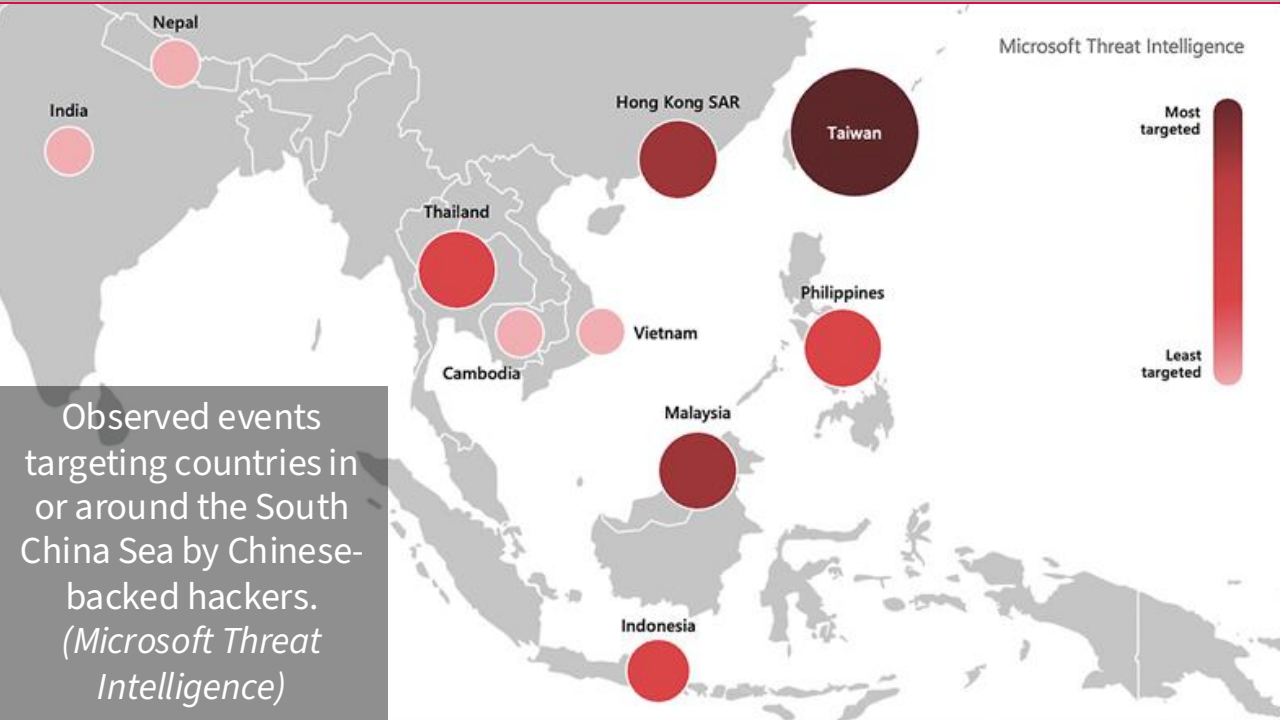
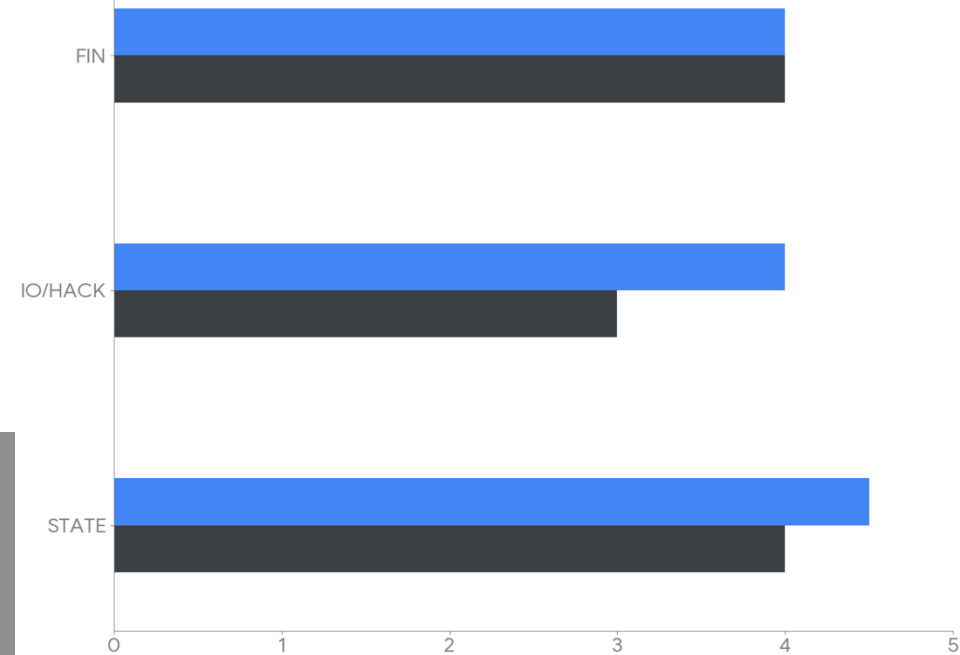
46
ransomware incidents

Australia remained a popular ransomware target.⁴ The country remained in the top 10 of countries impacted based on ransomware gang reporting of alleged victims.⁵

Threat landscape: Drivers of regional cyber threat activity

Frequency
Magnitude

APAC Region
Cyber Threat
Score: 6.4
(Google Threat
Intelligence)



Trends driving a heightened threat landscape



Top malware families targeting APAC

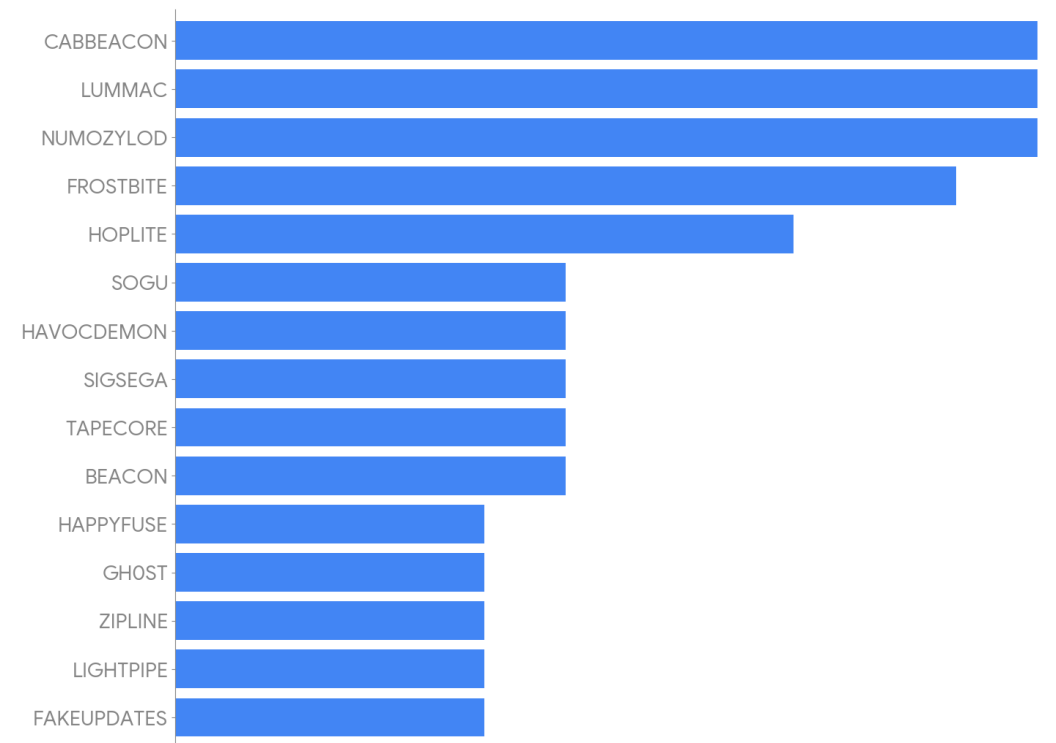
RANSOMWARE

Akira generally trended as the top ransomware throughout Q1 2025 with a significant spike in posted victims (241) at the end of May, according to vendor reporting. Asia accounted for approximately 11% of global ransomware activity mainly targeting manufacturing and engineering, with India and Japan seeing significant activity. In comparison, Oceania accounted for 2% of activity.⁵ Australia emerged as a top regional target, and there were several victims in Taiwan, Singapore, and Japan. Thailand also saw an unusual increase in victims.⁴

STEALERS

LUMMAC (aka Lumma) stealer was one of the top malware families targeting APAC in Q1 2025; however, its infrastructure was taken down in May 2025.⁶ While continued monitoring will be necessary to determine the takedown's long-term impact, LastPass TIME analysts predict a correlated decrease in Lumma stealer infections over the next quarter.⁷ Long-standing groups such as Vidar and Stealc will be well positioned to increase their market share, as well as other newer families like Acreed. HOPLITE has been attributed to the North Korean government and was recently used by suspected India-backed hackers.

Want to learn about the infostealer threat? The Australian Cyber Security Center (ACSC) published a report breaking down how cybercriminals use stealer malware to compromise corporate networks.⁸



Observed malware targeting APAC included CABBEACON (reconnaissance), LUMMAC and HOPLITE (credential stealers), NUMOZYLOD and LIGHTPIPE (downloaders), and various backdoors.

(Source: Google Threat Intelligence)

Top threat actors targeting APAC



TEMP.Hex

aka Mustang Panda, Red Delta, Winnti Group, Earthpreta

- A prolific Chinese actor, TEMP.Hex targets a wide variety of public and private entities around the globe aligned with Beijing's strategic interests.
- Google Threat Intelligence Group recently observed an espionage campaign targeting organizations in Taiwan and Southeast Asia within the energy, government, and aerospace industries.



Salt Typhoon

aka GhostEmperor, FamousSparrow

- Salt Typhoon demonstrates a high level of sophistication and targets government entities and telecom companies in SE Asia.
- Linked to numerous attacks on global telecom providers, Salt Typhoon remains active, hitting networks across the globe since December 2024. The group compromised Cisco network devices across five telecom networks based in the U.S., Thailand, Italy, and South Africa.



Bitter

aka UNC2464

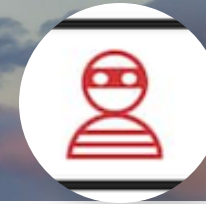
- India-backed espionage group primarily targeting South Asian governments, diplomatic entities, and defense organizations.
- Its geographic scope has expanded to include China, Saudi Arabia, South America, and Turkey.
- Uses spear-phishing emails, often sent from compromised government accounts or free email providers, to deploy malware.



APT36

aka Transparent Tribe, Mythic Leopard

- APT36 is a Pakistani espionage group focused on collecting political and military intelligence, primarily targeting entities in India's government and defense sectors.
- The actor's tactics, techniques, and procedures (TTPs) have remained broadly consistent over time, including phishing for initial access, social engineering to harvest victim credentials, and the SEEDOOR backdoor.



Akira

- Active since March 2023, Akira is a ransomware variant and deployment entity that steals information and conducts double extortion to force victims into paying the ransom.
- Uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement.
- Most common ransomware targeting APAC in Q1 2025.

Key regional incidents

Fog ransomware attack on Asia financial org used legit software, open-source tools.⁹

A cyberattack on an Asia-based financial institution in May 2025 used a legitimate employee monitoring software called Syteca and open-source pen-testing tools, which are unusual tools for a ransomware attack. After the ransomware was deployed, the attackers sought to establish persistence on the victim network.

The campaign combining legitimate employee monitoring software with open-source penetration tools to build attack chains is covert and highly effective. Instead of deploying malware, attackers used repurposed legitimate tools to possibly harvest credentials and monitor employee behavior.

Chinese hackers breached entities in Southeast Asia.¹⁰

Chinese-backed Billbug (aka Lotus Panda) breached multiple government and business orgs in an unnamed Southeast Asian country between August 2024-February 2025. The attacks involved multiple custom-made tools including credential stealers and backdoors. Targets included a government ministry, an air traffic control organization, a telecoms operator, and a construction company.

This campaign deployed two custom tools designed to steal credentials from the Chrome web browser, taking advantage of hardcoded credentials frequently saved in browser extensions. Chinese hackers have frequently targeted Southeast Asian entities as Beijing seeks to bolster its claims over Taiwan and islands in the South China Sea, elevating the regional threat.

Japan orgs targeted by CoGUI phishing kit.¹¹

A campaign used the CoGUI phishing kit to steal usernames, passwords and payment information from Japanese organizations. The campaigns spoofed Amazon, payment cards, transport cards, popular banks, retailers, and Japan's national tax agency.

Proofpoint said that due to the use of the CoGUI phish kit, Japan "has become one of the most targeted countries...based on campaign volume." Japan was the most targeted country in the region in 2024.

Fake Update campaigns hit New Zealand, others.¹²

Researchers reported a significant rise in Fake Update campaigns, where attackers trick victims into installing supposed browser updates (such as for Chrome or Opera) that deliver malware. This wave in Q2 hit New Zealand, Belgium, Germany, and others particularly hard.

These types of campaigns can surge in a short timeframe before settling back into quieter periods.

Australian, New Zealand cyber landscape changing.¹³

Australia and New Zealand's leading cyber security provider CyberCX's annual 2025 Threat Report for 2025 revealed that business email compromise (BEC) remained the top incident type the company responded to, with 75% of these incidents involving session hijacking to bypass MFA. Additionally, espionage-related incidents took more than two weeks longer to discover in 2024 than in 2023.

These changes in the threat landscape reflect threat actors' constant evolution of tactics to remain effective. It also aligns with the broader trend of session hijacking becoming more prevalent.

Deep dive of the month

Australia’s pension funds hit by wave of credential-stuffing attacks

Summary

A credential stuffing campaign during March 29-30, 2025, targeted multiple large Australian superannuation funds, compromising over 20,000 member accounts.¹⁴ Some of the country's largest profit-to-member superannuation funds confirmed that some of their members' accounts were breached in these attacks. The attackers aimed to commit fraud, attempting fund transfers, though successful financial impacts varied across the affected organizations.

How did it happen?

This was a coordinated OAuth token manipulation campaign coupled with advanced credential-stuffing techniques targeting API vulnerabilities in the funds’ member portals.	The attack vector appears to have utilized SQL injection techniques specifically targeting database vulnerabilities in the fund administration systems.
Credential stuffing takes advantage of users who reuse email and password combination, and the campaign appeared to leverage a distributed botnet utilizing compromised credentials from previous breaches, taking advantage of accounts without multi-factor authentication (MFA) in place.	Additionally, the campaign occurred during early morning hours to prevent members from immediately noticing session hijacking alerts and password change notifications.

How can you protect yourself?

Given the volume of exposed, publicly-available credentials from data breaches and the growing threat from infostealers, use tools like Have I Been Pwned to see if your email or phone number has been compromised in a data breach. Using unique credentials for all accounts prevents credential-stuffing attacks from succeeding. Additionally, implementing other best security practices, like requiring MFA for accounts, provides an additional layer of protection.	TIME analysts highly recommend reading the Australian Signals Directorate’s Australian Cyber Security Center’s (ACSC) latest Annual Cyber Threat Report. ¹⁵ The report summarizes the regional cyber threat environment facing the public and private sectors. The data includes trends and information on threat actor tactics and techniques as well as recommended actionable steps organizations and individuals can take to help mitigate these threats. LastPass’s blog article summarizes the key takeaways. ¹⁶
--	--

Trends on tap

Critical infrastructure under attack: There is growing concern about the size and scope of Chinese hacking into critical infrastructure (CI) globally, including telecommunications entities, internet service providers (ISPs), and managed service providers (MSPs). Chinese-backed hackers have historically targeted CI in APAC countries, especially Taiwan.

Credentials are key: Chinese hackers frequently seek out credentials and use them to try to maintain long-term access, which makes it harder for defenders to kick them out of systems. By leveraging valid account credentials harvested within the compromised network, they can access remote systems, move laterally, and spread their malware across the network, increasing their foothold and potential impact. They also constantly evolve their tactics to remain stealthy and effective.

For example, Silk Typhoon is targeting remote management tools and cloud services in supply chain attacks that give them access to downstream customers. The group has also shifted from primarily using zero-day vulnerabilities to abusing stolen API key and compromised credentials.¹⁷

Threats are growing: While China has attacked CI in the past, they've recently become more aggressive but have stopped short of disruptive or destructive attacks. They are focused on gathering intelligence for a variety of purposes—from espionage to intellectual property (IP) theft—and prepositioning themselves in the event of an active conflict.

The series of recent CI attacks underscores the global threat from Chinese-backed hackers. Global telecom networks remain a key target for Chinese hackers because they can siphon off huge amounts of data for political and economic purposes.

LastPass TIME analysts assess China will continue targeting global telecommunications providers, including ISPs and MSPs, due to the amount and high value of communications data that flows through these networks, and the downstream access they can gain from their customers and third-party providers.

There seems to be a growing trend in nation-state actors targeting credentials to bypass traditional security controls and maintain persistent access.

What can you do?

With the constant threat from malicious cyber actors and a dynamic geopolitical environment, what steps can you and/or your organization take to protect yourself? Here's some advice, drawn largely from the Australian Signals Directorate's Australian Cyber Security Centre Essential Eight maturity model.¹⁸

PATCH APPLICATIONS

Keeping your applications up to date with the latest version helps prevent exploitation by malicious actors through security vulnerabilities.

PATCH OPERATING SYSTEMS

As with applications, it's critical to update your operating systems regularly as new vulnerabilities are constantly discovered and threat actors are quick to exploit them.

USE A PASSWORD MANAGER

Storing strong and unique passwords for every account in a password manager helps add an extra layer of protection against infostealers, which frequently target browser-based credentials.




ENABLE MULTI-FACTOR AUTHENTICATION

Adding another layer of authentication provides more security in the event your password is exposed. Biometric verification or other Authenticators can help make this process easy and more secure.

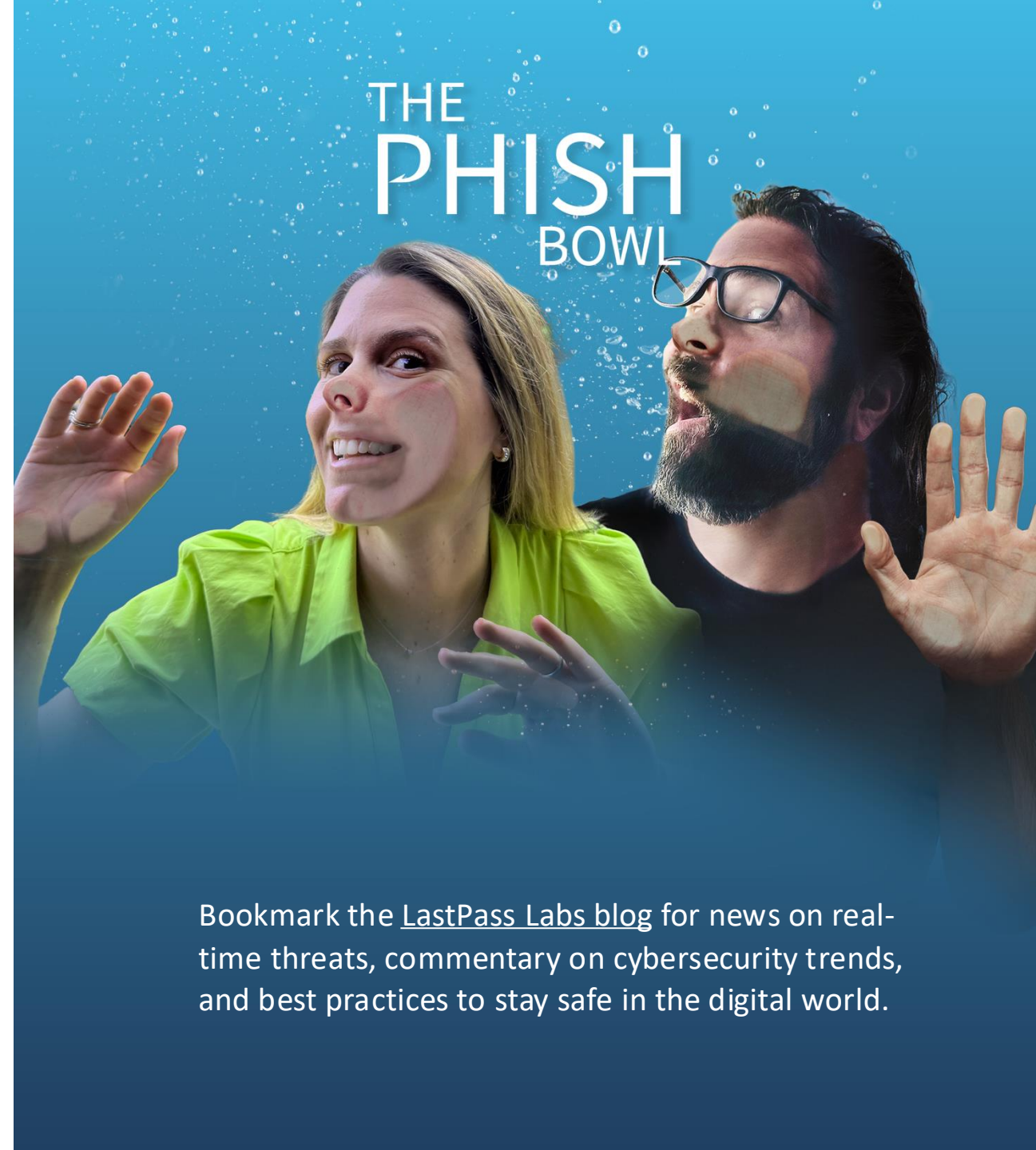
LIMIT PRIVILEGES FOR USERS

Remember that not everyone needs to access everything in your network. Limiting access can also help limit the damage in the event a threat actor does get access to a user's account.

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](#)



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. [IBM X-Force 2025 Threat Intelligence Index](#)
2. [Verizon's 2025 Data Breach Investigation Report](#)
3. [One in Four Cyberattacks in 2024 Traced to Infostealers, Huntress Reports \(Hudson Rock\)](#)
4. [2025 Ransomware: Business as Usual, Business is Booming \(Rapid7\)](#)
5. [The State of Ransomware in the First Quarter of 2025: Record-Breaking 126% Spike in Public Extortion Cases \(Check Point Research\)](#)
6. [Lumma Stealer Takedown Reveals Sprawling Operation \(DarkReading\)](#)
7. [Dark Side of the Lumma: What the Lumma stealer takedown means for the infostealer market and your personal data \(LastPass Blog\)](#)
8. [The silent heist: cybercriminals use information stealer malware to compromise corporate networks \(Australian Signals Directorate\)](#)
9. [Fog Ransomware: Unusual Toolset Used in Recent Attack \(Symantec\)](#)
10. [Billbug: Intrusion Campaign Against Southeast Asia Continues \(Symantec\)](#)
11. [CoGUI Phish Kit Targets Japan with Millions of Messages \(Proofpoint\)](#)
12. [Gen Q1/2025 Threat Report \(Gen Digital\)](#)
13. [CyberCX 2025 Threat Report reveals cyber landscape is changing \(CyberCX\)](#)
14. [Cybercriminals are trying to loot Australian pension accounts in new campaign \(The Record Media\)](#)
15. [Annual Cyber Threat Report 2023-2024 \(Australian Signals Directorate\)](#)
16. [ACSC 2024 Report Implications \(LastPass Blog\)](#)
17. [Silk Typhoon is targeting remote management tools and cloud services in supply chain attacks \(Microsoft Security\)](#)
18. [Australian Signals Directorate Essential Eight](#)