Cyberint

Impactful Intelligence

TOP ASIA /APAC CYBERSECURITY THREATS OF 2023

November 2023

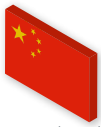
TABLE OF CONTENTS

INTRODUCTION

When it comes to cybersecurity in Asia today, some of the key threats that organizations face – like ransomware and phishing – are consistent risks that all cybersecurity teams are surely familiar with. But others are more fluid and may evolve rapidly. Cyberattacks related to hacktivism, for example, are a growing threat in the APAC region, and generative AI technology is also impacting Asia cybersecurity challenges in novel ways.

For teams tasked with protecting against cyber threats in APAC, identifying and blocking all of these risks – old and new – is critical. To provide guidance, Cyberint has collected data about threat techniques and goals that are surging as of 2023 in the following countries:


India


China (PRC)


Vietnam


Thailand


Cambodia


Laos


Malaysia


Singapore


Indonesia


Philippines


South Korea


Japan


Australia


New Zealand

Figure 1 //

TOP 7
CYBERSECURITY THREATS TO APAC

Phishing

- Smishing
- Vishing
- Social Media Impersonation

InfoStealers

- Redline
- Vidar
- Etc.

MFA Bypass

- Fake 2FA pages
- Session hijacking

Ransomware

- Attacks on the rise
- Stats on APAC ransomware attacks

Supply Chain Attacks

- Many big breaches
- 3rd party risks

Hacktivism

- Cyber criminals and hacktivists join forces

Generative AI

- New risks from generative AI
- The risk of a hacked ChatGPT account

This article walks through each of these risks and explains how they impact Asia-based organizations in particular.

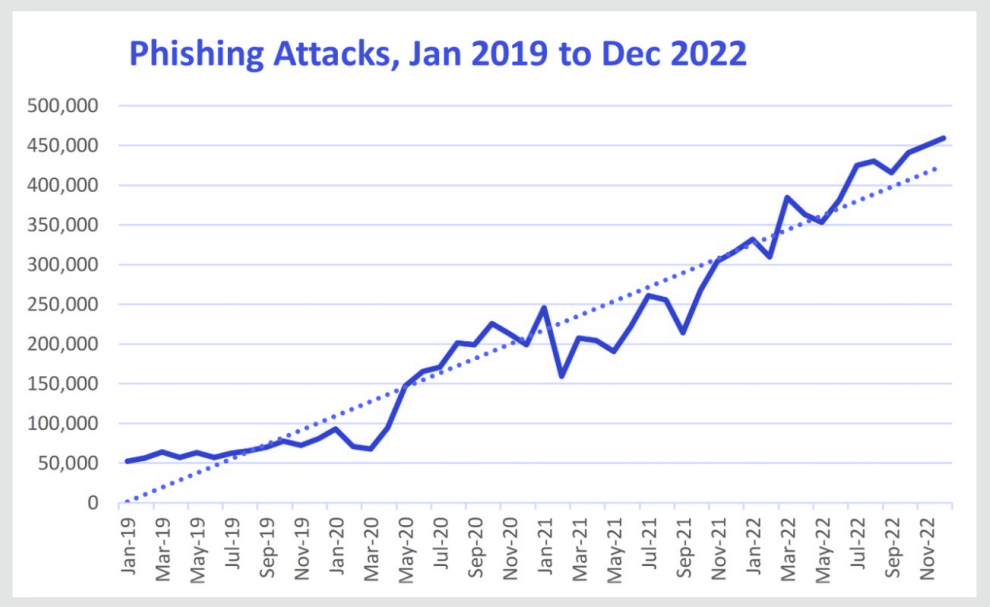
PHISHING

Let's start with phishing, which remains one of the most pervasive cyber threats in APAC and beyond. "Phishing is on the rise, and anyone who uses email, text messaging, and other forms of communication is a potential victim," CNBC notes.

As the following graph illustrates, the frequency of phishing attacks in Asia continues to grow. About 5 million attacks have been observed since 2022, and we're seeing a 150 percent year-over-year increase in phishing globally.

Figure 2 //

GROWTH IN PHISHING ATTACKS IN ASIA



Source: Anti-Phishing Working Group - https://apwg.org/trendsreports/

As for how phishing attacks in Asia actually take place, Cyberint research shows that threat actors leverage four main vectors.

Figure 3 //

THE 4 MAIN PHISHING VECTORS IN ASIA

Let's take a look at what each type of phishing entails and how organizations can block it.

EMAIL PHISHING

Phishing attacks that happen via email often use one of the following methods in a bid to trick victims into handing over sensitive information:

- **Malicious links:** This remains the most common vector of attack for email phishing. Victims click a link – which is often obfuscated behind an image or misleading text, so that the actual link is not the same as the text indicated on the screen – that redirects them to a phishing website.
- **Malicious attachments:** Attackers can also attach files to emails that contain links to malicious sites.
- **Reply requests:** This is a less common type of email phishing method, but it's also harder to block because you can't detect it by simply scanning email contents. Attackers send emails that do not contain any links or attachments, but that simply ask the victim to reply. The attackers' goal is to open a conversation. If the victim responds, the attacker will follow up with messages that contain malicious links or attachments.

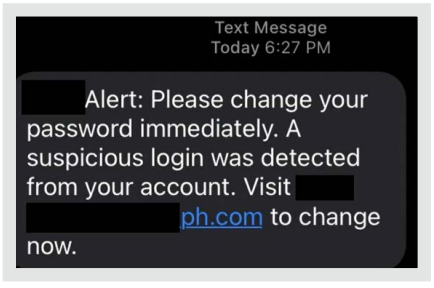
To protect against these risks, businesses should scan email systems for unusual messages and activity. User education also plays a role.

SMISHING

Phishing via SMS, or smishing, also remains a prevalent cybersecurity risk. Tools for sending mass SMS messages are relatively cheap; $50 can buy attackers as many as 10,000 messages. And because SMS technology is quite old, it's difficult for businesses to leverage modern security tooling to detect and block smishing attacks.

Figure 4 //

GROWTH IN PHISHING ATTACKS IN ASIA



For that reason, user education is critical for protecting against smishing.

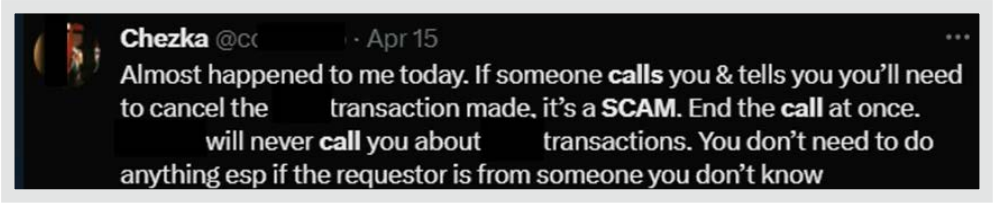
VISHING

Vishing is the use of voice calls to convince victims to give up sensitive information. Voice-based phishing allows attackers to make their engagements more interactive and customize their content for specific victims– also known as social engineering– which increases the chances that their targets will fail to detect the malicious activity.

In addition, vishing gives attackers more control over the timing of attacks (since attackers can't monitor when someone has opened an email or SMS but they can determine whether or not they've answered a live phone call). This is valuable from threat actors' perspective because it helps them coordinate vishing interactions with login activity to corporate sites, allowing them to trigger requests for MFA authentications or one-time password (OTP) codes.

Figure 5 //

VISHING EDUCATION



Here again, user education is key to stopping vishing. Businesses can also monitor voice chats on their networks, and consider blocking access to untrusted calling apps or services.

SOCIAL MEDIA IMPERSONATIONS

A more novel trend in Asia phishing attacks, especially in the Philippines, is the use of social media to impersonate businesses and/or employees of those organizations.

For example, a bank might maintain a social media page where customers post comments requesting support. Because the page is public, threat actors monitor the comment section to identify users desperate for support. Then, they contact those users, claiming to be representatives of the bank and using fake social media profiles to make themselves appear legitimate.

This approach allows them to trick users into sharing credentials or clicking links. Attackers may also be able to coordinate MFA logins using this method, since they can interact with customers in real time.

We don't see any sign that sophisticated phishing attacks like these will slow down. Phishing remains very profitable, and advanced attack techniques make it all the more lucrative by increasing the rate of successful attacks.

The best way to stop social media impersonations is to monitor social platforms for signs of impersonation.

INFOSTEALERS

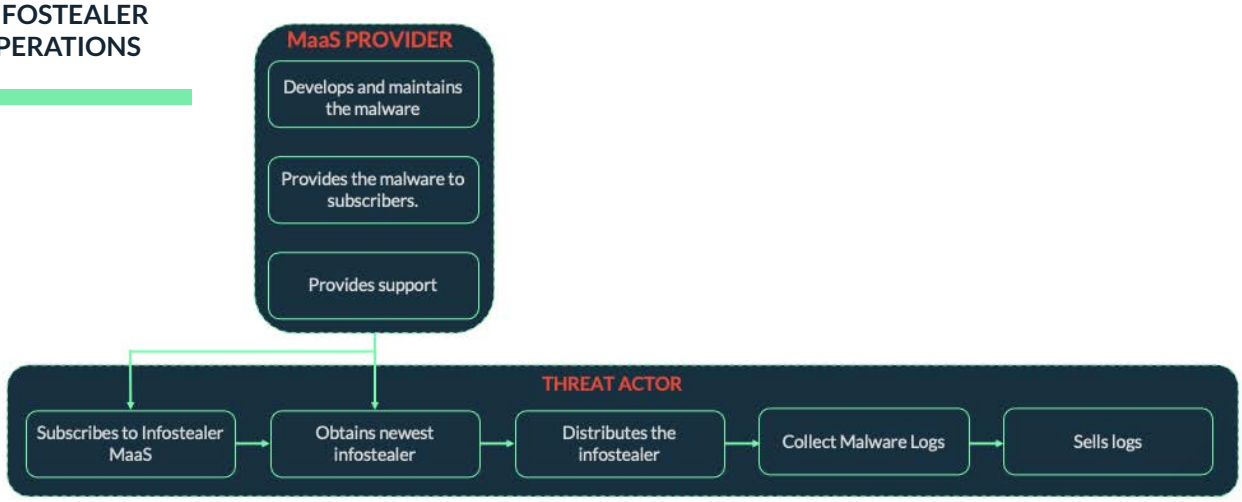
InfoStealers are a special type of malware that has existed since early 2020, but they are becoming increasingly prevalent.

InfoStealers work by harvesting sensitive data from a compromised computer or server, then sending it to attackers. For example, InfoStealing can lead to breaches of access credentials, financial information, personal information, website cookies, offline wallets, operating system details, and even screenshots of the machine's desktop and file structure. After collecting this data, InfoStealer groups sell it on the Dark Web – which means that Dark Web scanning is one way to help detect this type of attack.

Prominent InfoStealer families include RedLine, Aurora, Raccoon, and Vidar. The criminals who develop these malware families often similarly to a legitimate company, complete with a CEO, support staff, technical staff, research and development and so on.

Figure 6 //

INFOSTEALER OPERATIONS



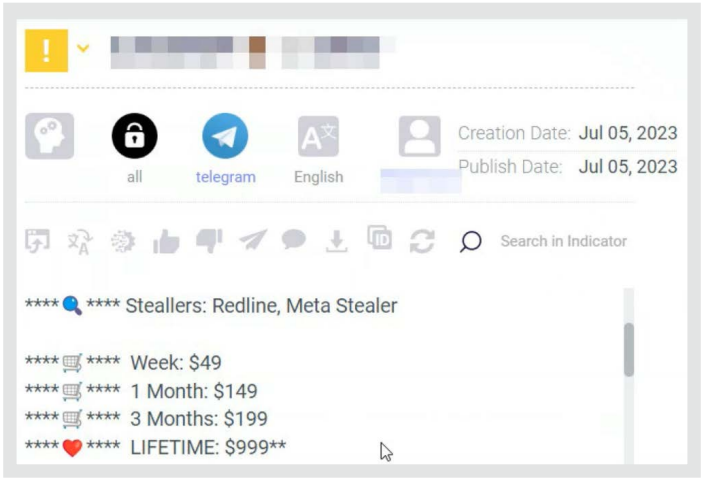
Malware operators offer what they call malware-as-a-service, which means they sell their software and accompanying support services to other threat actors who want to steal private data from organizations or individuals. Threat actors obtain their software either via drives or through downloads. They then coax victims into downloading the malware through a variety of techniques, such as phishing, malicious emails, social media impersonation, and so on.

Because malware operators are constantly updating their software, subscribers have access to malware whose signature is not yet present in standard threat or antivirus databases.

Subscription prices for these services vary from as little as $49.99, up to $999 for a lifetime subscription. According to our research, threat actors who subscribe for just $150 per month are capable of spreading around 10,000 malware infections within just that month. 10,000 malware logs at $10 each can make $100k from a seed investment of just $150.

Figure 7 //

REDLINE STEALER SUBSCRIPTIONS



Cyberint research shows that in Asia, InfoStealing is particularly prevalent in the following countries:

Figure 8 //

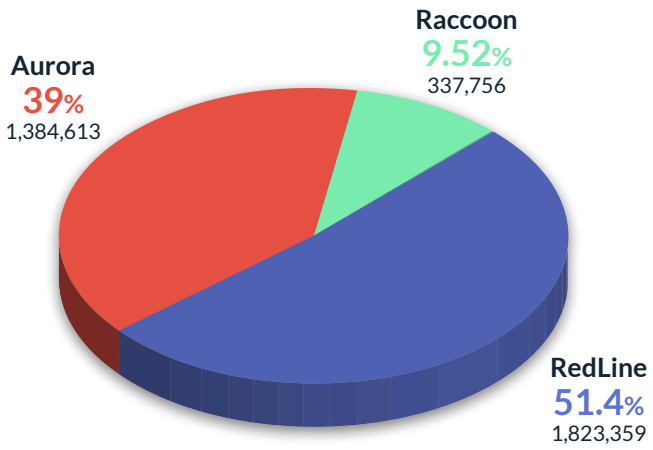
TOP 10 NATIONS TARGETED BY INFOSTEALERS IN APAC

Vietnam, India and the Philippines likely top the list because their Internet users tend to be less aware of cybersecurity best practices, placing them at a higher risk of clicking links or installing software that plants InfoStealing malware on their devices.

More than half of the InfoStealer activity we've detected in APAC is linked to RedLine, which dominates the market because it operates like a well-organized company. Aurora and Raccoon also have a notable presence in this market.

Figure 9 //

INFOSTEALER ACTIVITY SPLIT

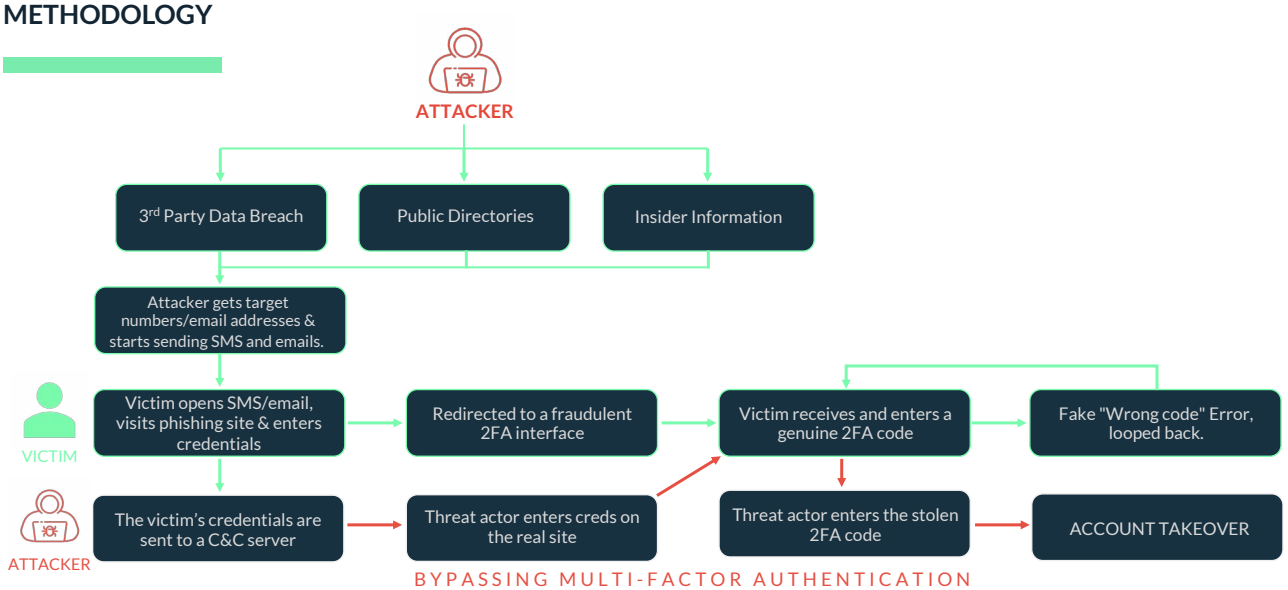


MFA BYPASS

MFA bypass is the practice of working around multi-factor authentication controls. In Asia, we're seeing threat actors bypass MFA in two main ways.

Figure 10 //

MFA BYPASS METHODOLOGY



METHODOLOGY 1

The first uses a phishing strategy to obtain MFA credentials from victims in real time.

Threat actors use a third-party service to identify potential victims. The threat actors then target those victims with a fraudulent phishing link. If the victim falls for the attack, they enter their real credentials into a fraudulent login portal. The threat actor then in real time enters those details into the legitimate website or app that the user thinks they are logging into. For example, an attacker who has stolen a victim's username and password for a banking app could initiate a login request to the app using those credentials (right after the victim does on the phishing site).

Then, when the app prompts the attacker for an MFA login step, the attacker redirects the user to a fraudulent MFA interface asking for a 6 digit code to continue with the service. The victim receives and enters the genuine MFA code to the phishing MFA website, which the threat actor then receives. The threat actor enters it into the actual website and takes over the account.

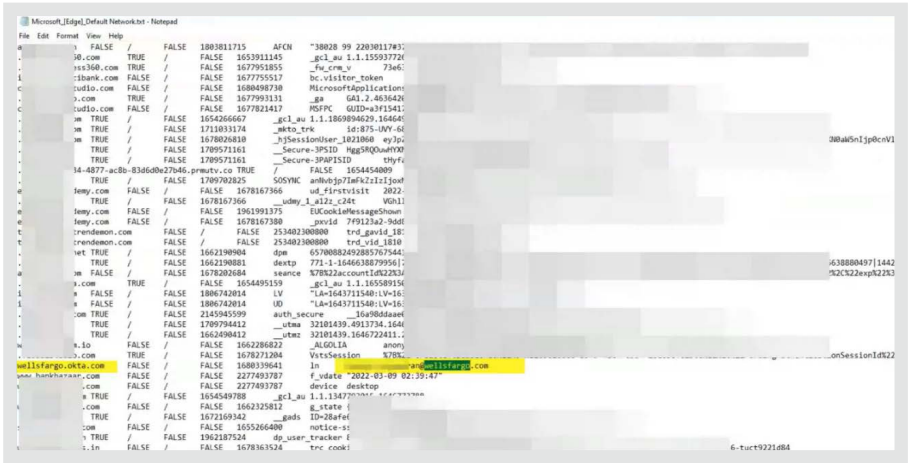
Sophisticated attackers can take this form of MFA bypass further. Banks are cautious and often request an additional MFA to send money. When the threat actor requests a bank transfer another MFA code is requested. The phishing site will display an error code and ask them to retry. This time they enter the second MFA code enabling the threat actor to input it and permit the bank transfer. In this way, they can bypass MFA even in cases where apps require MFA prompts each time a user performs a high-risk action, like sending money.

METHODOLOGY 2

A second form of MFA bypass is the use of InfoStealers to steal website cookies. Cookies can be used to store login information so that users don't have to enter usernames and passwords or complete an MFA authentication step every time they connect.

Figure 11 //

MFA BYPASS USING COOKIES



If attackers are able to copy these cookies, they can then plant them on a device they own and use them to bypass login requirements, including MFA in cases where the app is configured to skip MFA prompts if the user recently completed one.

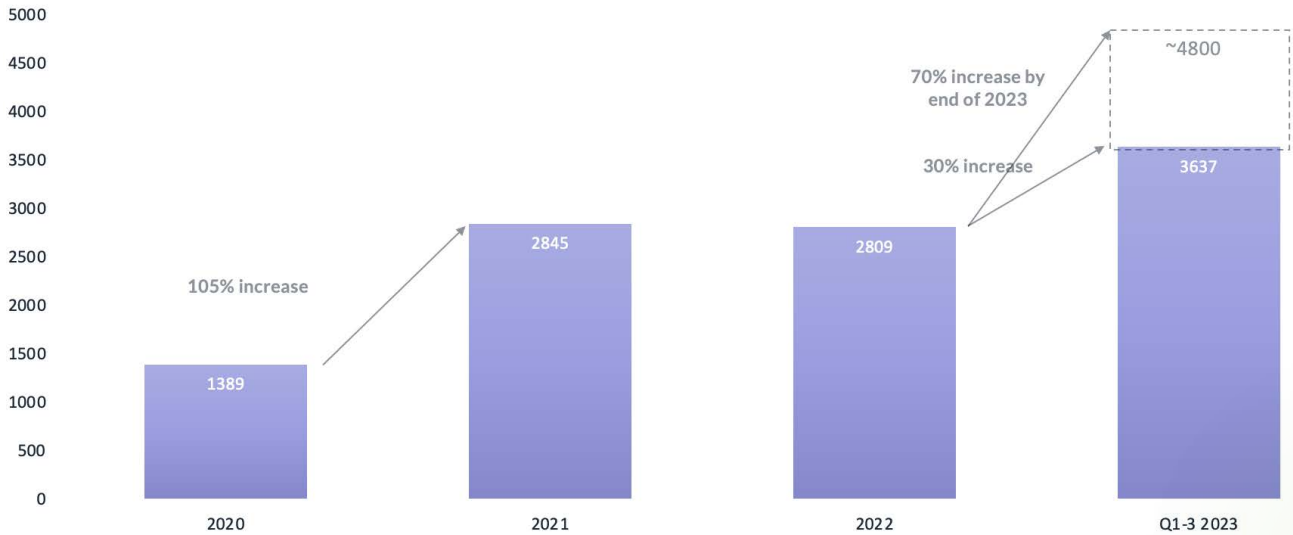
There are other methods of MFA bypass, too, but the two described above are what we're seeing most often in Asia cybersecurity attacks.

RANSOMWARE APAC CYBER THREATS

We were only nine months into 2023 when we collected data about ransomware in Asia, but by that point, ransomware attacks had already increased 30 percent compared to the previous year. That puts us on track to see a 70 percent overall increase in ransomware in Asia by the end of 2023.

Figure 12 //

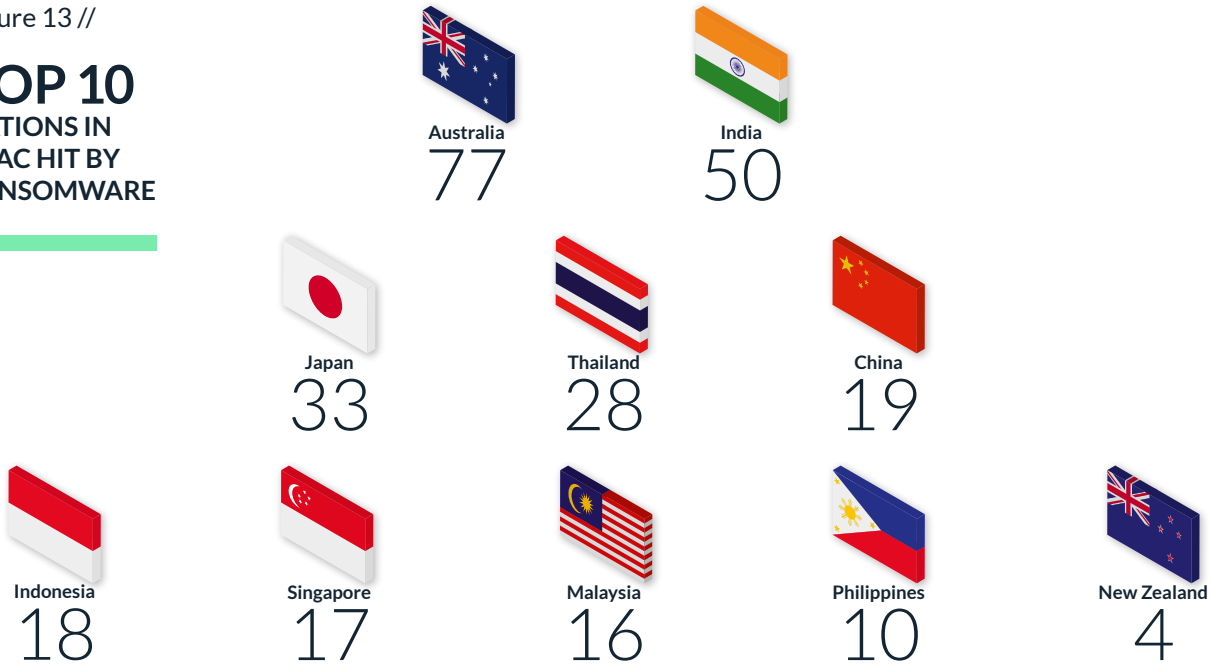
NUMBER OF RANSOMWARE ATTACKS PER ANNUM, GLOBALLY



The following countries top the list of those affected by ransomware in APAC:

Figure 13 //

TOP 10
NATIONS IN APAC HIT BY RANSOMWARE



Australia, India and Japan probably top the list because they are home to more businesses, making them compelling targets for threat actors hoping to get victims to pay a ransom. Ransomware gangs also tend to study which countries have more capability of paying.

Cyberint research also shows that the frequency of ransomware attacks in Asia varies significantly between different industries, with professional services and engineering businesses being targeted most often:

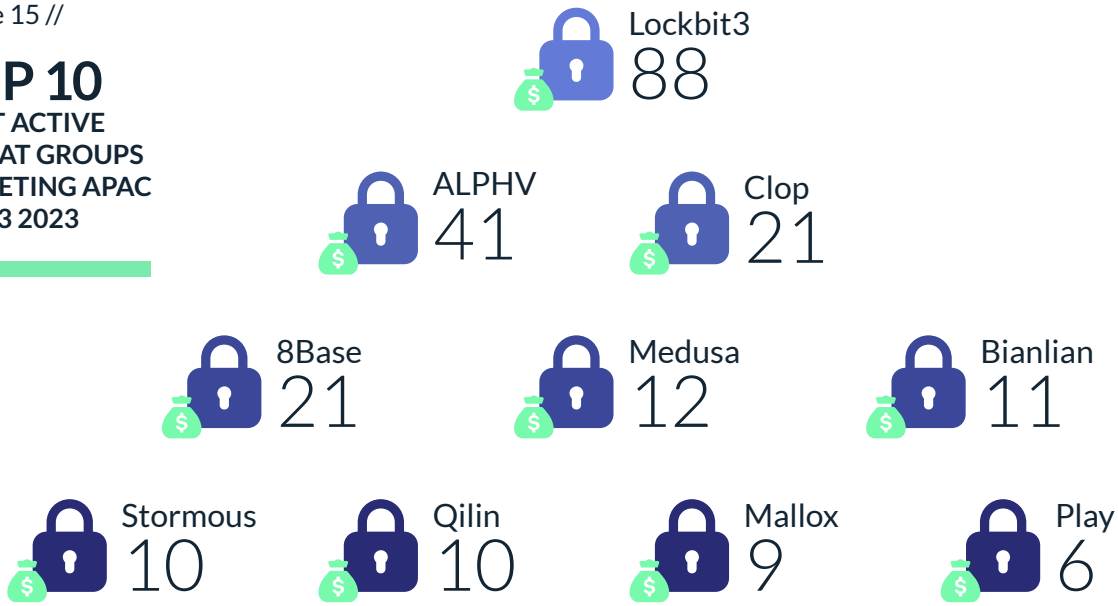
Figure 14 //

TOP 10
INDUSTRIES TARGETED IN APAC Q1-Q3 2023

For Asia Pacific, the most common or the most acting threat or ransomware group that is targeting us is LockBit 3.0 followed by ALPHV/Blackcat.

Figure 15 //

TOP 10
MOST ACTIVE THREAT GROUPS TARGETING APAC Q1-Q3 2023



The good news is that, on the whole, organizations are improving their ransomware defenses. Our data shows that more companies are performing daily backups so they can recover from ransomware without paying the ransom.

This, however, is causing ransomware groups to shift tactics to encryption-less attacks. Encryption is highly laborious and relatively easy to detect, making it a less attractive technique for lazy threat actors.

Some ransomware attackers are now simply aiming to steal sensitive data so they can threaten to expose it publicly if businesses don't pay a ransom. Backups don't help in this case. Once the ransomware attackers have stolen the file and exfiltrated the sensitive data, it's very difficult for the victims to ensure that it isn't dumped on the darkweb without actually paying. The only thing businesses can do is prevent data exfiltration from occurring in the first place.

SOFTWARE SUPPLY CHAIN ATTACKS

Software supply chain attacks, which research suggests account for 62 percent of all intrusions, happen when attackers compromise third-party software that a company uses, then uses it to attack the company. Supply chain attacks – such as the MOVEit breach, a prominent recent supply chain attack that allowed threat actors to exploit a vulnerability to target not just customers who had paid for MOVEit, but also non-MOVEit customers, as illustrated below:

Supply chain attacks come in many forms, but you are potentially at risk if third-party vendors have privileged access to your systems or data, or if they supply technology to you.

Figure 16 //

DIFFERENT TYPES OF SUPPLIERS, SIMILAR TYPES OF RISKS

Unfortunately, protecting against supply chain attacks can be hard. The typical business has dozens or possibly hundreds of different suppliers, each with unique products, making it challenging to identify risks in each one. In addition, different suppliers may have different levels of access to assets – some may store your company's usernames and passwords, for example, while others can view API tokens or SSH keys that provide access to critical systems. Plus, the level of supply chain risk that businesses can tolerate may vary from one company to the next, so risk assessment requires a lot of nuance.

The fact that users inside businesses sometimes onboard third-party apps without official IT approval, leading to what's known as shadow IT, complicates supply chain risks, because some third-party software may not be properly validated. To protect against this risk, you should be scanning all of your software assets continuously; periodic audits are not enough for detecting risks before they lead to potential attacks.

The solution to protecting against supply chain risks is, first, to inventory your vendors and suppliers so that you identify any blind spots you may be overlooking. From there, you must assess the risk that each supplier poses, using both evaluations of their cyber hygiene as well as continuous monitoring of the Deep and Dark Web for indications of other threats facing those 3rd parties, such as exposed credentials, malware infections, data leaks, and more. All of this should be conducted on a continuous, ongoing basis.

HACKTIVISM

Hacktivism, which means carrying out cyberattacks to support activist causes, is a growing threat in Asia and beyond.

Simplistic takes on hacktivism tend to assume that all hacktivists are ideologically motivated. However, as Tennille W. Scott and O. Shawn Cup write on the ethics of hacktivism, "hacktivists consist of a number of subgroups with a variety of motivations not secured to a good-bad continuum." They also note that hacktivists cause real harm when they disrupt systems, regardless of their motives.

Traditionally, threat actors have been placed into three distinct categories:

- **Cyber criminals** – Financially motivated groups and individuals who treat hacking like a business, with the primary goal of monetary gain.
- **Nation-state actors** – Sophisticated threat actors and threat actor groups focused on espionage - obtaining classified information from adversary governments. They are funded by governments and are therefore not financially motivated.
- **Hacktivists** – Ideologically motivated, non-governmental individuals or groups, who do not seek financial gain.

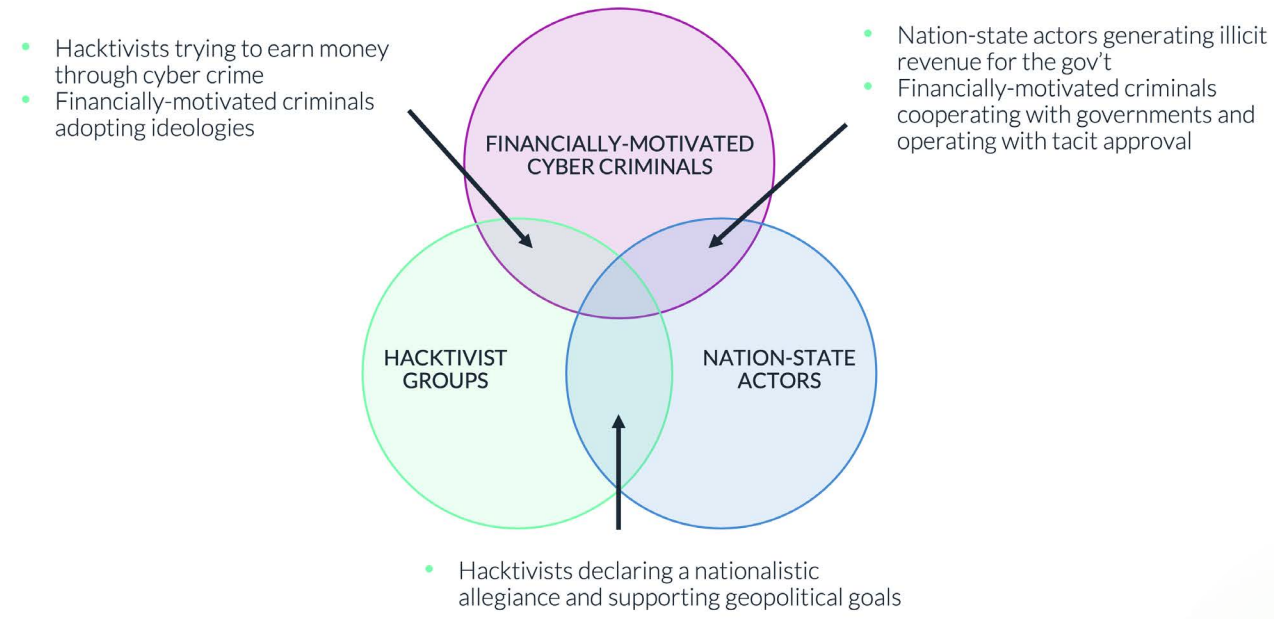
However, these distinctions are becoming fuzzy. The Cyberint research team has observed instances where the lines between the above categories are becoming blurred.

- Hacktivists have joined forces with Cyber criminals for financial gain.
- Cyber criminals have, in some cases, declared allegiances to nation-states and taken sides in geopolitical conflicts.
- Hacktivists have developed affiliations with nation-states to further their mutual causes e.g. Anonymous Sudan. Anonymous Sudan is a hacktivist group unofficially aligned with Sudan. There have also been several Hacktivists groups who have declared allegiance to Russia or Ukraine following the conflict that began in February 2022 e.g. SiegedSec
- Nation-state actors have been observed committing economic crimes e.g. North Korean state actors have been observed stealing cryptocurrency and Chinese state actors have been spotted committing economic espionage and stealing intellectual property.
- Nation-state actors have been observed disguising their espionage activities as a cryptojacking malware campaign in order to obfuscate their true objectives and confuse attribution efforts.

Therefore, the lines between Hacktivists, Cyber criminals and Nation-state actors are blurring.

Figure 17 //

THE COMPLEXITY OF THE HACKTIVISM THREAT



THE RISE IN HACKTIVISM- RELATED CYBERATTACKS

Hacktivism-related cyberattacks are happening around the world, but some prominent recent incidents have taken place in Asia. For example, a group backed by the North Korean government recently stole $3 billion, possibly to fund a weapons program.

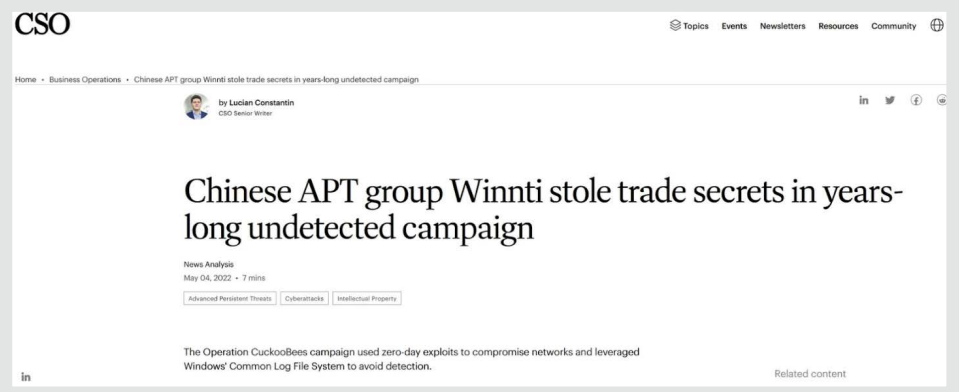
Figure 18 //

NORTH KOREA HACKER STEALING CRYPTOCURRENCY

Likewise, a Chinese APT group recently compromised trade secrets.

Figure 19 //

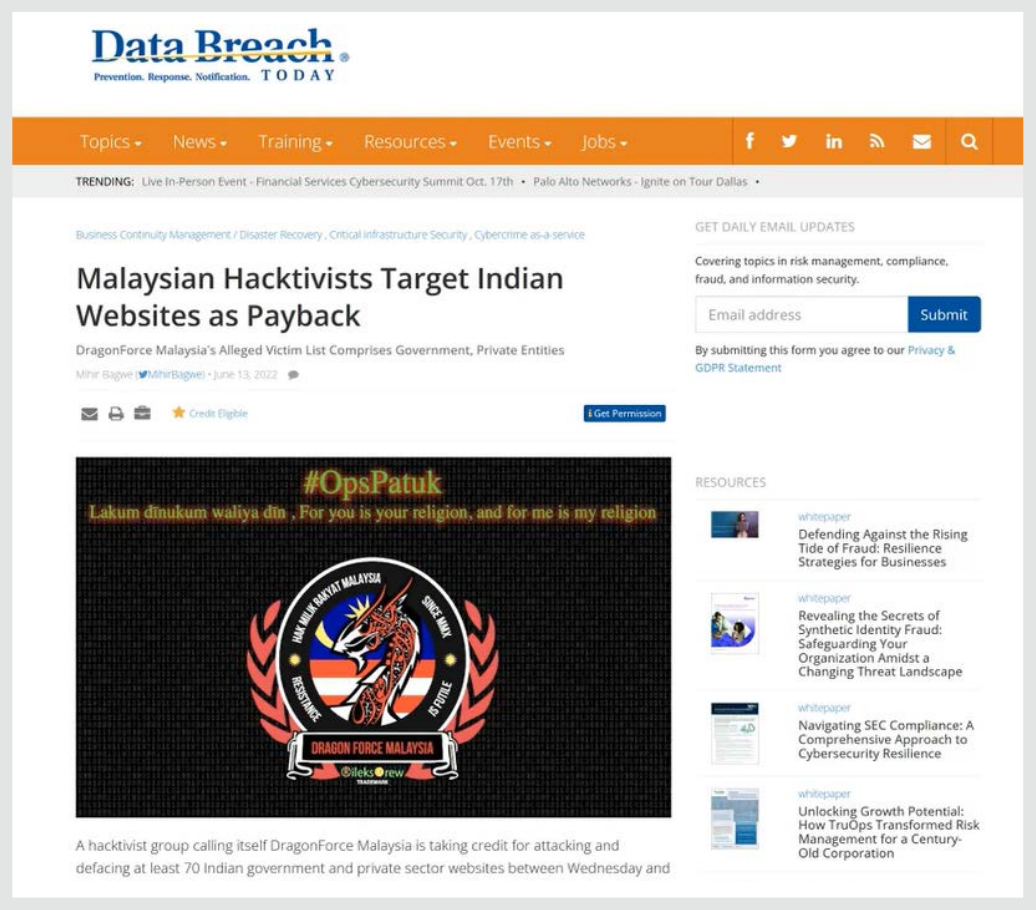
CHINESE APT GROUP STEALING TRADE SECRETS



And a Malaysian hacker group that was evidently not officially backed by the Malaysian government, but was apparently ideologically motivated, carried out attacks against foreign websites:

Figure 20 //

MALAYSIAN HACKTIVISTS



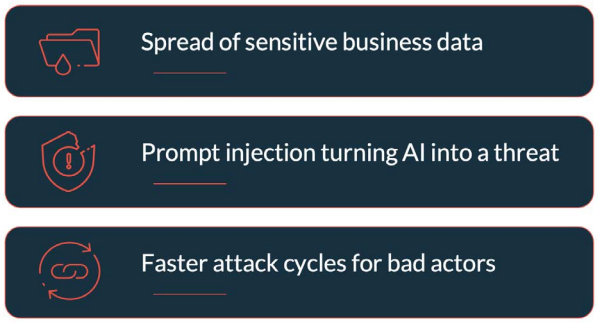
For APAC organizations, the takeaway is clear: Now is the time to get ahead of hacktivist-linked attacks before they become even more common.

GENERATIVE AI

Generative AI technology has opened up many exciting opportunities, but it also creates novel cybersecurity challenges. In particular, threat actors are using genAI tools like ChatGPT to accelerate their attacks. ChatGPT can help them write content to drive phishing campaigns, for example.

Figure 21 //

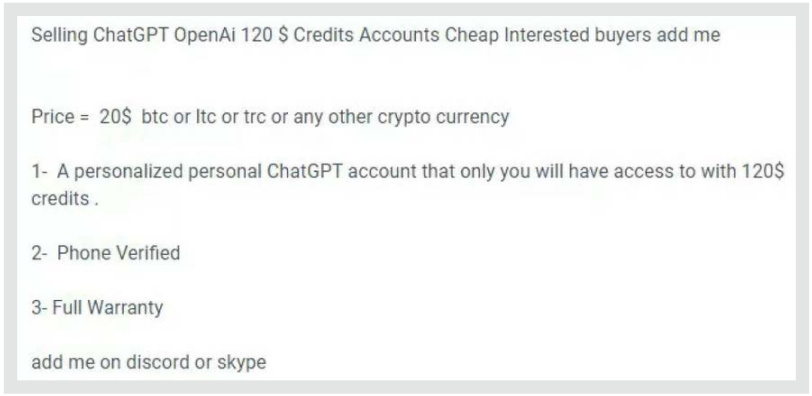
THE RISK OF AI



In addition, some threat actors are now selling access to compromised ChatGPT accounts. The following Cyberint screenshots shows a real-world example of such an attack.

Figure 22 //

REAL-WORD EXAMPLE OF CHATGPT ATTACK



On top of this, there is a risk that sensitive data that users share with generative AI services will become accessible to threat actors who target these services. Using techniques like prompt injection, threat actors can trick the large language model (LLM) behind a genAI service into exposing users' private data, which they can then use to support further attacks.

HOW TO PROTECT AGAINST APAC CYBER THREATS

The list of cybersecurity threats that impact Asia-based organizations is long, and there is no simple solution to them. Instead, businesses must deploy a multi-pronged strategy that both mitigates attackers' ability to target them in the first place and detects attacks once they are underway so that companies can limit their scope.

An effective cyberdefense strategy today includes all of the following:

- **Patch management:** Businesses must know which software is out of date and patch it before attackers exploit vulnerabilities.
- **Workforce training:** User education plays a key role in protecting against risks like phishing attacks and MFA bypass.
- **Security-first culture:** Everyone at the organization – not just security personnel– should make security a priority in every decision or action they undertake.
- **Monitoring:** Everything a business owns – from physical devices, to websites, to social media accounts and beyond – must be monitored for risks.
- **Threat intelligence:** Threat intelligence drawn from the Dark Web helps reveal how threat actors are operating and what their goals are.
- **Third-party risk management:** Businesses must identify and mitigate risks not only within their own software and systems, but also within those of third-party suppliers or partners.

Cyberint plays a central role in empowering businesses to establish a comprehensive cybersecurity strategy. Cyberint's impactful intelligence combines cyber threat intelligence, external attack surface management, brand protection, and digital supply chain intelligence into a single, powerful platform. By leveraging autonomous discovery of all of an organization's external-facing assets, coupled with open, deep & dark web intelligence, the solution enables cybersecurity teams to accelerate the detection and disruption of their most pressing cyber risks. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, malware, fraud, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.

Contact us to learn more about how Cyberint can help protect your company.

Cyberint

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL
Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM
Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

USA – TX
Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

SINGAPORE
Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA
Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

JAPAN
Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.