ENSIGN INFOSECURITY

Cyber Threat Landscape Report 2025

Version 1.4 | 21 July 2025

Editorial Foreword

The cyber threat landscape continues to evolve with geopolitical tensions, trade tensions, internal strife and the evolving adversarial behaviours fuelling the changes. Across the Asia Pacific, we have seen threats becoming more persistent, more targeted, and more difficult to defend against. We have developed this report to share our observations on the key trends and developments shaping the region's cyber threat landscape.

This year's edition includes observations from across ASEAN, East Asia and the South Pacific. As our regional presence grows, we remain committed to bring an Asia Pacific focussed view of the cybersecurity situation of the digital environment we operate in, whether through the threat intelligence we gather, the incidents we respond to, or the platforms we contribute to.

The environments in which we operate are complex. From geopolitical flashpoints and trade tensions, to localised unrest and cross-border criminal activity, each region presents its own unique cyber risk profile. Such an environment has proven fertile for the thriving underground economy, which we observe to have active collaborations and subcontracting, leading to increasing capability developments, and increased scale and efficacy of cyber-attacks and campaigns.

The widening use of diverse technologies, including those from established Western vendors, open-source solutions, and the emerging Eastern technology solutions, have led to increasingly the fragmented digital ecosystems. This complexity makes defending against Ransomware, state-linked cyber-attack campaigns, cybercrime, and hacktivism not only more challenging, but also more urgent.

Ransomware in particular, has become endemic in the region, if not globally. We are seeing variants that bypass EDR and XDR systems with increasing success. Hacktivists are also becoming more tactically capable, moving beyond surface-level disruption and website defacements, to leverage advanced exploit platforms. Meanwhile, organised cybercrime groups are expanding in number and sophistication, with many of them working in concert with larger threat actors. These collaborations are increasing the complexity to determine the motivation and "mastermind" behind attacks.

Ensign remains committed to monitor how these developments are reshaping the threat landscape. This report outlines key defensive considerations and offers recommendations that security leaders can act on to stay ahead of a threat environment that shows no sign of slowing down.

As a Research Sponsor to the MITRE Center for Threat Informed Defense and an advocate for the threat-informed defence concept, we continue to provide tactics, techniques and procedures (TTPs) for the observed threats leveraging the MITRE ATT&CK framework, version 17 this year, with the MITRE ATT&CK Navigator JSON files for cyber defenders to use in monitoring, threat hunting, red teaming, risk assessments, and other cyber defence operations.

ENSIGN INFOSECURITY

Ensign InfoSecurity is the largest cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address our clients' cybersecurity needs.

Our core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response.

Underpinning these competencies is in-house research and development in cybersecurity.

Ensign has more than two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

For more information, visit www.ensigninfosecurity.com or email marketing@ensigninfosecurity.com

Table of Contents

Executive Summary

Executive Summary

Since the formation of Ensign in 2018, we have released these threat reports to help our clients and the general community understand the state of the threat environment in Asia Pacific. In 2025, we note the growing geopolitical and trade tensions around the world and observed the growing cyber activities by a number of threat groups.

For 2025, key insights to note:

1. State-sponsored threat groups are increasing their activities. They are likely to be pre-positioning, in light of geopolitical and trade tensions, to maintain strategic opportunities for future effects by compromising digital infrastructure and the cyber supply chain. Whether this is for the purposes of staging for future attacks, espionage or disruption. The intentions are multi-fold, but we suspect this will grow significantly, posing concerns for the public sector and critical infrastructure operators.
2. Ransomware continues to be the endemic "digital flu" that plagues companies across the world. Criminal groups are collaborating and competing in the underground economy for a larger share of the prize. New capabilities are being developed and the efficacy of attacks will grow. We note:
    - Initial Access Brokers (IABs) pursuing a "breach once, sell to many" approach.
    - Mastermind threat groups subcontracting cyber-attack tasks to other parties to create multi-prong and distraction effects in their cyber campaign.
    - Multiple income streams pursued for financial gain amongst organised crime groups.
3. Finally, attacks are also targeting the weaker but highly important links in our economic systems. In particular, we are witnessing attacks on our business and professional services (BPS) firms, including legal firms, accounting companies and professional services firms. These companies hold (or are custodians of) significant assets but are not large enough to mount deep defences, and have come under increasing attacks from threat groups.

The cyber space is not a benign place and as digitisation grows, and the use of AI becomes more pervasive, the threats will commensurately grow. Ensign remains committed to defending and protecting our customers in this environment.

Developments and Insights

Top Developments and Insights of 2024

Ransomware adopted capabilities to circumvent defences and canvass victims

- Ransomware adopted EDR/XDR stealth and process killing capabilities to impair defences.
- Ransomware adapting programming languages which provide performance, stealth and multi-platform targeting to reach more victims.

Organisations should review and ensure that the asset defence coverage is adequate, configurations are hardened, and EDR/XDR solutions are competent and updated.

State-sponsored threat groups adjusted pre-positioning for future effects

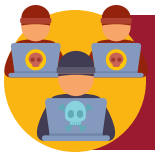
- Geopolitical tensions fuelled state-sponsored activities.
- State-sponsored threat groups have adjusted their pre-positions to adapt for future effects of disruption and espionage.

As APTs they generally demonstrate strategic patience in their campaigns to maintain opportunities for future intents and missions.

IABs adopted "breach once, sell to many" approaches for access & opportunistically sold assets

- IABs have fractured into individuals and small groups, capitalising on multi-income streams.
- Opportunistic exfiltration of digital assets are sold for additional financial gains.
- Ransomware affiliate programmes are prioritised with subsequent sales for ongoing exploitation.

Victims can expect recurring attacks from many different threat actors.



Hacktivists are evolving through collaboration & capability adaptation

- Previous hacktivist groups are observed to collaborate with organised crime groups and state-sponsored actors, blurring their identity.
- Adaptation of leaked Ransomware source codes and playbooks are leading to them evolving into organised crime groups with significant capability upgrade.

Increasing organisation of these groups can help defenders better profile and defend against them. Organisations need to be aware of perceived ideological bias and attractivity to hacktivists.

AI exploited for influence operations & compromise of cyber supply chains

- Phishing and scams are amplified by threat actors exploiting generative AI for higher believability.
- AI used to exploit recruitment processes with remote work opportunities to implant personnel as insiders into the cyber supply chain.

Organisations need to enhance cybersecurity awareness programmes to educate approaches to defend against AI-enhanced attacks. Solutions to detect AI generated communications, audio and visual to bolster defences.

Technology bifurcation & mixed implementation creating fragmented digital attack surface

- Increasing adoption and integration of Western technology solutions, open source solutions, and emerging Eastern technology solutions have fragmented the digital attack surface, creating more integration-oriented vulnerabilities
- Poor familiarity in addressing different technologies adding to the strain managing vulnerabilities.

Organisations should reconsider their digital supply chain (hardware, software and vendors), avoiding over diversification to ensure the organisation's ability to support and defend against respective threats.

Developments and Insights

The Asia Pacific region experienced a high intensity of cyber threat activity in 2024, fuelled by geopolitical tensions (e.g., South-China Sea disputes, PRC-ROC tensions, PRC-DPRK-Russia involved activities), increasing economic competition (e.g., US tariffs, US-China tensions), challenges (e.g., Myanmar civil unrest, organised crime syndicates operating along Thailand's border), and uneven progress made in digitalisation and cyber defence maturity (laws and operations).

Across the territories, Ensign observed increasing variety of technologies implemented, from well-established and familiar Western solutions, open source and open source adapted solutions, and Eastern (predominantly driven by Chinese companies) solutions. The rising diversification of technologies used in the organisations' digital attack surface elevates the complexity and challenges organisations face in maintaining effective defences against the increasingly competent and sophisticated cyber threats.

In the midst of the situation in 2024, the public sectors and organisations have been making steady progress in bolstering the cyber defences. Governments across the world have updating their regulations to provide greater guidance on how to lay out the cyber controls for businesses and critical infrastructure – the EU updated the NIS legislation to enhance cybersecurity resilience and digital defence, Singapore updated the Cybersecurity Act, Indonesia's Personal Data Protection Law and Malaysia's Cyber Security Act came into effect in 2024, just to name a few. Amidst these regulatory developments, regional and international efforts are also underway to build up capacity and capability through collaborative efforts and exercises – the efforts through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore, and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand, the establishment of the ASEAN-CERT, the annual EU Locked Shields exercise, and continued dialogue and proliferation of the UN cyber norms, just to name a few.

Developments and Insights

RANSOMWARE, with (i) the leaks of Ransomware platform source codes (e.g., LockBit and Conti) and Ransomware-as-a-Service (RaaS) operations playbooks, (ii) the reorganisation of constituent operators (i.e., initial access brokers, RaaS operators, negotiators, crypto mixers and launderers), the barrier to entry for parties with malicious intent to rapidly adopt Ransomware operations has been lowered.

Supported by the now commonplace pervasiveness of generative AI solutions, both in the public and deep and dark web (DDW), threat actors are now more rapidly evolving their exploits, techniques, playbooks and platforms to increase their success rates in penetrating organisations and extracting value from them, whether that be (i) information and monetary value, or (ii) to cause pain through disruption, compromise of operations and destruction of technology services.

The prevalent RaaS variants in 2024 have developed novel capabilities which advance the Ransomware groups' financial gain objectives, notably, (i) the ability to evade endpoint detection & response (EDR) and extended detection & response (XDR) solutions, (ii) having the ability to kill processes through bring your own vulnerable driver (BYOVD) – particularly to impair defences, and (iii) adopting unique programming languages to enhance performance, target multi-platform and achieve stealth objectives.

This situation in aggregate, has raised the profile of Ransomware as the new digital endemic "flu". Within Ensign's operating territories, **LockBit Gang**, **Kill Ransomware**, **RansomHub** and **Sarcoma Ransomware** are the most active, in ranking order.

Developments and Insights

HACKTIVISM related activities have been driven by the troubled times we live in today. The World Economic Forum (WEF) and the United Nations (UN) have both acknowledged that we are in a modern period of a confluence of conflicts, disagreements and disruptions around the world, with some stakeholders taking on a "might is right" approach, and others taking a more insular approach towards trade and international engagements.

Enabled by the increasingly mature underground collaboration and sharing of capabilities and services, we observed the evolution of some hacktivists taking on advanced capabilities beyond the conventional distributed denial of service (DDoS) attacks, website defacements, and data breaches. **DragonForce Ransomware** emerged, with some connectivity to the previously reported **DragonForce Malaysia** hacktivist group, which most recently attacked retail brands in the United Kingdom[1] (i.e., Marks and Spencer, Co-op, and Harrods). It first posted, in July 2022, the desire to become a RaaS, and has been observed to have refactored/forked its Ransomware from the leaked source codes from LockBit and Conti.

We are also rapidly observing Hacktivists accelerating their development of exploit platforms, e.g., MegaMedusa DDoS platform for the **RipperSec** hacktivist group, and the increased collaboration with other hacktivist or organised crime groups as seen in the collaboration between **R00TK1T** and the **Cyber Army of Russia**. When hacktivists rally behind state-linked causes, they also participate in grey zone conflicts which complicate the treatment to these groups. This also presents as a boon and a bane – the advantage of increased organisation means that it becomes easier for defenders to profile and defend against these groups' cyber-attacks, with the knowledge that they will likely become more competent and successful. The active hacktivist groups observed targeting the territories include **Bjorka**, **ETHERSEC Team Cyber**, **R00TK1T** and **RipperSec**.

INITIAL ACCESS BROKERS (IABs) active in the territories are generally observed to be individual or small groups of individuals working as mercenaries for hire. While some of the IABs have affiliations with unique threat groups, especially RaaS groups, others generally collaborate with any other threat group as long as the price is right.

Increasingly, IABs have adopted a "breach once, sell to many" practice, working with RaaS groups with advantageous affiliate programs for prioritised access, but subsequently sell access to other parties after the "embargoed" period. IABs are also observed to opportunistically collect/exfiltrate data assets upon breach to be put up for sale as additional income streams; these are commonly called infostealers.

IABs are observed to leverage alternative authentication material's such as session keys, OAuth tokens and the like to gain access rather than directly accessing user credentials, although, there is no shortage of leaked user credentials available on the region's users.

1. https://www.bbc.com/news/articles/c0el31nqnpvox

Developments and Insights

ORGANISED CRIME group activities have been steadily rising with the increased digitalisation of the region with many territories having electronic public sector services, and digital banking and payment ecosystems.

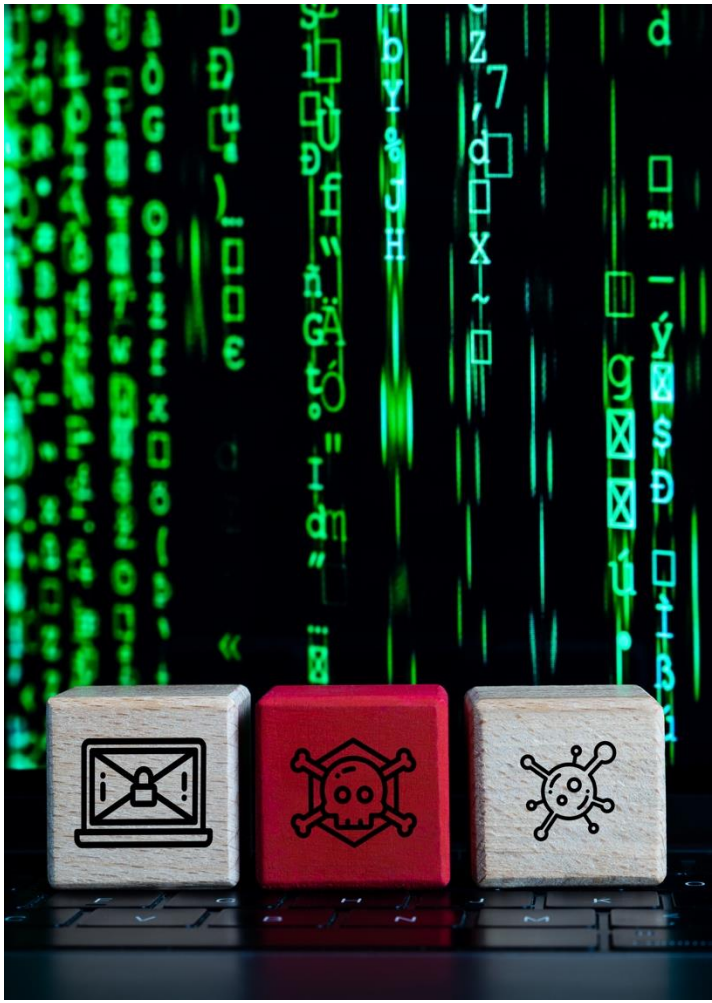
The proliferating collaborations in the underground community have also given rise to subcontracting work leading to more (individual) initial access brokers (IABs) supporting other "mastermind" threat actor groups. IABs exploiting the use of AI, are now more effective and efficient in gathering credentials, performing target reconnaissance, and identifying vulnerabilities for exploitation.

Organised crime groups have been observed to leverage AI most with enhancing the efficacy of phishing attacks by enhancing the believability of the phishing content, and adapting a multi-channel strategy (e.g., initial contact on one communication platform, and asking the victims to follow through payments in other platforms) towards getting their victims to execute actions triggering compromise. The multi-channel strategy aims to throw off the digital trails in being easy to identify them, but also to confuse victims for payments.

The past year saw a doubling of Organised Crime groups actively targeting the territories (from 5 to 10). This is despite having successful law enforcement activities taking down threat actors, e.g., the arrest of **GhostR/0mid16B/DESORDEN** in Thailand[2].

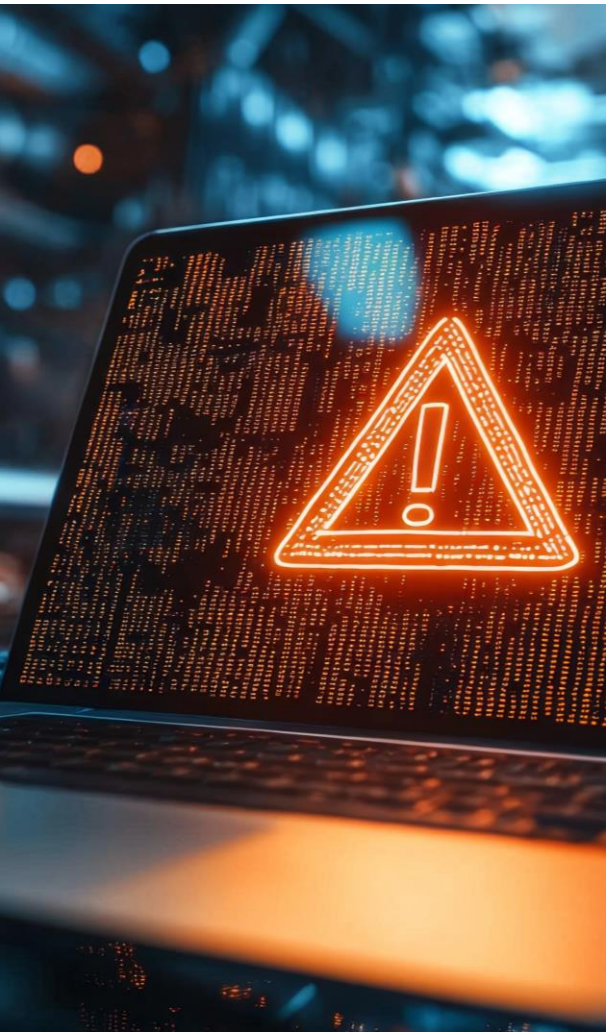
Other than operating RaaS, some of these Organised Crime groups are observed to have been subcontracted to perform data breaches, service disruptions, compromise supply chains, to help "mastermind" threat groups achieve their campaign objectives.

The Organised Crime groups observed in the territories include **BITTER**, **Blackwood**, **Bronze Highland**, **FIN11**, **FIN7**, **GhostR**, **Pseudo Hunter**, **SharpPanda**, **TIDRONE**, with **Void Arachne**. **BITTER**, **Blackwood**, **Bronze Highland**, **Pseudo Hunter**, and **Void Arachne** observed to pre-dominantly target the Greater China Region (GCR).



2 https://www.channelnewsasia.com/singapore/spf-royal-thai-police-global-hacker-arrested-altdos-desorden-ghostr-0mid16b-4963661

Developments and Insights



STATE-SPONSORED threat groups have been observed to represent **close to 40% of cyber activities in the region** (39.8%), with deepening significance in their attacks. Many of these threat groups are observed to be well-resourced, have high-level capabilities, with a strategically patient approach in their compromise. These observations correlate with the industry term of advanced persistent threat (APT) where the threat actor breaches an environment and may not actively cause detrimental (and overtly observable) symptoms until it is necessary for their interest or mission.

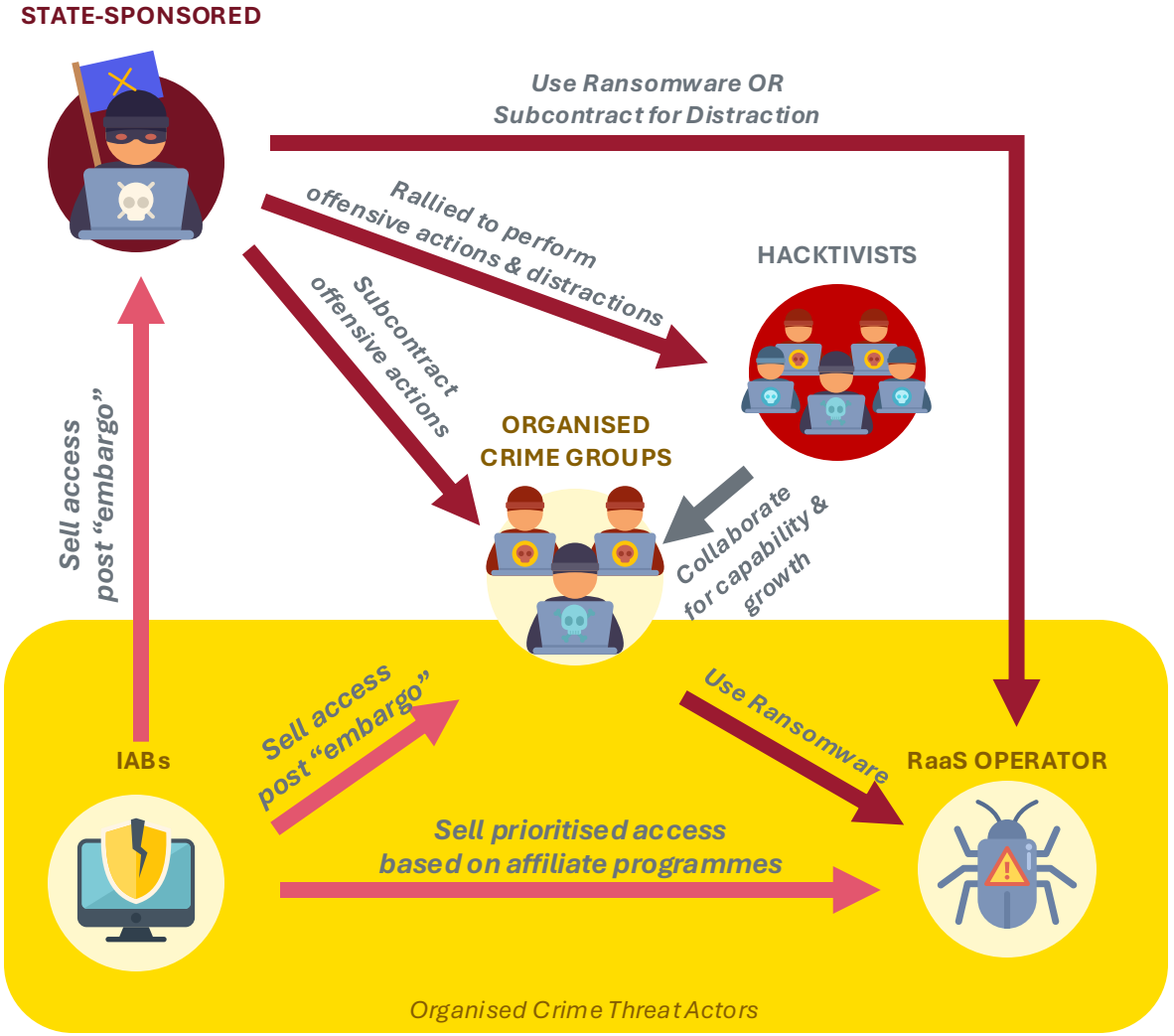
Some threat groups in this category was observed to have exploited vulnerabilities in a variety of network devices, ranging from widely used Ubiquiti routers, Cisco and Fortinet network devices, and VPN solutions with the intent to stage their capabilities. Many of these devices typically provide trusted access between networks or are part of the unmanaged and "outside of perimeter" infrastructure. Such efforts can then enable **disruption of services** and/or **espionage**. We note that these threat groups leverage the challenges organisations face in managing a complete inventory of assets and the growing vulnerability patching debt to maintain persistent access, aside from cyber hygiene issues.

Increasingly, we observed higher sophistication attacks targeting hypervisors and container infrastructure, which typically have no security defence solutions, to provide persistence, stealth and deeper access into technology environments.

ADVERSARY ECOSYSTEM is now observed to have matured to an underground economy which is rich with subcontracting work, mutually reinforced evolution and capability enhancements due to competition and collaboration, which lead to material growth in reach and sophistication. The ecosystem, coupled with the already thriving use of AI (including agentic AI) and automation can make the adversaries more effective in their exploits of their targets and victims. The following illustrates our view of the interactions between threat actors in the underground.

Developments and Insights

OBSERVED INTERACTION MAP OF THREAT GROUPS



MOTIVATIONS

STATE-SPONSORED THREAT GROUP

- Espionage & Surveillance
- Intelligence collection
- Disruption/Destruction
- Pre-positioning/staging for future effects
- Cognitive effects, e.g., influence operations

ORGANISED CRIME GROUP

- Financial gain; from contracts or directly from victim

RaaS OPERATOR

- Financial gain; from contracts, and/or directly/indirectly from victim
- Disruption and shaming for effect
- Indirectly funding and developing the underground economy

INITIAL ACCESS BROKER

- Financial gain; from contracts or direct from victim
- *"Breach once, sell to many"*

HACKTIVISTS

- Ideological achievements
- Disruption; Shaming
- Hungry for greater impact

Developments and Insights

INDUSTRIAL CONTROL SYSTEMS (ICS) attacks continue to evolve and deepen their impact into organisations which use or rely on operational technologies (OT). Other than the specialised targeting of unique OT such as field controllers, programmable logic controllers (PLCs), sensors and actuators, specialised threat groups are also targeting the IT equipment, such as networking devices, and operating systems, which are connected to the OT to gain access to the industrial operations – which can result in cyber-physical impact.

Often state-sponsored threat groups pre-position their capabilities in OT environments to enable the opportunity to disrupt operations or destroy equipment, especially for organisations who are critical information infrastructure operators, e.g., utilities and transportation.

We are also seeing the rapid prototyping of exploit tools and platforms targeting unique OT used in the ICS environments. Notably, there are observed exploit tools targeting commonplace industry solutions from Siemens, Unitronics, Rockwell, Honeywell, amongst others. While many of these exploits may not have the same sophistication as those targeting IT environments, their rise in evolution and pervasiveness may be attributed to (i) the rising industrialisation of the exploit making industry, and (ii) the use of AI to prototype and develop these exploit solutions. Combined by the fact that technology refresh and patching generally takes a longer duration of time compared to IT (e.g., 10 years or longer), the vulnerabilities will also persist for the same (long) duration, exposing organisations to cyber-attacks.

Developments and Insights

INCIDENT-RESPONSE DWELL time has significantly changed across the territories based on our observations. Given the increased technology sprawl, variety of technologies deployed (open source, Western and Eastern technology stacks), and rising sophistication of cyber-attacks, the dwell times have all increased compared to 2023 statistics in our 2024 report.

INDUSTRY GROUP	AVERAGE DWELL (DAYS)	MINIMUM DWELL (DAYS)	MAXIMUM DWELL (DAYS)
Banking, Finance Services & Insurance (BFSI)	**21**	**10**	**33**
Utilities	**23**	**7**	**27**
Business & Professional Services	**24**	**21**	**34**
Retail	**28**	**9**	**51**
Others	**70**	**15**	**201**

The **maximum dwell** observed has risen from 49 to **201 days**. The **minimum dwell** observed has risen from 3 to **7 days**. The average dwell has also risen:- **Retail** from 5 to **28 days**, and the **Others** from 33 to **70 days**.

Developments and Insights

TOP TARGETED INDUSTRIES has also seen some reshuffling given the changing times.

TERRITORY	TOP TARGETED INDUSTRIES *(Sorted in alphabetical order)*				
SG	BFI	Business & Professional Services	Hospitality	Retail	TMT
MY	Automotive & Mobility Defence & Law Enforcement Energy & Utilities	BFI	Hospitality	Public Sector	TMT
ID	BFI	Defence & Law Enforcement	Hospitality	Public Sector	TMT
SK	Aviation	BFI	Public Sector	TMT	Transport
AU	Aviation	BFI	Public Sector	TMT	Transport
GCR	BFI	Healthcare	Public Sector	TMT	Transport

The most common targeted industry groups were **Technology, Media and Telecommunications (TMT)**, **Banking, Finance and Insurance (BFI)**, and **Public Sector**.

Both **TMT** and **BFI** industry groups saw targeting across the territories. BFI targeting is a common stay with the processing of financial transactions being attractive to threat groups for financial gain and to cause social unrest. TMT targeting is largely fuelled by the continued adoption of Cloud services, also fuelled by AI solutions adoption.

Developments and Insights

TOP OBSERVED EFFECTS of cyber incidents in the territories saw **Data Breach**, **Denial of Service,** and **Ransom** dominate the rankings.

	RANK				
TERRITORY	**1ST**	**2ND**	**3RD**	**4TH**	**5TH**
SG	Data Breach	Ransom	Denial of Service	Sale of Access	Data Leak Sale of Data
MY	Data Breach	Denial of Service	Ransom	Defacement	Initial Access
ID	Denial of Service	Data Breach	Defacement	Data Leak	Initial Access
SK	Denial of Service	Data Breach	Ransom	Initial Access Data Leak	-
AU	Denial of Service	Data Breach	Ransom	Defacement	Data Leak
GCR	Data Breach	Initial Access	Data Leak	Ransom	Denial of Service

Throughout this report, Ensign has provided key MITRE ATT&CK techniques for each relevant context for readers to use for follow-on defensive actions such as Red Teaming, threat hunting, and to tune the detection and mitigation measures.

*Full versions of the techniques heatmaps can be found in **Appendix A** with links to download MITRE ATT&CK Navigator JSON files for further review. Full versions of the vulnerabilities observed in the territories can be found in **Appendix B**. **Appendix C** has the ICS oriented techniques heatmap with links to JSON files.*

Developments and Insights

OBSERVED ACTIVE RANSOMWARE THREAT GROUPS ANALYSES (1/2)

	VICTIM TERRITORY						OBSERVED KEY CHARACTERISTICS				OBSERVED LANGUAGE USED		
THREAT GROUP	**SG**	**MY**	**ID**	**SK**	**AU**	**GCR**	**DLS**	**MULTI-EXTORTION**	**EDR/XDR STEALTH**	**BYOVD**	**RUST**	**GOLANG**	**C/C++**
Akira	Ma				Ma		●	Decrypt; Leak	●	●	●		●
Brian Cipher			Ma				●	Decrypt; Leak; Data Sale	●				●
DragonForce Ransomware	Po		Po			Po	●	Decrypt; Leak	●	●			●
Kill Ransomware	Po		Po	Po	Po	Po	●	Decrypt; Leak		●			●
LockBit Gang	Ma	Ma	Ma	Ma	Ma	Po	●	Decrypt; Leak	●	●			●
Qilin Ransomware	Po				Ma		●	Decrypt; Leak	●	●	●	●	
RansomHub	Po	Po	Po		Po		●	Decrypt; Leak		●		●	●
Sarcoma Ransomware	Im	Po	Po		Ma		●	Decrypt; Leak; Data Sale	●	●			●

While it is generally observed that all the active Ransomware threat groups in the territories operate a **Data Leak Site (DLS)** and practice **multi-extortion**, the newer capabilities to **evade anti-malware solutions** and **escape detections** vary across the variants. It is noteworthy that the newer Ransomware threat groups generally are observed to have forked or refactored a combination of **LockBit**, **Conti**, and other leaked Ransomware source codes.

The ability for **EDR/XDR Stealth** generally stems from the Ransomware (i) targeting the hypervisor, (ii) using containers and/or virtual machine images, or (iii) leveraging hard to fingerprint binaries created from **RUST** programming language.

We also observe that the prevalence in sharing or acquiring compromised drivers and modules with "EDR killing" capabilities to be embedded as payload in the Ransomware through **BYOVD**. This allows for the Ransomware to **kill processes** relating to identified anti-malware solutions, thereby impairing the victim endpoint's defences.

The use of **Golang** enhances the Ransomware with write-once, use on many platforms capabilities. The conventional **C/C++** languages enable high performance and speed for the Ransomware, particularly for (i) encryption/decryption, and (ii) exfiltration purposes.

***Legend: Ma** – Material **Im** – Impending **Po** – Potential **In** – Insubstantial **BYOVD** – Bring Your Own Vulnerable Driver*

Developments and Insights

OBSERVED ACTIVE RANSOMWARE THREAT GROUPS ANALYSES (2/2)

These developments mean that organisations need to redouble efforts in bolstering their cyber defences. These include:

1. **Performing inventory of endpoints** (on premise, containerised, virtualised, or in the Cloud) and ensuring that **security monitoring is as comprehensive as possible** across both the perimeter and the internal environment
2. **Ensuring that anti-malware solutions**, particularly endpoint detection and response (EDR) and extended detection and response (XDR) solutions, **are competent and updated**. *Organisations can review MITRE ATT&CK Evaluations for reference on their capabilities.*
3. **Perform regular threat hunting informed by threat intelligence**. Leveraging threat intelligence advisories, particularly focussed on known threat actor behaviours (or tactics, techniques and procedures) to uncover compromised environments which may not have demonstrated symptoms.
4. **Reviewing backup and archival processes**, ensuring that there is adherence to the **3-2-1-1 backup and archival strategy** and that the organisation is prepared with **golden images for critical system rebuild** in the face of Ransomware.
    - 3-2-1-1 generally refers to having 3 copies of data, stored on 2 different types of media, keeping 1 copy offsite, and keeping 1 offline copy. Permutations of the strategy include having a copy online for fast recovery, and having one kept offsite and offline. Having the offline copy set to immutable generally enhances the opportunity for recovery.
    - Preparing for system rebuild through golden images generally bolsters the organisation's confidence in having a fallback option to recover from the Ransomware-induced business disruptions.

5. **OPTION** to consider planning for **non-production "Third Recovery Site"**. This option should be considered by organisations needing high resilience outcomes for business. It requires the minimal planning and preparation for rebuilding critical systems and services to enable critical business operations to continue. This "Third Recovery Site" can be considered a cold site, with no connectivity to production systems, but with the necessary assets to allow rapid setup to operational status. Such planning and preparation will often rely on Cloud services to leverage on demand scaling up of resources, and the organisation having prepared to leverage containerised service architectures and virtual machines.
6. **Drill and exercise processes and procedures** relating to **Ransomware response and disaster recovery**, integrating it with the organisation's wider **business continuity management** practices, **crisis communications** processes, and **legal and regulatory engagement** processes.

https://evals.mitre.org/

Developments and Insights

MITRE ATT&CK v17

OBSERVED OPERATIONAL TECHNOLOGY (OT) THREATS ANALYSES (1/2)

There are two groups of threat actors typically targeting OT operators:

1. **Organised Crime Groups**, especially RaaS, who opportunistically exploit (i) the legacy technologies' vulnerabilities, (ii) lower cyber hygiene, (iii) connected and exposed remote services.
2. **State-sponsored** threat groups who are invested in compromising the field controllers and PLCs, and at times, staging at the connected IT assets, such as the networking equipment and administration endpoints and servers.

Organised Crime Groups exploit the significance of operational disruption to extort the organisations for fear of significant losses due to disruptions and the especially if they are critical infrastructure operators.

State-sponsored threat groups exploit these organisations with the intent to cause disruptions or perform espionage to understand the significance of impact which can be caused by disruptions. Our observations indicate that there are staging activities targeted at networking and remote access solutions at these organisations which may not be typically managed or defended by the organisations themselves, thus leaving them vulnerable through the supply chain.

OBSERVED INHERENT WEAKNESSES

Due to legacy systems and network designs, organisations are often vulnerable due to poor segmentation of functional technology operations. E.g., lack of separation between the enterprise or administration zone from the operations or supervisory zone (referencing IEC 62443 or the Purdue model). If possible, zero trust architecture (ZTA) principles should also be considered.

Many organisations are now leveraging remote access solutions to address their large real estate deployments of field controllers, programmable logic controllers (PLCs), sensors and actuators, often including Internet of Things (IoT) devices. This set of equipment are commonly without cybersecurity features thus making them easy targets for compromise.

Organisations relying on a misunderstood and often poorly implemented concept of airgap concepts are relying on a false sense of confidence that they are protected, but subsequently discovering connection pathways, both continuous and intermittent, allowing exploitation to occur.

Under the reasoning of operational efficacy, often organisations choose to have relaxed access and authentication controls, making it easy for exploitation. E.g., use of shared passwords, absent multi-factor authentication.

Low monitoring coverage completeness and use of default configurations are also allowing for easy lateral movement opportunities for threat groups which have breached the networks.

Techniques of Concern

ICS MATRIX

TA108: Initial Access
- T0819: Exploit Public Facing Application
- T0883: Internet Accessible Device
- T0886: Remote Services

TA0101: Command and Control
- T0885: Commonly Used Port
- T0869: Standard Application Layer Protocol

TA0106: Impair Process Control
- T0836: Modify Parameter
- T0855: Unauthorised Command Message

TA105: Impact
- T0813: Denial of Control
- T0826: Loss of Availability
- T0827: Loss of Control
- T0828: Loss of Productivity and Revenue
- T0829: Loss of View
- T0831: Manipulation of Control
- T0832: Manipulation of View

ENTERPRISE MATRIX

TA0001: Initial Access
- T1078: Valid Accounts

TA0011: Command and Control
- T1071: Application Layer Protocol

TA0010: Exfiltration
- T1048: Exfiltration Over Alternative Protocol

*The detailed **Techniques Heatmap** can be found in **Appendix C**. The MITRE ATT&CK techniques should be used by organisations for their detections of threats and the implementation of protection mitigations.*

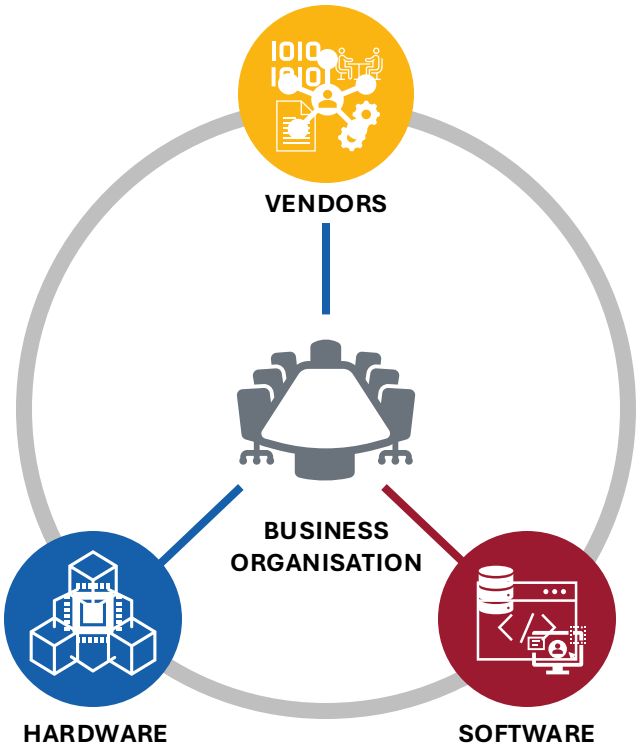
Developments and Insights

OBSERVED OPERATIONAL TECHNOLOGY (OT) THREATS ANALYSES (2/2)

OT Operators can consider the following measures to bolster their defences:

1. **Review and secure remote access connections**, implementing multi-factor authentication (MFA), security gateways and tightening authentication and access controls.
2. **Progressively arrange and architect the network of technology assets to be segmented**, so as to limit the opportunities for lateral movement and to limit the impact radius when compromise occurs. Applying Zero Trust Architecture (ZTA) principles and adopting the Purdue model as advocated in IEC 62443.
3. **Reconsider and phase technology refresh cycles to accommodate modern cybersecurity defences**. Adopting threat-informed practices by becoming more aware of threats targeting OT and implementing controls and defences during component or system technology refresh to progressively update the defence posture. This helps to reduce the legacy technology vulnerabilities and their exposure.
4. **Deliberately perform risk assessments and develop containment strategies for legacy technology use** by limiting interaction and access pathways to them. Understand that "air gap" systems are not fully disconnected – that they have connection pathways when there are maintenance activities, including for reconfiguration, patching and upgrades.
5. **Enhance cyber hygiene** by avoiding the use of shared passwords, disabling unused services and functions in systems, and restricting access (including privileged access) to the OT. Hardening the configurations of connected systems to OT will further help to bolster the risks to safety and operations.
6. **Maintain inventory of assets in the environment, instrument and monitor across these assets** by implementing OT monitoring solutions to avail the earliest opportunity to observe anomalies across operational performance and security indicators.
7. **Regularly practice and revise response and recovery actions** by performing drills and exercises to bolster confidence and review capacity for organisational resilience in facing incidents and crises.

Developments and Insights



OBSERVED CYBER SUPPLY CHAIN ATTACKS (1/3)

The cyber supply chain is made up of the **vendors**, **hardware**, and **software** which business organisations use.

Vendors are often targeted to gain trusted access to their clients which may be in a threat actor's target list. **Business and Professional Services** (BPS), as an industry group, can be made up of custodians which possess large amounts of intimate data of a business organisation. Examples of these vendors include law firms, accounting firms, and data processors. They may possess legal contracts, personal data, business arrangements, audit reports and evidences. The exposure or loss of such data can result in significant and widespread implications to their immediate stakeholders and relations.

Hardware and **software** are often targeted to gain stealthy access to target organisations, providing access and lateral movement opportunities to the threat actor. Hardware is the highest level of privileged access to digital systems we use today. Compromising hardware can provide wide-ranging access with low observability. Compromising software is useful to create lateral movement chaining opportunities. Subject to the vulnerabilities exploited, compromised software can lead to remote code execution, execution of code without user interaction, and persistence.

In 2024, we observed threat groups **targeting networking equipment and remote access solutions** {e.g., virtual private network (VPN) solutions, and virtual desktop infrastructure (VDI) solutions}; **hypervisors and container infrastructure**; and **compromising reusable software components** (e.g., open source libraries), web browsers, and productivity tools. In these categories of compromise, the threat groups exploited vulnerabilities in the cyber supply chain.

The development of threat groups **compromising networking equipment and remote access solutions** is significant in that many of these solutions are provided as managed services from service providers, and the user organisation has no direct control over their configuration and management. These devices form the unmanaged assets and services space, which cannot be directly hardened or monitored, even for the mature and well-resourced organisations. Also, these assets can be "employed" as botnet nodes, which provide compute resources and network traffic proxy services which help to obfuscate cyber-attacks.

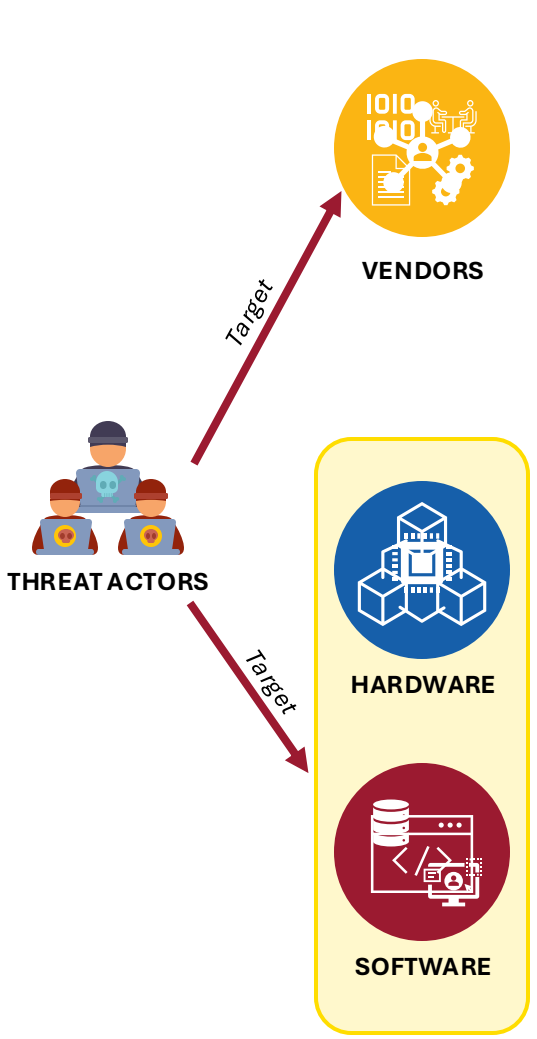
Developments and Insights

OBSERVED CYBER SUPPLY CHAIN ATTACKS (2/3)

The added observation of threat groups **compromising the hypervisor and container infrastructure** is significant also as there are no comprehensive cybersecurity solutions to monitor and protect these technologies, which increasingly form the digital infrastructure for virtualised environments and containerised architectures. Other than relying on conventional access controls and configuration hardening, it is difficult for organisations to have continuous visibility if there are anomalous activities happening at the hypervisor and container infrastructure layers.

Complicated by pervasive and persistent cyber hygiene challenges, especially in the **BPS** industry group, in the form of the use of default passwords, exposed and unsecured network services, and lack of access controls, many victims were the result of (i) having inadequate visibility of the assets in their environment, (ii) lack of system configuration hardening to strengthen the protection position, (iii) unaware of technology integration vulnerabilities, and (iv) the lack of monitoring and awareness of malicious activities occurring in the technology environment.

Furthermore, we observed that there were threat groups which performed a range of **phishing and scams**, some engaging in deliberate and complex operations **to gain employment into organisations as remote workers into** vendor organisations, by exploiting recruitment processes, to **implant compromised insiders into the cyber supply chain**, thereby creating persistent and trusted access into the cyber supply chain and provide privileged access for lateral movement into their targets – supply chain compromise via insiders.



LEVERAGE
- Possession of sensitive data
- Trusted access to target organisations

ADVERSARIAL ACTIONS
- Implant insiders as employees for persistent and privileged access.

LEVERAGE
- Complexity of software applications, reusable software components
- Implementation vulnerabilities
- Unmanaged network devices and remote access software
- Limited controls in hypervisor and container infrastructure
- Stealthy and widespread access to target organisations

ADVERSARIAL ACTIONS
- Exploit vulnerabilities in unmanaged devices
- Exploit hypervisors and container infrastructure

Developments and Insights

OBSERVED CYBER SUPPLY CHAIN ATTACKS (3/3)

Businesses will do well to consider implementing the following to manage the cyber supply chain risks.

1. **Perform inventory and identify the hardware, software and vendors** that make up the cyber supply chain used by the business.
2. **Review the materiality of the vendors and their significance** to the business operations.
3. **Review the contractual obligations and service level agreements** against the cybersecurity requirements expected by the business.
4. **Perform continuous review, risk assessments and monitor for material changes** in the hardware, software and vendors used by the business. This may be supported by the inventory and enabling monitoring through regular audits on vendors, applying threat intelligence monitoring, and vulnerability intelligence analysis.
5. **Engage and involve vendors in incident response drills and exercises** to build up confidence in collaborative actions and protocols to ensure success in response and recovery from cybersecurity incidents and crises.
6. **Extend training and awareness of cybersecurity threats and the role of the stakeholders in cybersecurity** by including vendors into the cybersecurity awareness programme.
7. **Participate in industry groups and professional communities** to gain awareness and access to community in relation to collective defence effects.

Developments and Insights

ACTIVELY EXPLOITED VULNERABILITIES ACROSS RELEVANT TERRITORIES

				VICTIM TERRITORY					
CVE Identifier	Affected System (s)	CVSS	EPSS	SG	MY	ID	SK	AU	GCR
CVE-2024-21887	Ivanti Connect Secure and Policy Secure - Web component	9.1	0.94416	●		●			
CVE-2017-11882	Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016	7.8	0.94384				●		●
CVE-2024-24919	Check Point Security Gateways	8.6	0.94327		●	●		●	
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons for ZTA - SAML component	8.2	0.9432	●		●			
CVE-2024-1709	ConnectWise ScreenConnect	10	0.9431				●		
CVE-2024-21412	Microsoft Defender SmartScreen	8.1	0.93777	●					●
CVE-2023-23397	Microsoft Outlook	9.8	0.93547				●		
CVE-2022-42475	FortiOS SSL-VPN and FortiProxy SSL-VPN	9.8	0.93196	●				●	
CVE-2023-20273	Cisco IOS XE Software - Web UI feature	7.2	0.92717	●	●	●			
CVE-2019-9621	Zimbra Collaboration Suite	7.5	0.91807	●	●				
CVE-2024-21762	Fortinet FortiOS	9.8	0.91602	●				●	
CVE-2024-23108	Fortinet FortiSIEM	9.8	0.88633	●				●	
CVE-2024-21338	Certain IOCTL of “appid.sys” known as AppLocker‘s driver	7.8	0.80512				●	●	●
CVE-2017-5070	V8 in Google Chrome	8.8	0.803						●
CVE-2024-38193	Windows Ancillary Function Driver	7.8	0.73164				●	●	●
CVE-2023-28252	Windows Common Log File System	7.8	0.52956			●			

Leveraging EPSS values of the observed exploited vulnerabilities in the territories (measured in June 2025), the following are the key insights:

1. Many of the vulnerabilities have CVSS base scores of 7 or higher, i.e., **High and Critical severity**.
2. Despite approximately more than six (6) months past 2024, the EPSS values are still high (more than 0.5 EPSS), indicating continued exploitation.
3. Categorically, the common types of software under active exploitation are related to:
    - Operating System
    - Network and VPN Equipment
    - Common Productivity Solutions
    - Web Browsers

Note: This is a non-exhaustive list. EPSS is accurate as of June 2025.

Developments and Insights

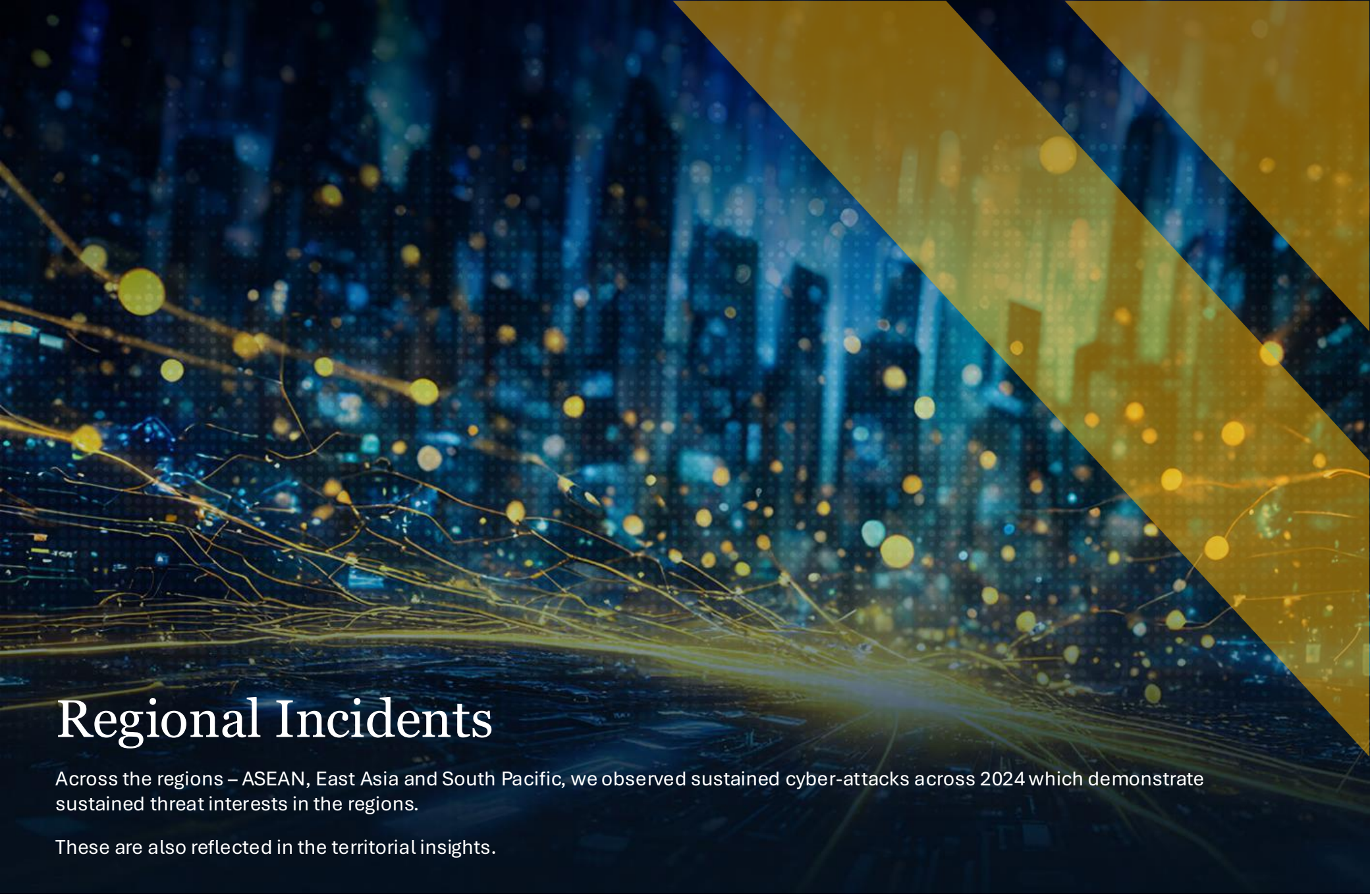
OBSERVED REGIONAL THREAT GROUPS ANALYSES

RANSOMWARE THREAT GROUP	VICTIM TERRITORY					
	SG	MY	ID	SK	AU	GCR
Akira	Ma				Ma	
Brian Cipher			Ma			
DragonForce Ransomware	Po		Po			Po
Kill Ransomware	Po		Po	Po	Po	Po
LockBit Gang	Ma	Ma	Ma	Ma	Ma	Po
Qilin Ransomware	Po				Ma	
RansomHub	Po	Po	Po		Po	
Sarcoma Ransomware	Im	Po	Po		Ma	

TARGETING THREAT GROUP PROFILE DISTRIBUTION	VICTIM TERRITORY					
	SG	MY	ID	SK	AU	GCR
Hacktivist	7 %	22%	17%	-	8%	-
Organised Crime	53%	44%	58%	38%	62%	53%
State-sponsored	40%	33%	25%	63%	31%	47%

ENSIGN THREAT CLASSIFICAT-ION MATRIX	→→→ *Increasing levels of threat to the subject* →→→			
	Insubstantial (In)	Potential (Po)	Impending (Im)	Material (Ma)
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

THREAT GROUP *(excl. Ransomware)*	ASSOCIATED TERRITORY	PROFILE	VICTIM TERRITORY					
			SG	MY	ID	SK	AU	GCR
BITTER	Unknown	Organised Crime						Ma
Bjorka	Indonesia	Hacktivist			Ma			
Blackwood	GCR	Organised Crime						Ma
Bronze Highland	GCR	Organised Crime						Ma
ETHERSEC Team Cyber	Indonesia	Hacktivist			Ma			
FIN11	Unknown	Organised Crime					Im	
FIN7	Russia	Organised Crime					Po	
GhostR	Unknown	Organised Crime	Im					
Pseudo Hunter	South Korea	Organised Crime						Ma
R00TK1T	Unknown	Hacktivist		Ma				
RipperSec	Malaysia	Hacktivist	Im	Po			Po	
SharpPanda	GCR	Organised Crime		Im	Im			
TIDRONE	Unknown	Organised Crime				Ma		
Void Arachne	GCR	Organised Crime						Ma
State-sponsored Threat Groups			Ma	Ma	Ma	Ma	Ma	Ma



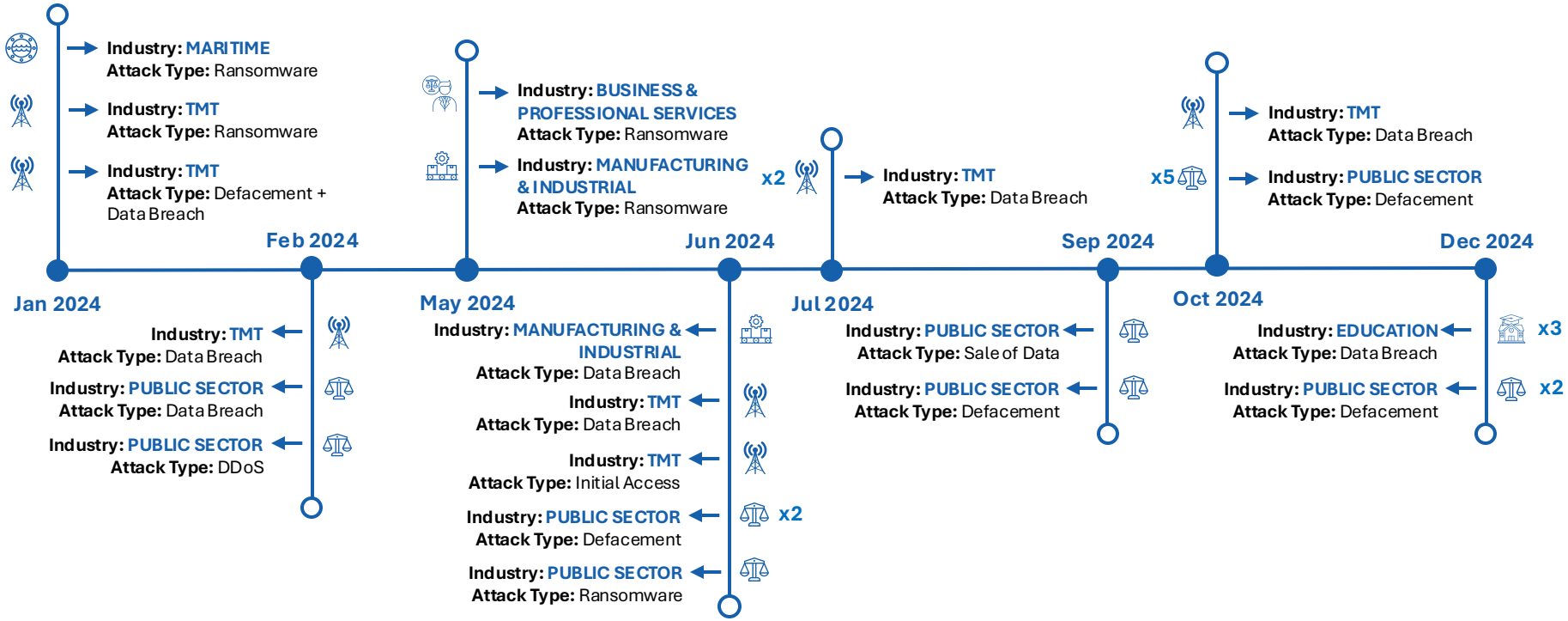
Regional Incidents

Across the regions – ASEAN, East Asia and South Pacific, we observed sustained cyber-attacks across 2024 which demonstrate sustained threat interests in the regions.

These are also reflected in the territorial insights.

ASEAN

NOTABLE CYBER INCIDENTS



ANALYSIS

Across the ASEAN region attacks were predominantly targeting **Public Sector** and **TMT** industries.

Public Sector Industry Targeting

State-sponsored threat groups, fuelled by espionage interests relating to trade, foreign affairs and observed staging for possible future cyber-attacks. **Hacktivists** motivated by regional and international conflicts relating to geo-politics and religion.

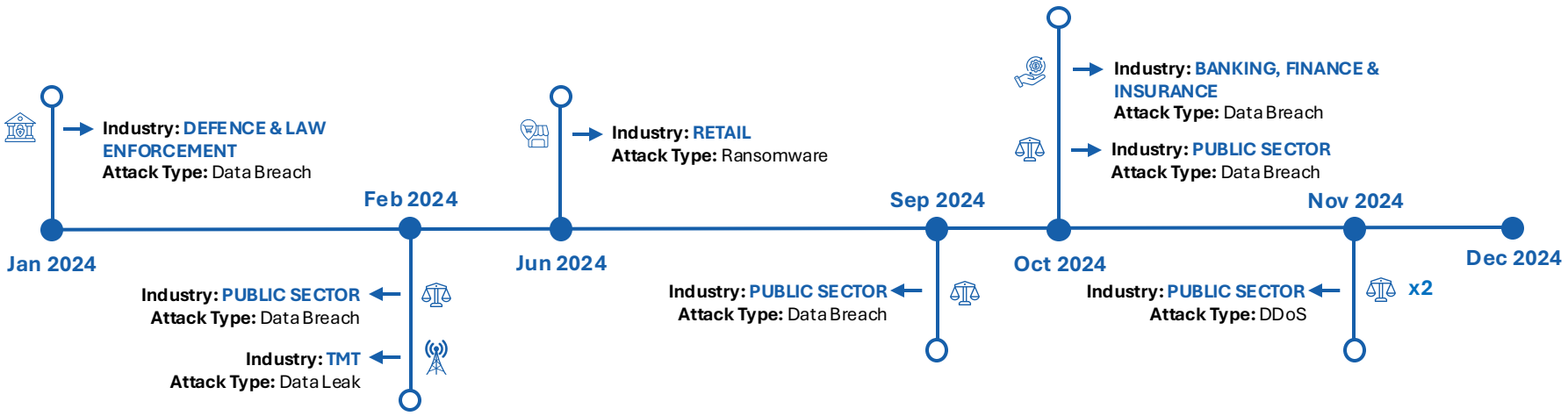
TMT Industry Targeting

State-sponsored threat groups targeted TMT for their significance in the cyber supply chain, with critical infrastructure in focus for espionage and disruption as key observed effects and to access, through the supply chain, their eventual targets. Staging for possible future attacks were also observed on critical infrastructure. **Organised crime groups**, predominantly RaaS, targeted this industry for their significance in the cyber supply chain for financial gain.

INDUSTRY	ATTACK TYPE
TMT	• Data Breach • Defacement • Initial Access • Ransomware
Public Sector	• Data Breach • Defacement • Distributed Denial of Service (DDoS) • Ransomware • Sale of Data

East Asia

NOTABLE CYBER INCIDENTS



ANALYSIS

Across East Asia the attacks were predominantly targeting **Public Sector**; and the **civilian population**.

Public Sector Industry Targeting

State-sponsored threat groups, fuelled by espionage interests relating to trade, foreign affairs and observed staging for possible future cyber-attacks. These threat groups were also interested in the military activities in relation to capabilities and its industry.

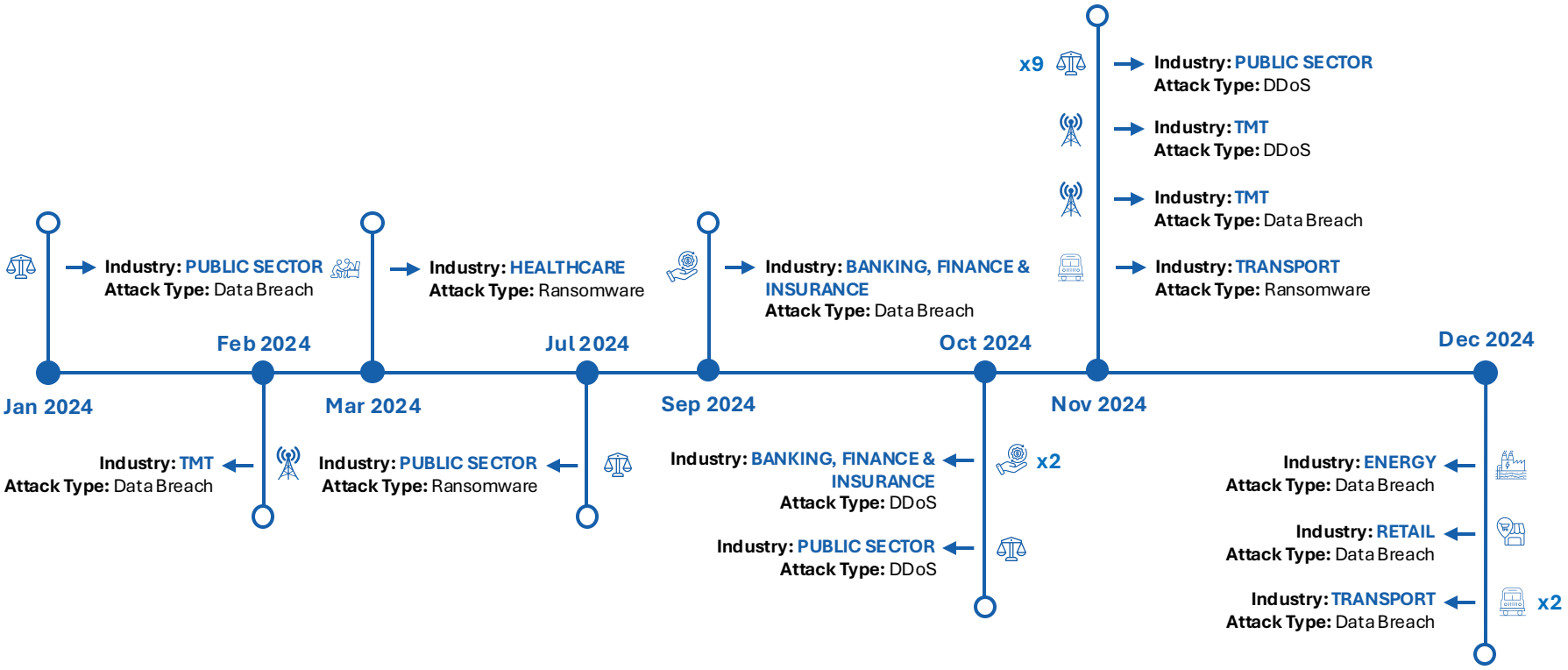
Civilian Population Targeting

State-sponsored threat groups and associated Organised Crime Groups were focussed on monitoring and information/influence operations relating to the dissidents, civil disruptions and elections. Uniquely, these groups also leveraged vulnerabilities in region-specific applications on computers and mobiles for their attacks.

INDUSTRY	ATTACK TYPE
Public Sector	• Data Breach • Distributed Denial of Service (DDoS)

South Pacific

NOTABLE CYBER INCIDENTS



ANALYSIS

In the South Pacific the attacks were predominantly targeting the **Public Sector** and **TMT.**

While Organised Crime Groups were uniquely targeting both industries in these cyber-attacks, the possibility of subcontracting from state-sponsored threat actors cannot be excluded. With Ransomware being the dominant signature of attacks in this region, exfiltration is a part of the modus operandi, which can be used to support espionage purposes as well. This possibility can be relating to trade, foreign affairs and defence industry developments in the region. Particularly, the AUKUS arrangements, geo-political posturing of global leaders in the South Pacific.

TMT forms the digital foundation for the digital economy and naturally attracts adversarial attention for threat groups. It also provides pathways for access to the entities in the cyber supply chain.

INDUSTRY	ATTACK TYPE
Public Sector	• Data Breach • Distributed Denial of Service (DDoS) • Ransomware
TMT	• Data Breach • DDoS

Territorial Insights

Singapore

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• DragonForce Ransomware • Kill Ransomware • Qilin • Ransomware• RansomHub	• GhostR • RipperSec • Sarcoma Ransomware	• Akira • LockBit Gang • State-sponsored Threat Groups
	→→→ *Increasing levels of threat to the subject* →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

- **Banking, Finance & Insurance**
- **Business & Professional Services**
- **Hospitality**
- **Retail**
- **TMT**

New affected industries observed in 2024

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Data Breach	**36%**
Ransom	**21%**
Denial of Service	**16%**
Sale of Access	**8%**
Data Leak	**5%**
Sale of Data	**5%**

Techniques of Concern

MITRE ATT&CK v17

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- T1189: Drive-by Compromise
- T1091: Replication Through Removable Media

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1090: Proxy
- T1573: Encrypted Channel
- T1001: Data Obfuscation
- T1219: Remote Access Tools
- T1102: Web Service
- T1105: Ingress Tool Transfer
- T1095: Non-Application Layer Protocol
- T1568: Dynamic Resolution
- T1665: Hide Infrastructure
- T1572: Protocol Tunnelling
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1571: Non-Standard Port

TA0010: Exfiltration
- T1567: Exfiltration Over Web Service
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1030: Data Transfer Size Limits
- T1537: Transfer Data to Cloud Account

TA0040: Impact
- T1486: Data Encrypted for Impact
- T1491: Defacement
- T1490: Inhibit System Recovery
- T1499: Endpoint Denial of Service
- T1657: Financial Theft
- T1489: Service Stop
- T1485: Data Destruction
- T1498: Network Denial-of-Service
- T1561: Disk Wipe
- T1496: Resource Hijacking

Insights for Singapore

While **organised crime groups** are the predominant threat groups targeting Singapore, both **state-sponsored** and **hacktivist** threat groups' activities have risen. Organised crime groups are motivated by the international financial hub status Singapore has for financial gain. Cyber activity associated with **state-sponsored** and **hacktivist** threat groups is largely fuelled by the increasing geopolitical and trade tensions, and the significance of Singapore's role in international trade.

The **TMT** industry group, as the top targeted industry group, forms the underlying infrastructure and the cyber supply chain. Targeting this industry group generally provides potential access to a large number of victims, and has high disruption opportunities. **Retail** and **BFI** possess large quantities of personal data and credit information which are valuable for financially motivated threat groups. **Retail**, having a business to consumer (B2C) orientation, is more susceptible to scams and phishing, especially in fast moving businesses like e-commerce. Singapore elevated its attractivity in 2024 in MICE[3], notably attracting Taylor Swift to have the only Asian tour location for her concerts. In association, **retail** and **hospitality**, which directly relate to tourism and events, may have attracted increased targeting from financially motivated threat groups. The continued targeting of **Business & Professional Services** is not surprising as this industry group posses/process large amounts of sensitive information, including personal data, and generally having lower cyber defences.

Singapore's efforts in carrying out law enforcement action on known threat groups had also borne fruit with the arrest of the threat actor behind **GhostR/0mid16B/DESORDEN** through regional collaborative action.

Singapore observed the highest number of variants of **Ransomware** in 2024. This could be due to threat actors exploiting of Singapore's position as a financial hub for financial gain. Separately, both **Ransomware** groups and **state-sponsored** threat groups may also be exploiting Singapore's digital infrastructure as test beds for their eventual targets of other digitally advanced territories, and to exploit Singapore's trusted economy as supply chain pathway to gain access to other targets, whether in Singapore or elsewhere.

KEY TAKEAWAYS

- **Organised crime groups** are the most representative threat group targeting Singapore.
- **State-sponsored** threat groups and **Hacktivists** representation targeting Singapore has risen.
- Top targeted industry groups are respectively **TMT**, **Retail**, and **BFI**.
- **Retail** and **Hospitality** are newly observed top targeted industry groups.
- Top notable cyber-attack effects are respectively **Data Breach**, **Ransom**, and **Denial of Service**.
- Singapore observed the **highest variety of Ransomware variants** targeting the territory.

3. MICE – Meetings, Incentives, Conferences and Events.

Malaysia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• RansomHub • RipperSec • Sarcoma Ransomware	SharpPanda	• LockBit Gang • R00TK1T • State-sponsored Threat Groups
	→→→ *Increasing levels of threat to the subject* →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

Automotive & Mobility
Defence & Law Enforcement
Energy & Utilities

Banking, Finance & Insurance

Hospitality

Public Sector

TMT

New affected industries observed in 2024

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Data Breach	41.1%
Denial of Service	30.1%
Ransom	8.2%
Defacement	6.8%
Initial Access	6.8%

Techniques of Concern

MITRE ATT&CK v17

TA0001: Initial Access
- T1566: Phishing
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- T1078: Valid Accounts
- T1189: Drive-by Compromise

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1573: Encrypted Channel
- T1102: Web Service
- T1095: Non-Application Layer Protocol
- T1219: Remote Access Tools
- T1001: Data Obfuscation
- T1568: Dynamic Resolution
- T1105: Ingress Tool Transfer
- T1104: Multi-Stage Channels
- T1572: Protocol Tunnelling
- T1132: Data Encoding
- T1008: Fallback Channels
- T1665: Hide Infrastructure

TA0010: Exfiltration
- T1567:Exfiltration Over Web Service
- T1048: Exfiltration over Alternative Protocol
- T1041 Exfiltration Over C2 Channel
- T1030: Data Transfer Size Limits

TA0040: Impact
- T1491: Defacement
- T1486: Data Encrypted for Impact
- T1499: Endpoint Denial of Service
- T1498: Network Denial of Service
- T1489: Service Stop
- T1490: Inhibit System Recovery
- T1485: Data Destruction
- T1657: Financial Theft
- T1496: Resource Hijacking
- T1529: System Shutdown/Reboot

Insights for Malaysia

While **organised crime groups** are the predominant threat groups targeting Malaysia, **hacktivist** threat groups have risen. **Organised crime** groups targeting Malaysia may be subcontracted by other mastermind threat groups to perform their cyber-attacks, obfuscating the true intentions of attacks.

Cyber-attacks by **state-sponsored** threat groups may be motivated by ASEAN's developments and thus interested in performing espionage for information leverage on geopolitical and trade oriented advantages. **Hospitality** may be targeted for surveillance objectives of politically exposed persons (PEPs) and officials who participate in these international conferences and meetings in-country to monitor their movements and behaviours.

Malaysia's increased economic interest to develop the **TMT** industry group and attract foreign direct investments in **TMT** may also draw attention to threat groups who are interested to gain access to the data they process and/or the trusted access they provide to their targets.

Energy & utilities, as a newly observed top targeted industry group, may be in relation to Malaysia's role and involvement in the regional grid initiative and the energy trading fluctuations observed in 2024.

Hacktivists targeting Malaysia may be motivated by its perceived alignment relating to the conflicts in the Middle-east. **DragonForce Ransomware**, now an organised crime group, and associated with the previous moniker of **DragonForce Malaysia**, evolved from being a hacktivist group to a RaaS operator.

KEY TAKEAWAYS

- **Organised crime groups** are the most representative threat group targeting Malaysia.
- **Hacktivists** have significantly risen in representation targeting Malaysia.
- Top targeted industry groups are respectively **Public Sector**, **TMT**, and **Hospitality**.
- **Hospitality**, **BFI**, **Automotive & Mobility**, **Defence & Law Enforcement**, and **Energy & Utilities** are newly observed top targeted industry groups.
- Top notable cyber-attack effects are respectively **Data Breach**, **Denial of Service**, and **Ransom**.

Indonesia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• *DragonForce Ransomware* • *Kill Ransomware* • *RansomHub* • *Sarcoma Ransomware*	SharpPanda	• Bjorka • Brain Cipher • ETHERSEC Team Cyber • LockBit Gang • State-sponsored Threat Groups
	→→→ Increasing levels of threat to the subject →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

- **Banking, Finance & Insurance**
- **Defence & Law Enforcement**
- **Hospitality**
- **Public Sector**
- **TMT**

New affected industries observed in 2024

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Denial of Service	**56%**
Data Breach	**24.9%**
Defacement	**7.5%**
Data Leak	**4.6%**
Initial Access	**2.9%**

MITRE ATT&CK v17

Techniques of Concern

TA0001: Initial Access
- T1190: Exploit Public-Facing Application
- T1566: Phishing
- T1133: External Remote Services
- T1078: Valid Accounts
- T1199: Trusted Relationship
- T1659: Content Injection
- T1195: Supply Chain Compromise
- T1189: Drive-by Compromise

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1219: Remote Access Tools
- T1102: Web Service
- T1001: Data Obfuscation
- T1573: Encrypted Channel
- T1090: Proxy
- T1105: Ingress Tool Transfer
- T1659: Content Injection
- T1568: Dynamic Resolution
- T1104: Multi-Stage Channels
- T1095: Non-Application Layer Protocol
- T1572: Protocol Tunnelling
- T1132: Data Encoding
- T1008: Fallback Channels

TA0010: Exfiltration
- T1567: Exfiltration Over Web Service
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1030: Data Transfer Size Limits

TA0040: Impact
- T1486: Data Encrypted for Impact
- T1491: Defacement
- T1489: Service Stop
- T1657: Financial Theft
- T1490: Inhibit System Recovery
- T1485: Data Destruction
- T1496: Resource Hijacking
- T1529: System Shutdown/Reboot

Insights for Indonesia

Organised crime groups are the dominant threat groups targeting Indonesia. **Hacktivists** threat groups are observed to have increased targeting on Indonesia as well. **Hacktivists** have been observed to continue their attacks on different industries in Indonesia with the motivation to increase the awareness of cybersecurity (and privacy) amongst businesses and the public sector.

Cyber-attacks by **state-sponsored** threat groups are interested in espionage for information leverage on geopolitical and trade oriented advantages. The targeting of the **public sector** industry group can be attributed by the collective interest from **hacktivists** and **state-sponsored** threat groups.

Technology companies' interest to build out data centres and provide technology services in Indonesia, coupled by the public sector's increased desire for greater digital penetration into the population, have driven the **TMT** industry group to be the second highest targeted industry group.

Hospitality is new to the top targeted industry group, which could be due to increased interest by threat actors in performing surveillance on politically exposed persons, arising from the elections. Interest in the **defence & law enforcement** industry group could have arisen due to the increased interest in defence activities arising from geopolitical tensions relating to the South China Sea.

Bjorka and **ETHERSEC Team Cyber** are hacktivist groups which have publicly shamed public sector's efforts in cyber defence as one of their key motivations. They claimed that their efforts have helped to raise awareness for the cybersecurity industry to improve.

KEY TAKEAWAYS

- **Organised crime groups** are the most representative threat group targeting Indonesia.
- **Hacktivism** continues to be prominent in Indonesia.
- Top targeted industry groups are respectively **Public Sector**, **TMT**, and **Hospitality**.
- **Hospitality** and **Defence & Law Enforcement** are newly observed top targeted industry groups.
- Top notable cyber-attack effects are respectively **Denial of Service**, **Data Breach**, and **Defacement**.
- **Hacktivists** targeting Indonesia are mostly focussed on the **Public Sector** with expressed interest at driving the awareness of the perceived lack of cyber defences across the country.

South Korea

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• Kill Ransomware	*NIL*	• LockBit Gang • TIDRONE • State-sponsored Threat Groups
	→→→ *Increasing levels of threat to the subject* →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

- **Aviation**
- **Banking, Finance & Insurance**
- **Public Sector**
- **TMT**
- **Transport**

New affected industries observed in 2024

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Denial of Service	**84.4%**
Data Breach	**6.4%**
Ransom	**2.9%**
Initial Access	**2.3%**
Data Leak	**2.3%**

Techniques of Concern

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1189: Drive-by Compromise
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1199: Trusted Relationship
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
- T1669: Wi-Fi Networks

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1102: Web Service
- T1090: Proxy
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1573: Encrypted Channel
- T1105: Ingress Tool Transfer
- T1219: Remote Access Tools
- T1092: Communication Through Removable Media
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1571: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunnelling
- T1205: Traffic Signalling

TA0010: Exfiltration
- T1567: Exfiltration Over Web Service
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1030: Data Transfer Size Limits

TA0040: Impact
- T1561: Disk Wipe
- T1491: Defacement
- T1485: Data Destruction
- T1489: Service Stop
- T1529: System Shutdown/Reboot
- T1486: Data Encrypted for Impact
- T1657: Financial Theft
- T1490: Inhibit System Recovery
- T1498: Network Denial of Service

Insights for South Korea

State-sponsored threat groups are actively targeting South Korea with significant interest from neighbouring countries on (i) the political and civil situation, (ii) the geopolitical alliances, (iii) industry development (particularly in semiconductors), (iv) North Koreans and human rights activists resident in South Korea.

With the ongoing trade discussions, **state-sponsored** threat groups may also be interested to gain information leverage through espionage.

The most notable targeting outside of industry groups is the **civilian population**, with observed surveillance interests in South Korea, especially from the number of malicious mobile apps targeted at the residents.

The targeting of **public sector**, **BFI** and **TMT** industry groups are respectively due to (i) geopolitical interests, (ii) financial gain, and (iii) leveraging vendors to gain access to targeted victims.

Thematically, the elections in South Korea and the global trade tensions, particularly relating to semiconductor manufacturing, drew threat actors' interests in targeting the **public sector** and **TMT** industry groups.

The **transport** and **aviation** industry groups were newly observed top targeted industry groups. The aviation incident may have also contributed to additional opportunities for threat actors targeting.

Denial of Service is predominant in the cyber-attack effects, which is aligned to the significant targeting from state-sponsored threat groups with interests in disrupting services. **Data Breach** is directly related to espionage related activities.

Threat actors have also adapted their TTPs to exploit commonly used local applications such as Kingsoft WPS Office and local mobile applications.

KEY TAKEAWAYS

- **State-sponsored** threat groups are the most representative threat group targeting South Korea.
- There are **no observed hacktivism-related activities**.
- Top targeted industry groups are respectively **Public Sector**, **BFI**, **TMT**.
- **Transport** and **Aviation** are newly observed top targeted industry groups.
- The **civilian population** is targeted for surveillance objectives.
- Top notable cyber-attack effects are respectively **Denial of Service**, **Data Breach**, and **Ransom**.
- Notable that threat actors exploit commonly used local applications

Australia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• FIN7 • RipperSec • Kill Ransomware • RansomHub	• FIN11	• Akira • LockBit Gang • Qilin Ransomware • Sarcoma Ransomware • State-sponsored Threat Groups
	→→→ Increasing levels of threat to the subject →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

- **Aviation**
- **Banking, Finance & Insurance**
- **Public Sector**
- **TMT**
- **Transport**

New affected industries observed in 2025

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Denial of Service	**58%**
Data Breach	**13.7%**
Ransom	**13%**
Defacement	**6.9%**
Data Leak	**3.1%**

MITRE ATT&CK v17

Techniques of Concern

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- T1189: Drive-by Compromise
- T1091: Replication Through Removable Media

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1090: Proxy
- T1573: Encrypted Channel
- T1102: Web Service
- T1001: Data Obfuscation
- T1105: Ingress Tool Transfer
- T1568: Dynamic Resolution
- T1219: Remote Access Tools
- T1095: Non-Application Layer Protocol
- T1132: Data Encoding
- T1008: Fallback Channels
- T1571: Non-Standard Port
- T1665: Hide Infrastructure
- T1104: Multi-Stage Channels
- T1572: Protocol Tunnelling

TA0010: Exfiltration
- T1567: Exfiltration Over Web Service
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1030: Data Transfer Size Limits
- T1537: Transfer Data to Cloud Account

TA0040: Impact
- T1486: Data Encrypted for Impact
- T1491: Defacement
- T1561: Disk Wipe
- T1490: Inhibit System Recovery
- T1489: Service Stop
- T1485: Data Destruction
- T1499: Endpoint Denial of Service
- T1657: Financial Theft
- T1498: Network Denial of Service
- T1496: Resource Hijacking
- T1529: System Shutdown/Reboot

Insights for Australia

Organised crime groups are actively targeting Australia, pursuing financial gain and causing disruptions, through **Ransomware** attacks and data breaches with threats of **ransom**.

Both **state-sponsored** threat groups and **hacktivist** activities targeting Australia have risen. **State-sponsored** threat groups activities may be attributed to the rising geopolitical tensions and increased interest in the geopolitical influences in the South China Sea and the Pacific Islands. Trade tensions are also leading to increased interests to perform espionage for information leverage in negotiations. The rise of **hacktivists** targeting could be attributed to perceived support to parties in the Middle East conflicts.

The targeting of the **public sector** is focussed on foreign relations and trade, which predominantly are due to espionage interests. Some of the targeting on the **public sector** industry group is attributed to **hacktivists'** displeasure on Australia's position regarding the Middle East conflicts.

The targeting of **TMT** is correlated with the intention of threat groups interested in leveraging its position as digital infrastructure to gain access to a wider group of targets through the cyber supply chain, and the industry group's potential as data processors for high value information such as personal data and financial transactions. The **BFI** industry group usually attracts threat groups motivated by financial gain by exploiting the collection of personal data and credit information.

The new targeting of **transport** and **aviation** is noteworthy as Australia is a key trade and logistics hub for the South Pacific. Disruption to these industry groups can detrimentally impact trade, logistics and transportation in the region.

KEY TAKEAWAYS

- **Organised crime** groups are the most representative threat group targeting Australia.
- Top targeted industry groups are respectively **Public Sector**, **TMT**, and **BFI**.
- **Transport** and **Aviation** are newly observed top targeted industry groups.
- Top notable cyber-attack effects are respectively **Denial of Service**, **Data Breach**, and **Ransom**.

Greater China Region

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	• DragonForce Ransomware • Kill Ransomware • LockBit Gang	*NIL*	• BITTER • Blackwood • Bronze Highland • Pseudo Hunter • Void Arachne • State-sponsored Threat Groups
	→→→ Increasing levels of threat to the subject →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

MOST AFFECTED INDUSTRY GROUPS

The following observations are based on Ensign Proprietary Data and Cyber Threat Intelligence data. Sorted in alphabetical order

- Banking, Finance & Insurance
- Healthcare
- Public Sector
- TMT
- Transport

New affected industries observed in 2024

TOP NOTABLE cyber-attack EFFECTS OBSERVED

Data Breach	41.7%
Initial Access	15.2%
Data Leak	15.2%
Ransom	12.1%
Denial of Service	8.3%

Techniques of Concern

MITRE ATT&CK v17

TA0001: Initial Access
- T1566: Phishing
- T1189: Drive-by Compromise
- T1078: Valid Accounts
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1102: Web Service
- T1132: Data Encoding
- T1573: Encrypted Channel
- T1105: Ingress Tool Transfer
- T1090: Proxy
- T1001: Data Obfuscation
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1219: Remote Access Tools
- T1572: Protocol Tunneling
- T1568: Dynamic Resolution
- T1008: Fallback Channels
- T1665: Hide Infrastructure
- T1104: Multi-Stage Channels
- T1205: Traffic Signaling

TA0010: Exfiltration
- T1048: Exfiltration Over Alternative Protocol
- T1567: Exfiltration Over Web Service
- T1041: Exfiltration Over C2 Channel
- T1020: Automated Exfiltration
- T1052: Exfiltration Over Physical Medium
- T1030: Data Transfer Size Limits

TA0040: Impact
- T1491: Defacement
- T1561: Disk Wipe
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1490: Inhibit System Recovery
- T1489: Service Stop
- T1657: Financial Theft
- T1498: Network Denial of Service
- T1529: System Shutdown/Reboot

Insights for Greater China Region

Organised crime groups are the predominant threat group targeting the Greater China Region, motivated by the rising prominence of the financial hubs in the region, especially with its position as the second largest economy. Many of these threat groups uniquely operate within the GCR.

State-sponsored threat groups interest in the region are attributed to the rising influence the region plays in geopolitics and global trade, with these threat groups interested to gain information leverage for negotiations.

The targeting of the **TMT** can be attributed to the observed rise of developments in the region's semiconductor industry, artificial intelligence (AI) related companies and the significance of their capabilities, e.g., the "DeepSeek moment", and also, the attention on social media platforms and their perceived role in influence operations. The industry group also provides access to a wide range of digital businesses and avails disruption opportunities to threat actors.

The **BFI** industry group attracts the financially motivated threat groups and threat groups interested to understand how the economy is structured or organised to respond to global economic changes. This is especially due to the rising global concerns on the health of the second largest economy and if there are opportunities for threat actors to leverage the situation. The targeting of the **public sector** industry group is attributed to interests relating to geopolitics, trade, and human rights matters.

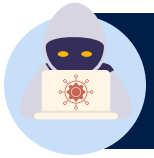
The newly observed targeting of the **healthcare** sector may be due to continued interests relating to the region's role in addressing the Covid-19 pandemic, and how it is preparing against more frequent waves of illnesses across the region. The targeting of the **transport** sector is related to the rising prominence of the region's role in electric vehicles manufacturing and the electric charging infrastructure build out. Additionally, the completion of major rail and road infrastructure networks associated with the Belt and Road initiative continues to draw attention from threat groups looking to benefit from it, whether for financial gain or information.

KEY TAKEAWAYS

- **Organised crime** groups are the most representative threat group targeting the Greater China Region.
- There are **no observed hacktivism-related activities**.
- Top targeted industry groups are respectively **TMT**, **BFI**, and **Public Sector**.
- **Healthcare** and **Transport** are newly observed the top targeted industry groups.
- Top notable cyber-attack effects are respectively **Data Breach**, **Initial Access**, and **Data Leak**.

Outlook of Cyber Threats for 2025

Outlook of Cyber Threats for 2025



Ransomware experimentation and consolidation will continue with increased collaboration

- Ransomware groups which refactor/fork leaked Ransomware source codes and playbook will emerge and adapt to determine if they are viable operations. If found lacking sustainability and competency in operations and security, they will collapse or be consolidated.
- Capability enhancements to evade or impair defences will continue with experimentation and collaboration in the underground economy, leading to rising efficacy of compromise.

Organisations should continue to adopt multi-pronged and multi-layered defences (e.g., Zero Trust Architecture principles) and ensure defence solutions are competent and updated.

State-sponsored threat groups will overtly create effects for geopolitical leverage

- Continued adjustments of pre-positioning and chosen effects of cyber-attacks may be leveraged for geo-political and trade negotiations.
- Systemic implications are to be expected from such effects on peripheral organisations through the connected cyber supply chain.

Organisations will do well to progressively collaborate and work with authorities to leverage collective defence opportunities

Incident frequency will rise due to rising technology environment complexities

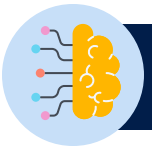
- The already complex mix and variety of technologies implemented in organisations, incomplete asset inventory records and monitoring, and the lag between vulnerability discovery and patching will exacerbate vulnerabilities exposure windows, due to implementation and integration.
- Vulnerabilities (reported and unknown) will continue to be exploited by threat actors, with rising frequencies, and increasing patching debt in organisations.

Practise threat-informed vulnerability prioritisation and accelerate patching with solutions for virtual patching and automatic patch deployments to reduce vulnerability exposure windows.

Complex cyber supply chains and redrawing of suppliers will elevate cyber supply chain compromise risks

- Trade tensions are forcing organisations to rethink and rearrange their supply chains, including digital ones.
- In the transition from the current state to a new one, vulnerabilities will occur, across vendors, hardware and software dimensions of the cyber supply chain, elevating cyber supply chain compromise risks.

Perform inventory of the cyber supply chain (hardware, software and vendors) and coupling it with deliberate threat intelligence analysis to proactively monitor for impending vulnerabilities and risks from supply chain compromise.



Accelerated AI adoption and absence of security solutions for AI will lead to more data leaks

- Security solutions for AI are not adapting fast enough to address the rapid experimentation of AI technologies and the iteration of use cases by organisations.
- Unfettered access to data repositories in organisations for AI will cause entity-oriented exposure of datasets.
- Data security oriented solutions, while fundamental, may not be flexible enough to help organisations balance AI exploitation from risk management, leading to the control gap, leading to a potential rise in data leaks.

Implement UEBA solutions and tighten identity access controls on entities and services. Establish data security controls, prioritising sensitive datasets.

Defensive Actions for Cyber Defenders and Leaders

Defensive Actions for Cyber Defenders & Leaders

Based on the compiled adversarial techniques observed in 2024, we identified the essential defensive measures and detection data sources that organisations can adopt to mitigate risks in Initial Access, Command and Control, Exfiltration, and Impact tactics as outlined in the MITRE ATT&CK™ framework.

The thematic defence strategies highlighted below centres on the crucial necessity for consistent monitoring across the digital attack surface, and integrating cyber threat intelligence analysis to embrace a threat-informed approach, especially in responding to impending and material threats.

Ensure that KRIs are tied to threats and mapped to security monitoring measurements

Review/revise key risk indicators (KRIs) based in threat-informed scenarios and ensure that the KRIs are mapped to security monitoring indicators.

Prepare for selected KRIs to be updated on high frequency during incidents to support decision making during incidents and crises.

Rehearse, drill and practice all incident-to-crisis processes to build up readiness and resilience in cyber defence

Establish a programme to regularly familiarise, train and build confidence (and capacity) in the personnel and leaders to be able to respond and recover from cyber-related incidents and crisis, ensuring that all functional teams coordinate and collaborate to navigate the situation.

Evaluate the sufficiency of resources and shifts to support these processes.

Adopt the 3-2-1-1 backup, archival and recovery strategy

Ensure that the organisation has 3 copies of data backups, in two separate mediums, with at least one kept in a remote, offline and immutable form to be resilient to Ransomware attacks.

Enhance the chances of recovery by preparing for Golden Images to allow for full rebuild of systems from the last known good state.

Enhance Asset Inventory and Monitoring Coverage, Leveraging Threat Intelligence

Progressively complete the asset inventory, ensuring as comprehensive a coverage for cybersecurity monitoring as possible, leveraging threat intelligence to proactively monitor/hunt for impending threats.

Leverage automation and artificial intelligence to scale up monitoring efficacy, focussed on adversarial behaviours, e.g., TTPs.

Review and harden configurations of systems and platforms, including key user interaction interfaces

Review the configurations of systems and services (including Cloud, hypervisor and container services and solutions) ensuring that authentication and access controls are restricted appropriately and unsafe or unnecessary services and features are disabled.

Pay attention to hypervisors, container infrastructure, web browsers, email applications and network devices, as they are often exploited for access and persistence.

Integrate incident response plans to crisis management plans, ensuring whole-of-organisation coordination

Success in addressing incidents and cyber-related crisis requires multifunctional teams across the organisation to coordinate and collectively address the situation, including crisis communications, stakeholder engagements, reporting, digital forensics, business continuity management and disaster recovery.

Collaborate with industry and regulators to bolster collective defence outcomes.

Technique	Mitigation(s)	Detection Log Source(s)
TA0001: Initial Access		
T1566: Phishing	M1049: Antivirus/Antimalware M1047: Audit M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1054: Software Configuration M1017: User Training	DS0015: Application Log DS0022: File DS0029: Network Traffic
T1078: Valid Accounts	M1036: Account Use Policies M1015: Active Directory Configuration M1013: Application Developer Guidance M1032: Multi-factor Authentication M1027: Password Policies M1026: Privileged Account Management M1018: User Account Management M1017: User Training	DS0028: Logon Session DS0002: User Account
T1190: Exploit Public-Facing Application	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1035: Limit Access to Resource Over Network M1030: Network Segmentation M1026: Privileged Account Management M1051: Update Software M1016: Vulnerability Scanning	DS0015: Application Log DS0029: Network Traffic
T1133: External Remote Services	M1042: Disable or Remove Feature or Program M1035: Limit Access to Resource Over Network M1032: Multi-factor Authentication M1030: Network Segmentation	DS0015: Application Log DS0028: Logon Session DS0029: Network Traffic
T1195: Supply Chain Compromise	M1013: Application Developer Guidance M1046: Boot Integrity M1033: Limit Software Installation M1051: Update Software M1018: User Account Management M1016: Vulnerability Scanning	DS0022: File DS0013: Sensor Health
T1199: Trusted Relationship	M1032: Multi-factor Authentication M1030: Network Segmentation M1018: User Account Management	DS0015: Application Log DS0028: Logon Session DS0029: Network Traffic
T1189: Drive-by Compromise	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1021: Restrict Web-Based Content M1051: Update Software M1017: User Training	DS0015: Application Log DS0022: File DS0029: Network Traffic DS0009: Process
T1091: Replication Through Removable Media	M1040: Behavior Prevention on Endpoint M1042: Disable or Remove Feature or Program M1034: Limit Hardware Installation	DS0016: Drive DS0022: File DS0009: Process
T1659: Content Injection	M1041: Encrypt Sensitive Information M1021: Restrict Web-Based Content	DS0022: File DS0029: Network Traffic DS0009: Process
T1669: Wi-Fi Networks	M1041: Encrypt Sensitive Information M1032: Multi-factor Authentication M1030: Network Segmentation	DS0018: Firewall DS0029: Network Traffic

Organisations should consider the following to address the key Initial Access techniques:

- **Enforce strong password policies, implement multi-factor authentication (MFA)**, regularly review and monitor user account activity to detect unauthorised access, and promptly revoke access for terminated employees to mitigate the risk of account compromise.
- **Educate employees on identifying and avoiding phishing attempts**, raise awareness about the risks associated with external threats and trusted relationships, and provide regular security training to promote a culture of security awareness within the organisation.
- **Regularly scan and patch public-facing applications for vulnerabilities, implement secure coding practices, employ web application firewalls (WAFs)** to filter and monitor incoming traffic, and conduct regular security assessments and penetration testing to detect and remediate potential exploits.
- **Regularly update and patch external-facing systems**, employ strong authentication mechanisms for remote access, and implement firewalls and intrusion detection/prevention systems to monitor and defend against external threats.
- **Establish vendor risk management programs** to assess and monitor the security posture of third-party vendors and partners, including those within the supply chain, to mitigate the risk of supply chain compromises and ensure that trusted relationships do not introduce security vulnerabilities.
- **Restrict the use of removable media devices** such as USB drives and ensure that only authorised and encrypted devices are permitted. Implement endpoint protection solutions to scan and block potentially malicious files from removable media to prevent replication through these devices.
- **Maintain updated browsers**, enforce script-blocking plugins or content security policies (CSP), and educate users to avoid suspicious links to reduce exposure to drive-by download attacks. Implement URL filtering and DNS-based protections to block access to known malicious sites.
- **Apply WPA3 or strong WPA2 encryption for Wi-Fi networks**, segment wireless access from critical internal resources, implement MAC address filtering and wireless IDS, and disable SSID broadcasting for sensitive networks to limit exposure to unauthorized access.

Technique	Mitigation(s)	Detection Log Source(s)
TA0011: Command and Control		
T1071: Application Layer Protocol	M1037: Filter Network Traffic M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1090: Proxy	M1037: Filter Network Traffic M1031: Network Intrusion Prevention M1020: SSL/TLS Inspection	DS0029: Network Traffic
T1573: Encrypted Channel	M1031: Network Intrusion Prevention M1020: SSL/TLS Inspection	DS0029: Network Traffic
T1001: Data Obfuscation	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1219: Remote Access Tools	M1042: Disable or Remove Feature or Program M1038: Execution Prevention M1037: Filter Network Traffic M1034: Limit Hardware Installation M1031: Network Intrusion Prevention	DS0016: Drive DS0029: Network Traffic DS0009: Process
T1102: Web Service	M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content	DS0029: Network Traffic
T1105: Ingress Tool Transfer	M1031: Network Intrusion Prevention	DS0017: Command DS0022: File DS0029: Network Traffic
T1095: Non-Application Layer Protocol	M1047: Audit M1037: Filter Network Traffic M1031: Network Intrusion Prevention M1030: Network Segmentation	DS0029: Network Traffic
T1568: Dynamic Resolution	M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content	DS0029: Network Traffic
T1665: Hide Infrastructure	-	DS0038: Domain Name DS0035: Internet Scan DS0029: Network Traffic
T1572: Protocol Tunnelling	M1037: Filter Network Traffic M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1008: Fallback Channels	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1104: Multi-Stage Channels	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1571: Non-Standard Port	M1031: Network Intrusion Prevention M1030: Network Segmentation	DS0029: Network Traffic
T1132: Data Encoding	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1659: Content Injection	M1041: Encrypt Sensitive Information M1021: Restrict Web-Based Content	DS0022: File DS0029: Network Traffic DS0009: Process
T1092: Communication Through Removable Media	M1042: Disable or Remove Feature or Program M1028: Operating System Configuration	DS0016: Drive
T1571: Non-Application Layer Protocol	M1047: Audit M1037: Filter Network Traffic M1031: Network Intrusion Prevention M1030: Network Segmentation	DS0029: Network Traffic
T1205: Traffic Signalling	M1042: Disable or Remove Feature or Program M1037: Filter Network Traffic	DS0029: Network Traffic DS0009: Process
T1572: Protocol Tunneling	M1037: Filter Network Traffic M1031: Network Intrusion Prevention	DS0029: Network Traffic

Organisations should consider the following to address the key Command and Control techniques:

- **Implement robust data loss prevention (DLP) solutions** and conduct regular audits to detect and prevent data obfuscation.
- **Enforce strict controls on removable media usage** and employ endpoint protection solutions to scan and block communication through such channels.
- **Utilise application layer firewalls and intrusion detection/prevention systems** to detect and block malicious activities exploiting application layer protocols.
- **Deploy proxy solutions** with advanced threat detection capabilities to identify and block unauthorised traffic.
- **Implement network segmentation and access controls** to mitigate lateral movement through non-application layer protocols and web services.
- **Monitor network traffic** for anomalies and indicators of compromise and restrict the use of remote access software to authorised personnel.
- **Employ dynamic resolution techniques** and regularly audit network configurations to detect and mitigate the use of non-standard ports and protocol tunnelling.
- **Ensure encryption of communication channels** to protect sensitive data.
- **Conduct regular security awareness training** for employees to recognise and report suspicious activities, including potential content injection attempts.
- **Implement deception technologies** or monitoring for fallback and multi-stage channels to identify staged or backup communications used by threat actors.
- **Apply infrastructure hiding detection measures** such as monitoring for fast-flux DNS or use of bulletproof hosting providers to identify potential covert C2 infrastructure.

Technique	Mitigation(s)	Detection Log Source(s)
TA0010: Exfiltration		
T1567: Exfiltration Over Web Service	M1057: Data Loss Prevention M1021: Restrict Web-Based Content	DS0015: Application Log DS0017: Command DS0022: File DS0029: Network Traffic
T1048: Exfiltration Over Alternative Protocol	M1057: Data Loss Prevention M1037: Filter Network Traffic M1031: Network Intrusion Prevention M1030: Network Segmentation M1022: Restrict File and Directory Permissions M1018: User Account Management	DS0015: Application Log DS0010: Cloud Storage DS0017: Command DS0022: File DS0029: Network Traffic
T1041: Exfiltration Over C2 Channel	M1057: Data Loss Prevention M1031: Network Intrusion Prevention	DS0017: Command DS0022: File DS0029: Network Traffic
T1011: Exfiltration Over Other Network Medium	M1042: Disable or Remove Feature or Program M1028: Operating System Configuration	DS0017: Command DS0022: File DS0029: Network Traffic
T1052: Exfiltration Over Physical Medium	M1057: Data Loss Prevention M1042: Disable or Remove Feature or Program M1034: Limit Hardware Installation	DS0017: Command DS0016: Drive DS0022: File DS0009: Process
T1030: Data Transfer Size Limits	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1537: Transfer Data to Cloud Account	M1057: Data Loss Prevention M1037: Filter Network Traffic M1054: Software Configuration M1018: User Account Management	DS0015: Application Log DS0010: Cloud Storage DS0029: Network Traffic DS0020: Snapshot
T1567:Exfiltration Over Web Service	M1057: Data Loss Prevention M1021: Restrict Web-Based Content	DS0015: Application Log DS0017: Command DS0022: File DS0029: Network Traffic
T1048: Exfiltration over Alternative Protocol	M1057: Data Loss Prevention M1037: Filter Network Traffic M1031: Network Intrusion Prevention M1030: Network Segmentation M1022: Restrict File and Directory Permissions M1018: User Account Management	DS0015: Application Log DS0010: Cloud Storage DS0017: Command DS0022: File DS0029: Network Traffic
T1041 Exfiltration Over C2 Channel	M1057: Data Loss Prevention M1031: Network Intrusion Prevention	DS0017: Command DS0022: File DS0029: Network Traffic

Organisations should consider the following to address the key Exfiltration techniques:

- **Implement robust network monitoring solutions** capable of detecting anomalous data transfer patterns indicative of automated exfiltration.
- **Enforce data transfer size limits** to prevent large-scale exfiltration attempts and implement alerting mechanisms for unusual data transfer volumes.
- **Employ intrusion detection/prevention systems (IDPS)** to detect and block exfiltration over command-and-control (C2) channels, and regularly update signatures to identify emerging threats.
- **Monitor network traffic** for suspicious activity indicative of exfiltration over alternative protocols, such as DNS or ICMP, and deploy deep packet inspection (DPI) solutions to identify and block unauthorised data transfers.
- **Implement strict access controls and encryption mechanisms** for web service interactions to prevent unauthorised data exfiltration via cloud or API-based platforms.
- **Restrict or monitor the use of physical media**, such as USB drives and external hard disks, and apply data loss prevention (DLP) solutions to prevent unauthorised physical exfiltration.

Technique	Mitigation(s)	Detection Log Source(s)
TA0040: Impact		
T1486: Data Encrypted for Impact	M1040: Behavior Prevention on Endpoint M1053: Data Backup	DS0010: Cloud Storage DS0017: Command DS0022: File DS0033: Network Share DS0009: Process
T1491: Defacement	M1053: Data Backup	DS0015: Application Log DS0022: File DS0029: Network Traffic
T1490: Inhibit System Recovery	M1053: Data Backup M1038: Execution Prevention M1028: Operating System Configuration M1018: User Account Management	DS0010: Cloud Storage DS0017: Command DS0022: File DS0009: Process DS0019: Service DS0020: Snapshot DS0024: Windows Registry
T1499: Endpoint Denial of Service	M1037: Filter Network Traffic	DS0015: Application Log DS0029: Network Traffic DS0013: Sensor Health
T1657: Financial Theft	M1018: User Account Management M1017: User Training	DS0015: Application Log
T1489: Service Stop	M1030: Network Segmentation M1060: Out-of-Band Communications Channel M1022: Restrict File and Directory Permissions M1024: Restrict Registry Permissions M1018: User Account Management	DS0017: Command DS0022: File DS0009: Process DS0019: Service DS0024: Windows Registry
T1485: Data Destruction	M1053: Data Backup M1032: Multi-factor Authentication M1018: User Account Management	DS0010: Cloud Storage DS0017: Command DS0022: File DS0007: Image DS0030: Instance DS0009: Process DS0020: Snapshot DS0034: Volume
T1498: Network Denial-of-Service	M1037: Filter Network Traffic	DS0029: Network Traffic DS0013: Sensor Health
T1561: Disk Wipe	M1053: Data Backup	DS0017: Command DS0016: Drive DS0027: Driver DS0009: Process
T1496: Resource Hijacking	-	DS0015: Application Log DS0025: Cloud Service DS0017: Command DS0022: File DS0029: Network Traffic DS0009: Process DS0013: Sensor Health
T1498: Network Denial of Service	M1037: Filter Network Traffic	DS0029: Network Traffic DS0013: Sensor Health
T1529: System Shutdown/Reboot	-	DS0017: Command DS0009: Process DS0013: Sensor Health

Organisations should consider the following to address the key Impact techniques:

- **Implement regular, encrypted backups stored offline or in immutable storage**, and conduct restoration drills to ensure rapid recovery in case of ransomware or destructive attacks.
- **Deploy web application firewalls (WAFs)** and content integrity monitoring solutions to detect and prevent website defacement attempts, and regularly audit exposed web assets.
- **Enforce endpoint protection with rollback capabilities**, disable unnecessary services, and restrict user privileges to prevent attackers from stopping critical services.
- **Implement anti-DDoS measures**, such as rate limiting, traffic filtering, and cloud-based protection services, to mitigate both endpoint and network-level denial-of-service attacks.
- **Segment and monitor systems**, enforce strict access controls, and use behavioural analytics to detect anomalies indicative of financial fraud or theft.
- **Apply strict controls on disk management utilities** and monitor for signs of low-level disk modification to prevent destructive operations like disk wiping.
- **Monitor resource usage anomalies** (e.g., high CPU/GPU load) and implement policy controls to detect and prevent unauthorized cryptocurrency mining or resource abuse.
- **Apply restrictions on user-initiated system shutdown/reboot permissions** and monitor for unauthorised commands that may disrupt availability.

Contributors

ENSIGN ATHENA THREAT INTELLIGENCE ANALYSIS TEAM

Performs threat research and analysis for predictive measures to detect advanced cyber threats, to safeguard critical assets of enterprises and the public sector. We adopt a threat-informed defence approach and apply all-source intelligence to improve our clients' prioritisation of risks and defensive actions.

ENSIGN SECURITY OPERATIONS CENTRES (ENSOCS)

Are located across APAC, in Singapore, Malaysia, and Hong Kong. We offer advanced detection and response services, round-the-clock, to detect and mitigate threats in all environments of on-premise IT, Cloud, OT, and IoT.

ENSIGN LABS

Generates insights from analysing proprietary large volume datasets relating to telemetry in the region, coupled with vulnerability intelligence and tradecraft, to support discovery of Early Warning Indicators (EWIs).v

ENSIGN HUNT AND INCIDENT RESPONSE OPERATIONS (HIRO) TEAM

Performs threat hunting, and digital forensics and incident response (DFIR). Our operations are supported by threat intelligence and leverage our proprietary DFIR and continuous threat hunting platforms, ARTEMIS and APOLLO, to accelerate the investigation-to-decision cycle to help our clients minimise the business impact of incidents.

ENSIGN EXECUTIVE ADVISORS

Perform threat profiling for organisations, sectors, and nations to uncover strategic planning considerations, detections, and mitigations to address "meet the threat" objectives using the threat-informed defence approach. Applying a multi-disciplinary approach, they inform and support Leaders and Management in understanding the changes in the threat landscape and how they affect their business activities.

KEY CONTRIBUTORS

Non-exhaustive list, alphabetical order

- Au N.
- Bach H.
- Basedow A.
- Burger S.
- Kumaradasa W.
- Lee J.
- Li J.
- Lim J.
- Lim L.
- Mok J.
- Nugraputra A.
- Rahumatulla S.
- Seah M.
- Sim WC.
- Tan AT.
- Tanadi J.
- Teo XZ.
- Yunus M.

APPENDIX A

Techniques Heatmaps by Territory

Techniques heatmap for Singapore

Link to MITRE ATT&CK Navigator JSON File: - https://ensign.global/SG

SHA256 File Hash: 16266f2faebd154bd69efa603ed3f24b4b926b591f95bdb93159cbb1ca7cebc7

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1566: Phishing	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1078: Valid Accounts	T1070: Indicator Removal	T1003: OS Credential Dumping	T1087: Account Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1590: Gather Victim Network Information	T1588: Obtain Capabilities	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1027: Obfuscated Files or Information	T1555: Credentials from Password Stores	T1069: Permission Groups Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1090: Proxy	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1589: Gather Victim Identity Information	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1204: User Execution	T1546: Event Triggered Execution	T1546: Event Triggered Execution	T1562: Impair Defenses	T1110: Brute Force	T1082: System Information Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1573: Encrypted Channel	T1041: Exfiltration Over C2 Channel	T1490: Inhibit System Recovery
T1596: Search Open Technical Databases	T1584: Compromise Infrastructure	T1133: External Remote Services	T1569: System Services	T1098: Account Manipulation	T1098: Account Manipulation	T1036: Masquerading	T1056: Input Capture	T1018: Remote System Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1001: Data Obfuscation	T1011: Exfiltration Over Other Network Medium	T1499: Endpoint Denial of Service
T1593: Search Open Websites/Domains	T1586: Compromise Accounts	T1195: Supply Chain Compromise	T1047: Windows Management Instrumentation	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1218: System Binary Proxy Execution	T1552: Unsecured Credentials	T1016: System Network Configuration Discovery	T1072: Software Deployment Tools	T1213: Data from Information Repositories	T1219: Remote Access Tools	T1052: Exfiltration Over Physical Medium	T1657: Financial Theft
T1591: Gather Victim Org Information	T1585: Establish Accounts	T1199: Trusted Relationship	T1203: Exploitation for Client Execution	T1133: External Remote Services	T1574: Hijack Execution Flow	T1078: Valid Accounts	T1606: Forge Web Credentials	T1083: File and Directory Discovery	T1091: Replication Through Removable Media	T1119: Automated Collection	T1102: Web Service	T1030: Data Transfer Size Limits	T1489: Service Stop
T1598: Phishing for Information	T1608: Stage Capabilities	T1189: Drive-by Compromise	T1072: Software Deployment Tools	T1574: Hijack Execution Flow	T1548: Abuse Elevation Control Mechanism	T1553: Subvert Trust Controls	T1556: Modify Authentication Process	T1497: Virtualization/Sandbox Evasion		T1602: Data from Configuration Repository	T1105: Ingress Tool Transfer	T1537: Transfer Data to Cloud Account	T1485: Data Destruction
T1594: Search Victim-Owned Websites	T1650: Acquire Access	T1091: Replication Through Removable Media	T1651: Cloud Administration Command	T1505: Server Software Component	T1484: Domain or Tenant Policy Modification	T1574: Hijack Execution Flow	T1558: Steal or Forge Kerberos Tickets	T1057: Process Discovery		T1114: Email Collection	T1095: Non-Application Layer Protocol		T1498: Network Denial of Service
T1592: Gather Victim Host Information			T1129: Shared Modules	T1136: Create Account	T1055: Process Injection	T1480: Execution Guardrails	T1212: Exploitation for Credential Access	T1614: System Location Discovery		T1113: Screen Capture	T1568: Dynamic Resolution		T1561: Disk Wipe
				T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1497: Virtualization/Sandbox Evasion	T1621: Multi-Factor Authentication Request Generation	T1049: System Network Connections Discovery		T1123: Audio Capture	T1665: Hide Infrastructure		T1496: Resource Hijacking
				T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1548: Abuse Elevation Control Mechanism	T1040: Network Sniffing	T1046: Network Service Discovery			T1572: Protocol Tunneling		
				T1112: Modify Registry	T1068: Exploitation for Privilege Escalation	T1484: Domain or Tenant Policy Modification	T1528: Steal Application Access Token	T1010: Application Window Discovery			T1008: Fallback Channels		
				T1556: Modify Authentication Process	T1134: Access Token Manipulation	T1055: Process Injection	T1649: Steal or Forge Authentication Certificates	T1482: Domain Trust Discovery			T1104: Multi-Stage Channels		
				T1542: Pre-OS Boot		T1550: Use Alternate Authentication Material	T1539: Steal Web Session Cookie	T1518: Software Discovery			T1571: Non-Standard Port		
				T1197: BITS Jobs		T1140: Deobfuscate/Decode Files or Information		T1135: Network Share Discovery					
				T1653: Power Settings		T1564: Hide Artifacts		T1120: Peripheral Device Discovery					
						T1112: Modify Registry		T1012: Query Registry					
						T1222: File and Directory Permissions Modification		T1033: System Owner/User Discovery					
						T1556: Modify Authentication Process		T1007: System Service Discovery					
						T1542: Pre-OS Boot		T1217: Browser Information Discovery					
						T1014: Rootkit		T1654: Log Enumeration					
						T1134: Access Token Manipulation		T1040: Network Sniffing					
						T1197: BITS Jobs		T1124: System Time Discovery					
						T1006: Direct Volume Access		T1673: Virtual Machine Discovery					
						T1211: Exploitation for Defense Evasion							
						T1656: Impersonation							
						T1599: Network Boundary Bridging							

MITRE ATT&CK v17

Legend: *Increasing levels of observations*

Techniques heatmap for Malaysia

Link to MITRE ATT&CK Navigator JSON File: - [*https://ensign.global/MY*](https://ensign.global/MY)

SHA256 File Hash: 916a9ff2df9368e57f662f1ef8031876eb84202a567d6f3e45948b1639d70358

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595: Active Scanning	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1003: OS Credential Dumping	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1491: Defacement
T1590: Gather Victim Network Information	T1583: Acquire Infrastructure	T1190: Exploit Public-Facing Application	T1053: Scheduled Task/Job	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1027: Obfuscated Files or Information	T1110: Brute Force	T1614: System Location Discovery	T1570: Lateral Tool Transfer	T1056: Input Capture	T1573: Encrypted Channel	T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1596: Search Open Technical Databases	T1587: Develop Capabilities	T1133: External Remote Services	T1569: System Services	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1562: Impair Defenses	T1555: Credentials from Password Stores	T1497: Virtualization/Sandbox Evasion	T1550: Use Alternate Authentication Material	T1005: Data from Local System	T1102: Web Service	T1041: Exfiltration Over C2 Channel	T1499: Endpoint Denial of Service
T1593: Search Open Websites/Domains	T1586: Compromise Accounts	T1195: Supply Chain Compromise	T1204: User Execution	T1098: Account Manipulation	T1098: Account Manipulation	T1480: Execution Guardrails	T1056: Input Capture	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1602: Data from Configuration Repository	T1095: Non-Application Layer Protocol	T1030: Data Transfer Size Limits	T1498: Network Denial of Service
T1598: Phishing for Information		T1199: Trusted Relationship	T1203: Exploitation for Client Execution	T1546: Event Triggered Execution	T1484: Domain or Tenant Policy Modification	T1574: Hijack Execution Flow	T1040: Network Sniffing	T1083: File and Directory Discovery	T1072: Software Deployment Tools	T1213: Data from Information Repositories	T1090: Proxy		T1489: Service Stop
T1594: Search Victim-Owned Websites		T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1133: External Remote Services	T1546: Event Triggered Execution	T1484: Domain or Tenant Policy Modification		T1018: Remote System Discovery		T1074: Data Staged	T1219: Remote Access Tools		T1490: Inhibit System Recovery
		T1189: Drive-by Compromise	T1129: Shared Modules	T1505: Server Software Component	T1548: Abuse Elevation Control Mechanism	T1553: Subvert Trust Controls		T1046: Network Service Discovery		T1113: Screen Capture	T1001: Data Obfuscation		T1485: Data Destruction
			T1072: Software Deployment Tools	T1136: Create Account	T1055: Process Injection	T1497: Virtualization/Sandbox Evasion		T1135: Network Share Discovery		T1123: Audio Capture	T1568: Dynamic Resolution		T1657: Financial Theft
				T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1548: Abuse Elevation Control Mechanism		T1057: Process Discovery		T1119: Automated Collection	T1105: Ingress Tool Transfer		T1496: Resource Hijacking
				T1112: Modify Registry	T1078: Valid Accounts	T1140: Deobfuscate/Decode Files or Information		T1012: Query Registry			T1104: Multi-Stage Channels		T1529: System Shutdown/Reboot
				T1542: Pre-OS Boot	T1134: Access Token Manipulation	T1036: Masquerading		T1049: System Network Connections Discovery			T1572: Protocol Tunneling		
				T1078: Valid Accounts	T1037: Boot or Logon Initialization Scripts	T1055: Process Injection		T1010: Application Window Discovery			T1132: Data Encoding		
				T1197: BITS Jobs	T1068: Exploitation for Privilege Escalation	T1218: System Binary Proxy Execution		T1040: Network Sniffing			T1008: Fallback Channels		
				T1037: Boot or Logon Initialization Scripts		T1112: Modify Registry		T1069: Permission Groups Discovery			T1665: Hide Infrastructure		
						T1542: Pre-OS Boot		T1518: Software Discovery					
						T1014: Rootkit		T1016: System Network Configuration Discovery					
						T1550: Use Alternate Authentication Material		T1033: System Owner/User Discovery					
						T1078: Valid Accounts		T1007: System Service Discovery					
						T1134: Access Token Manipulation		T1673: Virtual Machine Discovery					
						T1197: BITS Jobs							
						T1656: Impersonation							
						T1599: Network Boundary Bridging							
						T1221: Template Injection							

MITRE ATT&CK v17

Legend: *Increasing levels of observations*

Techniques heatmap for Indonesia

Link to MITRE ATT&CK Navigator JSON File: - https://ensign.global/ID

SHA256 File Hash: 62a0f8adfee301eb3cdc946b106d201c367c01e81f604dcfeac02e5aac5097fd

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1070: Indicator Removal	T1555: Credentials from Password Stores	T1083: File and Directory Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1590: Gather Victim Network Information	T1588: Obtain Capabilities	T1566: Phishing	T1053: Scheduled Task/Job	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1027: Obfuscated Files or Information	T1003: OS Credential Dumping	T1082: System Information Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1219: Remote Access Tools	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1593: Search Open Websites/Domains	T1586: Compromise Accounts	T1133: External Remote Services	T1569: System Services	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1562: Impair Defenses	T1110: Brute Force	T1087: Account Discovery	T1550: Use Alternate Authentication Material	T1056: Input Capture	T1102: Web Service	T1041: Exfiltration Over C2 Channel	T1489: Service Stop
T1596: Search Open Technical Databases	T1587: Develop Capabilities	T1078: Valid Accounts	T1203: Exploitation for Client Execution	T1133: External Remote Services	T1078: Valid Accounts	T1574: Hijack Execution Flow	T1056: Input Capture	T1057: Process Discovery	T1210: Exploitation of Remote Services	T1213: Data from Information Repositories	T1001: Data Obfuscation	T1030: Data Transfer Size Limits	T1657: Financial Theft
T1594: Search Victim-Owned Websites	T1650: Acquire Access	T1199: Trusted Relationship	T1072: Software Deployment Tools	T1078: Valid Accounts	T1098: Account Manipulation	T1480: Execution Guardrails	T1040: Network Sniffing	T1018: Remote System Discovery	T1072: Software Deployment Tools	T1602: Data from Configuration Repository	T1573: Encrypted Channel		T1490: Inhibit System Recovery
T1592: Gather Victim Host Information		T1659: Content Injection	T1204: User Execution	T1098: Account Manipulation	T1543: Create or Modify System Process	T1078: Valid Accounts	T1557: Adversary-in-the-Middle	T1614: System Location Discovery		T1074: Data Staged	T1090: Proxy		T1485: Data Destruction
T1598: Phishing for Information		T1195: Supply Chain Compromise	T1047: Windows Management Instrumentation	T1543: Create or Modify System Process	T1484: Domain or Tenant Policy Modification	T1140: Deobfuscate/Decode Files or Information	T1528: Steal Application Access Token	T1049: System Network Connections Discovery		T1113: Screen Capture	T1105: Ingress Tool Transfer		T1496: Resource Hijacking
T1597: Search Closed Sources		T1189: Drive-by Compromise	T1674: Input Injection	T1546: Event Triggered Execution	T1546: Event Triggered Execution	T1484: Domain or Tenant Policy Modification	T1539: Steal Web Session Cookie	T1497: Virtualization/Sandbox Evasion		T1557: Adversary-in-the-Middle	T1659: Content Injection		T1529: System Shutdown/Reboot
			T1106: Native API	T1112: Modify Registry	T1055: Process Injection	T1112: Modify Registry	T1552: Unsecured Credentials	T1135: Network Share Discovery		T1123: Audio Capture	T1568: Dynamic Resolution		
			T1129: Shared Modules	T1505: Server Software Component	T1068: Exploitation for Privilege Escalation	T1497: Virtualization/Sandbox Evasion		T1007: System Service Discovery		T1119: Automated Collection	T1104: Multi-Stage Channels		
				T1136: Create Account	T1548: Abuse Elevation Control Mechanism	T1036: Masquerading		T1010: Application Window Discovery			T1095: Non-Application Layer Protocol		
				T1542: Pre-OS Boot	T1134: Access Token Manipulation	T1055: Process Injection		T1046: Network Service Discovery			T1572: Protocol Tunneling		
				T1197: BITS Jobs	T1037: Boot or Logon Initialization Scripts	T1218: System Binary Proxy Execution		T1040: Network Sniffing			T1132: Data Encoding		
				T1037: Boot or Logon Initialization Scripts		T1550: Use Alternate Authentication Material		T1012: Query Registry			T1008: Fallback Channels		
				T1653: Power Settings		T1542: Pre-OS Boot		T1016: System Network Configuration Discovery					
						T1553: Subvert Trust Controls		T1482: Domain Trust Discovery					
						T1548: Abuse Elevation Control Mechanism		T1120: Peripheral Device Discovery					
						T1134: Access Token Manipulation		T1069: Permission Groups Discovery					
						T1197: BITS Jobs		T1518: Software Discovery					
						T1656: Impersonation		T1033: System Owner/User Discovery					
						T1599: Network Boundary Bridging		T1673: Virtual Machine Discovery					
						T1014: Rootkit							
						T1221: Template Injection							

MITRE ATT&CK v17

Legend:  *Increasing levels of observations*

Techniques heatmap for South Korea

Link to MITRE ATT&CK Navigator JSON File: - https://ensign.global/SK

SHA256 File Hash: cdcc56af7983e957353025e037b33f5e3921f71d3beb5a2063731e5e13eebdca

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1027: Obfuscated Files or Information	T1555: Credentials from Password Stores	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1561: Disk Wipe
T1598: Phishing for Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1574: Hijack Execution Flow	T1055: Process Injection	T1070: Indicator Removal	T1003: OS Credential Dumping	T1087: Account Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1102: Web Service	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1593: Search Open Websites/Domains	T1587: Develop Capabilities	T1189: Drive-by Compromise	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1574: Hijack Execution Flow	T1036: Masquerading	T1557: Adversary-in-the-Middle	T1083: File and Directory Discovery	T1534: Internal Spearphishing	T1557: Adversary-in-the-Middle	T1090: Proxy	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1591: Gather Victim Org Information	T1584: Compromise Infrastructure	T1190: Exploit Public-Facing Application	T1559: Inter-Process Communication	T1543: Create or Modify System Process	T1053: Scheduled Task/Job	T1562: Impair Defenses	T1110: Brute Force	T1057: Process Discovery	T1210: Exploitation of Remote Services	T1005: Data from Local System	T1132: Data Encoding	T1030: Data Transfer Size Limits	T1489: Service Stop
T1595: Active Scanning	T1585: Establish Accounts	T1133: External Remote Services	T1203: Exploitation for Client Execution	T1505: Server Software Component	T1543: Create or Modify System Process	T1055: Process Injection	T1056: Input Capture	T1518: Software Discovery	T1091: Replication Through Removable Media	T1056: Input Capture	T1001: Data Obfuscation		T1529: System Shutdown/Reboot
T1596: Search Open Technical Databases	T1608: Stage Capabilities	T1199: Trusted Relationship	T1106: Native API	T1078: Valid Accounts	T1078: Valid Accounts	T1218: System Binary Proxy Execution	T1040: Network Sniffing	T1614: System Location Discovery	T1072: Software Deployment Tools	T1114: Email Collection	T1573: Encrypted Channel		T1486: Data Encrypted for Impact
T1594: Search Victim-Owned Websites	T1586: Compromise Accounts	T1091: Replication Through Removable Media	T1569: System Services	T1542: Pre-OS Boot	T1548: Abuse Elevation Control Mechanism	T1574: Hijack Execution Flow	T1111: Multi-Factor Authentication Interception	T1016: System Network Configuration Discovery		T1213: Data from Information Repositories	T1105: Ingress Tool Transfer		T1657: Financial Theft
	T1650: Acquire Access	T1195: Supply Chain Compromise	T1072: Software Deployment Tools	T1098: Account Manipulation	T1134: Access Token Manipulation	T1564: Hide Artifacts	T1528: Steal Application Access Token	T1497: Virtualization/Sandbox Evasion		T1119: Automated Collection	T1219: Remote Access Tools		T1490: Inhibit System Recovery
		T1669: Wi-Fi Networks	T1047: Windows Management Instrumentation	T1546: Event Triggered Execution	T1098: Account Manipulation	T1553: Subvert Trust Controls	T1539: Steal Web Session Cookie	T1120: Peripheral Device Discovery		T1113: Screen Capture	T1092: Communication Through Removable Media		T1498: Network Denial of Service
				T1133: External Remote Services	T1546: Event Triggered Execution	T1078: Valid Accounts	T1552: Unsecured Credentials	T1033: System Owner/User Discovery		T1123: Audio Capture	T1008: Fallback Channels		
				T1112: Modify Registry	T1037: Boot or Logon Initialization Scripts	T1548: Abuse Elevation Control Mechanism		T1046: Network Service Discovery		T1185: Browser Session Hijacking	T1104: Multi-Stage Channels		
				T1037: Boot or Logon Initialization Scripts	T1484: Domain or Tenant Policy Modification	T1134: Access Token Manipulation		T1040: Network Sniffing		T1039: Data from Network Shared Drive	T1095: Non-Application Layer Protocol		
				T1137: Office Application Startup	T1068: Exploitation for Privilege Escalation	T1542: Pre-OS Boot		T1012: Query Registry		T1025: Data from Removable Media	T1571: Non-Standard Port		
				T1197: BITS Jobs		T1550: Use Alternate Authentication Material		T1049: System Network Connections Discovery			T1572: Protocol Tunneling		
				T1136: Create Account		T1497: Virtualization/Sandbox Evasion		T1010: Application Window Discovery			T1205: Traffic Signaling		
				T1176: Software Extensions		T1140: Deobfuscate/Decode Files or Information		T1622: Debugger Evasion					
				T1205: Traffic Signaling		T1112: Modify Registry		T1007: System Service Discovery					
						T1484: Domain or Tenant Policy Modification		T1124: System Time Discovery					
						T1480: Execution Guardrails							
						T1656: Impersonation							
						T1620: Reflective Code Loading							
						T1221: Template Injection							
						T1197: BITS Jobs							
						T1622: Debugger Evasion							
						T1006: Direct Volume Access							
						T1211: Exploitation for Defense Evasion							
						T1202: Indirect Command Execution							
						T1014: Rootkit							
						T1205: Traffic Signaling							
						T1220: XSL Script Processing							

MITRE ATT&CK v17

Legend: *Increasing levels of observations*

Techniques heatmap for Australia

Link to MITRE ATT&CK Navigator JSON File: - https://ensign.global/AU

SHA256 File Hash: 73823108702a2b8a80f7834a173ece9eeaf24662a6cc3ae01dd745adfccc529a

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1078: Valid Accounts	T1027: Obfuscated Files or Information	T1003: OS Credential Dumping	T1497: Virtualization/Sandbox Evasion	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1593: Search Open Websites/Domains	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1555: Credentials from Password Stores	T1087: Account Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1090: Proxy	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1595: Active Scanning	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1562: Impair Defenses	T1056: Input Capture	T1069: Permission Groups Discovery	T1570: Lateral Tool Transfer	T1056: Input Capture	T1573: Encrypted Channel	T1041: Exfiltration Over C2 Channel	T1561: Disk Wipe
T1591: Gather Victim Org Information	T1584: Compromise Infrastructure	T1133: External Remote Services	T1569: System Services	T1505: Server Software Component	T1546: Event Triggered Execution	T1036: Masquerading	T1110: Brute Force	T1082: System Information Discovery	T1210: Exploitation of Remote Services	T1005: Data from Local System	T1102: Web Service	T1011: Exfiltration Over Other Network Medium	T1490: Inhibit System Recovery
T1596: Search Open Technical Databases	T1608: Stage Capabilities	T1195: Supply Chain Compromise	T1047: Windows Management Instrumentation	T1546: Event Triggered Execution	T1574: Hijack Execution Flow	T1553: Subvert Trust Controls	T1558: Steal or Forge Kerberos Tickets	T1614: System Location Discovery	T1534: Internal Spearphishing	T1213: Data from Information Repositories	T1001: Data Obfuscation	T1030: Data Transfer Size Limits	T1489: Service Stop
T1590: Gather Victim Network Information	T1585: Establish Accounts	T1199: Trusted Relationship	T1203: Exploitation for Client Execution	T1574: Hijack Execution Flow	T1098: Account Manipulation	T1218: System Binary Proxy Execution	T1552: Unsecured Credentials	T1083: File and Directory Discovery	T1091: Replication Through Removable Media	T1557: Adversary-in-the-Middle	T1105: Ingress Tool Transfer	T1537: Transfer Data to Cloud Account	T1485: Data Destruction
T1594: Search Victim-Owned Websites	T1586: Compromise Accounts	T1189: Drive-by Compromise	T1559: Inter-Process Communication	T1098: Account Manipulation	T1055: Process Injection	T1497: Virtualization/Sandbox Evasion	T1557: Adversary-in-the-Middle	T1018: Remote System Discovery	T1072: Software Deployment Tools	T1113: Screen Capture	T1568: Dynamic Resolution		T1499: Endpoint Denial of Service
T1592: Gather Victim Host Information	T1650: Acquire Access	T1091: Replication Through Removable Media	T1106: Native API	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1078: Valid Accounts	T1606: Forge Web Credentials	T1016: System Network Configuration Discovery		T1114: Email Collection	T1219: Remote Access Tools		T1657: Financial Theft
			T1651: Cloud Administration Command	T1136: Create Account	T1548: Abuse Elevation Control Mechanism	T1574: Hijack Execution Flow	T1556: Modify Authentication Process	T1057: Process Discovery		T1123: Audio Capture	T1095: Non-Application Layer Protocol		T1498: Network Denial of Service
			T1674: Input Injection	T1133: External Remote Services	T1484: Domain or Tenant Policy Modification	T1055: Process Injection	T1621: Multi-Factor Authentication Request Generation	T1046: Network Service Discovery		T1119: Automated Collection	T1132: Data Encoding		T1496: Resource Hijacking
			T1129: Shared Modules	T1542: Pre-OS Boot	T1134: Access Token Manipulation	T1140: Deobfuscate/Decode Files or Information	T1528: Steal Application Access Token	T1049: System Network Connections Discovery		T1125: Video Capture	T1008: Fallback Channels		T1529: System Shutdown/Reboot
			T1072: Software Deployment Tools	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1548: Abuse Elevation Control Mechanism	T1649: Steal or Forge Authentication Certificates	T1033: System Owner/User Discovery			T1571: Non-Standard Port		
				T1112: Modify Registry	T1068: Exploitation for Privilege Escalation	T1484: Domain or Tenant Policy Modification	T1539: Steal Web Session Cookie	T1010: Application Window Discovery			T1665: Hide Infrastructure		
				T1556: Modify Authentication Process		T1480: Execution Guardrails		T1135: Network Share Discovery			T1104: Multi-Stage Channels		
				T1197: BITS Jobs		T1550: Use Alternate Authentication Material		T1012: Query Registry			T1572: Protocol Tunneling		
						T1564: Hide Artifacts		T1518: Software Discovery					
						T1542: Pre-OS Boot		T1482: Domain Trust Discovery					
						T1134: Access Token Manipulation		T1120: Peripheral Device Discovery					
						T1112: Modify Registry		T1124: System Time Discovery					
						T1222: File and Directory Permissions Modification		T1217: Browser Information Discovery					
						T1656: Impersonation		T1622: Debugger Evasion					
						T1556: Modify Authentication Process		T1654: Log Enumeration					
						T1014: Rootkit		T1007: System Service Discovery					
						T1197: BITS Jobs		T1673: Virtual Machine Discovery					
						T1622: Debugger Evasion							
						T1006: Direct Volume Access							
						T1211: Exploitation for Defense Evasion							
						T1202: Indirect Command Execution							
						T1599: Network Boundary Bridging							
						T1620: Reflective Code Loading							
						T1221: Template Injection							
						T1220: XSL Script Processing							

MITRE ATT&CK v17

Legend: *Increasing levels of observations*

Techniques heatmap for Greater China Region

Link to MITRE ATT&CK Navigator JSON File: - [*https://ensign.global/GCR*](https://ensign.global/GCR)

SHA256 File Hash: 6ab48c61c2d2f12e2a5b12ab8319d13b2c4c0e11ccd5c4eea2b3c6a56af839b7

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1598: Phishing for Information	T1583: Acquire Infrastructure	T1566: Phishing	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1027: Obfuscated Files or Information	T1056: Input Capture	T1082: System Information Discovery	T1021: Remote Services	T1056: Input Capture	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1189: Drive-by Compromise	T1204: User Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1036: Masquerading	T1003: OS Credential Dumping	T1518: Software Discovery	T1072: Software Deployment Tools	T1560: Archive Collected Data	T1102: Web Service	T1567: Exfiltration Over Web Service	T1561: Disk Wipe
T1591: Gather Victim Org Information	T1608: Stage Capabilities	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1070: Indicator Removal	T1555: Credentials from Password Stores	T1083: File and Directory Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1132: Data Encoding	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1593: Search Open Websites/Domains	T1584: Compromise Infrastructure	T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1218: System Binary Proxy Execution	T1557: Adversary-in-the-Middle	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle	T1573: Encrypted Channel	T1020: Automated Exfiltration	T1486: Data Encrypted for Impact
T1595: Active Scanning	T1587: Develop Capabilities	T1133: External Remote Services	T1559: Inter-Process Communication	T1112: Modify Registry	T1548: Abuse Elevation Control Mechanism	T1574: Hijack Execution Flow	T1110: Brute Force	T1016: System Network Configuration Discovery	T1570: Lateral Tool Transfer	T1119: Automated Collection	T1105: Ingress Tool Transfer	T1052: Exfiltration Over Physical Medium	T1490: Inhibit System Recovery
	T1585: Establish Accounts	T1091: Replication Through Removable Media	T1569: System Services	T1546: Event Triggered Execution	T1055: Process Injection	T1562: Impair Defenses	T1552: Unsecured Credentials	T1497: Virtualization/Sandbox Evasion	T1091: Replication Through Removable Media	T1005: Data from Local System	T1090: Proxy	T1030: Data Transfer Size Limits	T1489: Service Stop
	T1650: Acquire Access	T1195: Supply Chain Compromise	T1072: Software Deployment Tools	T1078: Valid Accounts	T1546: Event Triggered Execution	T1548: Abuse Elevation Control Mechanism	T1040: Network Sniffing	T1049: System Network Connections Discovery	T1534: Internal Spearphishing	T1113: Screen Capture	T1001: Data Obfuscation		T1657: Financial Theft
		T1199: Trusted Relationship	T1047: Windows Management Instrumentation	T1505: Server Software Component	T1078: Valid Accounts	T1055: Process Injection		T1033: System Owner/User Discovery	T1563: Remote Service Session Hijacking	T1123: Audio Capture	T1095: Non-Application Layer Protocol		T1498: Network Denial of Service
			T1106: Native API	T1098: Account Manipulation	T1134: Access Token Manipulation	T1497: Virtualization/Sandbox Evasion		T1057: Process Discovery	T1080: Taint Shared Content	T1115: Clipboard Data	T1571: Non-Standard Port		T1529: System Shutdown/Reboot
			T1610: Deploy Container	T1542: Pre-OS Boot	T1098: Account Manipulation	T1564: Hide Artifacts		T1124: System Time Discovery		T1602: Data from Configuration Repository	T1219: Remote Access Tools		
			T1129: Shared Modules	T1133: External Remote Services	T1484: Domain or Tenant Policy Modification	T1112: Modify Registry		T1046: Network Service Discovery		T1213: Data from Information Repositories	T1572: Protocol Tunneling		
				T1197: BITS Jobs	T1068: Exploitation for Privilege Escalation	T1553: Subvert Trust Controls		T1012: Query Registry		T1025: Data from Removable Media	T1568: Dynamic Resolution		
				T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1078: Valid Accounts		T1614: System Location Discovery		T1125: Video Capture	T1008: Fallback Channels		
				T1137: Office Application Startup		T1140: Deobfuscate/Decode Files or Information		T1018: Remote System Discovery			T1665: Hide Infrastructure		
				T1653: Power Settings		T1550: Use Alternate Authentication Material		T1007: System Service Discovery			T1104: Multi-Stage Channels		
				T1205: Traffic Signaling		T1134: Access Token Manipulation		T1010: Application Window Discovery			T1205: Traffic Signaling		
						T1542: Pre-OS Boot		T1482: Domain Trust Discovery					
						T1484: Domain or Tenant Policy Modification		T1622: Debugger Evasion					
						T1480: Execution Guardrails		T1135: Network Share Discovery					
						T1222: File and Directory Permissions Modification		T1040: Network Sniffing					
						T1202: Indirect Command Execution		T1120: Peripheral Device Discovery					
						T1216: System Script Proxy Execution							
						T1221: Template Injection							
						T1197: BITS Jobs							
						T1622: Debugger Evasion							
						T1610: Deploy Container							
						T1656: Impersonation							
						T1620: Reflective Code Loading							
						T1205: Traffic Signaling							
						T1220: XSL Script Processing							

MITRE ATT&CK v17

Legend: *Increasing levels of observations*

APPENDIX B

Territorial Observed Top Exploited Vulnerabilities

Overview of Territorial Insights

NOTABLE CVES ACROSS RELEVANT TERRITORIES (1/2)

				VICTIM TERRITORY					
CVE Identifier	**Affected System (s)**	**CVSS**	**EPSS**	**SG**	**MY**	**ID**	**SK**	**AU**	**GCR**
CVE-2024-21887	Ivanti Connect Secure and Policy Secure - Web component	9.1	0.94416	●		●			
CVE-2017-11882	Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016	7.8	0.94384				●		●
CVE-2024-24919	Check Point Security Gateways	8.6	0.94327		●	●		●	
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons for ZTA - SAML component	8.2	0.9432	●		●			
CVE-2024-1709	ConnectWise ScreenConnect	10	0.9431				●		
CVE-2024-21412	Microsoft Defender SmartScreen	8.1	0.93777	●					●
CVE-2023-23397	Microsoft Outlook	9.8	0.93547				●		
CVE-2022-42475	FortiOS SSL-VPN and FortiProxy SSL-VPN	9.8	0.93196	●				●	
CVE-2023-20273	Cisco IOS XE Software - Web UI feature	7.2	0.92717	●	●	●			
CVE-2019-9621	Zimbra Collaboration Suite	7.5	0.91807	●	●				
CVE-2024-21762	Fortinet FortiOS	9.8	0.91602	●				●	
CVE-2024-23108	Fortinet FortiSIEM	9.8	0.88633	●				●	
CVE-2024-21338	Certain IOCTL of “appid.sys” known as AppLocker‘s driver	7.8	0.80512				●	●	●
CVE-2017-5070	V8 in Google Chrome	8.8	0.803						●
CVE-2024-38193	Windows Ancillary Function Driver	7.8	0.73164				●	●	●
CVE-2023-28252	Windows Common Log File System	7.8	0.52956			●			

Note: This is a non-exhaustive list. EPSS is accurate as of June 2025.

Overview of Territorial Insights

NOTABLE CVES ACROSS RELEVANT TERRITORIES (2/2)

				VICTIM TERRITORY					
CVE Identifier	Affected System (s)	CVSS	EPSS	SG	MY	ID	SK	AU	GCR
CVE-2024-1708	ConnectWise ScreenConnect	8.4	0.49314				●		
CVE-2024-30051	Windows DWM Core Library	7.8	0.48997				●	●	
CVE-2024-23113	Fortinet FortiOS, FortiProxy, FortiPAM, FortiSwitchManager	9.8	0.45024					●	
CVE-2024-7262	Kingsoft WPS Office version on Windows	7.8	0.25173						●
CVE-2024-38178	Microsoft Windows systems	7.5	0.1704				●		
CVE-2024-39717	Versa Director GUI	7.2	0.05514	●				●	
CVE-2024-23109	Fortinet FortiSIEM	9.8	0.04986	●				●	
CVE-2021-30869	iOS and macOS	7.8	0.04229						●
CVE-2024-5274	V8 in Google Chrome	9.6	0.01792				●	●	●
CVE-2024-38106	Windows NT Operating System Kernel Executable	7	0.00403				●	●	●
CVE-2024-4947	V8 in Google Chrome	9.6	0.00354				●	●	●
CVE-2024-7971	V8 in Google Chrome	9.6	0.00351				●	●	●
CVE-2024-3400	Palo Alto Networks PAN-OS Global Protect Feature	10	0.0035	●	●	●			
CVE-2024-7263	Kingsoft WPS Office version on Windows	7.8	0.00052						●
CVE-2024-4577	Apache and PHP-CGI on Windows	9.8	0.0005						●
CVE-2023-20198	Cisco IOS XE Software - Web UI feature	10	0.00014	●	●	●			
CVE-2024-50570	FortiClientWindows and FortiClientLinux	5	0.00007		●	●		●	

Note: This is a non-exhaustive list. EPSS is accurate as of June 2025.

APPENDIX C

ICS oriented Techniques Heatmaps

ICS-oriented Techniques Heatmap – ICS Matrix

Link to MITRE ATT&CK Navigator JSON File: - [*https://ensign.global/IcsTech*](https://ensign.global/IcsTech)

SHA256 File Hash: b7732aff849cf91090d16ad0110f03e6cb2304db26d68108121d3fc440285928

TA0108: Initial Access	TA0104: Execution	TA0110: Persistence	TA0111: Privilege Escalation	TA0103: Evasion	TA0102: Discovery	TA0109: Lateral Movement	TA0100: Collection	TA0101: Command and Control	TA0107: Inhibit Response Function	TA0106: Impair Process Control	TA0105: Impact
T0819: Exploit Public-Facing Application	T0807: Command-Line Interface					T0886: Remote Services		T0885: Commonly Used Port		T0836: Modify Parameter	T0813: Denial of Control
T0883: Internet Accessible Device								T0869: Standard Application Layer Protocol		T0855: Unauthorized Command Message	T0826: Loss of Availability
T0886: Remote Services											T0827: Loss of Control
											T0828: Loss of Productivity and Revenue
											T0829: Loss of View
											T0831: Manipulation of Control
											T0832: Manipulation of View

MITRE ATT&CK v17

Legend:  *Increasing levels of observations*

ICS-oriented Techniques Heatmap – Enterprise Matrix

Link to MITRE ATT&CK Navigator JSON File: - [*https://ensign.global/IcsEnt*](https://ensign.global/IcsEnt)

SHA256 File Hash: 3d868f75fcba7fc716f7f69f6dfc8d2234779707a2e8626c84a89ba93ff2975b

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595: Active Scanning		T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1027: Obfuscated Files or Information	T1110: Brute Force			T1005: Data from Local System	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1491: Defacement
T1592: Gather Victim Host Information				T1078: Valid Accounts	T1078: Valid Accounts	T1078: Valid Accounts							
T1590: Gather Victim Network Information													
T1593: Search Open Websites/Domains													
T1594: Search Victim-Owned Websites													

MITRE ATT&CK v17

Legend: *Increasing levels of observations*