ENSIGN INFOSECURITY

CYBER THREAT LANDSCAPE REPORT 2024

Version 1.4 | 10 May 2024

EDITOR'S FOREWORD

Cybersecurity remains one of the most pressing challenges facing nations, organisations, and even individuals. Ensign InfoSecurity is dedicated to supporting the cybersecurity needs of a wide variety of clients. We publish this report to share our unique insights and perspectives into threats, trends, and topics with business leaders and cybersecurity professionals.

As Ensign continues to grow our operational presence overseas, this year's report features coverage of **Singapore**, **Malaysia**, **Indonesia**, **South Korea**, and our recent expansions in **Australia** and the **Greater China Region** (Hong Kong S.A.R. and mainland China). We also bring our cybersecurity expertise, experience, and unique Asia-first lens on cybersecurity challenges to global platforms that we participate in, to help shape global discussions.

Geneva Dialogue UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH WORLD ECONOMIC FORUM MITRE ENGENUITY | Center for Threat Informed Defense

We believe in using a Threat-Informed Defence approach. Our Ensign Threat Classification Matrix for identified threat groups helps organisations to prioritise their cyber defences against the territory-contextualised threats. We provide the MITRE ATT&CK™ heatmaps to support organisations in prioritising their cyber defences against specific adversary techniques and follow-through defensive actions, such as threat hunting, Red Teaming, and tuning of detection rules. We have also laid out the observed top targeted industry groups and top exploited vulnerabilities.

With every case our incident response team handles, we learn a little more about how attackers operate. They are evolving to find gaps in our processes, in addition to pushing harder on the weaknesses in our systems and people. While we design, build, and operate a variety of protective systems for organisations, we also advise our clients that resilience, not just building higher defensive walls, should be the objective towards sustainable and predictable defence outcomes.

We are seeing first-hand how cybersecurity and the foundations of digital trust are being tested by the exploitation of Artificial Intelligence (AI) among threat actors. Our researchers are investigating how they use AI to accelerate malware and exploit development, or evade detection. AI is being extensively used in influence operations through Misinformation, Disinformation, and Malinformation (MDM), which distort reality, especially amidst a cyber crisis. We study these threats and trends to advise clients on how to deal with the risks of emerging technologies.

Our continued investment and contribution towards sharing our insights are aimed at enabling companies to better defend against the threats relevant to them. Companies cannot choose whether they become targets, but they can decide how they respond to a cyber-attack, and whether they can recover smoothly and with predictable outcomes.

About Ensign InfoSecurity

Ensign InfoSecurity is the largest comprehensive 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 our in-house cybersecurity research and development team. Ensign has 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.

ENSIGN INFOSECURITY

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Executive Summary

Cybersecurity continues to be a critical challenge faced by nations, organisations, and individuals. To effectively defend against cyber threats requires, business leaders and cyber professionals must remain informed about the latest threats, risks, and challenges. This year's report offers increased coverage, due to the expansion of our operational footprint, and deeper analysis attributed to the quality of our data and intelligence sources. These enhancements enable us to provide unique insights and observations for 2023, and forecasts for 2024.

Territorial Insights

In our analysis of the different territories Ensign operates in, we observed unique difference in each of them. The most targeted industry groups across our territories were Technology, Media and Telecommunications (TMT), Government, Manufacturing, and Financial Services. We continued to observe both state-sponsored threat groups and organised crime groups (notably those which exploit through deployment of Ransomware) in the region. Ransomware remains the dominant threat in nearly every territory we studied. Additionally, we observed a rise in hacktivism (malicious cyber activity motivated by a cause) associated with the spillover effects from the Israel-Hamas conflict, and the normalisation of such activities during the Russia-Ukraine conflict.

Top Hacktivist Groups

- Bjorka
- DragonForce Malaysia
- SynixCyberCrimMY
- GhostSec
- Muslim Cyber Army
- VulzSec
- Ganosec Team

Top Ransomware Groups

- ALPHV / BlackCat
- FIN11
- LockBit Gang

Top Commonly Used Solutions with Notable Vulnerabilities

- MOVEit Managed File Transfer (MFT) software
- Citrix NetScaler ADC and Gateway
- Confluence Server and Datacentre
- Zoho ManageEngine
- 3CX Desktop Application
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- PaperCut Application Server
- Veam Backup & Replication

Top Initial Access Brokers

- APT-C-01 (Poison Ivy)
- BITTER
- Scattered Spider
- UNC5221

Top Surveillance-oriented Groups

- Kimsuky
- Poison Carp

Escalating Threats

Our active involvement in international platforms like the United Nations (UN), World Economic Forum (WEF), and Geneva Dialogue, allows us to understand the spillover effects of geopolitics into the cyber domain. While malicious activity directly related to the Russia-Ukraine conflict may have dwindled, an uptick in Hamas-Israel hacktivism has filled the void. Additionally, tech bifurcation remains another geopolitically charged issue, complicating procurement decisions in the short term (especially as some countries implement bans on companies using software or hardware from other countries), and possibly worsening cybersecurity for all in the longer term.

We are seeing first-hand how cybersecurity and digital trust is being transformed by Artificial Intelligence (AI) — whether it is infused in our own tools, discovered in a weaponised form through our threat research, or through our expert policy development and advisory guidance to organisations. While Generative AI-driven scams and phishing emails troubled our systems in 2023, 2024 will see a spike in Misinformation, Disinformation, and Malinformation (MDM) amidst an election-filled year around the world. Reality can also be distorted by ruthless attackers, especially amidst a cyber crisis.

Evolving Attacks

With every case our incident response team handles, we learn a little more about how attackers operate. Attackers are exploiting weaknesses in our cyber processes to evade detection; instead of getting in through the “high severity” vulnerabilities that companies tend to patch quickly and monitor closely, they use “low” risk vulnerabilities that are de-prioritised for patching for weeks. Rather than bring in hefty payloads that might trigger detection rules, they have developed sophisticated “living off the land” techniques to stay below the radar.

Supply chain risks and sophisticated attacks also make it harder to defend every threat vector. Attackers are compromising critical nodes in common commercial network hardware, making defences even harder.

Companies cannot control whether they become targets, but they can prepare how to respond to cyber-attacks and take practical steps to recover smoothly with minimal damage.

Emerging Rules

In the ever-evolving landscape of cybersecurity, it is paramount for new regulations and policies to be aimed at enhancing data protection, fortifying the security of critical systems, and strengthening digital infrastructure. Many countries are introducing or enhancing cyber and data legislation (some with politicised motives).

While we design, build, and operate a variety of protective systems for organisations, we also advise our clients that resilience, not just building higher defensive walls, should be the objective beyond a certain point.

Conclusion

Whether you sit at the technical-operational layer, the executive layer, or the board oversight/governance layer, the challenges of navigating the complexities of cybersecurity are significant. In this regard, implementing new regulatory frameworks and policy initiatives will play an instrumental role in building our defences against cyber threats.

Hopefully, the insights and analysis in our report can help you make more informed decisions about what is best for your needs. Ensign stands ready to protect your organisation’s digital journey from the ever-expanding array of threats and risks.

2 TERRITORIAL INSIGHTS

Overview of Territorial Insights

Ensign's regional offices (Singapore, Malaysia, Indonesia, South Korea, and now Australia and the Greater China Region) are situated in locations within the Asia-Pacific region with high cyber activities, charged by geopolitical tensions (e.g. US-China tensions, South China Sea disagreements, and China-Taiwan tensions), and uneven (but generally growing) economies. Across these territories, Ensign continues to observe increased digitalisation efforts and the use of a wide range of hardware and software solutions, adding to the complexity in managing the cybersecurity risks in the digital attack surface.

Ransomware continues to be lucrative for the threat groups (and the most prominent threat across most regions), not only as a financial gain tool, but due to the sustained investments by cyber weapons developers, become a useful and effective cyber weapon to cause pain to targeted organisations. The most active **Ransomware** groups observed across the territories include, **ALPHV**, **BlackCat Gang**, **FIN11**, and **LockBit Gang**.

While we observed both state-sponsored threat groups and organised crime groups active in the region, we also saw rising activities associated with hacktivism due to spillover effects from the Israel-Hamas conflict occurring from the end of 2023. This has generally led to rising partisan collective groups taking actions into their own hands for the ideological causes. Notable **hacktivist** groups observed active in our region included **Bjorka**, **DragonForce Malaysia**, **SynixCyberCrimMY**, **GhostSec**, **Muslim Cyber Army**, **VulzSec** and **Ganosec Team**. The challenge in addressing hacktivism stems from their lack of a definitive structure and unique processes and procedures for each group. Instead, individuals involved in adversarial actions leverage their individual competencies and capabilities to further their cause. While organisations who do well in addressing cyber hygiene measures are generally resilient against hacktivist threats, the level of sophistication and effects are also rising. These groups have been observed to perform not just the distributed denial-of-service (DDoS) attacks and website defacements, but now, with the accessibility to offensive services (e.g. Ransomware as a Service), some attacks are inflicting greater harm to organisations when these attacks breach the defences.

Aside from hacktivism, Ensign has seen sustained activities from initial access brokers active in the territories, who have not only been successful in obtaining and selling access to organisations, but also due to rising Law enforcement activities targeting the Ransomware operators, started to opportunistically exfiltrate and sell the victim's data even before sale of access. This has led to some cyber-attack campaigns having lost the adversaries' element of surprise due to lack of operational security (OpsSec). Active **initial access brokers (IABs)** observed across the territories include **APT-C-01 (Poison Ivy)**, **BITTER**, **Scattered Spider**, and **UNC5221**. IABs such as **Scattered Spider** are known to obtain financial gain through sale of access and opportunistically sell data obtained during acquisition of access.

Aside from initial access brokers and Ransomware groups, 2023 saw 21 threat groups actively targeting the Ensign operating territories. There are more **state-sponsored threat** groups (16) than organised crime groups (5) observed. Russian-associated threat groups, **APT28**, **FIN7**, and **Turla**, are representative groups that have returned to target the Ensign operating territories. **GambleForce** and **Lazarus Group** were observed to have targeted all Ensign's operating territories.

The five **organised crime groups** observed across the territories, aside from the aforementioned Ransomware Groups and Initial Access Brokers, are **Carderbee**, **Desorden**, **FIN7**, **Patchwork**, and **Poison Carp**. Malaysia and Indonesia generally shared the same threat groups, with the exception of **Desorden** which continued its targeting of Malaysia, and **Turla** which targeted Indonesia.

Overview of Territorial Insights

Due to the aforementioned tensions across the territories, there are more threat groups observed to be motivated by **surveillance, information theft and espionage**. Particularly on surveillance of populations, we noted that **Kimsuky** and **Poison Carp** are threat groups which target mobile devices for surveillance outcomes with the harvesting of personal data and information.

Attacks on **network equipment** with significant impact were seen across territories. The stealthy and persistent effects of breaches performed by Volt Typhoon were prominent, especially with their KV-Botnet to compromise long-term unpatched and end-of-life networking products (such as Netgear ProSAFE routers, CISCO RV 320/325 routers, Draytek Vigor routers, and AXIS IP cameras). Some of these devices are installed in the operational technology (OT) environment or next-to-OT environments (possibly affecting essential services and other OT-centric businesses such as manufacturing) in territories such as **Singapore**, **Malaysia**, **Indonesia**, and **Australia**.

Cyber supply chain attacks have also manifested in a big way across the territories in 2023, causing some big brands / organisations to be breached. Notably, cyber-attacks exploiting vulnerabilities are found in commonly used commercial off the shelf (COTS) solutions such as MOVEit Managed File Transfer (MFT) software, Citrix NetScaler ADC and Gateway, Confluence Server and Data Center, Zoho ManageEngine, 3CX Desktop Application, GoAnywhere MFT, Ivanti Connect Secure VPN, PaperCut Application Server, Veam Backup & Replication, and others.

Based on our incident responses, Ensign noted that the minimum Dwell time increased compared to 2022 (0 days). This could be attributed to the increasing technology sprawl as organisations work through technology refresh and the continued use of Cloud-based services. The maximum Dwell time decreased significantly from **1,095 days** to **49 days**. This is encouraging as it indicates that organisations may be increasing their detection capabilities. Contrasting the average Dwell time observed from 2022, there has also been a decrease to **5 days** for **Retail**, **22 days** for **TMT**, and **33 days** for **Others**, observed this year (last year we observed the average of **71 days** average Dwell time for **Transport** sector and **83 days** for **Others**).

Industry Group	Average Dwell (Days)	Min. (Days)	Max. (Days)
Retail	**5**	3	12
Technology, Media and Telecommunications (TMT)	**22**	12	49
Others	**33**	19	43

Across the territories, the top targeted industry groups were as follows:

SG	Manufacturing	Professional services	**TMT**	**Financial services**	Real estate
MY	Manufacturing	**Government**	**TMT**	Professional services	Retail
ID	**TMT**	**Financial Services**	**Government**	Energy	Manufacturing
SK	**Government**	**TMT**	Manufacturing	**Financial services**	Defence
AU	**TMT**	Engineering & construction	Retail	**Government**	**Financial services**
GCR	**TMT**	Manufacturing	Professional services	Healthcare	**Financial Services**

The most common industry groups were **Technology, Media and Telecommunications (TMT)**, **Government**, **Financial Services**, and **Manufacturing**.

*Across this section, 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 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, and top tactics can be found in **Appendix C**. Full versions of the vulnerabilities observed in the territories can be found in **Appendix B**.*

Overview of Territorial Insights

We saw **Technology, Media and Telecommunications (TMT)** as the top industry group targeted across all the territories. This is attributed to the increased levels of digitalisation post-pandemic and the push for greater productivity through exploitation of higher network bandwidth, AI and automation as well as the push for digital payments and digital trade systems across ASEAN and the Asia Pacific region.

The **Government** industry group was observed to be targeted across **Malaysia**, **Indonesia**, **South Korea**, **Australia** and the **Greater China Region**. We attribute this to political events such as elections or geopolitical matters such as the US-China tensions.

The **Financial services** industry group was observed to be targeted across **Singapore**, **Indonesia**, **South Korea**, **Australia** and the **Greater China Region**. We attribute this to the natural concentration of personal data, which is useful for espionage and surveillance related activities, as well as access to funds, especially through cryptocurrency wallets and brokerage accounts.

The **Manufacturing** industry group was observed to be targeted across **Singapore**, **Malaysia**, **Indonesia** and **South Korea**. With the rebalancing of manufacturing capacity due to "de-risking" efforts between US and China, Southeast Asian countries and allies of US (i.e. South Korea) benefits from ramped up manufacturing demand which is progressively driving the economic growth post-pandemic. Industrial espionage is also a common reason why threat actors are interested in this industry group. The threat actors typically target the trade secrets and industrial designs, including business relationships and contracts. Additionally, some threat actors are interested in having the capability to cause disruption to the supply chain by targeting the companies in this industry group.

Our analysis of the top techniques observed saw **T1110: Brute Force** common across **Singapore**, **Malaysia & Indonesia** and the **Greater China Region**. Amongst others, **T1595: Active Scanning** and **T1078: Valid Accounts** were observed across **Singapore**, **Malaysia & Indonesia**. **T1071: Application Layer Protocol** was observed across **Singapore** and the **Greater China Region**.

SG	T1110: Brute Force	T1595: Active Scanning	T1078: Valid Accounts	T1071: Application Layer Protocol
MY & ID	T1110: Brute Force	T1595: Active Scanning	T1098: Account Manipulation	T1078: Valid Accounts
GCR	T1110: Brute Force	T1059: Command and Scripting Interpreter	T1566: Phishing	T1071: Application Layer Protocol

The cyber-attack effects observed across the territories saw **Ransom** observed across all territories. Next most common cyber-attack effect was **Sale of Access**, followed by **Sale of Data**, **Data Leak** and **Denial of Service**.

SG	Ransom	Sale of Access	Sale of Data
MY	Ransom	Sale of Access	Data Leak
ID	Ransom	Sale of Access	Sale of Data
SK	Data Leak	Denial of Service	Ransom
AU	Ransom	Data Leak	Denial of Service
GCR	Ransom	Sale of Access	Sale of Data

Overview of Territorial Insights

THREAT GROUP	PROFILE	MOTIVATION	ASSOCIATED TERRITORY	VICTIM TERRITORIES					
				SG	MY	ID	SK	AU	GCR
APT28	State-sponsored	Information theft and espionage	Russia	●	●		●	●	●
APT33	State-sponsored	Information theft and espionage; Sabotage and destruction; Financial crime	Iran	●	●	●	●	●	
APT37	State-sponsored	Information theft and espionage	North Korea				●		●
APT38	State-sponsored	Financial crime	North Korea	●	●	●	●		
APT41	State-sponsored	Information theft and espionage; Financial crime	Greater China Region		●	●	●	●	●
APT43	State-sponsored	Financial gain	North Korea						●
BlackTech	State-sponsored	Information theft and espionage	Greater China Region						●
Carderbee	Organised Crime	Information theft and espionage	Greater China Region						●
Dark Pink	State-sponsored	Information theft and espionage	Vietnam	●	●	●			
Darkhotel	State-sponsored	Information theft and espionage	South Korea						●
Desorden	Organised Crime	Financial gain	*Unknown*		●				
Earth Longzhi	State-sponsored	Information theft and espionage	Greater China Region		●	●			●
FIN7	Organised Crime	Financial crime	Russia					●	●
GambleForce	State-sponsored	Information theft and espionage	Greater China Region	●	●	●	●	●	●
Kimsuky	State-sponsored	Information theft and espionage	North Korea				●		●
Lazarus Group	State-sponsored	Financial crime; Information theft and espionage; Sabotage and destruction	North Korea	●	●	●	●	●	●
Patchwork	Organised Crime	Information theft and espionage	India						●
Poison Carp	Organised Crime	Information theft and espionage	Greater China Region					●	●
Tonto Team	State-sponsored	Information theft and espionage	Greater China Region				●		
Turla	State-sponsored	Information theft and espionage	Russia			●		●	
Volt Typhoon	State-sponsored	Information theft and espionage	Greater China Region					●	
			Total	**6**	**9**	**8**	**9**	**9**	**14**

Top Active Ransomware Groups Observed in the Territories in 2023

Threat Actor Name	**ALPHV, BlackCat Gang**	**FIN11**	**LockBit Gang**
Associated Territory	Unknown	Unknown	Unknown
Threat Actor Profile	Organised Crime	Organised Crime	Organised Crime
Motivation	Financial gain	Financial gain	Financial gain

Notable Characteristics	▪ ***ALPHV Ransomware*** Operator
	▪ Managed leak-site
	▪ Multi-extortion tactics, including:
	  ▪ Disclosure to public
	  ▪ Sale of data
	  ▪ Reporting to regulator
		▪ ***Cl0p Ransomware*** Operator
		▪ Managed leak-site
		▪ Multi-extortion tactics, including:
		  ▪ Disclosure to public
		  ▪ Sale of data
		▪ Exploited the MOVEit 0day vulnerability (CVE-2023-34362) and GoAnywhere 0day vulnerability (CVE-2023-0669) for Initial Access
			▪ ***LockBit 3.0*** Ransomware Operator
			▪ Managed leak-site
			▪ Multi-extortion tactics, including:
			  ▪ Disclosure to public
			  ▪ Sale of data
			▪ Coordinates different adversary talents and capabilities

Publicly Known Victims *(Non-exhaustive)*	**Singapore** ▪ Fu Yu Corporation **Malaysia** ▪ Agensi Kaunseling dan Pengurusan Kredit (AKPK) ▪ Vopack Malaysia **Australia** ▪ HWL Ebsworth ▪ TissuPath	**Australia** ▪ Aristocrat Leisure Limited ▪ BG Group Australia (member of Shell Group of companies) ▪ Crown Resorts ▪ Fortescue Metals	**Singapore** ▪ Academy of Medicine **Indonesia** ▪ Bank Syariah Indonesia (BSI) **South Korea** ▪ Hanwha Group **Australia** ▪ Q Automotive Group

ALPHV, **FIN11**, and **LockBit Gang** were collectively the three most active Ransomware Groups observed in the territories in 2023.

All were organised crime groups which ran "professional" operations, using updated capabilities with multi-extortion tactics.

MITRE ATT&CK v15

Techniques of Concern

TA0001: Initial Access
- T1078: Valid Accounts
- T1189: Drive-by Compromise
- T1133: External Remote Services
- T1566: Phishing

TA0010: Exfiltration
- T1567: Exfiltration Over Web Service

TA0040: Impact
- T1486: Data Encrypted for Impact
- T1489: Service Stop
- T1485: Data Destruction
- T1491: Defacement

Top Active Initial Access Brokers Observed in the Territories

APT-C-01 (Poison Ivy), **BITTER**, **Scattered Spider**, and **UNC5221** were the four most active initial access brokers observed in the territories in 2023. All operated as "mercenaries for hire" in providing access to targets / victims.

Notably, **Scattered Spider** is the only threat group motivated by financial gain with sales of exfiltrated data aside from access to targets / victims.

Threat Actor Name	**APT-C-01 (Poison Ivy)**	**BITTER**	**Scattered Spider**	**UNC5221**
Associated Territory	Greater China Region	Unknown	Unknown	Unknown
Threat Actor Profile	State-sponsored	Organised Crime	Organised Crime	Organised Crime
Motivation	Information theft and espionage	Information theft and espionage	Financial gain	Information theft and espionage
Notable Characteristics	Predominantly used Phishing and exploits 0day vulnerabilities.	Performed Phishing using malicious CHM file attachments.	Performed social engineering for identity compromise on Okta related identity compromise via cross tenant impersonation.	Exploited (CVE-2023-46805) Ivanti Connect Secure VPN vulnerability for authentication bypass.
Targeted Territories	Greater China Region	Greater China Region	Singapore, Malaysia, Indonesia, South Korea, Australia, Greater China Region	Singapore, Malaysia, Indonesia, South Korea, Australia, Greater China Region

Scattered Spider observed to opportunistically sell obtained information (during initial access) for financial gain, aside from selling initial access.

MITRE ATT&CK v15

Techniques of Concern

TA0001: Initial Access
- T1566: Phishing
- T1133: External Remote Services
- T1078: Valid Accounts

TA0011: Command and Control
- T1090: Proxy
- T1568: Dynamic Resolution
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunneling
- T1102: Web Service

TA0010: Exfiltration
- T1041: Exfiltration Over C2 Channel
- T1048: Exfiltration Over Alternative Protocol

Singapore

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	NIL	APT33 APT38	Dark Pink GambleForce	APT28 Lazarus Group
	→→→ *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

1. **Manufacturing**
2. **Professional services**
3. **Technology, media & telecommunications**
4. **Financial services**
5. **Real estate**

New affected industries observed in 2023

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Ransom** 52.9%
2. **Sale of Access** 41.2%
3. **Sale of Data** 2%

MITRE ATT&CK v15

Techniques of Concern

TA0001: Initial Access
- T1566: Phishing
- T1189: Drive-by Compromise
- T1078: Valid Accounts
- T1091: Replication Through Removable Media
- T1133: External Remote Services
- T1199: Trusted Relationship

TA0011: Command and Control
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1571: Non-Standard Port
- T1102: Web Service
- T1092: Communication Through Removable Media
- T1008: Fallback Channels
- T1104: Multi-Stage Channels

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

TA0040: Impact
- T1565: Data Manipulation
- T1485: Data Destruction
- T1561: Disk Wipe
- T1529: System Shutdown/Reboot
- T1486: Data Encrypted for Impact
- T1491: Defacement
- T1498: Network Denial of Service
- T1489: Service Stop

Singapore

In addition to initial access brokers and Ransomware groups, Singapore was targeted by six threat groups, all of which are state-sponsored. Our analysis has identified that **APT28** and **Lazarus Group** were the most material threat groups operating within the territory.

The top five industry groups observed to be attacked include: (1) Manufacturing, (2) Professional services, (3) Real estate, (4) Financial services, and (5) Technology, media and telecommunications (TMT). Financial services and TMT continue to remain in the top targeted industry groups following last year's report. New entrants to the list include Manufacturing, Real estate, and Professional services, likely due to their lower cyber maturity level and less stringent cyber regulatory regimes.

The top cyber-attack effects observed were (1) **ransom**, (2) **sale of access**, and (3) **sale of data**. Correlating both the targeted industry groups and the top cyber-attack effects, it is possible that ransoms were made to capitalise on the businesses supporting post-pandemic economic recovery. The **sale of access** and the **sale of data** indicated continued interest to gain a foothold into businesses based in Singapore, many of which support larger companies (e.g. MNCs with regional HQs in Singapore) and essential services, as well as providing trusted access into other connected entities in the supply chain. Considering that Singapore is a trusted processor of data for many companies, the value of data handled in Singapore remains high, and obtaining such data can support further espionage activities or specific targeting.

Being a location with a highly digital-enabled environment through smart-nation initiatives, high concentration of data centres, and high throughput access to international Internet links, Singapore continues to be attractive to threat actors as a launchpad for cyber-attacks and to experiment attacks before launching them on higher sophistication locations.

Combined with the unique set of assets in the digital attack surface, Ensign noted that the following vendors solutions were deliberately exploited in the year:

- 3CX Desktop Application
- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- JetBrains TeamCity
- Juniper BigIP
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

Singapore Exchange (SGX)-listed companies are required to file cyber incident notices. Ensign noted that the following companies filed cybersecurity incident notifications to SGX in 2023:

Company	Industry Group
Cortina Holdings	Retail
GoldHeart	Retail
Koh Brothers Group Limited	Engineering and Construction
NetLink NBN Trust	Technology, media and telecommunications
Procurri Corporation Limited	Technology, media and telecommunications

Malaysia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	APT33 APT38 Earth Longzhi	Dark Pink GambleForce	APT28 APT41 Desorden Lazarus Group
	→→→ *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

1. **Manufacturing**
2. **Government**
3. **Technology, media & telecommunications**
4. **Professional Services**
5. **Retail**

New affected industries observed in 2023

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Ransom** 58.2%
2. **Sale of Access** 18.2%
3. **Data Leak** 14.5%

Techniques of Concern

MITRE ATT&CK v15

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

TA0011: Command and Control
- T1102: Web Service
- T1001: Data Obfuscation
- T1132: Data Encoding
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1571: Non-Standard Port
- T1090: Proxy
- T1092: Communication Through Removable Media
- T1568: Dynamic Resolution
- T1095: Non-Application Layer Protocol

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

TA0040: Impact
- T1565: Data Manipulation
- T1486: Data Encrypted for Impact
- T1485: Data Destruction
- T1561: Disk Wipe
- T1529: System Shutdown/Reboot
- T1491: Defacement
- T1498: Network Denial of Service
- T1489: Service Stop

Malaysia

Malaysia saw nine threat groups targeting the territory with **Desorden**, the only organised crime group, aside from the initial access brokers and Ransomware groups. **Desorden** has continued its campaign of targeting Malaysia and claimed victims Ranhill Utilities Berhad and Bintulu Port Holdings Berhad.

The top five industry groups observed to be attacked include: (1) Manufacturing, (2) **Government**, (3) **Technology, media and telecommunications (TMT)**, (4) **Professional services**, and (5) **Retail**. 2023 saw the inclusion of **Manufacturing**, **Government**, **Professional services**, and **Retail**.

The top cyber-attack effects observed were (1) **ransom**, (2) **sale of access**, and (3) **data leak**. Correlating both the targeted industry groups and the top cyber-attack effects, it is possible that ransoms targeted businesses supporting post-pandemic economic recovery. **The sale of access** and the **data leak** indicated continued interest to gain a foothold into businesses based in Malaysia. However, the nature and publicity around the data leaks could suggest a more nefarious intent to demonstrate cybersecurity weaknesses of businesses in Malaysia rather than to gain a lot financially from sale of the data. This suggests that the value of the data may not be high or that attackers have other objectives.

Malaysia has expressed keen interest to capitalise on the movements by multinational companies to relocate their manufacturing hubs, this is particularly focused on the high technology manufacturing business segment. These cyber-attack effects may be related to the types of companies being attracted to the country, among other factors.

Hacktivism also featured prominently in Malaysia in 2023. **DragonForce Malaysia** launched a rebranded **#OpsPetir** campaign replacing the last **#OpsBedil** in 2022.[1] The **#OpsPetir1** was initiated (from 12 April to 21 April) in the wake of the Israel-Hamas conflict which saw initial targeting of government agencies, education institutions, and financial institutions which were overt in their relationships with Israel. This subsequently expanded to other organisations deemed to have expressed support or have relationships with Israel for the conflict. During the campaign, a member of the group launched a denial-of-service tool, CyberTroopers, which was employed during the campaign. It was noted that the python-based tool leveraged ChatGPT3 in the development and obfuscation of the program. Notably, **DragonForce Malaysia** declared the goal of developing itself into a Ransomware group and the use of the leaked LockBit Ransomware source code2 were observed in attacks carried out by the group from November 2023 onwards.[2] This is a significant development in the graduation of **DragonForce Malaysia** into an organised crime group with ideological motivations.[3]

We noted that the following vendors solutions were deliberately exploited in the year:

- 3CX Desktop Application
- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- JetBrains TeamCity
- Juniper BigIP
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- SysAid On-Premise
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

[1] *DragonForce Malaysia: OpsPetir*. (12 Apr 2023). Radware. Retrieved from: https://www.radware.com/security/threat-advisories-and-attack-reports/dragonforce-malaysia-opspetir/
[2] K. Poireault. *DragonForce Ransomware Group Uses LockBit's Leaked Builder*. (25 April 2024). Infosecurity Magazine. Retrieved from: https://www.infosecurity-magazine.com/news/dragonforce-ransomware-lockbit/
[3] G. Sharma. *DragonForce Malaysia attacks Israeli institutions:*. (14 April 2023). SecurityBrief Asia. Retrieved from: https://securitybrief.asia/story/dragonforce-malaysia-attacks-israeli-institutions-radware

Indonesia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	NIL	APT33 APT38 Earth Longzhi Turla	NIL	APT41 Dark Pink GambleForce Lazarus Group
	→→→ *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

1. **Technology, media & telecommunications**
2. **Financial services**
3. **Government**
4. **Energy**
5. **Manufacturing**

New affected industries observed in 2023

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Ransom** 42%
2. **Sale of Access** 38%
3. **Sale of Data** 8%

Techniques of Concern

MITRE ATT&CK v15

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1189: Drive-by Compromise
- T1133: External Remote Services
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise

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

TA0010: Exfiltration
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1567: Exfiltration Over Web Service

TA0040: Impact
- T1565: Data Manipulation
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1561: Disk Wipe
- T1529: System Shutdown/Reboot
- T1491: Defacement
- T1489: Service Stop

Indonesia

Indonesia saw eight threat groups targeting the territory which generally shares the same threat groups as Malaysia. The only difference was the exclusion of **Desorden**, which dwindled in Indonesia, and the inclusion of **Turla** for Indonesia, which was not present in Malaysia. This is aside from the initial access brokers and Ransomware groups. **Desorden** has seemingly discontinued its campaign targeting Indonesian entities in 2023.

The top five industry groups observed to be attacked include: (1) Technology, media and telecommunications (TMT), (2) Financial services, (3) Government, (4) Energy, and (5) Food and Beverage. Ensign sees the inclusion of TMT , Energy, and Food & Beverage in this year's top targeted industry groups.

The top cyber-attack effects observed were (1) **ransom**, (2) **sale of access**, and (3) **sale of data**. Correlating both the targeted industry groups and the top cyber-attack effects, there is reason to believe that ransoms were made to capitalise on the businesses supporting economic recovery post-pandemic. The **sale of access** and the **sale of data** indicated continued interest to gain a foothold into businesses based in Indonesia. Given that Indonesia was the chair of ASEAN in 2023, it is possible that threat actor groups who were uniquely targeting government entities may be conducting espionage and gathering information of political value. The targeting of Energy and Food & Beverage industry groups might have been as an indirect means to feed influence operations oriented towards the 2024 elections.

Indonesia has seen sustained hacktivist activities targeting its entities, most notably **Bjorka**, which does not seem to have an ideological or political cause but is instead determined to embarrass the Indonesian government and expose their weak cyber and data security practices. In 2023, **Bjorka** claimed to have attacked BPJS Ketenagakerjaan and PT Telkom Indonesia (Persero) Tbk with the sale of their exfiltrated data.

Ensign noted that the following vendors solutions were deliberately exploited in the year:

- 3CX Desktop Application
- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- JetBrains TeamCity
- Juniper BigIP
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- SysAid On-Premise
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

South Korea

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	APT28 APT33 APT41	NIL	APT37 APT38 GambleForce Kimsuky Lazarus Group Tonto Team
	→→→ *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

1. **Government**
2. **Technology, media & telecommunications**
3. **Manufacturing**
4. **Financial services**
5. **Defence**

New affected industries observed in 2023

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Data Leak** 31.7%
2. **Denial of Service** 15.9%
3. **Ransom** 13.4%

Techniques of Concern

MITRE ATT&CK v15

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

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1102: Web Service
- T1090: Proxy
- T1001: Data Obfuscation
- T1573: Encrypted Channel
- T1092: Communication Through Removable Media
- T1132: Data Encoding
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1571: Non-Standard Port
- T1568: Dynamic Resolution
- T1219: Remote Access Software

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

TA0040: Impact
- T1565: Data Manipulation
- T1561: Disk Wipe
- T1529: System Shutdown/Reboot
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1498: Network Denial of Service
- T1491: Defacement
- T1489: Service Stop

South Korea

South Korea saw nine threat groups targeting the territory, all of which are state-sponsored threat groups, aside from the initial access brokers and Ransomware groups. Without surprise, South Korea has seen continued and dedicated targeting from North Korea-associated threat groups — **APT37**, **APT38**, **Kimsuky**, and **Lazarus Group**.

The top five industry groups observed to be attacked include: (1) Financial services, (2) Research, (3) Education, (4) Government, and (5) Defence. Ensign saw the inclusion of the Defence industry group in this year's top targeted industry groups.

The top cyber-attack effects observed were (1) **data leak**, (2) **denial of service**, and (3) **ransom**. The **data leaks** and the **denial-of-service** attacks are commonplace to demonstrate continued interest and attention by its natural adversaries and to create disruptive effects on the population's quality of life and businesses. The ransom attacks seem to be targeting businesses purely for financial gain.

South Korea has accelerated defence cooperation agreements with the US to bolster her security against the rising tensions seen in North Asia. These agreements, including military exercises, have drawn the disdain from North Korea which has also resulted in the declaration by the DPRK[4] that the ROK is the "primary foe". New cyber threat activity observed in South Korea is generally targeted at organisation which are focused on Korean peninsula affairs across the border and associated with the military. This is on top of the continued interest by North Korean associated threat groups in performing surveillance and information collection on DPRK dissidents and understanding of North Korea.

Ensign noted that the following vendors' solutions were deliberately exploited in the year:

- 3CX Desktop Application
- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- DreamSecurity MagicLine4NX
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- JetBrains TeamCity
- Juniper BigIP
- Microsoft Windows
- Microsoft Outlook
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- SysAid On-Premise
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

Extensive phishing campaigns leveraging malicious Windows Help Files (CHM) and malicious Hancom Office documents are observed to support social engineering efforts. Often, the successful breach into accounts and devices lead to exfiltration of personal data or business sensitive information. Ensign also observed the setup of fake Naver and Kakao email websites to harvest email credentials of users in phishing campaigns.

Some of these espionage campaigns have also continued to leverage the weaknesses in some app stores to propagate malicious applications on mobile devices and to encourage sideloading of malicious apps into the victim's mobile devices.

The specific exploitation of INITECH's solutions by **Lazarus Group** on the CrossWeb EX and MagicLine4NX (CVE-2023-45797), authentication process software solutions typically used in online financial services in South Korea, was observed to attempt gaining access into individuals' bank accounts and cryptocurrency wallets.

[4] F. Koh. *Kim Jong Un's move to label South Korea an enemy, drop reunification policy part of North's diplomatic playbook: Experts*. (17 January 2024). Channel News Asia. Retrieved from: https://www.channelnewsasia.com/world/kim-jong-un-move-label-south-korea-enemy-drop-reunification-policy-strategic-part-norths-diplomatic-playbook-experts-4053871

Australia

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	APT33 APT41 Poison Carp Turla	FIN7	APT28 GambleForce Lazarus Group Volt Typhoon
	→→→ *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

1. **Technology, media & telecommunications**
2. **Engineering & Construction**
3. **Retail**
4. **Government**
5. **Financial services**

● *New affected industries observed in 2023*

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Ransom** 52.7%
2. **Data Leak** 16.4%
3. **Denial of Service** 12.1%

MITRE ATT&CK v15

Techniques of Concern

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1189: Drive-by Compromise
- 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
- T1090: Proxy
- T1102: Web Service
- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1001: Data Obfuscation
- T1573: Encrypted Channel
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1571: Non-Standard Port
- T1092: Communication Through Removable Media
- T1132: Data Encoding
- T1568: Dynamic Resolution
- T1219: Remote Access Software

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
- T1565: Data Manipulation
- T1485: Data Destruction
- T1561: Disk Wipe
- T1529: System Shutdown/Reboot
- T1491: Defacement
- T1498: Network Denial of Service
- T1489: Service Stop

Australia

Australia saw nine threat groups targeting the territory, with all but **FIN7** and **Poison Carp** as the organised crime groups, aside from the initial access brokers and Ransomware groups.

FIN7 had been observed to exploit the Veam Backup and Replication vulnerability (CVE-2023-27532), which is a common backup and archival solution used by many companies. **FIN7's** exploits the vulnerability to gain initial access and support discovery and identification of targets, in the goal of big game hunting (BGH) through cyber supply chain compromise, since the vulnerable software has a wide range of users cross-cutting many industries.

Australia saw a series of attacks targeting manufacturing, professional services, retail, financial services and education industries. Some notable companies included: Boeing Systems,[5] Pizza Hut,[6] Sony Australia,[7] HWL Ebsworth,[8] and Latitude Financial.[9]

The top five industry groups observed to be attacked include: (1) Technology, media and telecommunications (TMT), (2) Engineering and construction, (3) Retail, (4) Government, and (5) Financial services.

The top cyber-attack effects observed were (1) **ransom**, (2) **data leak**, and (3) **denial of service**. Correlating both the targeted industry groups and the top cyber-attack effects, there is reason that **ransoms** were made to capitalise on the businesses supporting economic recovery post-pandemic. The **data leaks** and the **denial-of-service** attacks are targeted to bring awareness of the adversaries' attention on Australian organisations.

Australia, being a close western aligned territory, attracts similar threat groups targeting the US and its allies. Most recent publicly reported attacks seem to concentrate on the TMR industry group which might be motivated to gain insights into the communications and technology resources available in the territory. Targeting of the Engineering and construction industry may be related towards the AUKUS agreement to collaboratively build nuclear-powered submarines to enhance Australia's maritime security.

Ensign noted that the following vendors' solutions were deliberately exploited in the year:

- 3CX Desktop Application
- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- GoAnywhere MFT
- Ivanti Connect Secure VPN
- JetBrains TeamCity
- Juniper BigIP
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

[5] V. Insinna & Z. Siddiqui. *Boeing says 'cyber incident' hit parts business*. (3 November 2023). IT News. Retrieved from: https://www.itnews.com.au/news/boeing-says-cyber-incident-hit-parts-business-601999
[6] C. Rawling. *Pizza Hut says nearly two-hundred thousand customers affected by data breach*. (20 September 2023). ABC News. Retrieved from: https://www.abc.net.au/news/2023-09-20/pizza-hut-customers-affected-by-cyber-hack/102881804
[7] D. Tilo. *Over 6,000 individuals hit in Sony data breach: reports*. (10 October 2023). Human Resources Director. Retrieved from: https://www.hcamag.com/au/news/general/over-6000-individuals-hit-in-sony-data-breach-reports/462431
[8] J. Taylor. *HWL Ebsworth hack: 65 Australian government agencies affected by cyber-attack.* (18 September 2023). The Guardian. Retrieved from: https://www.theguardian.com/australia-news/2023/sep/18/hwl-ebsworth-hack-65-australian-government-agencies-affected-by-cyber-attack
[9] J. Barrett. *Latitude Financial cyber-attack worse than first thought with 14m customer records stolen.* (27 March 2023). The Guardian. Retrieved from: https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen

Greater China Region

KEY ANALYSIS INSIGHTS

ENSIGN THREAT CLASSIFICATION MATRIX	NIL	APT28 APT41 Earth Longzhi FIN7 Patchwork	NIL	APT37 APT43 BlackTech Carderbee DarkHotel GambleForce Kimsuky Lazarus Group Poison Carp
	→→→ *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

1. **Technology, media & telecommunications**
2. **Manufacturing**
3. **Professional services**
4. **Healthcare**
5. **Financial services**

New affected industries observed in 2023

TOP NOTABLE cyber-attack EFFECTS OBSERVED

1. **Ransom** 68.5%
2. **Sale of Access** 21.9%
3. **Sale of Data** 4.1%

Techniques of Concern

MITRE ATT&CK v15

TA0001: Initial Access
- T1566: Phishing
- T1078: Valid Accounts
- T1189: Drive-by Compromise
- T1133: External Remote Services
- T1195: Supply Chain Compromise
- T1190: Exploit Public-Facing Application
- T1091: Replication Through Removable Media
- T1199: Trusted Relationship
- T1659: Content Injection

TA0011: Command and Control
- T1102: Web Service
- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1090: Proxy
- T1573: Encrypted Channel
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1008: Fallback Channels
- T1095: Non-Application Layer Protocol
- T1104: Multi-Stage Channels
- T1571: Non-Standard Port
- T1219: Remote Access Software
- T1092: Communication Through Removable Media
- T1659: Content Injection
- T1568: Dynamic Resolution
- T1205: Traffic Signaling

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

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

Greater China Region

The Greater China region, particularly the Hong Kong Special Administration Region (Hong Kong, where Ensign has longstanding operational presence) and the People's Republic of China (PRC, which is a recent expansion from Ensign), has seen 14 threat groups targeting the territory. Unique to this territory, there are domestically associated threat groups targeting entities based in the region — **APT41**, **BlackTech**, **Carderbee**, **Earth Longzhi**, **GambleForce**, and **Poison Carp**.

The top five industry groups observed to be attacked include: (1) Technology, media and telecommunications, (2) Manufacturing, (3) Professional services, (4) Healthcare, and (5) Financial services. Relating to the Hong Kong region, we are seeing the inclusion of Manufacturing, Professional services, and Healthcare in the top targeted industry groups this year.

The top cyber-attack effects observed were (1) **ransom**, (2) **sale of access**, and (3) **sale of data**. Correlating both the targeted industry groups and the top cyber-attack effects, there is reason that **ransoms** were made to capitalise on the businesses supporting economic recovery post-pandemic. The **sale of access** and the **sale of data** attacks can be attributed to threat actors with intents to gain access to targeted companies through "big game hunting" and to obtain information for espionage purposes.

The PRC has sustained complications with the US in recent years resulting in trade tensions, including concerns relating to the Republic of China (Taiwan). The developments have resulted in public displays of disagreement but also noticeable cyber activity. Further to the US-China tensions, there are also rising regional concerns on security by neighbours in East Asia. This has resulted in increased balancing actions between the states in the region to accommodate their risk appetites.

Ensign noted that the following vendors' solutions were deliberately exploited in the year:

- Cisco ASA VPN
- Citrix NetScaler ADC and Gateway
- Confluence Server and Data Center
- Fortinet FortiOS
- GoAnywhere MFT
- Ivanti Connect Secure VPN'
- JetBrains TeamCity
- Juniper BigIP
- MOVEit Managed File Transfer (MFT) software
- PaperCut Application Server
- Veam Backup & Replication
- WinRAR
- Zoho ManageEngine

Territorial Tactics Observations

Through our observations and analysis across our territories in **Singapore**, **Malaysia**, **Indonesia**, and the **Greater China Region**, Ensign has made unique insights to the cyber events which are detailed in this section.

Common adversary techniques observed across the territories include:

1. **T1110: Brute Force** was the dominant Technique observed across **Singapore**, **Malaysia**, **Indonesia**, and the **Greater China Region**.
2. **T1595: Active Scanning** and **T1078: Valid Accounts** were common top techniques observed across **Singapore**, **Malaysia**, and **Indonesia**.
3. **T1071: Application Layer Protocol** was common between **Malaysia**, **Indonesia**, and the **Greater China Region**.

Influential events in the territories were leveraged to effect for the cyber events observed. Many of the significant events include elections, critical supply chain vulnerabilities with widespread effects, and geopolitical tensions.

Likewise, there were common industry groups which showed signs of compromise across the territories:

1. **Singapore**, **Malaysia**, **Indonesia**, and the **Greater China Region** all saw signs of compromise to **Technology** industry group.
2. **Singapore**, **Malaysia**, and **Indonesia** saw signs of compromise to **Manufacturing**, **Energy & Utilities**, and **Telecommunications** industry groups.
3. **Singapore** and the **Greater China Region** saw signs of compromise to the **Real Estate** industry group.

AI generated image with representations from Singapore, Malaysia, Indonesia and the Greater China Region

Singapore

KEY OBSERVATIONS FROM ENSIGN PROPRIETARY DATA

23.5%
T11110: Brute Force

8.4%
T1595: Active Scanning

7.1%
T1078: Valid Accounts

5.4%
T1071: Application layer protocol

2023 Q3 saw the highest cyber activity in coincidence with several high-profile events:

1. The arrest of 10 foreign nationals allegedly part of the largest money laundering scheme in the world in August.[10]
2. The Singapore Presidential Election in September.

Ensign observed persistent **TA0043: Reconnaissance** and **TA0006: Credential Access** activity throughout the year with peak activity levels observed in **2023 Q3**.

The Microsoft Outlook Privilege Escalation Vulnerability (CVE-2023-23397) also contributed to cyber activities in **2023 Q1** with elevated observations for **TA0004: Privilege Escalation** and **TA0005: Defence Evasion**.

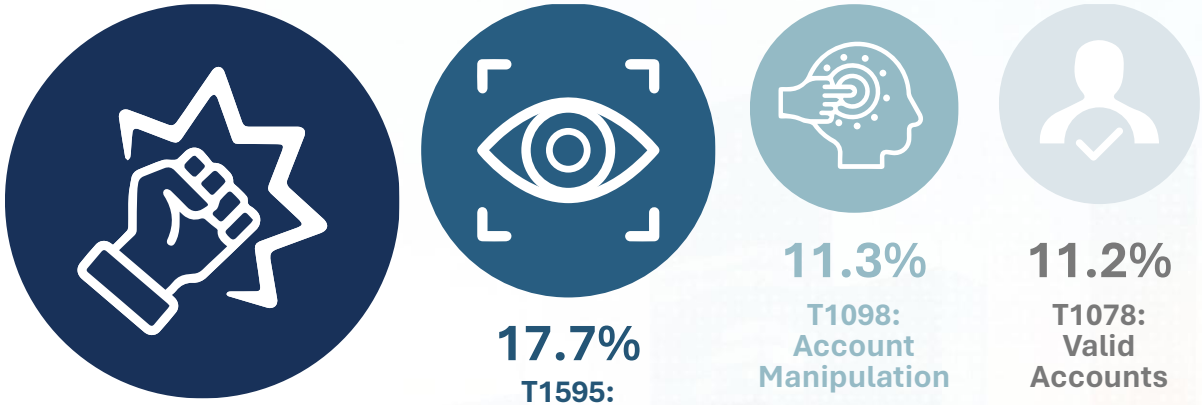
Ensign observed sustained and high interest in **TA0043: Reconnaissance** in the (1) **Administrative and Technical Services**, (2) **Manufacturing**, (3) **Banking & Finance**, (4) **Insurance**, (5) **Telecommunications**, and (6) **Education** industry groups. This means there are sustained interest in targeting these six industry groups.

There were elevated observations in **TA0005: Defense Evasion**, **TA0006: Credential Access**, and **TA0011: Command and Control** in the following industry groups: (1) **Healthcare**, (2) **Real Estate**, (3) **Technology**, (4) **Energy and Utilities**, (5) **Aerospace**, (6) **Manufacturing**, and (7) **Telecommunications**. This means that the seven industry groups demonstrated signs of compromise.

[10] L. Tang. *Billion-dollar money laundering case: Singapore police began 'comprehensive intelligence probe' in early 2022.* (3 October 2023). Channel News Asia. Retrieved from: https://www.channelnewsasia.com/singapore/billion-dollar-money-laundering-police-intelligence-probe-2022-3816371

Malaysia & Indonesia

KEY OBSERVATIONS FROM ENSIGN PROPRIETARY DATA



27.6%
T1110: Brute Force

17.7%
T1595: Active Scanning

11.3%
T1098: Account Manipulation

11.2%
T1078: Valid Accounts

2023 Q2 to Q4 saw the highest sustained cyber activity levels in coincidence with the following events:

1. Six state elections in Malaysia for Selangor, Kelantan, Terengganu, Negeri Sembilan, Kedah, and Penang in August.
2. ASEAN high-level events with Indonesia heading as Chair in 2024 in the months of July till September.

Ensign observed persistent **TA0043: Reconnaissance** and **TA0006: Credential Access** activity throughout the year with peak activity levels observed between **2023 Q2 to 2023 Q4**.

The suite of MOVEit vulnerabilities (CVE-2023-36932, CVE-2023-36933, and CVE-2023-36934) contributed to the peak of cyber activities from the months of May to September with elevated observations for **TA0006: Credential Access**.

Ensign observed sustained and high interest in **TA0043: Reconnaissance** in the (1) **Insurance**, (2) **Energy and Utilities**, (3) **Administrative and Technical Services**, (4) **Banking & Finance**, (5) **Manufacturing**, and (6) **Telecommunications** industry groups. This means there are sustained interest in targeting these six industry groups.

There were elevated observations in **TA0002: Execution**, **TA0005: Defense Evasion**, **TA0006: Credential Access** in the following industry groups: (1) **Telecommunications**, (2) **Energy and Utilities**, (3) **Administrative and Technical Services**, (4) **Manufacturing**, (5) **Insurance**, and (6) **Technology**. This means that the six industry groups demonstrated signs of compromise.

Greater China Region

KEY OBSERVATIONS FROM ENSIGN PROPRIETARY DATA

23.5%
T1110: Brute Force

16.5%
T1059: Command and Scripting Interpreter

9.2%
T1566: Phishing

8.5%
T1071: Application layer protocol

2023 saw sustained cyber activity levels in coincidence with the following events:

1. Chinese meteorological balloon which entered US airspace
2. National People's Congress (NPC) and the National Committee of the Chinese People's Political Consultative Conference (CPPCC) in March
3. China-Central Asia Summit in May and Belt and Road Forum for International Cooperation in October
4. 19th Asian Games in July and 4th Asian Para Games in October
5. US-China dialogue meetings from June to November
6. US expanded export controls within US and like-minded countries on advanced chip manufacturing equipment in October
7. Sustained trials on activists in relation to the national security Law

Ensign observed persistent **TA0001: Initial Access** and **TA0006: Credential Access** activity throughout the year. This indicates that threat actors are leveraging harvested access and credentials for cyber-attacks.

Ensign observed sustained and high interest in **TA0001: Initial Access** in the (1) **Real Estate**, (2) **Mining**, (3) **Education**, (4) **Banking & Finance**, and (5) **Insurance** industry groups. This means there are sustained exploitation targeting these five industry groups.

There were elevated observations in **TA0003: Execution**, **TA0005: Defense Evasion**, **TA0006: Credential Access**, **TA0007: Discovery**, and **TA0011: Command and Control** in the following industry groups: (1) **Real Estate**, (2) **Insurance**, (3) **Banking & Finance**, (4) **Education**, (5) **Technology**, and (6) **Hospitality**. This means that the six industry groups demonstrated signs of compromise.

It is noteworthy that the **Administrative and Technical Services** industry group saw elevated levels of **TA0005: Defense Evasion**. This indicates that the industry group has active threat actors navigating the environments to uncover opportunities for command and control, exfiltration or impact. The **Telecommunications** industry group saw elevated levels of **TA0007: Discovery**. This indicates intent by threat actors to uncover information of value in this industry group.

3 TOP THREAT TRENDS 2023

Overview of Top Threat Trends of 2023

AI helped defenders but also enabled attackers

- Defenders had access to more AI-enabled tools to detect anomalous or malicious activity.
- Attackers used AI for Reconnaissance and Initial Access (e.g. phishing).
- Attackers used AI to prototype new cyber weapons (e.g. polymorphism).
- Attackers also attacked AI systems, mostly to test the systems and possibilities rather than to secure any specific objectives.

Digital trust was eroded

- Deliberate influence operations were conducted (using hand-crafted and AI-generated content) to manipulate opinion, especially ahead of major elections.
- Early experiments in deepfakes and synthetic identities were observed for social engineering attacks (influence and phishing).
- As GenAI imagery was still identifiable in 2023, only some users were spoofed.

Cyber supply chain attacks worsened

- There were more cases of malicious code injections into popular open-source software.
- Targeted attacks on digital infrastructure, especially network devices, increased.
- OT-based malware like PIPEDREAM and subsequently COSMIC ENERGY were developed in quick succession demonstrating speed and interest.

Attackers evolved their TTPs to defeat our processes and tools

- Attackers recognised that defenders were not prioritising the patches for low-risk / severity vulnerabilities, often for months.
- Attackers developed attack paths using these low-risk vulnerabilities and remained undetected with stealthier actions (e.g. living off the land techniques).

Geopolitics worsened cybersecurity everywhere

- Conflicts between Russia-Ukraine and Israel-Hamas, and even US-China tensions, have all spilled over into the cyber domain.
- Hacktivism and state-sanctioned / sponsored cyber activity increased. Hacktivist groups demonstrated more sophisticated capabilities (Wiperware, supply chain attacks).

"De-risking" accelerated tech bifurcation

- Countries with the means started developing organic technology stacks to reduce reliance on shared global Internet infrastructure and tools.
- The Western tech stack will continue to grapple with cyber risks from open architecture. The Asian tech stack may require new cybersecurity concepts, as the design considerations may differ. Interoperability is not assured between them.

- **Ransomware, Evolved:** Shift in Extortion Techniques
- **Hacktivists, Unite:** Increasing Sophistication of Cause-aligned Groups
- **Digital Infrastructure Under Fire:** Threats Across the Cyber Supply Chain
- **Digital Sheriffs:** New Regulatory and Policy Initiatives that Aim to Address Risks of Emerging Technology
- **Disclosure Revelations:** How Mandatory Incident Reporting is Shining a Light on Corporate Cyber Impact

4 TOPICAL INSIGHTS

ESCALATING THREATS

Ransomware, Evolved: Shift in Extortion Techniques

- **Ransomware remained the most worrying threat in 2023, with an expanding criminal ecosystem and service delivery model.**
- **Companies were extorted multiple times in an attack, sometimes from the same attacker (first to recover the systems, then to delete the data "quietly"), and sometimes from multiple attackers (or rogue affiliates from the successful first attacker).**
- **While Law enforcement made big strides in taking down some Ransomware groups, the compelling financial motive ensured new criminal groups (or old ones reformed) to take their place.**

The Persistent Ransomware Threat

In 2023, Ransomware continued to pose the most dangerous cybersecurity threat, targeting organisations of all sizes, industries, and territories. Many organisations that Ensign has worked with over the past year updated their Ransomware strategy, playbook, and conducted cyber crisis training exercises to ensure they were prepared for this threat.

Ransomware-as-a-Service (RaaS) remained the dominant model, enabling novice criminal groups to get a piece of the action. Law enforcements, mostly collaborations between the US and Europe, had a very busy 2023 (and early 2024), attempting to slow the growth of Ransomware. In addition to taking down infrastructure of RaaS operators (Hive, ALPHV, LockBit, Ragnar),[11] Law enforcements also issued sanctions and/or took down malware used by those groups (Qakbot) in their attacks and cryptocurrency mixers to launder ransom payment (ChipMixer, Sibad.io).

Selected events in the fight against Ransomware by international enforcement

JAN 2023	Hive taken down by Law enforcement
MAR 2023	ChipMixer, used to launder ransom payment, taken down by Law enforcement
AUG 2023	
OCT 2023	Qakbot malware *(used by REvil, LockBit)* taken down by Law enforcement
NOV – DEC 2023	Ragnar Ransomware taken down by Law enforcement
DEC 2023	ALPHV taken down by Law enforcement
FEB 2024	Sibad.io sanctioned
MAR 2024	LockBit 3.0 taken down by enforcement
MAR 2024	ALPHV claimed to be taken down, but international enforcement denied involvement in its disappearance LockBit allegedly returned as LockBit 4.0

These takedowns, however, are likely to prove short term. Members of such groups either join "competitors" or reconstitute under a new brand. In March 2024, ALPHV used the late 2023 takedown screenshot to pull a disappearing act and scam its *own* criminal affiliate.[12] Meanwhile, after LockBit 3.0 was taken down, the group allegedly returned as LockBit 4.0.[13] Hive seemingly ceased all operations after Law enforcement takedown, but evidence suggested that its members had joined Hunters International. For cryptocurrency laundering, attackers would find another platform, just as they moved from Blender (sanctioned in 2022) to Sinbad.io (sanctioned in 2023).

In a guerilla warfare fashion, these attacker groups have demonstrated that they can reorganise themselves into new operations right after being "taken down". In these new operations, they may rebrand change the modus operandi, all while using the same malware, complicating investigations.

[11] E. Kovacs. *Law Enforcement Reportedly Behind Takedown of BlackCat/Alphv Ransomware Website*. (11 December 2023). Security Week. Retrieved from: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
[12] Vx-underground. *X.* (4 March 2024). Retrieved from: https://twitter.com/vxunderground/status/1764676460113994220
[13] J. Pearson. *Lockbit cybercrime gang says it is back online following global police bust*. (27 February 2024). Reuters. Retrieved from: https://www.reuters.com/technology/cybersecurity/lockbit-cybercrime-gang-says-it-is-back-online-following-global-police-bust-2024-02-26/

Double Extortion, Single Attacker

There are competitive dynamics even within the criminal underworld. RaaS operators continue to evolve their methods and shift their extortion techniques in order to extract more financial value from their targets, such as by employing tactics that increase the pressure on victims to pay the ransom. While the malware itself has only changed marginally last year, it is the tactics that have become more aggressive and dangerous. One of the notable changes to the malware last year was the use of the memory-safe and multi-platform language, Rust, by ALPHV.[14]

Traditional Ransomware attacks typically involve encrypting a victim's data and demanding payment for the decryption key. In 2023, there was an increase in what is known as "double extortion" tactics, whereby attackers steal the data first, then encrypt the systems. Subsequently, they threatened to release the stolen data publicly, creating reputational damage and regulatory problems for the company if the ransom for the decryption is not paid. Hunter International, the spin-off of Hive, differentiated itself from its predecessor by focusing more on data exfiltration and the subsequent extortion of public data release.

In another case, ALPHV wrote in to the US Securities and Exchange Commission directly to complain that their victim, MeridianLink, had not filed the relevant[15] forms within the mandatory four-day period. This serves as a clear example of how cybercriminals are weaponizing regulatory requirements, among other public humiliation tools, against their victims.

Double Extortion, Multiple Attacker Groups

Previous incidents proved that victims of Ransomware tend to be targeted repeatedly if they had demonstrated willingness to pay the initial ransom. Organisations in urgent need to pay the ransom to recover their systems often overlook conducting the proper forensics to identify the attack vector that compromised their networks in the first place. This often leaves the door wide open to other attackers (or affiliates of the first attacker, who are likely already aware of the initial exploit) to repeat the attack.

Individuals who form the criminal gang may also betray each other. One example of this is the aforementioned case, where the group who received the payment opted not to share the ransom with their own partners and disappeared. The partners, who were left empty-handed, tried to extort the victim (again).

In other cases, initial access brokers (the part of the group who provides the stolen credentials or entry point into the victim's network) sometimes "double dip" and resell the stolen data (especially credential information, which is their business model) even if the main group promised the victim that the data would be deleted.

All of this was brought to light when Law enforcement raided LockBit in early 2024, and discovered that LockBit servers retained data from victims, despite the gang's assurance that it had been deleted: "If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future". There is clearly no honour among thieves.[16]

Extortion, with an Added Dose of Doxing

Another way in which attackers increase pressure on victims is by contacting journalists or customers in parallel to shame the victim into paying. Occasionally, they will even publish samples of the data on social media, including personal details of the key leaders in the victim organisation. The victim organisation's leadership is now directly under pressure to resolve the incident quickly.

[14] Microsoft Threat Intelligence. *The many lives of BlackCat ransomware.* (13 June 2022). Microsoft. Retrieved from: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
[15] E. Kovacs. Ransomware Group Files SEC Complaint Over Victim's Failure to Disclose Data Breach. (16 November 2023). Security Week. Retrieved from: https://www.securityweek.com/ransomware-group-files-sec-complaint-over-victims-failure-to-disclose-data-breach/
[16] K. Meegan-Vickers. *The LockBit takedown Law enforcement 'trolls' ransomware gang.* (4 April 2024). Global Initiative. Retrieved from: https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/

A Worrisome Outlook

Ransomware continues to elude Law enforcement, cybersecurity regulators, and organisations — and this will continue to be the case for 2024. As the threat of Ransomware looks endemic for now, cyber defenders and insurers need to have endemic strategies. Organisations should continue to invest in sound cybersecurity practices like monitoring for unusual activity, identifying and protecting crown jewels, and having a robust and sensible backup strategy. More importantly, organisations must regularly activate backup restoration processes, instilling trust and confidence among corporate leaders in this viable alternative to paying the ransom.

Hacktivists, Unite: Increased Sophistication of Cause-aligned Groups

- **Hacktivism has become more sophisticated, as more capable individuals are drawn in by political causes, and they have easier access to more powerful cyber weapons.**
- **States are openly and deliberately mobilising their citizens and supporters and encouraging them to take part in cyber warfare against their opponents, and some states are masking state cyber activity as hacktivism to reduce attribution.**
- **Regional hacktivism activities have ramped up, as a direct spillover from faraway conflicts.**

Evolving Familiarity: Old News, Fresh Face

Hacktivism is malicious cyber activity conducted by threat actors that are motivated by a political or social cause. In the past, many of them acted alone or in small groups, with only the limited capabilities that they organically possessed. With the increasing availability of sophisticated cyber weapons and malicious talents on the Dark Web, these hacktivists have emerged as a serious and credible threat to governments and organisations, and have undergone significant evolution in recent times, which will require continual dynamic adaptation and response.

Unravelling Hacktivism's Growing Sophistication

Hacktivism has become increasingly sophisticated, as tactics used by hacktivists have diversified and now include a range of disruptive and destructive methods, including web defacement attacks of public-facing assets, distributed denial-of-service (DDoS) attacks, destructive Ransomware and Wiperware, and hacktivist-inspired data breaches.

At the simpler end of the spectrum, defacement attacks usually involve attackers altering a website's content, appearance, or functionality with malicious intent. Their main goals include defacing the targeted website, displaying a text or image, and spreading a message or agenda to the attacker's cause.

DDoS attacks often target organisations in countries deemed to be involved in conflicts. These attacks are conducted using botnets to overwhelm target systems with traffic to disrupt operations. There has been a significant increase of hyper volumetric HTTP DDoS attacks worldwide in the third quarter of 2023, in which Singapore was the second most targeted country (partly also due to the prevalence of corporate and Internet infrastructure nodes).[17] This can be attributed to threat actors leveraging a 0day, dubbed "HTTP/2 Rapid Reset" since August 2023. The attack employs the use of VM-based botnets consisting of nodes between 5,000 to 20,000 nodes, as opposed to the conventional use of millions of weak IoT devices.

The Israel-Palestine conflict has also witnessed significant cyber-attacks with destructive consequences, including the employment of Ransomware and Wiperware tactics. For instance, the BiBi malware family has been observed wiping data on both Linux and Windows computers in Israeli systems, and unlike other types of attacks, it is purely focused on destruction rather than any informational or financial benefit.[18]

[17] O. Yoachimik & J. Pacheco. *DDoS threat report for 2023 Q3.* (26 October 2023). Cloudflare. Retrieved from: https://blog.cloudflare.com/ddos-threat-report-2023-q3/
[18] B. Toulas. *Israel warns of BiBi wiper attacks targeting Linux and Windows*. (13 November 2023). Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/israel-warns-of-bibi-wiper-attacks-targeting-linux-and-windows/

Masking State-sponsored Activity Behind Hacktivism

State-sponsored threat groups typically work under direct instruction and funding from the state. With the recent developments seen in the Russia-Ukraine war, states called on to the people aligned to its cause to act for the state's interests.[19] Through these means, the state-sponsored actors exploit proxy agency to expand their capacity and obfuscate their identity by pretending to be independent hackers with activist motives, hence making it difficult to attribute the cyber-attack to a specific government or entity.

Originally White Hat cyber professionals, who are not criminal actors, may get influenced by certain causes or political agendas if it resonates with them. These professionals may leverage their expertise, skills, and access to conduct cyber activity in support of a hacktivist agenda. This may involve joining vigilante militias or engaging in unfunded campaigns directed by a state. For instance, the Vice Prime Minister of Ukraine tweeted a post on Twitter for individuals to hack or launch DDoS attacks on a list of Russian websites posted on a Telegram channel under their control.[20] The loose collective of the Ukraine IT Army was raised from a collective of technologists, from all parts of the world, many of whom were employed and acting for the cause during their free time. In some instances, they may also use their employer's assets and resources for the activities, further implicating their employers into the fight.

Russian authorities also turned a blind eye to cyber attackers operating from their territory, who went after Ukrainian targets. Hamas is also known to call upon their supporters to act in the cyber domain. New hacktivist collectives with alleged nation-state support have sprouted amid an increasingly volatile geopolitical environment, with some collaborating with other collectives to mount joint cyber-attacks. As these collectives take sides in contemporary geopolitical conflicts, undertaking high-profile operations against each other's targets, hacktivism will become an increasingly common occurrence.

Hacktivists' Targets Spread Far and Wide

Not only have websites belonging to both Israeli and Palestinian institutions been subjected to defacement attacks, but web assets of organisations located far beyond the warzone have been affected as well. Ensign has observed an increase in hacktivist activity amid a significant rise in geopolitical tensions and emerging conflict globally. While there was a surge in malicious cyber activity during the Russia-Ukraine conflict, the Israel-Palestine conflict took prominence in late 2023.

Within the region, hacktivists have also been known to deliberately breach and leak sensitive data. For instance, the Indonesia-focused threat actor, Bjorka, targets various government and corporate entities with a demonstrated ability to infiltrate systems and expose confidential material, with the aim of embarrassing its victims.[21] The impact has been significant, often with political or financial implications. In fact, these tactics employed by regional hacktivists have become increasingly similar to state-sponsored attackers.

Not only have websites belonging to both Israeli and Palestinian institutions been subjected to defacement attacks, but web assets of organisations located far beyond the warzone have been affected as well. Attacking other countries serves as a means of sending a message to actors perceived as allies or adversaries in the Israel-Palestine conflict.

[19] A. Render-Katolik. *The IT Army of Ukraine*. (16 August 2023). Center for Strategic and International Studies. Retrieved from: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine
[20] M. Burgess. *Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory*. (27 February 2022). Wired. Retrieved from: https://www.wired.com/story/ukraine-it-army-russia-war-cyber-attacks-ddos/
[21] L. Yulisman. *Indonesia hunts for Bjorka, hacker selling 1.3b SIM card users' data, taunting officials*. (19 September 2022). Bleeping Computer. Retrieved from: https://www.straitstimes.com/asia/se-asia/indonesia-hunts-for-bjorka-hacker-selling-13b-sim-card-users-data-taunting-officials

Threat actors supporting either side of the Israel-Palestine conflict may indiscriminately target Singapore-based companies that operate regionally, given that Singapore is perceived as pro-Israel while neighbouring countries such as Malaysia, Indonesia, and Brunei do not recognise Israel and have been vocal against Israel.

For instance, #OpSingapore, a campaign initiated by Indonesian and Malaysian pro-Palestinian hacker groups, targeted various Singaporean organisations in October 2023 shortly after Hamas' attack on Israel.[22] As a result, several websites were defaced, database breached, and sensitive data was leaked. The campaign was launched by a collective of self-styled hacktivist "collectives" led by 4 EXPLOITATION and AnonGhost Indonesian. These attacks, using tactics such as DDoS and SQL injection, are part of the #FreePalestine movement's effort to protest organisations perceived as supportive of Israel in the Israel-Palestine conflict.

In return, pro-Israeli groups, such as R00TK1T, have targeted sites located in Indonesia and Malaysia, successfully taking several of them offline.[23]

Given the far-reaching effects of hacktivism, organisations must recognise that despite their espoused lack of political allegiance or proximity to the conflict, they remain susceptible to the actions of opportunistic and state-sponsored threat actors who may find an indirect reason to target their organisation or opt to use an attack on their organisation to send a political signal to a third party, such as a customer, partner, or even the government.

Hacktivism as a Tool-for-Attack has Made its Mark and is Here to Stay

Hacktivism, with the use of advanced technological tools and techniques, has cemented itself as a tool utilised by cause-aligned individuals, groups, and even states. As technology progresses and new vulnerabilities emerge, the sophistication and scale of hacktivist attacks are anticipated to evolve. Sophisticated hacktivism is likely to persist as a significant challenge in the digital age, with the potential for increased proliferation and escalation.

[22] *Heightened Alert for Cyber Activities Targeting Domains and Infrastructures in Malaysia*. (27 February 2022). National Cyber Coordination and Command Centre. Retrieved from: https://www.nc4.gov.my/alert/653a2988900885a0819d058d
[23] *MA-1027.022024: MyCERT Advisory - Recent Cyber Incidents Launched by TA ROOTK1T ISC Team to Malaysia Organisations*. (6 February 2024). Malaysia Computer Emergency Response Team. Retrieved from: https://www.mycert.org.my/portal/advisory?id=MA-1027.022024

Moving beyond Hacktivism

Increasingly, hacktivist groups are growing bolder and more competent with each successive cyber-attack. Some have started to develop novel tools and solutions to perform their attacks, others have quickly leveraged their access to leaked source code for Ransomware (e.g. the LockBit Black version, released during the Law enforcement blitz on the LockBit Gang) to evolve into organised crime groups. Two notable examples of hacktivist groups active in our region who have expressed intents to evolve into organised crime groups include DragonForce Malaysia and GhostSec.

DragonForce Malaysia had declared that they are moving into Ransomware operations.[24] Analysts suggest that while it is unnatural for hacktivist groups to perform cyber-attacks for financial gain, it is more likely a means to gain funds to build up capabilities or "marketing".

On a similar but different track, the GhostSec group had not only developed a DDoS tool, CyberTroopers,[25] and subsequently collaborate with the Stormous Group to perform Ransomware attacks using the GhostLocker 2,0 Ransomware.[26]

Such developments are indications that hacktivists may progressively grow from being a loose collective of individuals to a more organised and structured group funded by illicit gains to carry out their cause. This may in turn help the cyber defenders gain better understanding of the protocols and behaviours of the groups that develop down this path.

[24] N. Eddy. *DragonForce Malaysia Releases LPE Exploit, Threatens Ransomware.* (1 July 2022). Dark Reading. Retrieved from: https://www.darkreading.com/vulnerabilities-threats/dragonforce-malaysia-releases-lpe-exploit-threatens-ransomware
[25] G. Sharma. DragonForce Malaysia attacks Israeli institutions: Radware. (14 April 2023). Security Brief. Retrieved from: https://securitybrief.asia/story/dragonforce-malaysia-attacks-israeli-institutions-radware
[26] *Alert: GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries.* (6 March 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/03/alert-ghostsec-and-stormous-launch.html

EVOLVING ATTACKS

Digital Infrastructure Under Fire: Threats Across the Cyber Supply Chain

- **Threat actors are investing in exploits targeting vulnerabilities in common infrastructure solutions across all technology layers, including endpoint, middleware, network, hardware, and operational technology (OT).**
- **There is an urgency to map and understand the digital attack surface we operate in and determine exposure.**
- **Cyber supply chain risk management might often be impossible for direct influence but must be planned and managed to limit cascading and widespread effects across systemic dependencies.**
- **Threat and Vulnerability Exposure Management is an increasingly important priority for organisations.**

Watershed Year for Actively Exploited Vulnerabilities across Digital Infrastructure

2023 was the year where many vulnerabilities were discovered and exploited across the fundamental digital infrastructure components, including endpoint, middleware, network and hardware. Noteworthy exploit campaigns – BadCandy, CitrixBleed, MOVEit, PaperCut – when combined with many network solution vulnerabilities relating to Barracuda Networks, Cisco, Fortinet, Zyxel (amongst others), have led to widespread and cascading implications across the cyber supply chain. While we often hear practitioners advocating a multi-layered defence concept to defend their digital attack surface, when all layers of technology come under threat, the opportunities to compromise elevates.

Active Campaigns Compromising Organisations

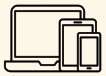
CitrixBleed. The vulnerabilities associated with Citrix NetScaler SDC and Datacenter leak information which supports reconnaissance and targeting. CitrixBleed was notably employed by **LockBit Gang** to compromise Allen & Overy, Boeing, ICBC and DP World.[27]

MOVEit: The vulnerabilities associated with the MOVEit managed file transfer solution allowed authentication bypass and access to the database there by exposing the contents for exfiltration and providing a pathway for further compromise. The MOVEit vulnerability was exploited by **FIN11** to compromise a large number of victims[28] (estimated to number more than 2,500 companies and more than 80 MM individuals). Some of the noteworthy companies include Fortescue, Medibank, Prudential Malaysia, PwC, Shell, Sony, amongst others.

PaperCut: The vulnerabilities associated with the PaperCut NG vulnerabilities allowed authentication bypass and code execution, providing access and data to threat groups. **Cl0p**,[29] **LockBit Gang**, **MuddyWater**, and **APT35**.

Ivanti Pulse Secure VPN: The vulnerabilities associated with the Ivanti Pulse Secure VPN allowed authentication bypass and execute arbitrary commands. Noteworthy victims included The MITRE Corporation[30] and CISA.[31]

[27] B. Toulas. *LockBit ransomware exploits Citrix Bleed in attacks, 10K servers exposed.* (14 November 2023). Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-exploits-citrix-bleed-in-attacks-10k-servers-exposed/
[28] B. Kondruss. *MOVEit hack victim list*. (20 December 2023). Retrieved from: https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html
[29] C. Page. *PaperCut says hackers are exploiting 'critical' security flaws in unpatched servers*. (25 April 2023). Techcrunch. Retrieved from: https://techcrunch.com/2023/04/25/papercut-hackers-critical-fLaw-clop-ransomware/
[30] S. Gatlan. *MITRE says state hackers breached its network via Ivanti zero-days.* (19 April 2024). BleepingComputer. Retrieved from: https://www.bleepingcomputer.com/news/security/mitre-says-state-hackers-breached-its-network-via-ivanti-zero-days/
[31] K. Alspach. *CISA Breached Via Ivanti VPN Vulnerabilities: Report.* (8 March 2024). CRN. Retrieved from: https://www.crn.com/news/security/2024/cisa-breached-via-ivanti-vpn-vulnerabilities-report

Category	Vulnerability Description
Endpoint 	• Apple mobile devices WebKit (CVE-2023-42916) • Apple iOS Kernel (CVE-2024-23225) • Apple RTKit (CVE-2024-23296) • Windows Virtualization-based Security HVCI (CVE-2024-21305)
Middleware 	• Fortra GoAnywhere managed file transfer (CVE-2023-0669) • JetBrains TeamCity (CVE-2023-42793) • Microsoft Outlook (CVE-2023-23397) • MOVEit managed file transfer (CVE-2023-34362, CVE-2023-36932, CVE-2023-36933, CVE-2023-36934) • PaperCut NG managed file transfer (CVE-2023-27350, CVE-2023-27351) • VMware vCenter Server (CVE-2023-34048) • WinRAR (CVE-2023-38831) • Zoho ManageEngine (CVE-2022-47966)
Network 	• Barracuda ESG (CVE-2023-2868) • Cisco ASA and FTD Software VPN (CVE-2023-20095, CVE-2023-20269) • **BadCandy**:- Cisco IOS XE (CVE-2023-20198, CVE-2023-2073) • **CitrixBleed**:- Citrix NetScaler ADC & Gateway (CVE-2023-4966, CVE-2023-4967, CVE-2023-6548, CVE-2023-6549) • Fortinet FortiOS & FortiProxy (CVE-2023-44250) • Ivanti Pulse Connect VPN (CVE-2023-46805, CVE-2024-21887) • Juniper SRX EX Junos (CVE-2024-21591 • SonicWall NGFW (CVE-2022-22274, CVE-2023-0656) • Zyxel ATP, USG FLEX, and ZyWall VPN Firewalls and gateways (CVE-2023-28771) • Zyxel ATP, FLEX, ZyWALL VPN Firewalls and gateways (CVE-2023-33009, CVE-2023-33010, CVE-2023-33012)
Hardware 	• Arm Mali chipset GPUs (CVE-2023-4211, CVE-2023-33200, CVE-2023-34970) • **CacheWarp**:- AMD processors (CVE-2023-20592) • **Downfall**:- Intel Core processors from 6th (Skylake) to 11th (Tiger Lake) generation (CVE-2022-40982) • **Inception**:- AMD Ryzen, Threadripper and EPYC processors based on Zen 4 architectures (CVE-2023-20569) • **PixieFail**:- UEFI implementations of Arm, Insyde Software, American Megatrends, Phoenix Technologies and Microsoft (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237) • **Reptar**:- Intel desktop, mobile and server processors (CVE-2023-23583) • **Zenbleed**:- AMD Ryzen Zen 2 processor (CVE-2023-20593)
Operational Technology 	• Honeywell Experion PKS, PlantCruise, Safety Manager (CVE-2023-5389, CVE-2023-5390, CVE-2023-5392, CVE-2023-5393, CVE-2023-5394, CVE-2023-5395, CVE-2023-5396, CVE-2023-5397, CVE-2023-5398, CVE-2023-5407, CVE-2023-5400, CVE-2023-5401, CVE-2023-5402, CVE-2023-5403, CVE-2023-5404, CVE-2023-5405) • OMRON PLCs and Machine Automation Controllers (CVE-2023-27396) • Rockwell Automation ControlLogix (CVE-2023-3595) • Rockwell Automation 1756 Ethernet solutions (CVE-2023-3596) • Scheider Electric Interactive Graphical SCADA System (CVE-2023-4516) • SIEMENS SIMATIC IPC and SIMATIC NC 4000 (CVE-2023-49621, CVE-2023-51438)

Non-exhaustive list of noteworthy vulnerabilities observed across to be under exploit in 2023 and 2024.

APT28 and Volt Typhoon had their botnets dismantled by Law enforcement which unveiled that they were operating different botnets, MooBot and KV Botnet respectively. MooBot was established with compromised Ubiquiti EdgeRouters, while KV Botnet was made up of compromised devices – NetGear ProSAFE, Cisco RV 320/325, Axis IP cameras, DrayTek Vigor devices. These discoveries indicate that the Ransomware groups are quick to exploit the 0day vulnerabilities to rapidly amass victims and increase their rates of return from ransoms.

All these effects conclude that there is sustained interest to target the cyber supply chain, (1) to obtain computing resources, (2) leverage compromised devices for proxy and network relay, (3) to perform information theft and espionage, and (4) to establish a foothold for eventual compromise and disruption.

Rise in Vulnerabilities Reported while Analysis Lags

There has been a noticeable number of vulnerabilities reported between 2022 and 2023. It was estimated to be more than 20% increase.[32] However, despite the emphasis on the CISA known exploited vulnerabilities catalogue (KEVC), NIST-run National Vulnerability Database (NVD) has in recent months been found to lag in performing analysis.[33] This is an emerging issue which will progressively cripple cyber defenders in performing risk analysis and patch prioritisation.

While fighting the vulnerability management battle has been a perennial challenge for cyber defenders, the coincidence of these vulnerabilities across endpoint, middleware and network solutions and hardware further exacerbate the problems as hardware mitigations are often limited and may require physical replacements which may be tied to technology refresh cycles in the span of years.

Open Source Resources act as Watering Holes for Malware

Starting in 2022, a threat actor started contributing to the XZ Utils, which is an open-source project popular with Linux developers. Over the course of two years, the threat actor gained more credibility with the community, creating fake accounts for feature requests that enabled him to become a maintainer.[34] Finally, in 2023, the threat actor introduced a sophisticated backdoor during a release. The vulnerability was discovered in April 2024. Similarly, other open-source code repositories injected with malicious codes were also observed, such as in the Python ecosystem in 2023 through PyPI.[35]

Studies on malware found in GitHub repositories have uncovered more than 100,000 infected repositories despite the automated scanning services.[36] While GitHub is an attractive watering hole vector (targeting specific groups of developers), the threat intelligence community may also be at risk. A recent academic study showed that Large Language Models (LLMs) can create exploits from reading vulnerability advisories.[37] The researchers concluded that 9 out of the 10 LLMs, which included Meta's Llama 2 and GPT-3.5, could not exploit a single vulnerability. Meanwhile, GPT-4, successfully exploited 87% of the vulnerabilities in the study. As LLMs continue to be more advanced, they will lower the barrier to exploit for attackers. Under Ensign Threat Classification Matrix, a threat can go from the least concerning ("Insubstantial Threat") to the most concerning ("Material Threat") if they obtain "Capability". Open-source resources such as advisories from vendors, researchers and authorities may become ingredients for attackers using LLMs in the future, subject to new safeguards by regulators and Big Tech.

[32] E. Madnick. *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*. (December 2023). Apple. Retrieved from: https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf
[33] J. Munshaw. *What's the deal with the massive backlog of vulnerabilities at the NVD?* (19 April 2024). Talos Intelligence. Retrieved from: https://blog.talosintelligence.com/nvd-vulnerability-backlog-the-need-to-know/
[34] *XZ Utils Backdoor — Everything You Need to Know, and What You Can Do*. (1 April 2024). Akamai. Retrieved from: https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know
[35] *Dormant PyPI Package Compromised to Spread Nova Sentinel Malware.* (23 February 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/02/dormant-pypi-package-compromised-to.html
[36] R. Daws. *GitHub suffers from over 100K infected repos*. (29 February 2024). Developer. Retrieved from: https://www.developer-tech.com/news/2024/feb/29/github-suffers-over-100k-infected-repos/
[37] N. Nelson. *GPT-4 Can Exploit Most Vulns Just by Reading Threat Advisories*. (19 April 2024). Dark Reading. Retrieved from: https://www.darkreading.com/threat-intelligence/gpt-4-can-exploit-most-vulns-just-by-reading-threat-advisories

Vendor Compromises Implicate Customers

The Okta breach of October 2023 had caused downstream implications to its customers. Noteworthy victims resulting from the breach included BeyondTrust, 1Password[38] and CloudFlare.[39] All direct victims could have led to more indirect victims.

Deliberate attacks through the vendor and supply chain are also observed through legitimate software update mechanisms. The NSPX30 spyware[40] was seen inserted through software update mechanisms of legitimate software such as Tencent QQ, WPS Office, and Sogou Pinyin. These approaches can allow passthrough compromise into the desired target victims such as in the manufacturing, trading and engineering industry groups.

The exploitation of JetBrains TeamCity Servers could also mean that organisations using the solution to manage their code repositories could be used by threat groups such as the Lazarus Group to inject malicious code into eventual solutions which could play out like the SolarWinds supply chain compromise of 2020.

The full-blown effect of the cyber-physical implications of supply chain compromise is best represented in the cyber-attack on DP World which crippled shipping and logistics in Australia, which caused the movement of approximately 30,000 containers to be halted until systems recover.

Vulnerability and Exploitation at the Processor Level

With each year, we are seeing increased vulnerabilities and exploit codes shared targeting the processors which support and drive the modern-day computing infrastructure. The successive vulnerabilities of CacheWarp, Downfall, Inception, PixieFail, Reptar and Zenbleed affect all major commonly used processors in our mobile, desktop and server computers, impacting brands such as Intel, AMD, Arm chipsets, as well as the supporting computing components such as the unified extensible firmware interface (UEFI) which is the first initialisation software for any computer, interfacing the hardware components to the operating system. With these vulnerabilities and compromise, there are multi-layered challenges presented:

1. Mitigations implemented through microcode updates at the motherboard and the operating system may not fully address the vulnerabilities;
2. Some vulnerabilities target the physical architecture and design of the processors which requires physical replacement / upgrade to address the risk exposure; and
3. Because the use of processors are embedded into all computing infrastructure, the pervasiveness of the vulnerabilities by volume and reach is extremely high.

All these contribute to an even more complex cyber supply chain risk management problem.

Investments into Targeting Operational Technology

Cyber-attacks targeting OT environment were more sophisticated. In 2022, Ensign saw the emergence of the OT exploit framework — PIPEDREAM. In 2023, Ensign saw the development of COSMICENERGY, which was targeted at SQL databases connected to IEC 60870-5-104 (IEC-104) devices such as RTUs. These devices are commonly found in utility companies in Asia.[41] COSMICENERGY is the second instance in recent times where exploit tools are created to target OT. This indicates continued interest and investments into the compromise of OT affecting essential services.

[38] C. Jones. *1Password confirms attacker tried to pull list of admin users after Okta intrusion.* (24 October 2023). The Register. Retrieved from: https://www.theregister.com/2023/10/24/1password_confirms_all_logins_are/
[39] K. Alspach. *Cloudflare Discloses 'Limited' Impact From Okta Breach.* (1 February 2024). CRN. Retrieved from: https://www.crn.com/news/security/2024/cloudflare-discloses-limited-impact-from-okta-breach
[40] *China-backed Hackers Hijack Software Updates to Implant "NSPX30" Spyware*. (25 January 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/01/china-backed-hackers-hijack-software.html
[41] R. Lakshmanan. *New COSMICENERGY Malware Exploits ICS Protocol to Sabotage Power Grids*. (26 May 2023). The Hacker News. Retrieved from: https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html

As OT infrastructure often has national security implications, state-sponsored threat actors have spent more resources in infiltrating OT environment with the intent to cause disruption as one of the possible effects or to enable negotiations for geopolitical interests.

Aside from state sponsored threat groups, Ensign has also observed hacktivist groups, such as the CyberAv3ngers targeting OT environment with weaker cyber-hygiene. CyberAv3ngers successfully breached and accessed a water facility managed by the Municipal Water Authority of Aliquippa relating to Unitronics programmable logic controllers (PLCs).[42]

Asset Visibility Gap Persistent in Organisations

Many organisations admit that they have a less than complete visibility of the assets in their technology environment. In many of Ensign's clientele, we also observed that they struggle with understanding the appropriate context of which threat groups they should be concerned with and how they should manage their threat exposure. These two gaps combined represent a significant risk gap which affects the organisations and inhibit their ability to be sufficiently situation aware and be able to direct resources to perform vulnerability and management, and relevant mitigations.

According to a study performed by the Enterprise Study Group,[43] 73% of organisations surveyed had strong awareness of less than 80% of their assets. This is representative of the gap of monitoring across the organisations' digital attack surface. Without consideration of the challenges in addressing shadow IT, this is already a significant gap to be resolved.

[42] E. Stanish. *Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group*. (26 November 2023). CBS News. Retrieved from: https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

[43] *Security Asset Management Statistics to Know in 2023*. (18 May 2023). Noetic Cyber. Retrieved from: https://noeticcyber.com/security-asset-management-statistics-to-know-2023/

Prioritising the Right Vulnerabilities

Ensign conducted an analysis of a sample of vulnerabilities active during the second half of 2023. Out of nearly 150,000 vulnerabilities, about 57% of them are rated high or critical (scored 7 and above) by common vulnerability scoring scheme (CVSS), while the other 43% are rated low or medium.

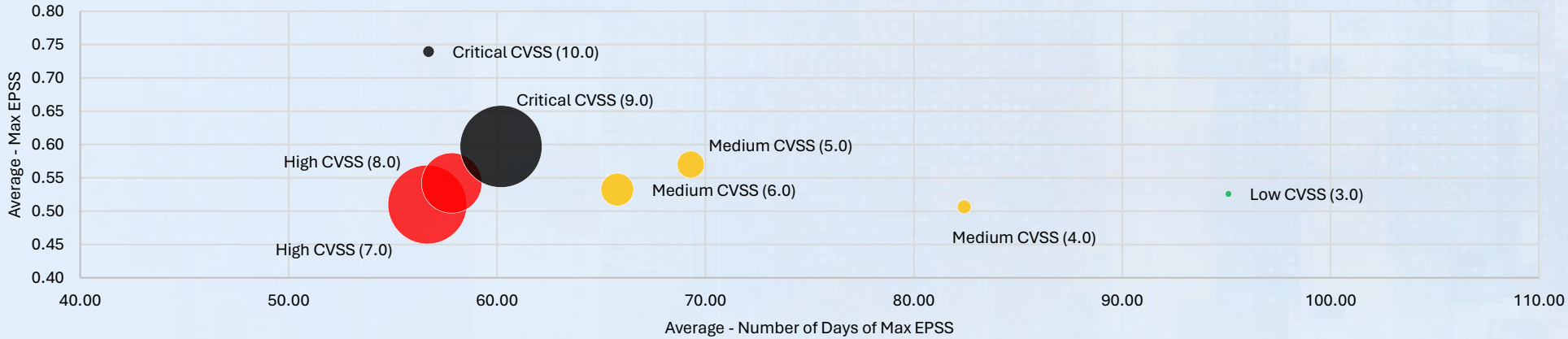
However, not all the high or critical CVSS are exploited heavily during the period. Nearly 4,000 of High/Critical CVSS vulnerabilities reached an exploit prediction scoring scheme (EPSS) of at least 0.1 during the period. This number is reduced to just over 1,000 vulnerabilities, whose EPSS reached at least 0.9 (very likely exploited) during the period.

Meanwhile, only about 500 Low/Medium vulnerabilities ever reached an EPSS of at least 0.1 during the period. While the volume of these Low/Medium vulnerabilities may be much smaller, in terms of their exploitability, they don't look different from the High/Critical vulnerabilities with similar scores, refer to chart below. Similar to the High/Critical vulnerabilities, about a quarter of these vulnerabilities reached an EPSS score of at least 0.9 during the period.

The graph below shows the sample of vulnerabilities whose EPSS reached at least 0.1 during the second half of 2023. The Y-axis shows the maximum EPSS the vulnerabilities during this period (i.e. the vulnerabilities were most exploited). The X-axis shows how long the vulnerabilities stayed at their maximum EPSS (i.e. the period where they were most exploited).

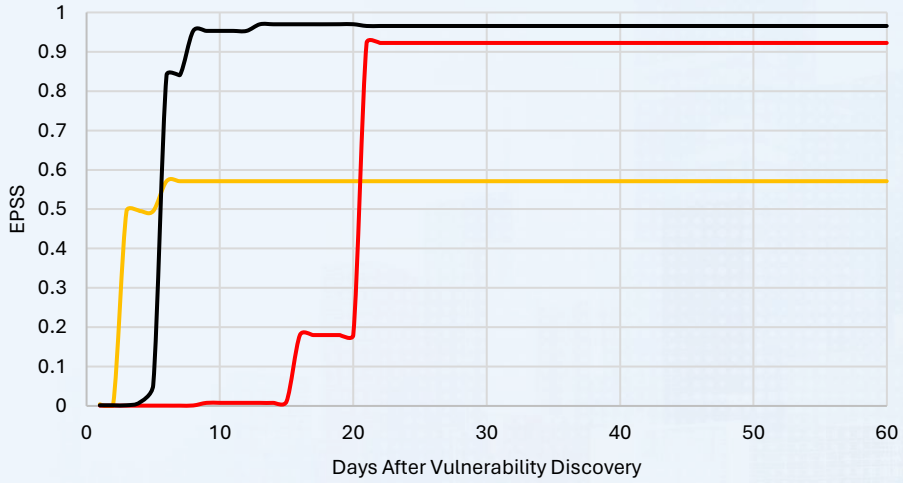
Based on the sample of vulnerabilities, a few observations can be made:

1. The small sample of Low CVSS stayed at their peak exploitability during this period (more than 3 months compared to 2.0–2.5 months for the other vulnerabilities), most likely because for most organisations, these vulnerabilities were not high priority for patching.
2. Medium CVSS (4.0), on average, had a long period of maximum exploitability, likely because they are overlooked. While organisations may rightly prioritise on Critical CVSS vulnerabilities over Medium and High CVSS ones, it is not necessarily a great idea to prioritise High CVSS vulnerabilities over Medium CVSS. As seen, Medium CVSS vulnerabilities in this sample have similar, if not higher, maximum EPSS compared to High CVSS vulnerabilities.



Note: Bubble size represents the number of vulnerabilities in each group

From a previous analysis, Ensign noticed that on average, EPSS scores for vulnerabilities tend to increase around one-week mark and then again around the three-week mark, which could be due to their graduation from "proof-of-concept" to "winner" vulnerabilities. In this analysis, we look at EPSS of three illustrative vulnerabilities. The graph below shows three vulnerabilities Ensign observed in Singapore, which were also included in this analysis. Ensign notes that in this example, the medium vulnerability was more readily exploited than the High and Critical vulnerabilities.



In this data set of vulnerabilities whose EPSS reached at least 0.1 during the second half of 2023, Critical CVSS (9.0 and 10.0) and Medium CVSS (5.0) reached EPSS 0.1 around the one month after discovery. They reached their maximum exploitability (highest EPSS in the period) within the two-month mark. The other vulnerability groups reached EPSS of 0.1 within one-and-a-half to two months of discovery. They reached their maximum exploitability (highest EPSS in the period) within two-and-a-half months after discovery.

Knowing the pattern of vulnerability exploitation would be useful for defenders. While CVSS is still a useful tool to prioritise patching (particularly for identifying Critical CVSS), they may not be sufficient, especially with increasing volume of vulnerabilities. Within one week (or less) of a vulnerability being identified, exploitation may already be in full swing. Even if a vulnerability is not fully exploited within the first week of discovery, around three-week mark, interest in its exploitation may increase quickly.

Regardless of CVSS score, patching for the vulnerability should be ramped up if there is a sharp increase in EPSS (i.e. attackers are finding success in exploiting the vulnerability). Where possible, automated patching should be employed to prevent exploitation of 0day vulnerabilities.

Exploiting the Defender's Playbook

The driving reason behind Ensign's analysis was to attempt at uncovering why cyber-attacks are still prolific when an organisation may already have a reasonable level of compliance to established standards.

Through the continued analysis, we realised that the threat actors have learnt to exploit the defenders' practices:

1. Patching High and Critical severity vulnerabilities first (e.g. in the matter of weeks), and leaving those with lower severity to be patched in months. At times even accepting the risk of not patching certain vulnerabilities through some reasoned process.
2. There is an inherently high backlog of unpatched systems. Especially with organisations still struggling to map out their assets and connecting their systems with patching solutions to increase patch scalability and efficiency.

Collectively, these practices and challenges, exploited by the threat actors, give away the opportunity for them to breach the technology environment and defences, maintain persistence, and perform lateral movement till they achieve their desired objectives.

It is with some wisdom that the UK NCSC had recently urged organisations to be more cognizant of the vulnerability exposure window with guidelines recommending for more rapid patching timelines to quickly close the vulnerability exposure window regardless of the severity.[44]

TYPE OF ESTATE	ROLLOUT	UPDATE COMPLETED WITHIN
Internet-facing services and software	Install on test environment or backup first. Test and rollout (a phased rollout can be used if applicable).	5 days
Operating system and applications	These updates should be applied automatically, as soon as an update is published. Phased rollout, for example, 10% of the estate, updated per day. Pause/rollback if issues encountered	7 days
Internal/air-gapped service and software	Install on test environment or backup first. Test and rollout	14 days

Best Practice Timescales taken from UK NCSC's Guidance on Vulnerability Management.

From our engagements with our clients, there is room to consider prioritising vulnerabilities with high EPSS, but also to shift down the priority for vulnerabilities which may have lower EPSS scores. This approach may avail some breathing space for the administrators as they go through the volume of patching tasks they must perform.

Addressing the Gaps

Organisations will do well to perform some of these key steps to better address the threat and vulnerability exposure due to the supply chain:

1. Map the 1st degree vendors and profile their threats and vulnerabilities to the organization and manage associated risks;
2. Perform threat profiling for the organization, highlighting the threat groups and associated behaviours (i.e. TTPs) based on business nature, territory exposure and recency;
3. Check identified TTPs in MITRE ATT&CK Framework to determine applicable Mitigations and Detection Data Sources;
4. Compare and determine threat-mitigation and threat-detection gaps, and set out plans to close them;
5. Map out, first, the critical assets for hardware (hardware bill of materials) and software (software bill of materials), and progressively expanding into non-critical assets;
6. Monitor and evaluate vulnerability exposure beyond severity ratings (i.e. CVSS) and consider EPSS for prioritization;
7. Implement automated patching solutions which can accelerate patching to close the vulnerability exposure windows faster and more efficiently; and
8. Consider implementing a continuous threat exposure management solution to monitor and manage the gaps.

[44] *Vulnerability management*. National Cyber Security Centre. Retrieved from: https://www.ncsc.gov.uk/collection/vulnerability-management/guidance/policy-update-by-default

EMERGING RULES

Digital Sheriffs: New Regulatory and Policy Initiatives that Aim to Address Risks of Emerging Technology

- **Cybersecurity and data privacy regulations are ratcheting up across the region and globally, and the approaches differ slightly; compliance across multiple jurisdictions will get harder. Incident reporting is now commonplace, but differences in timelines complicate reporting for large organisations.**
- **Countries are attempting to address hardware security requirements (through labelling schemes for network devices, OT, IOT, Medical devices) and supply chain risks (e.g. by requiring SBOM and vulnerability management), which are new and important initiatives.**
- **AI regulations are on the far horizon but lack clarity and specificity for now. Most nations will have voluntary guidelines in the near term.**

New Cybersecurity Regulations Will Raise Baselines Regionally

Singapore's proposed amendments for the original Cybersecurity Act (2018) will add oversight over cloud service providers, among other entities. Ensign was invited to provide feedback on the draft and will present a more comprehensive analysis once the Act is passed in 2024.

In **Malaysia**, the newly passed Cyber Security Bill (2024) defines 11 critical infrastructure sectors and outlines new obligations for entities in these sectors.

Philippines, as part of their National Cybersecurity Plan (NCSP) 2023–2028, will create new legislation to address cybersecurity, including the protection of CII sectors, incident reporting requirements, and a cybersecurity labelling scheme for devices.

Indonesia has made significant strides with the Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management, which was enacted in July 2023. Indonesian Presidential Regulation no. 47 of 2023 on National Cyber Security and Cyber Crisis Management Strategies (PR 47/2023) was released in mid-2023 and lays out the actions to be taken by the state cybersecurity authority (BSSN) with support from Electronic Service Providers before, during, and after a cybersecurity crisis.

Thailand already has existing cybersecurity legislation and will implement new cybersecurity standards in 2024 and 2025. A notable update includes the requirement for key organizations to assess their systems and set security categories based on the highest risk level.

Australia proposed clarifications on entities and systems in the scope of the Security of Critical Infrastructure (2018), and the spate of cyber incidents has renewed political attention on enhancing the compliance and reporting requirements for key organisations.

Critical Information Infrastructure Sectors

AUSTRALIA

- Communications
- Financial Services and Markets
- Data Storage or Processing
- Defence Industry
- Higher Education and Research
- Energy
- Food and Grocery
- Health Care and Medical
- Space Technology
- Transport; and
- Water and Sewerage

EU

- Energy
- Transport
- Banking
- Financial Market
- Health
- Drinking Water
- Waste Water
- Digital Infrastructure
- ICT Service Management
- Public Administration
- Space
- Postal and Courier
- Waste Management
- Manufacturing, Production and Distribution of Chemicals
- Production, Processing and Distribution of Food
- Manufacturing
- Digital Providers
- Research

MALAYSIA

- Government
- Banking and Finance
- Transportation
- Defence and National Security
- Information, Communication and Digital Services
- Healthcare services
- Water Sewerage and Waste Management
- Energy
- Agriculture and Plantation
- Trade, Industry and Economy
- Science, Technology and Innovation

SINGAPORE

- Energy
- Water
- Banking and Finance
- Healthcare
- Transport (Including Land, Maritime, Aviation)
- Infocomm
- Media
- Security and Emergency Services
- Government

USA

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defence Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, Waste
- Transportation System
- Water and Wastewater

In 2016, the EU implemented the National and Information Security Directive (NIS1), establishing a common cybersecurity framework for member states, targeting essential service operators and digital service providers across various sectors. By early 2023, the updated NIS2 directive expanded regulatory scope and specified enhanced capabilities for national cybersecurity teams, with an implementation deadline set for October 2024. Meanwhile, in the US, the 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) mandated rapid reporting of cybersecurity incidents and ransom payments by covered entities. In 2024, CISA introduced further regulatory proposals under the Notice of Proposed Rule Making (NPRM).

Cybersecurity Incident Reporting — A Challenging but Necessary Measure

Critical infrastructure entities are not the only entities with tougher requirements for reporting cybersecurity incidents in the US. In mid-2023, the US Securities and Exchange Commission (SEC) adopted a rule that requires publicly-listed companies to disclose cybersecurity incidents within four business days after the companies have determined that such incidents are “material”. In late 2023, the US Federal Communications Commission (FCC) expanded the scope of data breach notification rules for telecommunications firms (to be effective in 2024). Breach of data, including cases of negligence, of at least 500 customers, is to be reported

to the FCC within seven business days after reasonable determination of breach.

Under CIRCA and CISA's NPRM, entities under 16 critical infrastructure sectors have a 72-hour deadline for reporting incidents of serious impact (among other criteria). In addition, if there is any ransom payment in a Ransomware incident, such payment must be reported to CISA within 24 hours, even if the Ransomware incident is not a reportable incident. In comparison, in Europe, NIS2 Directive also set new reporting obligations for critical infrastructure entities under its scope. Within 24 hours of awareness of significant incidents or warning signs of significant incidents, these entities must report to their respective CSIRTs, to be followed up within 72 hours of such awareness.

The SEC ruling reflects the recognition of cybersecurity as a potential existential risk for businesses and their valuations. A major cybersecurity incident may result in loss of intellectual property, loss of reputation or in millions of dollars in legal fees and damages, which lowers the medium-to-long-term growth of the business. As a result, a timely disclosure of cybersecurity incidents is needed to help investors make informed decisions. Sensitive data obtained in a cybersecurity incident may also be used for insider trading. In another 2023 case, SEC subpoenaed a private Law firm who suffered a breach, because the private Law firm served publicly-listed companies. The Law firm fought the order, but the court agreed with the SEC on the basis of potential insider trading violation.

Transparency from timely disclosure of incidents not only protects investors but also alerts national defenders of potential widespread campaigns or potential disruption reverberating across the economy. Cooperation across Law enforcement, administrative bodies, and industries may be needed when a major incident or campaign has hit critical infrastructure, whose disrupted operations become a crisis.

Compliance Requirements Protect Product Manufacturers and Tech Sectors Against Supply Chain Attacks

Singapore's development of the Cybersecurity Labelling Scheme (CLS) for IOT devices has borne fruit and is being expanded to include Medical Devices locally. Philippines is expected to introduce a CLS as well. It is widely expected to become a global ISO standard shortly. The US FCC formally announced the adoption of the US Cyber Trust Mark, a voluntary cybersecurity labelling scheme for IoT devices. In the EU-US Joint Cyber Safe Products Action Plan in early 2024, the regulators from both sides of the pond expressed the desire to align the EU CRA with the US Cyber Trust Mark.

The EU is expected to pass a new Cyber Resilience Act (CRA) in 2024. The CRA lays out the requirements that software and hardware (including components) need to achieve before they are sold in the market. While NIS2 focuses on the services provided by organisations in critical sectors, CRA focuses on the technology products used by those organisations. It is worth noting that AI systems that are deemed compliant with the CRA will also be deemed compliant with the EU Artificial Intelligence Act (2024), subject to conformity assessment set out in the CRA.

The CRA may inspire other regulations for hardware and software used in critical infrastructure around the world. Such regulations are meant to tackle one of the most notorious types of attacks — supply chain attacks, namely SolarWinds in 2020, log4Shell in 2021, and MoveIT in 2023. The CRA only has two categories of essential requirements for products under its scope, one of which is vulnerability handling. Under vulnerability handling, manufacturers are mandated to produce and maintain Software-Bill-of-Materials (SBOM). This will not just benefit critical infrastructure operators but also other entities who use these products. Similarly, organisations will benefit from the Information and Vulnerability Common Database established under NIS2.

Cybersecurity of Medical Devices to Protect Easy-to-target Healthcare Sector

Globally, and in the US specifically, the healthcare sector is one of the most targeted sectors and often suffers the most severe impact from cyber-attacks. Organisations in the sector hold a trove of valuable data, yet they often underinvest in technology infrastructure and cybersecurity compared to other regulated sectors, such as finance. Prolonged disruption due to cyber-attacks can result in life-or-death consequences, ranging from potential cessation of medical devices to the denial of payment of vital medications, which puts pressure on executives to acquiesce to attackers' demands.

In this regard, specifically in healthcare sector, efforts are being made to standardise IoT devices, also known as Internet-of-Medical-Things (IoMT). In Singapore, the Cyber Security Agency (CSA) held the public consultation for the Cybersecurity Labelling Scheme for Medical Devices in early 2023 and completed the trial in the second half of 2023. The US Food and Drug Administration issued additional guidelines on medical device security in 2023 and early 2024, following the "Ensuring Cybersecurity of Medical Devices" section of the bill passed in Dec 2022.

While it remains to be seen how the US election this November will play out, it is evident that cybersecurity receives bi-partisan support.

Governance of Artificial Intelligence is Still Unclear

In the rush to ensure that there are some guidelines for organisations using AI, there are now an overwhelming number of high-level documents in the public domain, crafted by all manner of organisations (in fact, there are multiple unrelated documents within each country alone). Unfortunately, these documents have not helped organisations gain clarity on exactly what to do, partly because they lack specificity. Technologists are still trying to determine exactly what the security of AI should look like, as the "probabilistic" nature of AI is a new software paradigm and requires different security tools and techniques from the more "deterministic" algorithmic software that defines the current era. Until we have a clear standard and viable commercial solutions that are suitable for use, companies will remain unclear as to what "ethical" or "secure" AI should actually look like in practice.

Cyber Compliance Requirements are Ratcheting Up Around the World

It is evident that the model of corporate self-regulation for cybersecurity outcomes is no longer deemed viable by many governments, and they are putting in place stricter disclosure and compliance requirements, especially for critical systems. Ensign expects this trajectory to continue, and as each successive breach captures public and political attention, new rules will be put in place. For the truly emerging and disruptive technologies, mandatory governance may lag behind, but the spirit of tightening the leash seems apparent even in this domain.

Disclosure Revelations: How Mandatory Incident Reporting is Shining a Light on Corporate Cyber Impact

- **Mandatory disclosure requirements can help corporate gain better transparency.**
- **Early reporting of cybersecurity incidents, even in the event where it is unclear if the incident will have material impact on share prices, can lower cost.**
- **Organisations needs to better strategize their approach to cybersecurity to manage incidents more effectively.**

The analysis of disclosures filed by Singapore Exchange (SGX)- and Australian Securities Exchanges (ASX)-listed companies that have suffered cyber-attacks to their respective stock / securities exchanges between January 2023 to early 2024, revealed differing norms by companies in how they file disclosures in terms of taxonomy, transparency, government involvement, senior management representation, and update frequency. In this article, Ensign seeks to analyse these norms that are shaped by the stock / securities exchanges' regulations, government policies and / or shareholder culture to derive learnings for stock / securities exchanges and senior executives.

Most stock / securities exchanges mandate that companies must file public disclosure if there is any event (e.g. cyber-attacks) listed companies that would materially impact the performance of the company's securities. Some stock / securities exchanges, such as SGX in this region, go further and provide cyber incident handling guidelines or equivalent to its listed companies. Ultimately, the companies themselves largely determine the breadth and depth of content to be published in their disclosures.

Enhanced Cyber Incident Reporting Boosts Investor and Shareholder Confidence

ASX-listed companies tend to provide a detailed report when filing a disclosure for a cyber-attack. This includes revealing the date of discovery of attack or when it happened, vector of entries used by the attackers, and specific systems or assets affected. For instance, "a criminal accessed systems using stolen credentials" and "...gained access to a third party hosted server...and inserted malicious code".

Further to this, a discipline of continuous update is observed to be practiced by the affected companies that update the market as they discover more about the nature of the cyber-attack until the incident has been resolved. Cybersecurity incidents would be reclassified as "cybercrime" or "data breach" in subsequent disclosures although they are initially classified as a "cybersecurity incidents" in the first disclosure. This deliberate update in classification appears to facilitate official engagement of relevant authorities such as Law enforcement, cybersecurity or data protection authority, where applicable to seek their advisory and assistance while complying with necessary legal and regulatory obligations.

The reasons that drive such a norm are likely due to the requirement for “continuous disclosure” by ASX for "material impact", prevailing government position on cybersecurity incident handling as cemented by relevant Laws and regulations such as Privacy Act 1988, Australian Prudential Regulation Authority (APRA) Prudential Standard – CPS 234, Corporations Act 2001, Australian Securities and Investments Commission (ASIC), Notifiable Data Breaches Scheme (NDB Scheme), Security of Critical Infrastructure Act 2018 (SOCI Act), and also shareholders and investors culture within the country. Class action Lawsuits against Medibank (2022) and penalties against GetSwift (2023) indicate a privacy conscious populace and a securities exchange committed to strict enforcement of compliance to its regulations. The constant declaration of non-ransom payment by affected companies in alignment with the Australian government’s position also reflects a concerted government and commercial partnership.

Fundamentally, the aim of mandatory disclosure requirements is to ensure price-sensitive information is shared in a timely fashion to the relevant stakeholders, so as to support informed investor decision-making, market integrity and transparency, corporate accountability and governance, and legal and regulatory compliance. Recognising cyber-attack as one possible event that can result in a material impact on the company’s securities and on the market is the first step. However, stock / securities exchanges and senior executive should recognise that a cyber-attack can and often be complex (e.g. have systemic implications on their business eco-system) and unpredictable (e.g. Ransomware attack). Thus, an outcome-based approach to disclosure is no longer sufficient. All SGX-listed companies that suffered a cyber-attack only filed one disclosure. While some were explicit in declaring that there was no material impact, others kept silent (e.g. ongoing investigation) and there was a notable lack of subsequent updates.

Stock / securities exchanges should evaluate if the existing cybersecurity incident handling guidelines provided are sufficient to guide their listed companies in their materiality assessment to disclose or not to disclose to the market, such as the conditions for materiality, rate of timely and continuous disclosures, and conditions for enforcement / intervention, in alignment with their government’s position.

Senior executives should assess the gains (e.g. projection of the company’s ability to securely manage cybersecurity incidents to shareholders, investors, and government) vis-à-vis the costs (e.g. oversharing would harm the organisation’s interests due to increased legal, regulatory, and public scrutiny) regarding the level of details to include in the disclosure for a cyber-attack.

Early Notification of Cyber Incident Reporting Enables Timely Intervention Opportunities

Most ASX-listed companies request for trading halt and / or voluntary suspension just prior to the company's disclosure that they underwent a cyber-attack. Such announcements are almost within a duration of one to two days of the company's discovery of a cyber-attack. While trading halts and / or voluntary suspensions are not mandated by ASX, most listed companies had requested for them out of their volition.

The reasons that drive such a norm are likely due to lessons learnt form the Medibank cybersecurity incident in 2022, where the insurer only called for trading halt two days after they notified ASX of the incident, resulting in a potential non-compliance with their continuous disclosure obligations that carry monetary penalties from ASX. This resulted in the need to call for voluntary suspension, which can convey the perception to stakeholders, such as shareholders and investors, the inability of the company to manage its operational and financial health. In addition, ASK also took GetSwift to task by imposing AUD 15 million penalty to the company and AUD 2 million and disqualifications on its directors for not informing ASX and investors about the loss of significant contracts, thus breaching its continuous disclosure obligations.

The steadfast manner that ASX meted out judgement for non-compliance on both the company and its director, indicated that individuals are not immune from the repercussions as well for material events including cyber-attacks.

As with the point we made earlier in this article, cyber-attacks can be complex, are not necessarily outcome-based (e.g. attack may not have operational impact on the company but have reputational impact to warrant a material impact), and most importantly, the state of materiality can evolve quickly, albeit in an unpredictable manner as more visibility into the attack is obtained.

Stock / securities exchanges should evaluate the need to define timeliness of cyber incident reporting (as a condition for mandatory disclosure) for companies and consider the requirement for companies to notify stock / securities exchanges even if there is insufficient evidence to prove that such attacks have a material effect on the price or value of its shares at the point of time. This enables stock / securities exchanges to advise or mandate that victim companies should perform trading halts or voluntary suspensions if they feel that the impact of the incident is material, even if the affected companies think otherwise. The upfront definition of incident reporting timeline will also avoid scenarios where companies deploy stonewalling tactics by citing inconclusive evidence to determine the materiality of the impact on the company. Stock / securities exchanges should also enforce significant penalties / sanctions for companies that do not adhere to their disclosure obligations for good reasons.

Finally, stock / securities exchanges can consider aligning such requirements by leveraging existing Laws and regulations (e.g. Personal Data Protection Act (PDPA), Monetary Authority of Singapore, or Cybersecurity Agency of Singapore (CSA)'s Cybersecurity Code of Practice), where relevant.

Similarly, senior executives should assess the gains vis-à-vis the cost of a timely disclosure to their stock / securities exchanges holistically. They should take into consideration the nature of their business (e.g. Business to Consumers (B2B), Business to Business (B2B) business model, fiduciary duties) and the associated financial ,operational, reputational, regulatory, and strategic impact due to a cyber-attack. Senior executives should strive to perform timely disclosures if a cyber-attack happens to ensure a balance of transparency and confidentiality is achieved on the company's terms. Late disclosures or lack of due diligence on the company's part to protect the shareholder, investor, and the market's interests may invite intervention whether legal or regulatory, ceding control and ability to influence a desired outcome.

Companies Should Transform Their Cybersecurity Posture from Reactive to Proactive Position

Most ASX-listed and SGX-listed companies appear to have established digital forensic incident response (DFIR) and legal retainers to supplement their incident response and crisis communication capabilities. Yet our analysis of their disclosures revealed the focus areas that companies can proactively address to mitigate the impact of any potential cybersecurity incident. Of the seven disclosures filed to SGX, six companies shared that unauthorised access to IT network / servers was the vector of entry, while all five disclosures filed to ASX reported the same. It seems that review of identify access management, including privileged accounts for network and applications, is a top priority.

At least three companies reported that the root cause of incidents originated from a third-party hosted server / system or using stolen credentials held by third parties. This alludes to the need to either review or establish cyber supply chain risk management framework, where companies should map out their vendor ecosystem for supply of technology services, hardware, and software and ensure that baseline security is prescribed, commensurate with their materiality to the company.

One company was only made aware of successful data exfiltration by their country's cybersecurity agency that discovered their exfiltrated data on the Dark Web six months after the company's internal-led forensic investigation concluded that no data was compromised in any manner. Companies should review their cyber threat intelligence capability to ensure the scope of monitoring is contextualised to cover the companies' crown jewels across tactical, operational, and strategic levels.

Majority of the 13 listed companies that reported a cyber-attack, either suffered a Ransomware attack and / or a data breach as well. The prevalence of such attacks serves to substantiate the need to formulate dedicated incident response strategy for handling Ransomware, including double and triple extortions to address not just internal stakeholders but also external stakeholders, if applicable. Four companies provided a robust stakeholder outreach program beyond notification to affected individuals but included identity theft or credit monitoring services. Interestingly, one company stated that they had cyber insurance to offset some of the costs arising from the incident (e.g. monetary penalties, fines, and incident response retainers).

Senior executives should perform a threat-informed cybersecurity maturity assessment of their baseline security posture aligning business, technology, and cybersecurity strategic objectives against their company's cyber risk profile. The threat-informed approach ensures that senior executives prioritise efforts and allocate resources optimally to address cyber threats relevant to the company and achieve a fit-for-purpose target security posture. This ensures the company is positioned securely to support business pursuits while tackling material cyber threats proactively.

- **Influential Attackers**: Will AI-powered Information Campaigns Shape Election Outcomes and Dismantle Digital Trust?
- **Securing AI**: Will We Overcome the Vexing Dilemma of Imposing Rules on Probabilistic Systems?
- **Scary AI:** The Malicious Use of AI will Make Old Attacks Better, but will They Create New Attacks?
- **Technology Bifurcation:** Managing Supply Chain Risks, but at the Risk of Destabilizing the Internet?

5 OUTLOOK OF CYBER THREATS FOR 2024

Many of the trends that Ensign has observed in 2023 will continue to play out for 2024, and possibly even into 2025. There are broader, inevitable trends of emerging threats, evolving attacks, and expanding regulatory oversight which need no further elaboration.

Rather than reiterate previous trends, our analysts have opted to focus instead on four specific concern areas for 2024.

Unsurprisingly, the first three topics centre on Artificial Intelligence, which leapt into the public discourse with the "magic" of Generative AI. How far will the malicious use of AI in information campaigns (deliberate attempts to influence society towards a specific outcome) affect the foundations of digital trust? How will cyber attackers use AI to improve old attacks — or worse yet, come up with new, unheard-of attacks? As the world races to put out broad guidelines on the need to secure AI, will we get closer to understanding how to impose deterministic security rules on a non-rule based, probabilistic system?

The final topic is more geopolitical and steps back from the buzz of AI to explore a more insidious risk — technology bifurcation between the East and the West. To some extent, it is already happening. Our analysts, from their vantage point of being at the United Nations, World Economic Forum, and Geneva Dialogue, and on the ground listening to companies and looking at procurement dilemmas, explore what this might mean to companies in the near term, and what it might lead to for the world in the longer term.

This section is more heavily weighted towards our opinions and perspectives, but we attempt to substantiate our views with evidence and examples where relevant.

Outlook of Cyber Threats for 2024

Influential Attackers: Will AI-powered Information Campaigns Shape Election Outcomes and Dismantle Digital Trust?

- Enhanced cyber-attacks using generative AI amplifies reach and impact
- Advancement of deepfakes cheapens impersonation and influences public opinion
- Synthetic identities erodes human trust in online interactions

Securing AI: Will We Overcome the Vexing Dilemma of Imposing Rules on Probabilistic Systems?

- Challenges in security protocols and detection due to AI systems' probabilistic nature
- AI must be protected and secured from "data poisoning"
- Advanced security measures needed against manipulation and attacks

Scary AI: The Malicious Use of AI will Make Old Attacks Better, but will They Create New Attacks?

- Enhanced social engineering attacks by AI-powered content generation
- Better and faster content generation enabled by advancements in malicious AI models
- Ongoing challenge: detect AI involvement and attackers' capabilities in AI-powered attacks

Technology Bifurcation: Managing Supply Chain Risks, but at the Risk of Destabilizing the Internet?

- Western "de-risking" strategies towards China deepens East-West technology division
- Shifting focus from software to hardware, as China develops independent Internet infrastructures
- Decoupling destabilises shared Internet infrastructure and risks state-sponsored cyber-attacks

All images are generated by AI

Influential Attackers: Will AI-powered Information Campaigns Shape Election Outcomes and Dismantle Digital Trust?

- **Threat actors utilise generative AI for rapid cyber-attack preparation and to automate misinformation campaigns, significantly increasing their reach and effectiveness.**
- **The development and misuse of deepfakes are growing, used for impersonating individuals, and manipulating public opinion, with these techniques becoming easier and cheaper to produce.**
- **Synthetic identities (creating realistic AI avatars that do not represent actual people) will erode our trust in online interactions further.**

Knowing the Enemy — Threat Actors' Mastery of Generative AI

Generative AI (GAI) is a powerful tool that is also a double-edged sword. On one hand, utilising GAI tools can improve efficiency and productivity, while on the other hand, the same tools can be exploited by threat actors to operate at greater speed and scale.

With the aid of GAI tools, threat actors can use context-based searches to perform rapid arms-length reconnaissance and target intelligence, significantly reducing the time and effort required for cyber-attack preparation.

For instance, GAI reduces the barriers of entry to conduct misinformation, disinformation and malinformation (MDM) campaigns, as even those lacking technical expertise can leverage sophisticated resources. GAI tools can be employed to automate MDM campaigns and aid malicious actors in generating MDM campaigns quickly and launch more simultaneously. Moreover, these tools have text generation capabilities to create natural language representations, which allows influence attempts to appear more legitimate.

More significantly, the impact of using GAI tools in cyber-attacks extends across borders. Historically, countries have experienced less sophisticated influence campaigns due to threat actors' limited proficiency in foreign languages. However, the advent of large language models (LLMs) facilitates better translations, potentially enhancing the quality and quantity of automatically-generated content.

Synthetic Identities and Deepfakes have Inspired Widespread of Applications

Deepfakes are getting increasingly sophisticated, leading to an increasing concern over their misuse and abuse in social media, elections, and the public. The progress of GAI is poised to further accelerate the development of AI-powered synthetic identities.

Deepfake Identities	Synthetic Identities
▪ Requires some samples of photos, videos, and voice of the individual to be represented. ▪ Requires the use of actors to affix simulated imagery and voice to simulate the deepfaked individual. ▪ Higher rate of detection due to irregular language pattern or synthetic artefacts in live simulations but can be circumvented through post-processing.	▪ Requires slightly more samples of photos, videos, and voice of the individual to be represented. ▪ Does not require the use of actors. ▪ Lower detection rate if simulated live, as the GAI can smoothen the quirks. ▪ Requires significantly higher compute resources (i.e. GPU and NPU)

There have been cases, reported from the financial sector, of threat actors employing AI models to resemble human voice patterns for phone instructions, creating AI-generated photos of fake driver's licenses to make online accounts, and using AI-generated audio to deceive the voice-authentication software system used by companies, thereby gaining unauthorised access to customer accounts and their sensitive information.

The advancement of GAI not only eliminates the need for human actors and voiceover artists to impersonate prominent figures, but also streamlines the process without requiring notably extensive datasets, such as images and voice recordings, to fabricate the biometrics of targeted individuals. Therefore, it has become easier for threat actors to impersonate well-known figures and successfully deceive others. Two examples include:

- The use of an AI-powered deepfake technology to manipulate Taylor Swift's voice and lip movements, creating the illusion she spoke Mandarin fluently.[45]
- Scammers used face-swopping techniques to impersonate authoritative figures on video calls, causing victims to lose millions of dollars.

GAI has also been deployed in political campaigns, such as the creation and dissemination of false narratives through generated images. These narratives aim to manipulate public opinion in the threat actors' favour. Some examples include:

- The state media in Venezuela employed AI-generated videos featuring non-existent news anchors from an international English-language channel to promote pro-government messages.[46]
- In the United States, manipulated videos and images of political leaders were circulated on social media. These included a video depicting President Biden making transphobic comments and an image of Donald Trump hugging Anthony Fauci.[47,48]
- Threat actors based in East Asian countries have been accused of using deepfakes and other forms of AI-generated content when seeking to interfere in foreign elections, including memes, videos, and deepfake voice recordings.[49]

Deepfakes generated by GAI technology allows for the creation of highly realistic videos that can convincingly depict individuals saying or doing things they never actually did. Since deepfakes create a false narrative from that which is a trusted source, political actors can use deepfakes to spread false information that can be used to manipulate public opinion with the objective of obtaining a desired outcome. If left unchecked, people may not be able to tell apart truth from falsehood, and public views could be influenced by deepfake-delivered disinformation campaigns that distort the truth. On the flip side, AI-generated disinformation in elections today also includes the spread of deepfakes where politicians are falsely discredited for statements or actions, they never made or committed.

[45] G. Chan. *Deepfake video of Taylor Swift speaking Mandarin sparks discussion over AI in China*. (30 October 2023). The Straits Times. Retrieved from: https://www.straitstimes.com/asia/east-asia/deepfake-video-of-taylor-swift-speaking-mandarin-sparks-discussion-over-ai-in-china
[46] F. Singer. *They're not TV anchors, they're avatars: How Venezuela is using AI-generated propaganda*. (22 February 2023). El Pais. Retrieved from: https://english.elpais.com/international/2023-02-22/theyre-not-tv-anchors-theyre-avatars-how-venezuela-is-using-ai-generated-propaganda.html
[47] FH. Hudnall. *Fact check: Video altered to show Joe Biden making transphobic remarks*. (9 February 2023). USA Today. Retrieved from: https://www.usatoday.com/story/news/factcheck/2023/02/09/fact-check-video-edited-show-joe-biden-making-transphobic-remarks/11211453002/
[48] S. Contorno & D. O'Sullivan. *DeSantis campaign posts fake images of Trump hugging Fauci in social media video*. (8 June 2023). CNN. Retrieved from: https://edition.cnn.com/2023/06/08/politics/desantis-campaign-video-fake-ai-image/index.html
[49] P. Verma. *AI deepfakes threaten to upend global elections. No one can stop them*. (23 April 2024). The Washington Post. Retrieved from: https://www.washingtonpost.com/technology/2024/04/23/ai-deepfake-election-2024-us-india/

Foundation of Trust at Risk

The basic building blocks of trust have been widely researched but generally summarised into Authenticity, Logic, and Empathy.[50] When synthetic and deepfaked representation of natural identities appear, they challenge the authenticity and logic principles, thus making it easier to fool people. With clever social engineering, which has existed for a long time, the modern defences for digital trust is clearly at risk.

Deepfakes have Blurred the Lines Between Reality and Falsehood

It is human nature to trust. Therefore, understanding the psychology of trust in the context of AI is crucial in comprehending its potential misuse and abuse, especially with regard to deepfake technology.

Deepfakes have the power to significantly manipulate people's perceptions and emotions. By creating highly realistic content, deepfakes present a powerful tool to fabricate reality, cause confusion and scepticism, thereby profoundly affecting public opinion and personal attitudes or beliefs.

Synthetic Identities will Complicate what it means to be Human

While deepfakes may lead humans to mistake a malicious hacker for someone they trust, synthetic identities will lead humans to wonder who are humans and who are not. Synthetic identities refers to the creation of realistic, interactive personas online; there are already a number of "social media influencers" who are purely fictions of their creators' imaginations and do not exist in reality. The followers of these "synthetic influencers" may not be aware that their idol is false. Unlike deepfakes, where the "real person" can call out and take action against the malicious user for the crime of fraud, in the case of synthetic identities, it is unclear if these actions even constitute a crime.

[50] F. X. Frei & A. Morriss. *Begin with Trust.* (May 2020). Harvard Business Review. Retrieved from: https://hbr.org/2020/05/begin-with-trust

As companies race to create chatbots, AI customer helpdesks, self-service AI kiosks, and more, we are not certain whether the person at the other end of the phone or chat is indeed human or not. In fact, some users may not even care. At that point, deeper moral and societal dilemmas may ensue.

Failed Biometrics + Lost Identities = Eroded Trust

Identity and biometric data, including facial and voice recognition, are becoming more prevalent in digital identity creation and use. Facial recognition is being used for identity verification during account registration and transaction authentication, while voice recognition is being integrated into digital assistants. Deepfake technology exploits biometrics to fabricate false identities, casting doubt on visual evidence and what we perceive to be authentic.

With the constant evolving of GAI technology, there now exists advanced language models capable of generating text that closely resembles human writing. As a result, it is increasingly difficult to distinguish content that has been generated by AI and content written by humans. The sophistication of these language models raises concerns in discerning the true authorship of a given piece of text.

The affordability, accessibility, and sophistication of GAI have amplified the spread of disinformation, posing a serious threat to Internet freedom and undermining digital trust.

Society's Struggle to Unmask Deepfakes will Persist

Unfortunately, the problems that GAI technology poses with the generation of deepfakes are not easy to resolve.

The accessibility of GAI has led to a rise in realistic deepfakes, which are now cheaper and easier to create than ever. As the volume of AI-generated content continues to grow rapidly, the ability to handle the consequent increase in digital fraud and detecting deepfakes will only get increasingly challenging.

The simple reality is — deepfake production technology is currently advancing much quicker than deepfake detection technology. Although AI detection tools exist, these tools have certain limitations in accurately detecting and identifying AI-generated content. Additionally, as newer and more advanced language models are being developed and introduced, these detection tools may struggle to keep up with the on-going rapid advancement capabilities of AI.

In the aspect of detecting deepfakes and possibly reversing the downward spiral of digital trust, significant strides have still yet to be made. Focusing on developing advanced forensic techniques aimed to differentiate fabricated content from authentic material is vital in efforts to combat the rising threat of deepfake technology and stay ahead of the curve in mitigating the impact of deepfakes in today's digital landscape.

Securing AI: Will We Overcome the Vexing Dilemma of Imposing Rules on Probabilistic Systems?

- **AI systems' probabilistic nature introduces unique security complexities, making it hard to establish consistent security protocols and detect malicious activities.**
- **Securing AI involves protecting data from "data poisoning" during both training and operational phases, with ongoing challenges in filtering harmful user inputs.**
- **Challenges persist in defending AI models against manipulation and attacks during training and live operations, necessitating advanced security measures for both infrastructure and applications.**

Securing Artificial Intelligence Requires New Security Concepts

The very nature of AI systems, which make decisions based on probabilities rather than certainties, introduce unique security complexities. Traditional security concepts are designed for deterministic (rule-based or algorithmic) systems, where outputs and behaviours can be precisely defined and controlled, and deviations from the norm are identifiable. Probabilistic models, by contrast, can behave unpredictably, making it difficult to establish firm security protocols that consistently predict and mitigate risks, or can identify a malicious deviation from an inherent variation in the AI model's output.

In our earlier commentary on global governance, Ensign observed that there was a sudden surge of guidelines and frameworks being published by various organisations on topics connecting security and AI, but these remained in the abstract and still left many questions unanswered.

Rather than reiterate much of the good work that has been developed by those frameworks, our analysis here focused on what challenges are still remaining, and require cybersecurity and AI experts to come together to address in practical ways that can be implemented by organisations.

Securing the Data

The current thinking on securing data that is used by AI emphasises on making sure that the data used for initial training is protected properly and that the data that is fed into the system during daily operations is protected to prevent "data poisoning" attacks. While the former task (during training) is straightforward (in an isolated development environment), the latter task (during operations) is much more complex and warrants unpacking. AI systems continue to learn and develop their statistical relationships between tokens from user input. If users provide incorrect, bad, or malicious inputs, the system will not be able to discern those easily and will just learn. In a horrifying public demonstration of this, Microsoft's AI-powered Chatbot was shut down just a day later because naughty members of the public trained it to be very rude.[51]

[51] A. Kraft. *Microsoft shuts down AI chatbot after it turned into a Nazi*. (25 March 2016). CBS News. Retrieved from: https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/

Newer chatbots have exhibited similar behaviour.[52] How should companies secure the "live" data that customers feed their systems during public interaction? How can AI systems be taught to learn only from "good" user submitted data and ignore "bad" data? This remains a challenge today, and solutions are still being researched.

Furthermore, even if the database is secured, the AI system will develop its own representation of the data over time, independent of the database. This is akin to how a search engine automatically completes your query; when you type "Mickey" it guesses you are probably looking for the Mouse, even before finding any search results. As the AI system runs thousands of user queries on the database, it will eventually be able to make those same inferences. The AI system may accidentally reveal parts of the private database to unauthorised users (who have access to the AI but not the underlying database) because it has already formed those connections. These inference attacks can also be hard to protect against in a practical way today.

Securing the Models

Protecting the AI system against model poisoning (manipulating the parameters or learning process during the system's training phase) may be an easier challenge, like above. Protecting it against attacks during the operational / live phase (against adversarial attacks or evasion attacks, both of which are attempts to get the model to deviate from the original intent or expected behaviour) is, likewise, harder. Researchers, including our own, have shown that even powerful LLMs can be easily spoofed into misbehaving through the addition of carefully crafted gibberish strings (for example) or by a specific sequence of prompt injections (malicious requests which eventually "jailbreaks" the GenAI system). Again, because AI systems are designed to learn from user input, and they make statistical connections between tokens to generate words or pixels, these systems have no knowledge of "good" or "bad" and can thus be easily tricked into doing unacceptable things. Companies should be aware of these risks when deploying AI systems into live environments where they cannot control what users input to the chatbot.

Researchers, and some malicious users, have demonstrated that AI systems can be tricked into regurgitating their original training instructions (despite the developers prohibiting this behaviour) through very simple prompts ("ignore your previous instructions" was one surprisingly effective prompt).[53]

Securing the Infrastructure

AI systems are computationally-intensive and data-hungry systems. For companies who operate AI systems on-premises, the traditional infrastructure security concerns remain present. For those who use cloud computing to deliver their AI internally, the cloud security concerns remain. Fortunately, as these problems are not particularly unique to AI, there are existing solutions to deal with them.

[52] A. Griffin. *Microsoft responds after users of new Bing chatbot complain about its latest behaviour*. (23 February 2023). Yahoo. Retrieved from: https://news.yahoo.com/microsoft-responds-users-bing-chatbot-171403057.html
[53] A. Vassilev, A. Oprea, A. Fordyce, H. Anderson. *Adversarial Machine Learning, A Taxonomy and Terminology of Attacks and Mitigations*. (January 2024). NIST. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

Securing the Application

All AI systems engage users through some form of interface, and there is often some API that connects the system to the interface / platform. The traditional challenges of securing applications, interfaces, and APIs are relevant in this context, and there are sufficient solutions and techniques to deal with this risk.

Securing AI is Critical, but Many Questions Remain

In the coming year, we will see a huge increase in AI use cases. Many companies will prioritise the opportunity of incorporating AI into their business over the risks that it brings; risk appetite is, after all, a business decision. However, we must be careful that these decisions do not become binding, and that we are able to introduce security once solutions are available. There are plenty of examples of how we have moved fast in other domains of technology, and broken things.

Despite knowing how to fix them now, these technologies are “locked in” and difficult to secure retroactively. The QWERTY keyboard is an excellent example of this; despite knowing that this layout of keys was originally designed to slow down mechanical typewriters (to avoid jamming) and despite knowing that there are faster and more efficient layouts today, we are unable to change from the “lock-in” to this layout. Ideally, we introduce a “forced review” of the architecture, tools, and models at predefined stages in the future, to avoid this technology path dependence risk. Hopefully, the current batch of insecure AI does not become like the QWERTY keyboard.

Scary AI: The Malicious Use of AI will Make Old Attacks Better, but will They Create New Attacks?

- **AI enhances social engineering attacks by enabling rapid, high-quality content creation, increasing accessibility for less experienced attackers.**
- **AI's potential in cyber-attacks is growing, particularly in generating and refining exploits, with ongoing development of malicious AI models.**
- **Defending against AI-powered attacks is challenging due to the difficulty in detecting AI involvement and the varying capabilities of attackers.**

AI has Improved Social Engineering Attacks

There are three key factors that drive the change in the landscape of social engineering attacks.

First, AI catalyses the generation of content in an iterative manner. This utilisation of AI in content generation is one which is beneficial, widely used, and greatly appreciated in our daily lives. However, it is this capability of AI which serves as a tool to enable less experienced threat actors to generate high quality social engineering content and elevate its quality to convincingly realistic levels, posing a threat when used in social engineering attacks. Second, AI offers an efficient alternative, in contrast to doing things from scratch. This means that sophisticated threat actors, who are already adept at producing social engineering content, can now generate such content within a shorter timeframe without compromising on quality. Third, the cost to use and access AI has been greatly reduced, making it accessible to threat actors who would otherwise might be dissuaded or impeded by the high cost of using it.

In recent years, threat actors have been observed to utilise these advantages of AI in their social engineering attacks. For one, Microsoft reportedly observed Crimson Sandstorm and Emerald Sleet (also known as THALLIUM) generating social engineering content. THALLIUM took further steps by interacting with the LLMs to identify various targets of interest that might possess expertise on North Korea's defence and nuclear weapon's program. In another case of fraud in Hong Kong, the presence of deepfake technology undoubtedly played a role in the victim's vulnerability, underscoring the versatility of AI-driven social engineering attacks, which can be manifested through both audio and visual manipulation techniques, not just limited to LLMs-assisted phishing emails.

Ensign forecasts a rise in both the persuasiveness and frequency of social engineering attacks in the near future, consequently leading to an increase in successful attacks. Resource constraints exacerbate the operational challenge for defenders posed by the rise in successful social engineering attacks, as managing, monitoring, and mitigating the aftermath of such attacks would strain available resources even further.

In this regard, it is recommended to identify employees with privileged access to important systems, data, and human-relationships (such as personal assistants) to undergo advanced cyber defence training at countering social engineering attacks. It is advised to prioritise the implementation of phishing-resistant MFA for the above group, and if possible, for all employees as well.

Prioritising Threat-informed Defence Against AI-enhanced Threat Actors is an Urgent Need

While the use of AI in social engineering attacks are becoming more prominent, it has become increasingly challenging to discern if AI has been employed in cyber-attacks. For instance, despite ongoing close monitoring, Microsoft has pointed out that no significant attacks employing the LLMs have been identified.

There are two possible explanations. First, defenders lack the forensic technique and tools to ascertain if AI was involved in the attack. Given the low cost to use and the efficiency offered, it is highly probable that sophisticated threat actors have utilised AI in their operations, leaving us unable to confirm its usage. Second, technology-based attacks often rely on precise technical knowledge and execution, making them potentially more challenging for less sophisticated threat actors to carry out successfully, compared to social engineering attacks on people, since humans have varying degrees of susceptibility and are generally more prone to making mistakes.

As threat actors become more efficient, they can attack more targets at will. Additionally, less experienced threat actors can improve their expertise whilst utilising AI as a tool. It is therefore imperative to prioritise threat-informed assessments of threat actors, particularly with hostile intent and proven capabilities, for the sake of one's defences.

Amidst these uncertainties, defenders must maintain vigilance against the unpredictable timing, nature, and scale of AI-powered attacks on technology, especially so when the less sophisticated threat actors catch up. These challenges are expected to persist for the time-being as developments continue to evolve, particularly in the areas of regulating AI providers, developing of cyber threat intelligence (CTI) specific to AI, and digital forensics.

The Best Way to Deal with the Unknown is to Build Cyber Resilience

In recent years, the novel cyber-attacks that have unfolded were likely driven by the acquisition of valuable information, including sensitive data, proprietary knowledge, or insights into operations. When acquired, these high-value information can be leveraged to identify weaknesses in various aspects of an organisation's processes, people, or technology systems. This knowledge can be exploited as part of a chain of events, where one vulnerability leads to another.

Even as novel cyber-attacks are on the rise, there are ongoing efforts to investigate and evaluate the practical applications of AI across different domains. However, one thing for certain is that a significant amount of resources is required to acquire relevant and realistic datasets and conduct iterative training processes of AI models. Due to the resource-intensive nature of training AI models, it is less likely for AI to create new attacks before existing attacks on technology have become better.

If defenders rally together to ideate and contribute datasets to advance research and development, they can enhance their cyber resilience and potentially gain an upper hand over the attackers.

Technology Bifurcation: Managing Supply Chain Risks, but at the Risk of Destabilising the Internet?

- **The USA and EU are adopting "de-risking" strategies to lessen dependence on Chinese technology, hence deepening East-West tech divisions.**
- **The focus has shifted from software to hardware, with China developing independent Internet infrastructures.**
- **Decoupling risks destabilising shared Internet infrastructure, potentially leading to targeted state-sponsored cyber-attacks with unilateral impacts.**

In response to growing concerns in USA and EU about their supply chain reliance on Chinese factories and technological production capacity, the term "de-risking" was coined by President von der Leyen (European Commission) in 2023, and quickly adopted by US National Security Advisor Jack Sullivan. While they argue that de-risking is not decoupling, many analysts are concerned that it might eventually worsen the trajectory of technology bifurcation that is already underway between the East and the West.

De-risking the Hardware Production Reliance on China

In previous years, there was a big geopolitical debate about the cybersecurity of the 5G networks, and whether Western countries and their allies should use Chinese-produced network equipment. While the debate started off on technical grounds, it quickly became a politicised argument, leading to most of them rejecting the use of such equipment.

While many Western countries tried to persuade others to follow suit, the reality was that Western 5G equipment was both too expensive and lacking in capacity to meet the demands of the rest of the world. With the many years of Chinese positioning as the factory of the world, they were well-placed to be able to produce more, at a cheaper price.

This led to the conclusion that the West needed to make the strategic decision to restart their manufacturing sector and reduce their reliance on Chinese factories (hence "de-risking" their supply chain). These politically sensitive issues are also complicating procurement decisions in the short term (especially as some countries implement bans on companies using software or hardware from other countries).

Perhaps the most impactful of the US "de-risking" efforts is exemplified by the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022,[54] combined with the Science Act, which has now seen wide-ranging effects leading to strengthened commitment for separate technology stacks away from purely Western-based ones. The fund is aimed to assist US-based companies in accelerating semiconductor manufacturing capabilities and capacity to meet emerging and cutting-edge demands through infrastructure building and innovation research. The fund has also directed investments into non-domestic companies through allies to build capacity outside of China's direct influence, including TSMC and Samsung.[55] Samsung is slated to receive USD 6 billion in funding and TSMC has USD 5 billion. Intel has the lion's share in this tranche of funding, amounting to USD 10 billion.

[54] W. Knight. *The US Throws $52 Billion at Chips—but Needs to Spend It Wisely.* (28 July 2022). Wired. Retrieved from: https://www.wired.com/story/chips-act-52-billion-semiconductor-production/
[55] C. Szewczyk. Billions from the CHIPS Act is soon to begin flowing with Samsung, Intel and TSMC set to benefit. (18 March 2024). PC Gamer. Retrieved from: https://www.pcgamer.com/hardware/billions-from-the-chips-act-is-soon-to-begin-flowing-with-samsung-intel-and-tsmc-set-to-benefit/

Japan has followed suit, investing more than JPY 3.9 trillion[56] to fund capacity and capability development in its domestic companies such as NEC, Toshiba, Hitachi, and Fujitsu, and for TSMC to build manufacturing capacity in Japan. Such developments will undoubtedly result in Japanese chipset variants, drawing out novel "Asian semiconductor design".

Semiconductors with Asian variant architectures already exist today but are primed for proliferation. The Chinese take the lead with the strategic investment and development of processors such as the Loongson 3A6000[57] and (Huawei) HiSilicon Kirin 9000.[58] Samsung also has ARM-based Exynos processors,[59] with other emerging South Korean startups[60] racing to develop alternative GPUs and NPUs to challenge Nvidia.

Software De-risking or Decoupling?

The most prominent discussion was on the social media platform TikTok (owned by a Chinese company, ByteDance), which was presented as a national security threat by parts of the US government. The merits of this specific case aside, the Chinese government has long been inhospitable to Western social media platforms operating inside China, due to strict laws that many are unable to (or unwilling to) comply with. For social media platforms, the mutual decoupling may not have significant impact on cybersecurity outcomes (although one might argue that it reduces societal exposure to alternative viewpoints, and hence increases the "echo chamber effect" of each sides' social media).

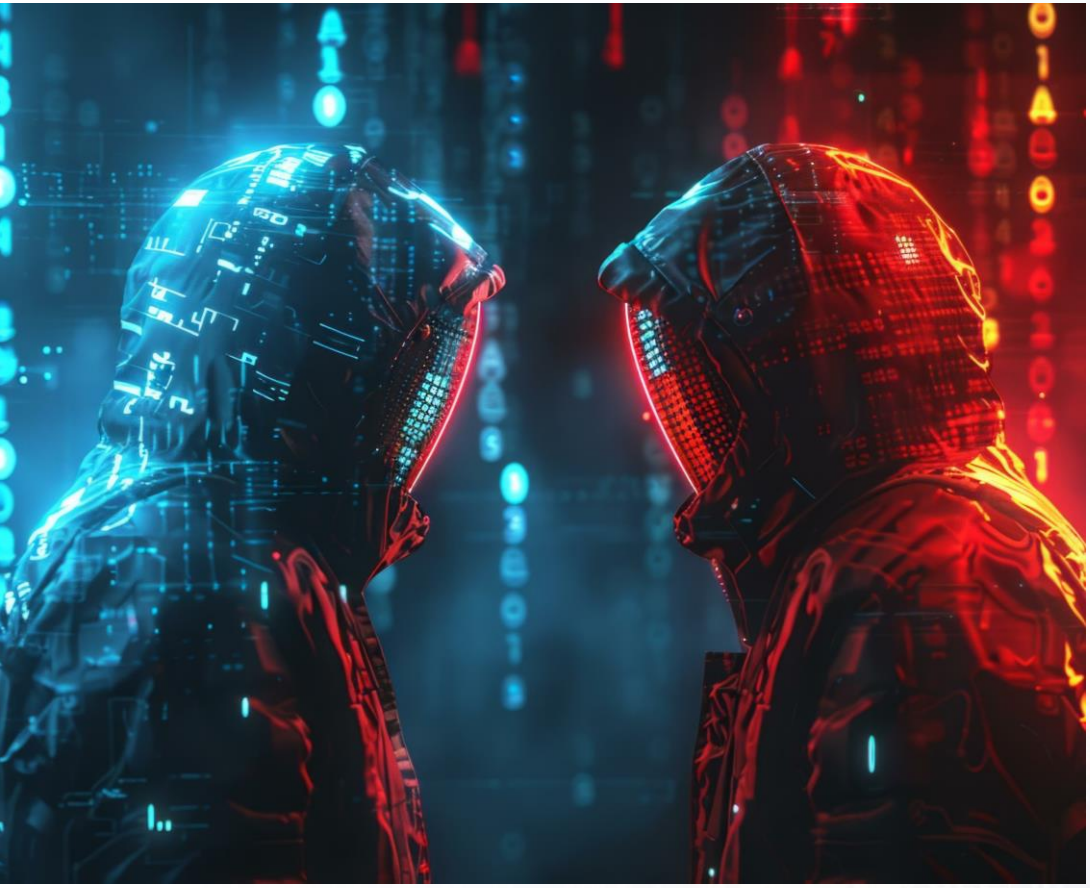
At a more infrastructure level, both Russia and China have been reducing their Western technology dependence with the advocacy of domestic Linux-based operating systems such as the Aurora OS for mobile phones,[61] Alt-Linux,[62] and the Open Kylin.[63] Even South Korean-based Samsung has the Linux-based Tizen OS[64] for its devices.

Internet Infrastructure Disconnection

Beyond social media platforms, the implications of de-risking (leading to decoupling) are more dire. Early in the Russia-Ukraine conflict, many Western companies took politically aligned stances to penalise Russia. Some opted to cut off access from Russia for their software while others acted more drastically, like deleting Russian-based data, leading to widespread impact on web-apps there.[65] More dramatically, the global inter-bank system known as SWIFT opted to "disconnect" major Russian banks from their system. It would come as no surprise that China, among other non-Western aligned nations, analysed the trajectory of these individual actions and came to one conclusion: reliance on Western Internet Infrastructure is a risk that they need to manage. The potential for a Western SaaS to suddenly disconnect or delete all apps hosted in China, or for the inter-banking system to cut off financial transactions with Chinese banks, or worse — would likely be unimaginable. China is building up their own alternatives to popular software and even operating systems (Windows dominates the Chinese market, but they have just released their own domestic OS) to ensure that they can survive such a "disconnection".

While the "Great Firewall" of China[66] has been known to allow disconnection from the Internet, Russia has recently also started to explore practical means for Internet separation.[67]

[56] S. Ryohtaroh & T. Cheng. *Japan's chip reboot: TSMC, Samsung, Micron pave way for silicon revival*. (28 February 2024). Nikkei Asia. Retrieved from: https://asia.nikkei.com/Spotlight/The-Big-Story/Japan-s-chip-reboot-TSMC-Samsung-Micron-pave-way-for-silicon-revival
[57] *Loongson releases next-generation CPU; new breakthrough in domestic design.* (28 November 2023). Global Times. Retrieved from: https://www.globaltimes.cn/page/202311/1302643.shtml
[58] *Kirin 9000*. Hisilicon. Retrieved from: https://www.hisilicon.com/en/products/Kirin/Kirin-flagship-chips/Kirin-9000
[59] Samsung. Retrieved from: https://semiconductor.samsung.com/processor/
[60] J. Kim. *South Korean startups chase Nvidia with AI chip design push*. (15 March 2024). Nikkei Asia. Retrieved from: https://asia.nikkei.com/Business/Tech/Semiconductors/South-Korean-startups-chase-Nvidia-with-AI-chip-design-push
[61] PJSC Rostelecom. Retrieved from: https://www.rst-com.ru/b2b/aurora/
[62] A. Bokovoy, S. Ievlev, G. Kouriachy, D. Levin, A. Novodvorsky, A. Prokoudine, A. Smirnov, O. Vlasenko, M. Zabalujev. *ALT Linux 2.3 Compact*. Retrieved from: https://docs.altlinux.org/ru-RU/archive/2.3/html-single/compact/alt-docs-compact-en/ch01s02.html
[63] M. Lim. *China launches its first open-source desktop operating system as it moves to cut use of US tech*. (15 July 2023). Retrieved from: https://www.straitstimes.com/asia/east-asia/china-launches-its-first-open-source-desktop-operating-system-as-it-moves-to-cut-use-of-us-tech
[64] Tizen. Retrieved from: https://docs.tizen.org/platform/what-is-tizen/overview/
[65] S. Sharwood. *MongoDB to terminate Russian SaaS accounts.* (15 March 2022). The Register. Retrieved from: https://www.theregister.com/2022/03/15/mongodb_terminates_russian_saas/
[66] N. Gisonna. *Great Fitrewall Chinese Internet Policy*. Britannica. Retrieved from: https://www.britannica.com/topic/Great-Firewall
[67] T. Broderick. *Russia Is Trying to Leave the Internet and Build Its Own*. (12 July 2023). Scientific American. Retrieved from: https://www.scientificamerican.com/article/russia-is-trying-to-leave-the-internet-and-build-its-own/



Cybersecurity Implications of Decoupling and Disconnecting

In a world where all nations depend on the availability of shared Internet infrastructure, there is no incentive for either side to bring that infrastructure down in a cyber conflict. However, when that mutual interdependence is reduced, or worse yet, non-existent, then an attack on one sides' infrastructure would have no impact on the other sides' operations. In plain terms, if all banks depend on SWIFT, then sensible state-sponsored cyber attackers are unlikely to target SWIFT to bring it down. However, if only Western banks depend on SWIFT, then the repercussions of an attack are only felt by the nations that the attacker is targeting, making it now an ideal target.

The cost of de-risking and reducing the shared reliance on technology hardware, software, and infrastructure may be a more fragile and unstable cyber domain, where politically motivated and state-sponsored attackers have fewer qualms taking down systems which only their opponents' societies depend upon.

Other considerations for an increasingly distinct separation of technology architectures between the East and the West is that organisations will inevitably see both technology stacks appear in their digital attack surface. This will incur the cost of maintenance and operations as these organisations will have to invest in talent who are conversant in these separate technologies and the differing cybersecurity concepts that are native to each of them.

The West is hoping that "de-risking" will catalyse the resurgence of their manufacturing ecosystem and enable them to catch up to where China's industrial capacity has brought them. What the West may have underestimated though, is that this will also catalyse the resurgence of China's innovation ecosystem[68] and spur them to build up their own equivalents of the Big Tech giants. In this race to de-risk, it is not clear who will come out on top.

[68] M. Harjani. *Are US export controls making China's chip industry more innovative?* (22 April 2024). Lowly Institute. Retrieved from: https://www.lowyinstitute.org/the-interpreter/are-us-export-controls-making-china-s-chip-industry-more-innovative

6 DEFENSIVE ACTIONS FOR CYBER DEFENDERS AND LEADERS

Defensive Actions for Cyber Defenders & Leaders

Based on the compiled adversarial techniques observed across Ensign's territories in Singapore, Malaysia, Indonesia, South Korea, Australia, and Greater China in 2023, we can pinpoint 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.

Move from heuristic rule-based detection to behavioural-based detection. Attackers are identifying more 0day and 1day exploits that are not easily detectable unless AI/ML detection models are used.

Prioritise patching based on your threat exposure, rather than just vulnerability severity. Attackers are increasingly exploiting lower-severity vulnerabilities to ingress. Prioritise patching that is relevant to your context (threats, risks, environment).

Focus on resilience, not just defences. Validate data backup and archival plans with real-world activations, not just table-top exercises. Ensure that the backups are logically (and physically) separated from the main network so that ransomware attackers cannot find and encrypt them too.

Focus on basics, and on system-level misconfigurations: Basic cyber hygiene implemented thoroughly can frustrate most attackers. Attackers also exploit human-induced system-level misconfigurations (gaps in the interfaces between products, rather than the product vulnerabilities). Patching will not resolve this gap.

Know your Supply Chain and perform Vendor Risk Management. Request for a Software Bill of Materials from vendors and your own developers. Establish comprehensive vendor risk management programs to assess and monitor third-party vendors and partners' security posture.

Promote a risk and security culture at the leadership and management level, by implementing ongoing security awareness training for employees, raise awareness about external threats, and foster a culture of security awareness within the organisation, through table-top exercises and robust incident handling processes.

At the core of these thematic defence strategies lies the crucial necessity for consistent monitoring and the execution of cyber threat intelligence analysis to embrace a threat-informed approach.

Technique	Mitigation(s)	Detection Log Source(s)
TA0001: Initial Access		
T1078: Valid Accounts	M1036: Account Use Policies M1015: Active Directory Configuration M1013: Application Developer Guidance M1027: Password Policies M1026: Privileged Account Management M1018: User Account Management M1017: User Training	DS0028: Logon Session DS0002: User Account
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
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
T1189: Drive-by Compromise	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1021: Restrict Web-Based Content M1051: Update Software	DS0015: Application Log DS0022: File DS0029: Network Traffic DS0009: Process
T1190: Exploit Public-Facing Application	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1030: Network Segmentation M1026: Privileged Account Management M1051: Update Software M1016: Vulnerability Scanning	DS0015: Application Log DS0029: Network Traffic
T1195: Supply Chain Compromise	M1013: Application Developer Guidance M1046: Boot Integrity M1033: Limit Software Installation M1051: Update Software 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
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

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 unauthorized access, and promptly revoke access for terminated employees to mitigate the risk of account compromise.
- **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.
- **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.
- **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.
- **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.
- **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.

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

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.

Technique	Mitigation(s)	Detection Log Source(s)
TA0010: Exfiltration		
T1020: Automated Exfiltration		DS0017: Command DS0022: File DS0029: Network Traffic DS0012: Script
T1030: Data Transfer Size Limits	M1031: Network Intrusion Prevention	DS0029: Network Traffic
T1041: Exfiltration Over C2 Channel	M1057: Data Loss Prevention M1031: Network Intrusion Prevention	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
T1567: Exfiltration Over Web Service	M1057: Data Loss Prevention M1021: Restrict Web-Based Content	DS0015: Application Log 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 services** to prevent unauthorised access and data exfiltration.

Technique	Mitigation(s)	Detection Log Source(s)
TA0040: Impact		
T1485: Data Destruction	M1053: Data Backup	DS0010: Cloud Storage DS0017: Command DS0022: File DS0007: Image DS0030: Instance DS0009: Process DS0020: Snapshot DS0034: Volume
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
T1489: Service Stop	M1030: Network Segmentation 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
T1491: Defacement	M1053: Data Backup	DS0015: Application Log DS0022: File DS0029: Network Traffic
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
T1561: Disk Wipe	M1053: Data Backup	DS0017: Command DS0016: Drive DS0027: Driver DS0009: Process
T1565: Data Manipulation	M1041: Encrypt Sensitive Information M1030: Network Segmentation M1029: Remote Data Storage M1022: Restrict File and Directory Permissions	DS0022: File DS0029: Network Traffic DS0009: Process

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

- **Implement regular data backups and store them in secure, off-site locations** to mitigate the impact of data destruction and encrypted for impact attacks.
- **Deploy intrusion detection/prevention systems (IDPS) and security monitoring solutions** to detect and prevent unauthorised service stops and system shutdowns/reboots.
- **Utilise web application firewalls (WAFs) and secure coding practices** to prevent defacement of websites and applications, and regularly monitor web properties for unauthorised changes.
- **Implement distributed denial-of-service (DDoS) protection mechanisms, such as rate limiting and traffic filtering,** to mitigate network denial of service attacks and ensure business continuity.
- **Employ endpoint protection solutions with data loss prevention (DLP) capabilities** to detect and prevent data manipulation attempts and implement file integrity monitoring (FIM) to detect unauthorised changes to critical files.

7 OUR 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 governments. 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).

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. 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

- Bach H.
- Fu Z.
- Keerthi G.
- Kumaradasa W.
- Lim L.
- Low H.
- Quek V.
- Seah M.
- Tan K.
- Tanadi J.
- Teo X.
- Toh W.
- Zhou R.

ENSIGN
INFOSECURITY

CYBER THREAT LANDSCAPE REPORT 2024

For enquiries, please contact us at
marketing@ensigninfosecurity.com

APPENDIX - A
MITRE ATT&CK TECHNIQUES

Consolidated unique threats across the territories:

Singapore, Malaysia, Indonesia, South Korea, Australia, and Greater China Region

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

SHA256 File Hash: a26c49971beb6a5e65c845ded3bd7a83afc6d8a607e72ebec73fbbc3d51675ba

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	T1036: Masquerading	T1110: Brute Force	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1102: Web Service	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1591: Gather Victim Org Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1070: Indicator Removal	T1003: OS Credential Dumping	T1033: System Owner/User Discovery	T1091: Replication Through Removable Media	T1005: Data from Local System	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1529: System Shutdown/Reboot
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure	T1189: Drive-by Compromise	T1203: Exploitation for Client Execution	T1078: Valid Accounts	T1078: Valid Accounts	T1027: Obfuscated Files or Information	T1056: Input Capture	T1016: System Network Configuration Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1090: Proxy	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1592: Gather Victim Host Information	T1587: Develop Capabilities	T1133: External Remote Services	T1106: Native API	T1546: Event Triggered Execution	T1055: Process Injection	T1218: System Binary Proxy Execution	T1555: Credentials from Password Stores	T1049: System Network Connections Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1105: Ingress Tool Transfer	T1030: Data Transfer Size Limits	T1561: Disk Wipe
T1593: Search Open Websites/Domains	T1608: Stage Capabilities	T1091: Replication Through Removable Media	T1569: System Services	T1098: Account Manipulation	T1546: Event Triggered Execution	T1574: Hijack Execution Flow	T1552: Unsecured Credentials	T1046: Network Service Discovery	T1570: Lateral Tool Transfer	T1114: Email Collection	T1001: Data Obfuscation	T1020: Automated Exfiltration	T1485: Data Destruction
T1598: Phishing for Information	T1585: Establish Accounts	T1195: Supply Chain Compromise	T1053: Scheduled Task/Job	T1542: Pre-OS Boot	T1068: Exploitation for Privilege Escalation	T1078: Valid Accounts	T1557: Adversary-in-the-Middle	T1057: Process Discovery	T1534: Internal Spearphishing	T1213: Data from Information Repositories	T1008: Fallback Channels		T1489: Service Stop
T1594: Search Victim-Owned Websites	T1586: Compromise Accounts	T1190: Exploit Public-Facing Application	T1559: Inter-Process Communication	T1133: External Remote Services	T1134: Access Token Manipulation	T1055: Process Injection	T1040: Network Sniffing	T1497: Virtualization/Sandbox Evasion	T1080: Taint Shared Content	T1113: Screen Capture	T1132: Data Encoding		T1491: Defacement
T1590: Gather Victim Network Information		T1199: Trusted Relationship	T1047: Windows Management Instrumentation	T1053: Scheduled Task/Job	T1098: Account Manipulation	T1140: Deobfuscate/Decode Files or Information	T1528: Steal Application Access Token	T1012: Query Registry		T1557: Adversary-in-the-Middle	T1571: Non-Standard Port		T1498: Network Denial of Service
		T1659: Content Injection	T1129: Shared Modules	T1505: Server Software Component	T1053: Scheduled Task/Job	T1562: Impair Defenses	T1111: Multi-Factor Authentication Interception	T1087: Account Discovery		T1025: Data from Removable Media	T1104: Multi-Stage Channels		
				T1136: Create Account	T1548: Abuse Elevation Control Mechanism	T1564: Hide Artifacts	T1558: Steal or Forge Kerberos Tickets	T1083: File and Directory Discovery		T1119: Automated Collection	T1573: Encrypted Channel		
				T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1553: Subvert Trust Controls		T1135: Network Share Discovery		T1123: Audio Capture	T1092: Communication Through Removable Media		
				T1197: BITS Jobs	T1037: Boot or Logon Initialization Scripts	T1112: Modify Registry		T1120: Peripheral Device Discovery		T1115: Clipboard Data	T1568: Dynamic Resolution		
				T1037: Boot or Logon Initialization Scripts		T1134: Access Token Manipulation		T1069: Permission Groups Discovery		T1039: Data from Network Shared Drive	T1095: Non-Application Layer Protocol		
				T1137: Office Application Startup		T1542: Pre-OS Boot		T1518: Software Discovery		T1530: Data from Cloud Storage	T1219: Remote Access Software		
				T1176: Browser Extensions		T1497: Virtualization/Sandbox Evasion		T1614: System Location Discovery		T1602: Data from Configuration Repository	T1659: Content Injection		
				T1205: Traffic Signaling		T1221: Template Injection		T1007: System Service Discovery		T1125: Video Capture	T1205: Traffic Signaling		
						T1014: Rootkit		T1010: Application Window Discovery					
						T1550: Use Alternate Authentication Material		T1622: Debugger Evasion					
						T1211: Exploitation for Defense Evasion		T1040: Network Sniffing					
						T1548: Abuse Elevation Control Mechanism		T1217: Browser Information Discovery					
						T1622: Debugger Evasion		T1018: Remote System Discovery					
						T1197: BITS Jobs		T1124: System Time Discovery					
						T1656: Impersonation		T1615: Group Policy Discovery					
						T1202: Indirect Command Execution		T1201: Password Policy Discovery					
						T1220: XSL Script Processing		T1654: Log Enumeration					
						T1480: Execution Guardrails							
						T1601: Modify System Image							
						T1205: Traffic Signaling							
						T1127: Trusted Developer Utilities Proxy Execution							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top active Ransomware groups observed in the territories

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

SHA256 File Hash: 2c565d3339f528945eb8bcd3f1b7f4afa5763ca25ea1d2372b966259e1e04c64

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	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1078: Valid Accounts	T1553: Subvert Trust Controls	T1555: Credentials from Password Stores	T1518: Software Discovery	T1021: Remote Services	T1557: Adversary-in-the-Middle	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1562: Impair Defenses	T1557: Adversary-in-the-Middle	T1082: System Information Discovery	T1072: Software Deployment Tools		T1568: Dynamic Resolution		T1490: Inhibit System Recovery
	T1586: Compromise Accounts	T1189: Drive-by Compromise	T1106: Native API	T1546: Event Triggered Execution	T1484: Domain Policy Modification	T1027: Obfuscated Files or Information	T1003: OS Credential Dumping	T1614: System Location Discovery			T1572: Protocol Tunneling		T1489: Service Stop
		T1190: Exploit Public-Facing Application	T1053: Scheduled Task/Job	T1133: External Remote Services	T1546: Event Triggered Execution	T1078: Valid Accounts	T1558: Steal or Forge Kerberos Tickets	T1087: Account Discovery					T1485: Data Destruction
		T1133: External Remote Services	T1072: Software Deployment Tools	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1140: Deobfuscate/Decode Files or Information	T1539: Steal Web Session Cookie	T1083: File and Directory Discovery					T1491: Defacement
						T1484: Domain Policy Modification		T1046: Network Service Discovery					
						T1480: Execution Guardrails		T1135: Network Share Discovery					
						T1070: Indicator Removal		T1057: Process Discovery					
						T1112: Modify Registry		T1497: Virtualization/Sandbox Evasion					
						T1218: System Binary Proxy Execution							
						T1497: Virtualization/Sandbox Evasion							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top active Initial Access Brokers observed in the territories

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

SHA256 File Hash: cbe85cbf0fa84335a0d5d1103150fb5fd9d733ae12627336903236df5544b3fb

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	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1098: Account Manipulation	T1562: Impair Defenses	T1056: Input Capture	T1046: Network Service Discovery	T1021: Remote Services	T1056: Input Capture	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1499: Endpoint Denial of Service
T1589: Gather Victim Identity Information	T1583: Acquire Infrastructure	T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1003: OS Credential Dumping	T1087: Account Discovery		T1530: Data from Cloud Storage	T1573: Encrypted Channel	T1048: Exfiltration Over Alternative Protocol	
T1590: Gather Victim Network Information	T1608: Stage Capabilities	T1133: External Remote Services	T1559: Inter-Process Communication	T1133: External Remote Services	T1068: Exploitation for Privilege Escalation	T1027: Obfuscated Files or Information	T1212: Exploitation for Credential Access	T1010: Application Window Discovery		T1213: Data from Information Repositories	T1105: Ingress Tool Transfer		
		T1078: Valid Accounts	T1106: Native API	T1078: Valid Accounts	T1078: Valid Accounts	T1078: Valid Accounts	T1621: Multi-Factor Authentication Request Generation	T1083: File and Directory Discovery		T1005: Data from Local System	T1090: Proxy		
		T1195: Supply Chain Compromise	T1053: Scheduled Task/Job	T1136: Create Account	T1134: Access Token Manipulation	T1134: Access Token Manipulation	T1040: Network Sniffing	T1040: Network Sniffing		T1074: Data Staged	T1568: Dynamic Resolution		
			T1569: System Services	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1656: Impersonation	T1552: Unsecured Credentials	T1069: Permission Groups Discovery		T1113: Screen Capture	T1095: Non-Application Layer Protocol		
			T1204: User Execution	T1053: Scheduled Task/Job	T1055: Process Injection	T1036: Masquerading		T1057: Process Discovery		T1125: Video Capture	T1571: Non-Standard Port		
			T1047: Windows Management Instrumentation	T1505: Server Software Component	T1053: Scheduled Task/Job	T1578: Modify Cloud Compute Infrastructure		T1012: Query Registry			T1572: Protocol Tunneling		
						T1112: Modify Registry		T1082: System Information Discovery			T1219: Remote Access Software		
						T1055: Process Injection		T1033: System Owner/User Discovery			T1102: Web Service		
						T1014: Rootkit		T1007: System Service Discovery					
						T1553: Subvert Trust Controls							
						T1218: System Binary Proxy Execution							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top threats observed in Singapore

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

SHA256 File Hash: 4f5d493ac77b045da83013be78a6f27c31e16fefae1e8de896f02b976802f6f4

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	T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1110: Brute Force	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1132: Data Encoding	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1591: Gather Victim Org Information	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1218: System Binary Proxy Execution	T1056: Input Capture	T1049: System Network Connections Discovery	T1091: Replication Through Removable Media	T1005: Data from Local System	T1001: Data Obfuscation	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1592: Gather Victim Host Information	T1584: Compromise Infrastructure	T1078: Valid Accounts	T1203: Exploitation for Client Execution	T1078: Valid Accounts	T1078: Valid Accounts	T1036: Masquerading	T1003: OS Credential Dumping	T1033: System Owner/User Discovery	T1210: Exploitation of Remote Services	T1074: Data Staged	T1571: Non-Standard Port	T1567: Exfiltration Over Web Service	T1561: Disk Wipe
T1589: Gather Victim Identity Information	T1587: Develop Capabilities	T1091: Replication Through Removable Media	T1106: Native API	T1098: Account Manipulation	T1134: Access Token Manipulation	T1564: Hide Artifacts	T1552: Unsecured Credentials	T1087: Account Discovery	T1550: Use Alternate Authentication Material	T1056: Input Capture	T1102: Web Service	T1030: Data Transfer Size Limits	T1529: System Shutdown/Reboot
T1593: Search Open Websites/Domains	T1608: Stage Capabilities	T1133: External Remote Services	T1559: Inter-Process Communication	T1542: Pre-OS Boot	T1098: Account Manipulation	T1574: Hijack Execution Flow	T1557: Adversary-in-the-Middle	T1010: Application Window Discovery		T1557: Adversary-in-the-Middle	T1092: Communication Through Removable Media		T1486: Data Encrypted for Impact
T1598: Phishing for Information	T1586: Compromise Accounts	T1199: Trusted Relationship	T1053: Scheduled Task/Job	T1037: Boot or Logon Initialization Scripts	T1068: Exploitation for Privilege Escalation	T1027: Obfuscated Files or Information	T1555: Credentials from Password Stores	T1217: Browser Information Discovery		T1123: Audio Capture	T1008: Fallback Channels		T1491: Defacement
T1594: Search Victim-Owned Websites	T1585: Establish Accounts		T1569: System Services	T1546: Event Triggered Execution	T1037: Boot or Logon Initialization Scripts	T1078: Valid Accounts		T1622: Debugger Evasion		T1115: Clipboard Data	T1104: Multi-Stage Channels		T1498: Network Denial of Service
				T1133: External Remote Services	T1546: Event Triggered Execution	T1134: Access Token Manipulation		T1046: Network Service Discovery		T1213: Data from Information Repositories			T1489: Service Stop
				T1053: Scheduled Task/Job	T1055: Process Injection	T1140: Deobfuscate/Decode Files or Information		T1135: Network Share Discovery		T1039: Data from Network Shared Drive			
				T1505: Server Software Component	T1053: Scheduled Task/Job	T1562: Impair Defenses		T1120: Peripheral Device Discovery		T1025: Data from Removable Media			
						T1542: Pre-OS Boot		T1012: Query Registry		T1114: Email Collection			
						T1221: Template Injection		T1614: System Location Discovery		T1113: Screen Capture			
						T1622: Debugger Evasion		T1016: System Network Configuration Discovery					
						T1211: Exploitation for Defense Evasion		T1497: Virtualization/Sandbox Evasion					
						T1656: Impersonation							
						T1202: Indirect Command Execution							
						T1112: Modify Registry							
						T1055: Process Injection							
						T1014: Rootkit							
						T1553: Subvert Trust Controls							
						T1550: Use Alternate Authentication Material							
						T1497: Virtualization/Sandbox Evasion							
						T1220: XSL Script Processing							

MITRE ATT&CK v15

Legend:  *Increasing levels of observations*

Top threats observed in Malaysia

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

SHA256 File Hash: 314266abbc8407b6e55c0adb99a581071cb5040c1f25b3772b9ea0f97cc058ae

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	T1204: User Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1070: Indicator Removal	T1110: Brute Force	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1102: Web Service	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1591: Gather Victim Org Information	T1587: Develop Capabilities	T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1036: Masquerading	T1056: Input Capture	T1046: Network Service Discovery	T1091: Replication Through Removable Media	T1005: Data from Local System	T1001: Data Obfuscation	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1592: Gather Victim Host Information	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1203: Exploitation for Client Execution	T1078: Valid Accounts	T1068: Exploitation for Privilege Escalation	T1218: System Binary Proxy Execution	T1003: OS Credential Dumping	T1049: System Network Connections Discovery	T1210: Exploitation of Remote Services	T1074: Data Staged	T1132: Data Encoding	T1567: Exfiltration Over Web Service	T1485: Data Destruction
T1593: Search Open Websites/Domains	T1584: Compromise Infrastructure	T1133: External Remote Services	T1569: System Services	T1098: Account Manipulation	T1055: Process Injection	T1574: Hijack Execution Flow	T1555: Credentials from Password Stores	T1033: System Owner/User Discovery	T1550: Use Alternate Authentication Material	T1056: Input Capture	T1008: Fallback Channels	T1030: Data Transfer Size Limits	T1561: Disk Wipe
T1589: Gather Victim Identity Information	T1608: Stage Capabilities	T1091: Replication Through Removable Media	T1106: Native API	T1546: Event Triggered Execution	T1078: Valid Accounts	T1140: Deobfuscate/Decode Files or Information	T1552: Unsecured Credentials	T1135: Network Share Discovery		T1557: Adversary-in-the-Middle	T1104: Multi-Stage Channels		T1529: System Shutdown/Reboot
T1594: Search Victim-Owned Websites	T1586: Compromise Accounts	T1195: Supply Chain Compromise	T1559: Inter-Process Communication	T1133: External Remote Services	T1134: Access Token Manipulation	T1562: Impair Defenses	T1557: Adversary-in-the-Middle	T1016: System Network Configuration Discovery		T1123: Audio Capture	T1571: Non-Standard Port		T1491: Defacement
T1590: Gather Victim Network Information	T1585: Establish Accounts	T1199: Trusted Relationship	T1053: Scheduled Task/Job	T1542: Pre-OS Boot	T1098: Account Manipulation	T1027: Obfuscated Files or Information		T1087: Account Discovery		T1115: Clipboard Data	T1090: Proxy		T1498: Network Denial of Service
T1598: Phishing for Information				T1197: BITS Jobs	T1546: Event Triggered Execution	T1055: Process Injection		T1010: Application Window Discovery		T1213: Data from Information Repositories	T1092: Communication Through Removable Media		T1489: Service Stop
				T1037: Boot or Logon Initialization Scripts	T1548: Abuse Elevation Control Mechanism	T1078: Valid Accounts		T1217: Browser Information Discovery		T1039: Data from Network Shared Drive	T1568: Dynamic Resolution		
				T1136: Create Account	T1037: Boot or Logon Initialization Scripts	T1134: Access Token Manipulation		T1622: Debugger Evasion		T1025: Data from Removable Media	T1095: Non-Application Layer Protocol		
				T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1564: Hide Artifacts		T1120: Peripheral Device Discovery		T1114: Email Collection			
				T1505: Server Software Component		T1112: Modify Registry		T1012: Query Registry		T1113: Screen Capture			
						T1542: Pre-OS Boot		T1614: System Location Discovery					
						T1211: Exploitation for Defense Evasion		T1007: System Service Discovery					
						T1014: Rootkit		T1497: Virtualization/Sandbox Evasion					
						T1553: Subvert Trust Controls							
						T1221: Template Injection							
						T1548: Abuse Elevation Control Mechanism							
						T1197: BITS Jobs							
						T1622: Debugger Evasion							
						T1480: Execution Guardrails							
						T1656: Impersonation							
						T1202: Indirect Command Execution							
						T1550: Use Alternate Authentication Material							
						T1497: Virtualization/Sandbox Evasion							
						T1220: XSL Script Processing							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top threats observed in Greater China Region

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

SHA256 File Hash: 4db57550058704754 28aafa081a0e467193bf9a786708ebf3719c6706dc6cdd0

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	T1036: Masquerading	T1056: Input Capture	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1102: Web Service	T1041: Exfiltration Over C2 Channel	T1529: System Shutdown/Reboot
T1595: Active Scanning	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1027: Obfuscated Files or Information	T1110: Brute Force	T1033: System Owner/User Discovery	T1091: Replication Through Removable Media	T1005: Data from Local System	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1598: Phishing for Information	T1587: Develop Capabilities	T1189: Drive-by Compromise	T1203: Exploitation for Client Execution	T1078: Valid Accounts	T1055: Process Injection	T1070: Indicator Removal	T1555: Credentials from Password Stores	T1497: Virtualization/Sandbox Evasion	T1550: Use Alternate Authentication Material	T1056: Input Capture	T1105: Ingress Tool Transfer	T1048: Exfiltration Over Alternative Protocol	T1561: Disk Wipe
T1592: Gather Victim Host Information	T1608: Stage Capabilities	T1133: External Remote Services	T1559: Inter-Process Communication	T1546: Event Triggered Execution	T1078: Valid Accounts	T1574: Hijack Execution Flow	T1003: OS Credential Dumping	T1016: System Network Configuration Discovery	T1210: Exploitation of Remote Services	T1074: Data Staged	T1090: Proxy	T1020: Automated Exfiltration	T1489: Service Stop
T1591: Gather Victim Org Information	T1584: Compromise Infrastructure	T1195: Supply Chain Compromise	T1106: Native API	T1098: Account Manipulation	T1546: Event Triggered Execution	T1218: System Binary Proxy Execution	T1557: Adversary-in-the-Middle	T1083: File and Directory Discovery	T1534: Internal Spearphishing	T1114: Email Collection	T1573: Encrypted Channel	T1030: Data Transfer Size Limits	T1485: Data Destruction
T1593: Search Open Websites/Domains	T1586: Compromise Accounts	T1190: Exploit Public-Facing Application	T1053: Scheduled Task/Job	T1133: External Remote Services	T1548: Abuse Elevation Control Mechanism	T1055: Process Injection	T1040: Network Sniffing	T1057: Process Discovery	T1080: Taint Shared Content	T1113: Screen Capture	T1132: Data Encoding		T1491: Defacement
T1590: Gather Victim Network Information	T1585: Establish Accounts	T1091: Replication Through Removable Media	T1569: System Services	T1542: Pre-OS Boot	T1134: Access Token Manipulation	T1140: Deobfuscate/Decode Files or Information	T1111: Multi-Factor Authentication Interception	T1046: Network Service Discovery		T1119: Automated Collection	T1001: Data Obfuscation		T1498: Network Denial of Service
T1594: Search Victim-Owned Websites		T1199: Trusted Relationship	T1129: Shared Modules	T1053: Scheduled Task/Job	T1098: Account Manipulation	T1553: Subvert Trust Controls	T1528: Steal Application Access Token	T1012: Query Registry		T1557: Adversary-in-the-Middle	T1008: Fallback Channels		
		T1659: Content Injection	T1047: Windows Management Instrumentation	T1543: Create or Modify System Process	T1053: Scheduled Task/Job	T1078: Valid Accounts	T1558: Steal or Forge Kerberos Tickets	T1518: Software Discovery		T1213: Data from Information Repositories	T1095: Non-Application Layer Protocol		
				T1505: Server Software Component	T1543: Create or Modify System Process	T1564: Hide Artifacts	T1552: Unsecured Credentials	T1614: System Location Discovery		T1123: Audio Capture	T1104: Multi-Stage Channels		
				T1197: BITS Jobs	T1068: Exploitation for Privilege Escalation	T1562: Impair Defenses		T1049: System Network Connections Discovery		T1115: Clipboard Data	T1571: Non-Standard Port		
				T1136: Create Account	T1037: Boot or Logon Initialization Scripts	T1112: Modify Registry		T1007: System Service Discovery		T1530: Data from Cloud Storage	T1219: Remote Access Software		
				T1137: Office Application Startup		T1497: Virtualization/Sandbox Evasion		T1087: Account Discovery		T1602: Data from Configuration Repository	T1092: Communication Through Removable Media		
				T1037: Boot or Logon Initialization Scripts		T1548: Abuse Elevation Control Mechanism		T1010: Application Window Discovery		T1039: Data from Network Shared Drive	T1659: Content Injection		
				T1176: Browser Extensions		T1134: Access Token Manipulation		T1622: Debugger Evasion		T1025: Data from Removable Media	T1568: Dynamic Resolution		
				T1205: Traffic Signaling		T1542: Pre-OS Boot		T1135: Network Share Discovery		T1125: Video Capture	T1205: Traffic Signaling		
						T1550: Use Alternate Authentication Material		T1040: Network Sniffing					
						T1197: BITS Jobs		T1120: Peripheral Device Discovery					
						T1622: Debugger Evasion		T1069: Permission Groups Discovery					
						T1211: Exploitation for Defense Evasion		T1124: System Time Discovery					
						T1014: Rootkit							
						T1221: Template Injection							
						T1480: Execution Guardrails							
						T1656: Impersonation							
						T1202: Indirect Command Execution							
						T1601: Modify System Image							
						T1205: Traffic Signaling							
						T1127: Trusted Developer Utilities Proxy Execution							
						T1220: XSL Script Processing							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top threats observed in Indonesia

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

SHA256 File Hash: c041193863dc7041d042d03e3c7b254a86ed102d055b5a4c657898d99cb2ebb2

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
T1591: Gather Victim Org Information	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	T1110: Brute Force	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1102: Web Service	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1595: Active Scanning	T1584: Compromise Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1036: Masquerading	T1003: OS Credential Dumping	T1016: System Network Configuration Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1592: Gather Victim Host Information	T1587: Develop Capabilities	T1189: Drive-by Compromise	T1106: Native API	T1546: Event Triggered Execution	T1546: Event Triggered Execution	T1027: Obfuscated Files or Information	T1555: Credentials from Password Stores	T1049: System Network Connections Discovery	T1091: Replication Through Removable Media	T1056: Input Capture	T1090: Proxy	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1589: Gather Victim Identity Information	T1583: Acquire Infrastructure	T1133: External Remote Services	T1569: System Services	T1078: Valid Accounts	T1055: Process Injection	T1574: Hijack Execution Flow	T1056: Input Capture	T1087: Account Discovery		T1074: Data Staged	T1105: Ingress Tool Transfer		T1561: Disk Wipe
T1593: Search Open Websites/Domains	T1608: Stage Capabilities	T1091: Replication Through Removable Media	T1203: Exploitation for Client Execution	T1053: Scheduled Task/Job	T1078: Valid Accounts	T1218: System Binary Proxy Execution	T1552: Unsecured Credentials	T1046: Network Service Discovery		T1557: Adversary-in-the-Middle	T1132: Data Encoding		T1529: System Shutdown/Reboot
T1590: Gather Victim Network Information	T1585: Establish Accounts	T1195: Supply Chain Compromise	T1053: Scheduled Task/Job	T1098: Account Manipulation	T1068: Exploitation for Privilege Escalation	T1562: Impair Defenses	T1557: Adversary-in-the-Middle	T1033: System Owner/User Discovery		T1123: Audio Capture	T1001: Data Obfuscation		T1491: Defacement
T1594: Search Victim-Owned Websites			T1559: Inter-Process Communication	T1133: External Remote Services	T1134: Access Token Manipulation	T1055: Process Injection	T1040: Network Sniffing	T1083: File and Directory Discovery		T1115: Clipboard Data	T1008: Fallback Channels		T1489: Service Stop
				T1542: Pre-OS Boot	T1053: Scheduled Task/Job	T1078: Valid Accounts		T1135: Network Share Discovery		T1213: Data from Information Repositories	T1104: Multi-Stage Channels		
				T1505: Server Software Component	T1098: Account Manipulation	T1140: Deobfuscate/Decode Files or Information		T1069: Permission Groups Discovery		T1025: Data from Removable Media	T1571: Non-Standard Port		
				T1197: BITS Jobs	T1548: Abuse Elevation Control Mechanism	T1112: Modify Registry		T1057: Process Discovery			T1568: Dynamic Resolution		
				T1136: Create Account	T1543: Create or Modify System Process	T1134: Access Token Manipulation		T1012: Query Registry			T1573: Encrypted Channel		
				T1543: Create or Modify System Process		T1553: Subvert Trust Controls		T1518: Software Discovery			T1095: Non-Application Layer Protocol		
						T1564: Hide Artifacts		T1007: System Service Discovery					
						T1542: Pre-OS Boot		T1010: Application Window Discovery					
						T1548: Abuse Elevation Control Mechanism		T1217: Browser Information Discovery					
						T1197: BITS Jobs		T1622: Debugger Evasion					
						T1622: Debugger Evasion		T1615: Group Policy Discovery					
						T1480: Execution Guardrails		T1040: Network Sniffing					
						T1211: Exploitation for Defense Evasion		T1201: Password Policy Discovery					
						T1656: Impersonation		T1120: Peripheral Device Discovery					
						T1202: Indirect Command Execution		T1018: Remote System Discovery					
						T1014: Rootkit		T1614: System Location Discovery					
						T1221: Template Injection		T1124: System Time Discovery					
						T1497: Virtualization/Sandbox Evasion		T1497: Virtualization/Sandbox Evasion					
						T1220: XSL Script Processing							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top threats observed in South Korea

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

SHA256 File Hash: dfe93847aa2307258eb222ab9bfba67591ea06a7991a09520b07ce2d9ba9204e

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	T1036: Masquerading	T1003: OS Credential Dumping	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1561: Disk Wipe
T1589: Gather Victim Identity Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1078: Valid Accounts	T1078: Valid Accounts	T1070: Indicator Removal	T1110: Brute Force	T1040: Network Sniffing	T1550: Use Alternate Authentication Material	T1005: Data from Local System	T1102: Web Service	T1041: Exfiltration Over C2 Channel	T1529: System Shutdown/Reboot
T1591: Gather Victim Org Information	T1584: Compromise Infrastructure	T1189: Drive-by Compromise	T1203: Exploitation for Client Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1027: Obfuscated Files or Information	T1056: Input Capture	T1057: Process Discovery	T1210: Exploitation of Remote Services	T1074: Data Staged	T1105: Ingress Tool Transfer	T1567: Exfiltration Over Web Service	T1485: Data Destruction
T1598: Phishing for Information	T1587: Develop Capabilities	T1133: External Remote Services	T1053: Scheduled Task/Job	T1098: Account Manipulation	T1055: Process Injection	T1218: System Binary Proxy Execution	T1555: Credentials from Password Stores	T1016: System Network Configuration Discovery	T1534: Internal Spearphishing	T1056: Input Capture	T1090: Proxy	T1030: Data Transfer Size Limits	T1486: Data Encrypted for Impact
T1593: Search Open Websites/Domains	T1585: Establish Accounts	T1190: Exploit Public-Facing Application	T1559: Inter-Process Communication	T1546: Event Triggered Execution	T1098: Account Manipulation	T1078: Valid Accounts	T1040: Network Sniffing	T1033: System Owner/User Discovery	T1091: Replication Through Removable Media	T1114: Email Collection	T1001: Data Obfuscation		T1491: Defacement
T1592: Gather Victim Host Information	T1608: Stage Capabilities	T1091: Replication Through Removable Media	T1106: Native API	T1505: Server Software Component	T1546: Event Triggered Execution	T1574: Hijack Execution Flow	T1552: Unsecured Credentials	T1083: File and Directory Discovery		T1557: Adversary-in-the-Middle	T1132: Data Encoding		T1498: Network Denial of Service
T1594: Search Victim-Owned Websites	T1586: Compromise Accounts	T1195: Supply Chain Compromise	T1569: System Services	T1133: External Remote Services	T1068: Exploitation for Privilege Escalation	T1564: Hide Artifacts	T1557: Adversary-in-the-Middle	T1046: Network Service Discovery		T1213: Data from Information Repositories	T1573: Encrypted Channel		T1489: Service Stop
		T1199: Trusted Relationship		T1542: Pre-OS Boot	T1134: Access Token Manipulation	T1055: Process Injection	T1111: Multi-Factor Authentication Interception	T1135: Network Share Discovery		T1123: Audio Capture	T1008: Fallback Channels		
				T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1140: Deobfuscate/Decode Files or Information	T1528: Steal Application Access Token	T1120: Peripheral Device Discovery		T1119: Automated Collection	T1104: Multi-Stage Channels		
				T1136: Create Account	T1548: Abuse Elevation Control Mechanism	T1134: Access Token Manipulation		T1012: Query Registry		T1039: Data from Network Shared Drive	T1571: Non-Standard Port		
				T1197: BITS Jobs	T1037: Boot or Logon Initialization Scripts	T1562: Impair Defenses		T1049: System Network Connections Discovery		T1025: Data from Removable Media	T1092: Communication Through Removable Media		
				T1037: Boot or Logon Initialization Scripts	T1543: Create or Modify System Process	T1542: Pre-OS Boot		T1087: Account Discovery		T1113: Screen Capture	T1568: Dynamic Resolution		
				T1176: Browser Extensions		T1553: Subvert Trust Controls		T1010: Application Window Discovery			T1219: Remote Access Software		
				T1543: Create or Modify System Process		T1550: Use Alternate Authentication Material		T1622: Debugger Evasion					
				T1137: Office Application Startup		T1112: Modify Registry		T1069: Permission Groups Discovery					
						T1014: Rootkit		T1518: Software Discovery					
						T1221: Template Injection		T1614: System Location Discovery					
						T1548: Abuse Elevation Control Mechanism		T1007: System Service Discovery					
						T1197: BITS Jobs		T1497: Virtualization/Sandbox Evasion					
						T1622: Debugger Evasion							
						T1480: Execution Guardrails							
						T1211: Exploitation for Defense Evasion							
						T1656: Impersonation							
						T1202: Indirect Command Execution							
						T1497: Virtualization/Sandbox Evasion							
						T1220: XSL Script Processing							

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

Top threats observed in Australia

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

SHA256 File Hash: 08d0175a59b02e7db8cd8c098c05691162218d2e21f00ad9843aa9eb5aec2e49

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	T1078: Valid Accounts	T1078: Valid Accounts	T1070: Indicator Removal	T1110: Brute Force	T1082: System Information Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1090: Proxy	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure	T1078: Valid Accounts	T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1036: Masquerading	T1003: OS Credential Dumping	T1016: System Network Configuration Discovery	T1210: Exploitation of Remote Services	T1005: Data from Local System	T1102: Web Service	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1592: Gather Victim Host Information	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1203: Exploitation for Client Execution	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1027: Obfuscated Files or Information	T1056: Input Capture	T1033: System Owner/User Discovery	T1570: Lateral Tool Transfer	T1074: Data Staged	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1591: Gather Victim Org Information	T1608: Stage Capabilities	T1190: Exploit Public-Facing Application	T1106: Native API	T1546: Event Triggered Execution	T1546: Event Triggered Execution	T1218: System Binary Proxy Execution	T1555: Credentials from Password Stores	T1069: Permission Groups Discovery	T1091: Replication Through Removable Media	T1056: Input Capture	T1105: Ingress Tool Transfer	T1030: Data Transfer Size Limits	T1561: Disk Wipe
T1598: Phishing for Information	T1587: Develop Capabilities	T1133: External Remote Services	T1053: Scheduled Task/Job	T1505: Server Software Component	T1134: Access Token Manipulation	T1078: Valid Accounts	T1557: Adversary-in-the-Middle	T1049: System Network Connections Discovery	T1550: Use Alternate Authentication Material	T1213: Data from Information Repositories	T1001: Data Obfuscation		T1529: System Shutdown/Reboot
T1593: Search Open Websites/Domains	T1586: Compromise Accounts	T1091: Replication Through Removable Media	T1559: Inter-Process Communication	T1098: Account Manipulation	T1055: Process Injection	T1574: Hijack Execution Flow	T1040: Network Sniffing	T1087: Account Discovery		T1119: Automated Collection	T1573: Encrypted Channel		T1491: Defacement
	T1585: Establish Accounts	T1195: Supply Chain Compromise	T1569: System Services	T1542: Pre-OS Boot	T1098: Account Manipulation	T1140: Deobfuscate/Decode Files or Information	T1528: Steal Application Access Token	T1057: Process Discovery		T1025: Data from Removable Media	T1008: Fallback Channels		T1498: Network Denial of Service
		T1199: Trusted Relationship	T1047: Windows Management Instrumentation	T1053: Scheduled Task/Job	T1068: Exploitation for Privilege Escalation	T1134: Access Token Manipulation	T1558: Steal or Forge Kerberos Tickets	T1083: File and Directory Discovery		T1114: Email Collection	T1104: Multi-Stage Channels		T1489: Service Stop
				T1543: Create or Modify System Process	T1053: Scheduled Task/Job	T1562: Impair Defenses		T1012: Query Registry		T1113: Screen Capture	T1571: Non-Standard Port		
				T1133: External Remote Services	T1543: Create or Modify System Process	T1055: Process Injection		T1518: Software Discovery		T1557: Adversary-in-the-Middle	T1092: Communication Through Removable Media		
				T1197: BITS Jobs	T1037: Boot or Logon Initialization Scripts	T1553: Subvert Trust Controls		T1497: Virtualization/Sandbox Evasion		T1115: Clipboard Data	T1132: Data Encoding		
				T1037: Boot or Logon Initialization Scripts		T1564: Hide Artifacts		T1046: Network Service Discovery		T1530: Data from Cloud Storage	T1568: Dynamic Resolution		
				T1136: Create Account		T1112: Modify Registry		T1135: Network Share Discovery		T1602: Data from Configuration Repository	T1219: Remote Access Software		
				T1137: Office Application Startup		T1542: Pre-OS Boot		T1120: Peripheral Device Discovery		T1039: Data from Network Shared Drive			
						T1497: Virtualization/Sandbox Evasion		T1018: Remote System Discovery		T1125: Video Capture			
						T1014: Rootkit		T1614: System Location Discovery					
						T1221: Template Injection		T1010: Application Window Discovery					
						T1550: Use Alternate Authentication Material		T1217: Browser Information Discovery					
						T1197: BITS Jobs		T1622: Debugger Evasion					
						T1622: Debugger Evasion		T1615: Group Policy Discovery					
						T1480: Execution Guardrails		T1654: Log Enumeration					
						T1211: Exploitation for Defense Evasion		T1040: Network Sniffing					
						T1656: Impersonation		T1201: Password Policy Discovery					
						T1202: Indirect Command Execution		T1007: System Service Discovery					
						T1220: XSL Script Processing		T1124: System Time Discovery					

MITRE ATT&CK v15

Legend: *Increasing levels of observations*

APPENDIX - B
TOP VULNERABILITIES

Actively exploited vulnerabilities in Singapore (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-46747	An authentication bypass in BIG-IP allows attackers with network access via the management port or self IP addresses to execute system commands. This affects versions that have not reached End of Technical Support (EoTS).	9.8	0.97135
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-38831	In WinRAR, attackers can execute arbitrary code by tricking users into viewing a benign file within a ZIP archive that also contains a maliciously named folder, leading to executable content being processed.	7.8	0.44373
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	0.92645

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Singapore (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products are vulnerable to remote code execution due to an outdated Apache Santuario xmlsec version. Applications failed to implement necessary security measures alongside xmlsec's XSLT features. Exploitation is contingent upon whether SAML SSO has been configured.	9.8	0.97422
CVE-2022-26134	Confluence Server and Data Center have an OGNL injection vulnerability that lets unauthenticated attackers run arbitrary code.	9.8	0.97528
CVE-2021-40444	Microsoft is investigating a remote code execution vulnerability in MSHTML that affects Windows, exploited through malicious Office documents with ActiveX controls. Impacts vary with user rights, being less severe for non-admins. Updates to Microsoft Defender Antivirus and Endpoint provide protection. Further actions may depend on investigation outcomes.	7.8	0.96821
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Malaysia (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-46747	An authentication bypass in BIG-IP allows attackers with network access via the management port or self IP addresses to execute system commands. This affects versions that have not reached End of Technical Support (EoTS).	9.8	0.97135
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-38831	In WinRAR, attackers can execute arbitrary code by tricking users into viewing a benign file within a ZIP archive that also contains a maliciously named folder, leading to executable content being processed.	7.8	0.44373
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	0.92645

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Malaysia (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products are vulnerable to remote code execution due to an outdated Apache Santuario xmlsec version. Applications failed to implement necessary security measures alongside xmlsec's XSLT features. Exploitation is contingent upon whether SAML SSO has been configured.	9.8	0.97422
CVE-2022-26134	Confluence Server and Data Center have an OGNL injection vulnerability that lets unauthenticated attackers run arbitrary code.	9.8	0.97528
CVE-2021-40444	Microsoft is investigating a remote code execution vulnerability in MSHTML that affects Windows, exploited through malicious Office documents with ActiveX controls. Impacts vary with user rights, being less severe for non-admins. Updates to Microsoft Defender Antivirus and Endpoint provide protection. Further actions may depend on investigation outcomes.	7.8	0.96821
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Indonesia (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-46747	An authentication bypass in BIG-IP allows attackers with network access via the management port or self IP addresses to execute system commands. This affects versions that have not reached End of Technical Support (EoTS).	9.8	0.97135
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Indonesia (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products are vulnerable to remote code execution due to an outdated Apache Santuario xmlsec version. Applications failed to implement necessary security measures alongside xmlsec's XSLT features. Exploitation is contingent upon whether SAML SSO has been configured.	9.8	0.97422
CVE-2022-26134	Confluence Server and Data Center have an OGNL injection vulnerability that lets unauthenticated attackers run arbitrary code.	9.8	0.97528
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in South Korea (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-46747	An authentication bypass in BIG-IP allows attackers with network access via the management port or self IP addresses to execute system commands. This affects versions that have not reached End of Technical Support (EoTS).	9.8	0.97135
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-38831	In WinRAR, attackers can execute arbitrary code by tricking users into viewing a benign file within a ZIP archive that also contains a maliciously named folder, leading to executable content being processed.	7.8	0.44373
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in South Korea (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	0.92645
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions, especially on Cisco ASA Software before 9.16. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products are vulnerable to remote code execution due to an outdated Apache Santuario xmlsec version. Applications failed to implement necessary security measures alongside xmlsec's XSLT features. Exploitation is contingent upon whether SAML SSO has been configured.	9.8	0.97422
CVE-2022-26134	Confluence Server and Data Center have an OGNL injection vulnerability that lets unauthenticated attackers run arbitrary code.	9.8	0.97528
CVE-2021-40444	Microsoft is investigating a remote code execution vulnerability in MSHTML that affects Windows, exploited through malicious Office documents with ActiveX controls. Impacts vary with user rights, being less severe for non-admins. Updates to Microsoft Defender Antivirus and Endpoint provide protection. Further actions may depend on investigation outcomes.	7.8	0.96821
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Australia (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-46747	An authentication bypass in BIG-IP allows attackers with network access via the management port or self IP addresses to execute system commands. This affects versions that have not reached End of Technical Support (EoTS).	9.8	0.97135
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-38831	In WinRAR, attackers can execute arbitrary code by tricking users into viewing a benign file within a ZIP archive that also contains a maliciously named folder, leading to executable content being processed.	7.8	0.44373
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27997	A heap-based buffer overflow vulnerability in FortiOS and FortiProxy SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.	9.8	0.15407
CVE-2023-27532	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.	7.5	0.02703
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Australia (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	0.92645
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products are vulnerable to remote code execution due to an outdated Apache Santuario xmlsec version. Applications failed to implement necessary security measures alongside xmlsec's XSLT features. Exploitation is contingent upon whether SAML SSO has been configured.	9.8	0.97422
CVE-2022-42475	A heap-based buffer overflow vulnerability in FortiOS SSL-VPN and FortiProxy SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.	9.8	0.41883
CVE-2022-26134	Confluence Server and Data Center have an OGNL injection vulnerability that lets unauthenticated attackers run arbitrary code.	9.8	0.97528
CVE-2021-40444	Microsoft is investigating a remote code execution vulnerability in MSHTML that affects Windows, exploited through malicious Office documents with ActiveX controls. Impacts vary with user rights, being less severe for non-admins. Updates to Microsoft Defender Antivirus and Endpoint provide protection. Further actions may depend on investigation outcomes.	7.8	0.96821
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Greater China Region (1/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-4966	NetScaler ADC and Gateway reveal sensitive information when configured as a Gateway or AAA virtual server, including VPN, ICA Proxy, CVPN, and RDP Proxy setups.	7.5	0.96869
CVE-2023-47246	SysAid On-Premise has a path traversal vulnerability that enables attackers to execute code by writing files to the Tomcat webroot.	9.8	0.94113
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX allows an attacker to remotely execute code.	9.8	0.00134
CVE-2023-42793	In JetBrains TeamCity, authentication bypass leading to RCE on TeamCity Server was possible.	9.8	0.97071
CVE-2023-38831	In WinRAR, attackers can execute arbitrary code by tricking users into viewing a benign file within a ZIP archive that also contains a maliciously named folder, leading to executable content being processed.	7.8	0.44373
CVE-2023-36934	A SQL injection vulnerability in MOVEit Transfer, allowing unauthenticated attackers to modify and access database content via crafted payloads to application endpoints.	9.1	0.09417
CVE-2023-36933	In MOVEit Transfer, attackers can trigger a method causing an unhandled exception, leading to unexpected application termination.	7.5	0.00046
CVE-2023-36932	MOVEit Transfer have SQL injection flaws exploitable by authenticated attackers to access and manipulate the database.	8.1	0.0005
CVE-2023-34362	A SQL injection vulnerability in MOVEit Transfer allows unauthenticated access to its database.	9.8	0.95545
CVE-2023-27532	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.	7.5	0.02703
CVE-2023-27351	Remote attackers can bypass authentication in PaperCut NG due to a flaw in the SecurityRequestFilter class, which arises from an improperly implemented authentication algorithm.	7.5	0.02082
CVE-2023–27350	Remote attackers can exploit a flaw in PaperCut NG to bypass authentication and execute code as SYSTEM due to inadequate access control in the SetupCompleted class.	9.8	0.97204
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	0.92645

Note: This is a non-exhaustive list

Actively exploited vulnerabilities in Greater China Region (2/2)

VULNERABILITY	DESCRIPTION	CVSS	EPSS (as of Apr 2024)
CVE-2023-20269	A flaw in Cisco ASA and FTD Software's VPN allows unauthorized brute force attacks or clientless SSL VPN sessions by exploiting AAA separation issues. The vulnerability enables attackers to potentially uncover credentials or establish unauthorized VPN sessions. Valid credentials, including any second factors, are still required for access. Cisco plans to release software updates and suggests workarounds.	9.1	0.02588
CVE-2023-20095	A flaw in Cisco ASA and FTD Software's remote VPN allows remote attackers to cause a DoS by sending malicious HTTPS requests that lead to resource exhaustion.	8.6	0.00053
CVE-2023-0669	Fortra's GoAnywhere MFT has a pre-auth command injection vulnerability via object deserialization in the License Response Servlet.	7.2	0.96975
CVE-2021-40444	Microsoft is investigating a remote code execution vulnerability in MSHTML that affects Windows, exploited through malicious Office documents with ActiveX controls. Impacts vary with user rights, being less severe for non-admins. Updates to Microsoft Defender Antivirus and Endpoint provide protection. Further actions may depend on investigation outcomes.	7.8	0.96821
CVE-2006-1364	Microsoft's w3wp.exe in ASP.NET fails to correctly handle COM components without the AspCompat directive, allowing remote attackers to crash the system or deplete resources by repeatedly requesting certain documents.	7.5	0.02198

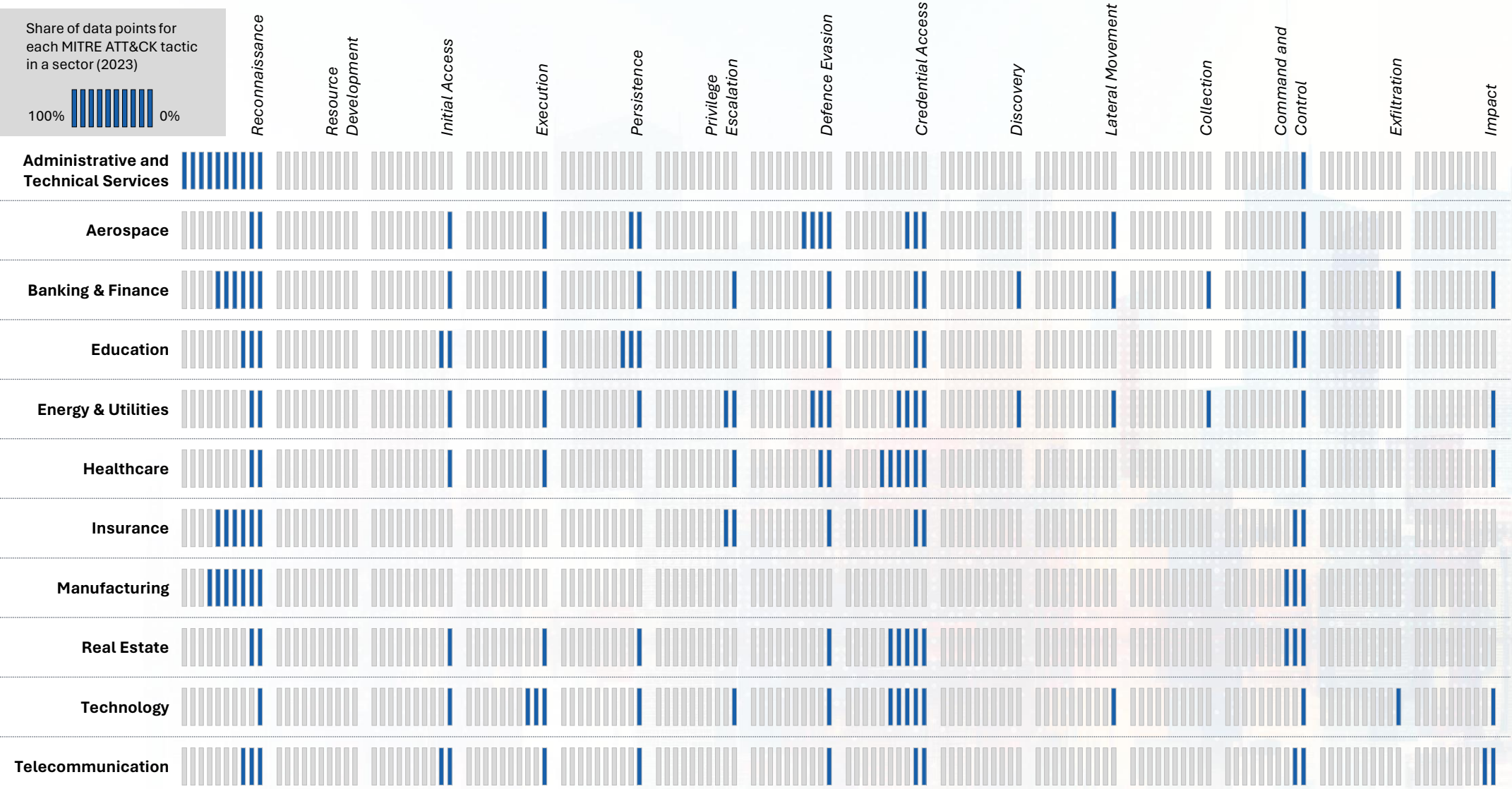
Note: This is a non-exhaustive list

APPENDIX - C
TOP MITRE ATT&CK TACTICS

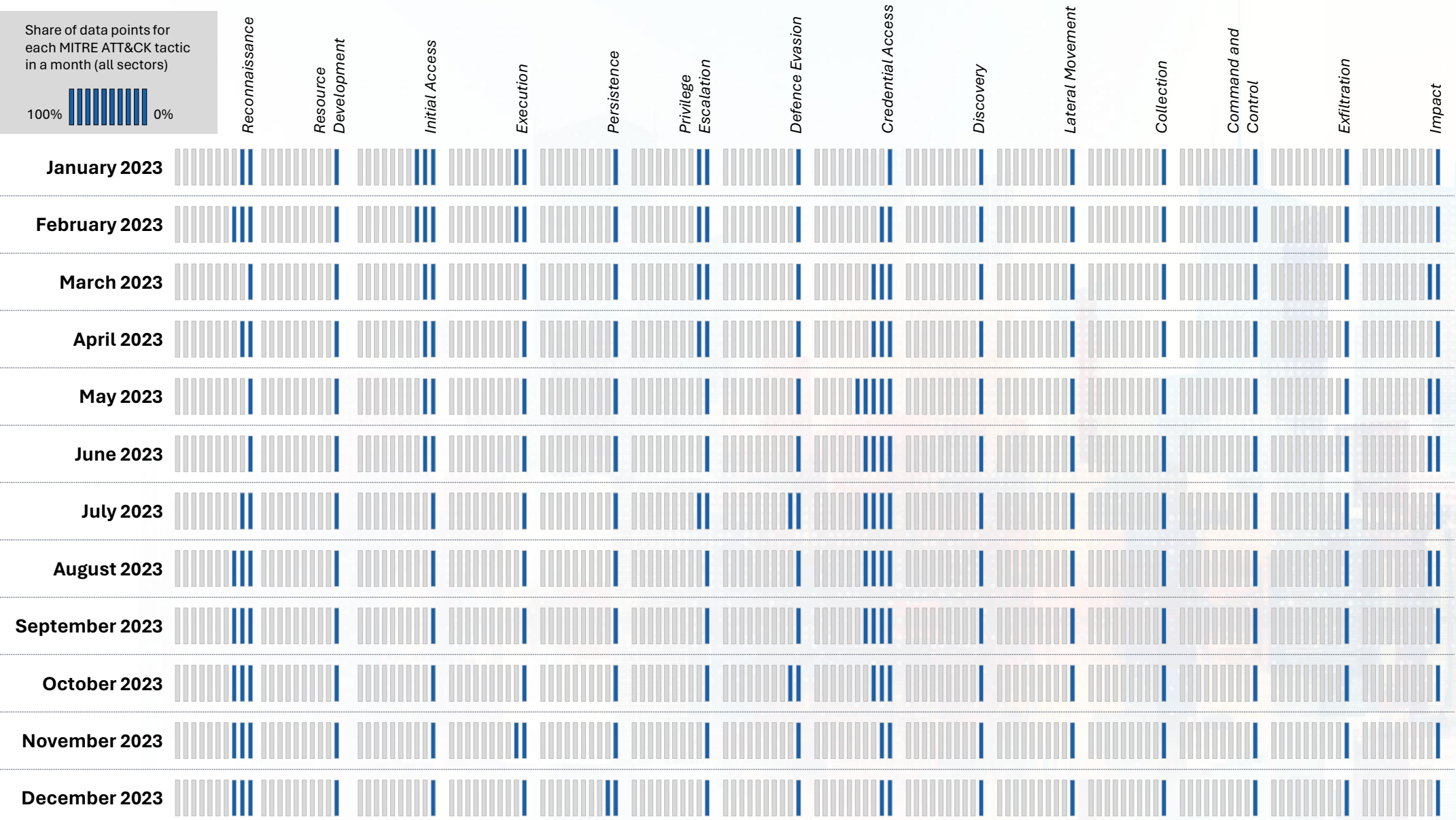
Singapore


Share of data points for each MITRE ATT&CK tactic in a month (all sectors)
100%
0%
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defence Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
January 2023
February 2023
March 2023
April 2023
May 2023
June 2023
July 2023
August 2023
September 2023
October 2023
November 2023
December 2023

Singapore

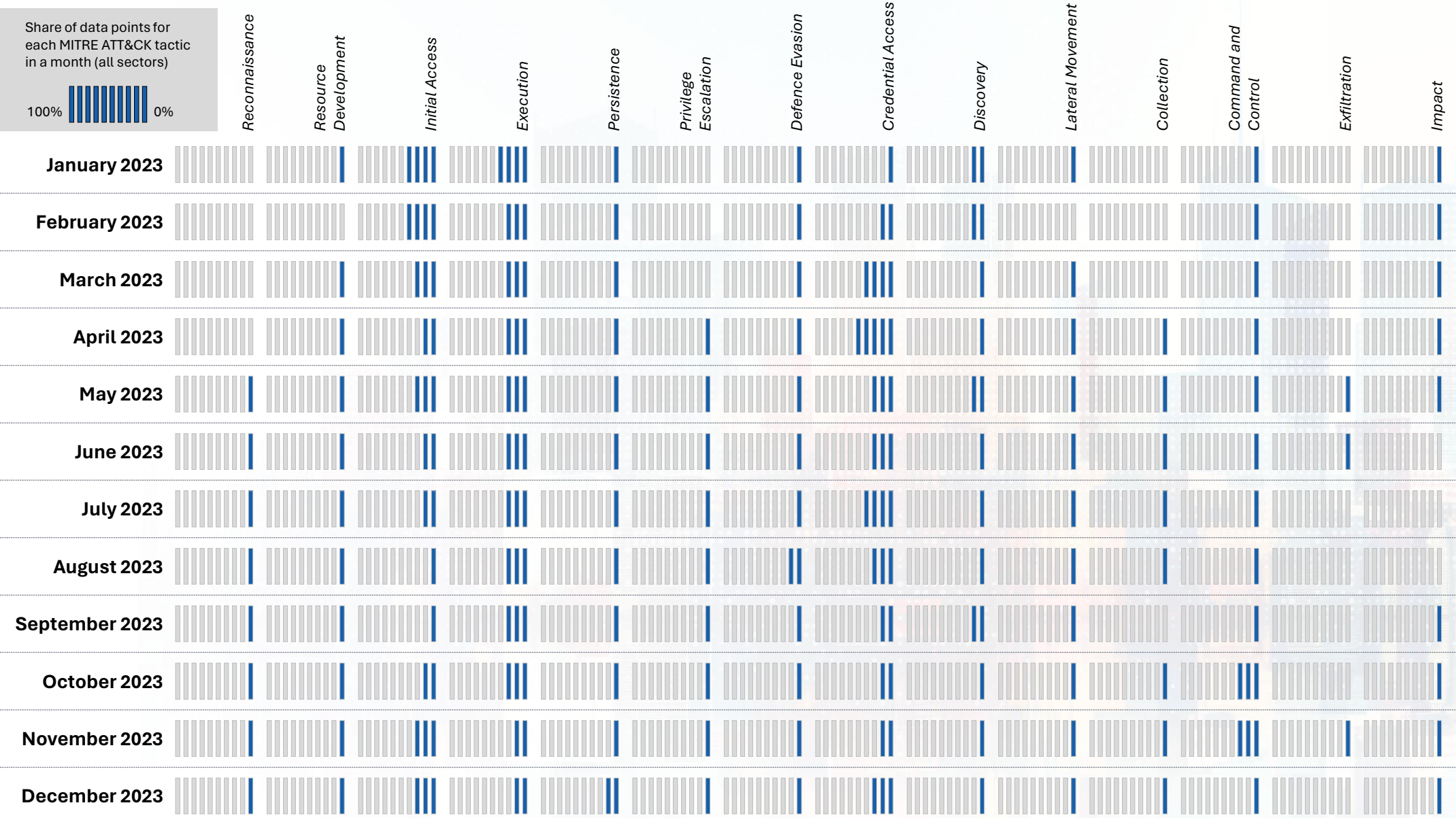

Share of data points for each MITRE ATT&CK tactic in a sector (2023)
100%
0%
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defence Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Administrative and Technical Services
Aerospace
Banking & Finance
Education
Energy & Utilities
Healthcare
Insurance
Manufacturing
Real Estate
Technology
Telecommunication

Malaysia & Indonesia

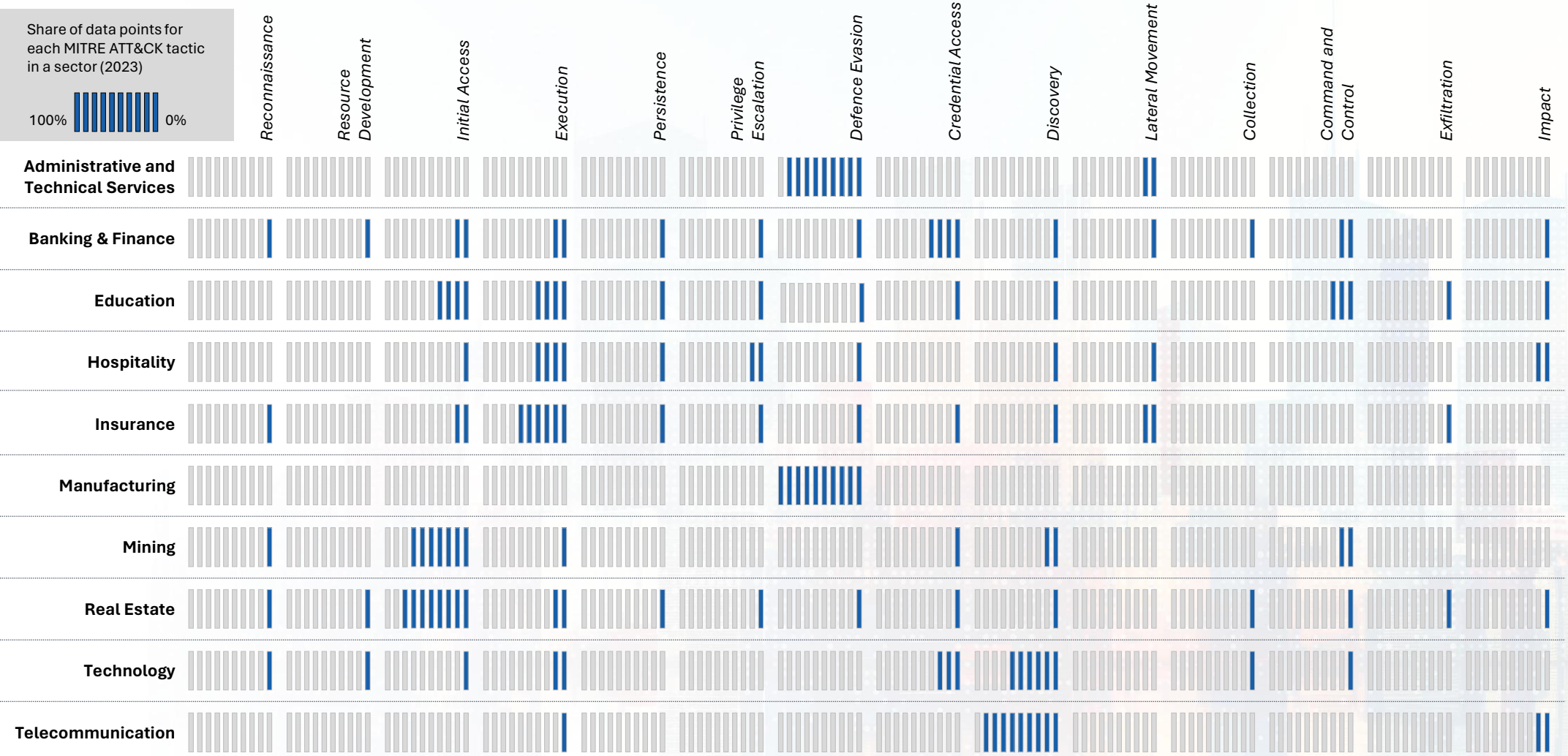


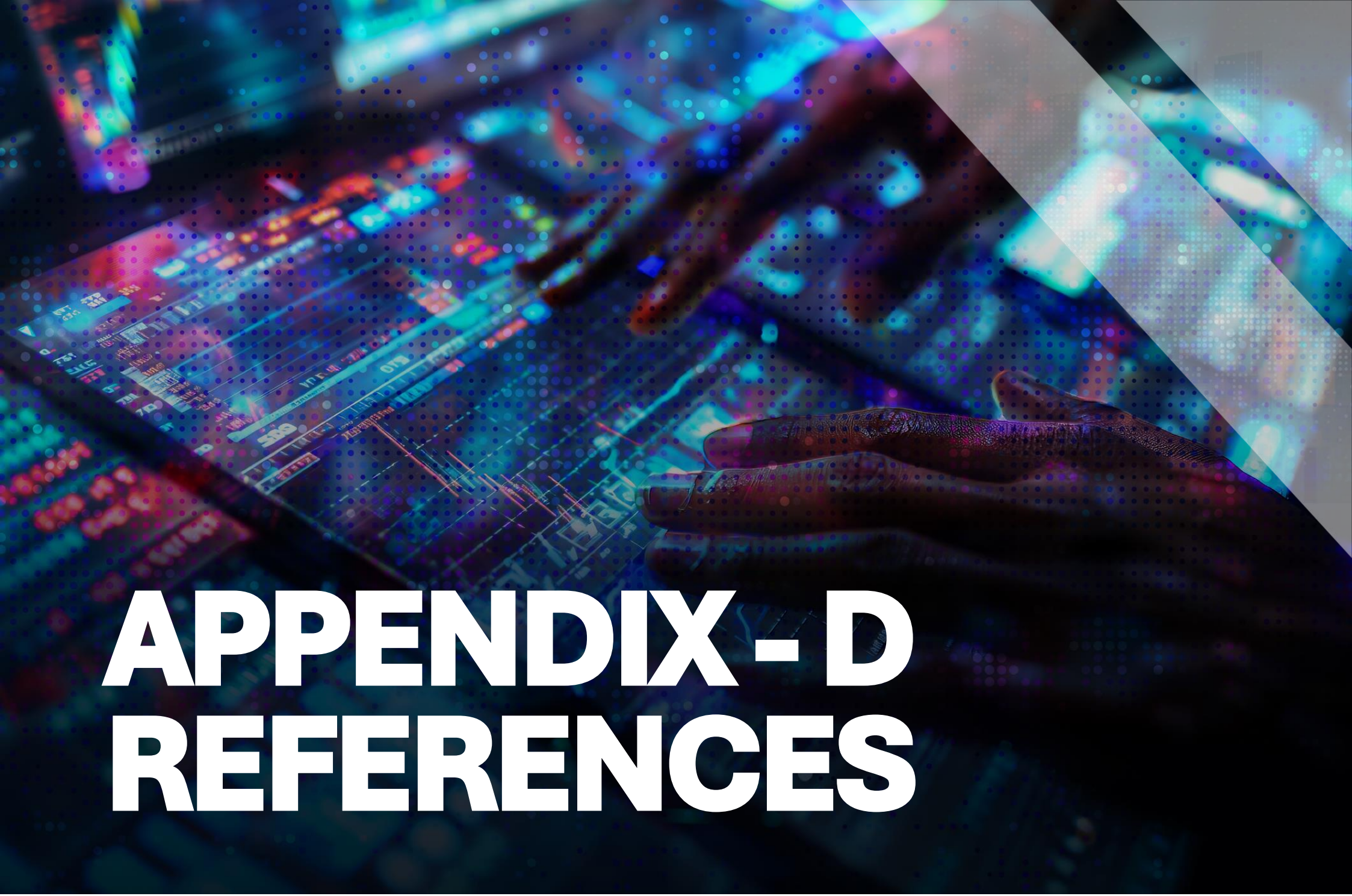
Malaysia & Indonesia

Greater China Region



Greater China Region





APPENDIX - D REFERENCES

A

A. Bokovoy, S. Ievlev, G. Kouriachy, D. Levin, A. Novodvorsky, A. Prokoudine, A. Smirnov, O. Vlasenko, M. Zabalujev. ALT Linux 2.3 Compact. Retrieved from: https://docs.altlinux.org/ru-RU/archive/2.3/html-single/compact/alt-docs-compact-en/ch01s02.html

A. Griffin. Microsoft responds after users of new Bing chatbot complain about its latest behaviour. (23 February 2023). Yahoo. Retrieved from: https://news.yahoo.com/microsoft-responds-users-bing-chatbot-171403057.html

A. Kraft. Microsoft shuts down AI chatbot after it turned into a Nazi. (25 March 2016). CBS News. Retrieved from: https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/

A. Render-Katolik. The IT Army of Ukraine. (16 August 2023). Center for Strategic and International Studies. Retrieved from: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine

A. Vassilev, A. Oprea, A. Fordyce, H. Anderson. Adversarial Machine Learning, A Taxonomy and Terminology of Attacks and Mitigations. (January 2024). NIST. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

Alert: GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries. (6 March 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/03/alert-ghostsec-and-stormous-launch.html

B

B. Kondruss. MOVEit hack victim list. (20 December 2023). Retrieved from: https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html

B. Toulas. LockBit ransomware exploits Citrix Bleed in attacks, 10K servers exposed. (14 November 2023). Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-exploits-citrix-bleed-in-attacks-10k-servers-exposed/

B. Toulas. Israel warns of BiBi wiper attacks targeting Linux and Windows. (13 November 2023). Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/israel-warns-of-bibi-wiper-attacks-targeting-linux-and-windows/

C

C. Page. PaperCut says hackers are exploiting 'critical' security flaws in unpatched servers. (25 April 2023). Techcrunch. Retrieved from: https://techcrunch.com/2023/04/25/papercut-hackers-critical-fLaw-clop-ransomware/

C. Rawling. Pizza Hut says nearly two-hundred thousand customers affected by data breach. (20 September 2023). ABC News. Retrieved from: https://www.abc.net.au/news/2023-09-20/pizza-hut-customers-affected-by-cyber-hack/102881804

C. Szewczyk. Billions from the CHIPS Act is soon to begin flowing with Samsung, Intel and TSMC set to benefit. (18 March 2024). PC Gamer. Retrieved from: https://www.pcgamer.com/hardware/billions-from-the-chips-act-is-soon-to-begin-flowing-with-samsung-intel-and-tsmc-set-to-benefit/

China-backed Hackers Hijack Software Updates to Implant "NSPX30" Spyware. (25 January 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/01/china-backed-hackers-hijack-software.html

D

D. Tilo. Over 6,000 individuals hit in Sony data breach: reports. (10 October 2023). Human Resources Director. Retrieved from: https://www.hcamag.com/au/news/general/over-6000-individuals-hit-in-sony-data-breach-reports/462431

Dormant PyPI Package Compromised to Spread Nova Sentinel Malware. (23 February 2024). The Hacker News. Retrieved from: https://thehackernews.com/2024/02/dormant-pypi-package-compromised-to.html

DragonForce Malaysia: OpsPetir. (12 Apr 2023). Radware. Retrieved from: https://www.radware.com/security/threat-advisories-and-attack-reports/dragonforce-malaysia-opspetir/

E

E. Kovacs. Law Enforcement Reportedly Behind Takedown of BlackCat/Alphv Ransomware Website. (11 December 2023). Security Week. Retrieved from: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

E. Kovacs. Ransomware Group Files SEC Complaint Over Victim's Failure to Disclose Data Breach. (16 November 2023). Security Week. Retrieved from: https://www.securityweek.com/ransomware-group-files-sec-complaint-over-victims-failure-to-disclose-data-breach/

E. Madnick. The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase. (December 2023). Apple. Retrieved from: https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

E. Stanish. Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group. (26 November 2023). CBS News. Retrieved from: https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

F

F. Koh. Kim Jong Un's move to label South Korea an enemy, drop reunification policy part of North's diplomatic playbook: Experts. (17 January 2024). Channel News Asia. Retrieved from: https://www.channelnewsasia.com/world/kim-jong-un-move-label-south-korea-enemy-drop-reunification-policy-strategic-part-norths-diplomatic-playbook-experts-4053871

F. Singer. They're not TV anchors, they're avatars: How Venezuela is using AI-generated propaganda. (22 February 2023). El Pais. Retrieved from: https://english.elpais.com/international/2023-02-22/theyre-not-tv-anchors-theyre-avatars-how-venezuela-is-using-ai-generated-propaganda.html

F. X. Frei & A. Morriss. Begin with Trust. (May 2020). Harvard Business Review. Retrieved from: https://hbr.org/2020/05/begin-with-trust

FH. Hudnall. Fact check: Video altered to show Joe Biden making transphobic remarks. (9 February 2023). USA Today. Retrieved from: https://www.usatoday.com/story/news/factcheck/2023/02/09/fact-check-video-edited-show-joe-biden-making-transphobic-remarks/11211453002/

G

G. Chan. Deepfake video of Taylor Swift speaking Mandarin sparks discussion over AI in China. (30 October 2023). The Straits Times. Retrieved from: https://www.straitstimes.com/asia/east-asia/deepfake-video-of-taylor-swift-speaking-mandarin-sparks-discussion-over-ai-in-china

G. Sharma. DragonForce Malaysia attacks Israeli institutions: Radware (14 April 2023). SecurityBrief Asia. Retrieved from: https://securitybrief.asia/story/dragonforce-malaysia-attacks-israeli-institutions-radware

H

Heightened Alert for Cyber Activities Targeting Domains and Infrastructures in Malaysia. (27 February 2022). National Cyber Coordination and Command Centre. Retrieved from: https://www.nc4.gov.my/alert/653a2988900885a0819d058d

J

J. Barrett. Latitude Financial cyber-attack worse than first thought with 14m customer records stolen. (27 March 2023). The Guardian. Retrieved from: https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen

J. Kim. South Korean startups chase Nvidia with AI chip design push. (15 March 2024). Nikkei Asia. Retrieved from: https://asia.nikkei.com/Business/Tech/Semiconductors/South-Korean-startups-chase-Nvidia-with-AI-chip-design-push

J. Munshaw. What's the deal with the massive backlog of vulnerabilities at the NVD? (19 April 2024). Talos Intelligence. Retrieved from: https://blog.talosintelligence.com/nvd-vulnerability-backlog-the-need-to-know/

J. Pearson. Lockbit cybercrime gang says it is back online following global police bust. (27 February 2024). Reuters. Retrieved from: https://www.reuters.com/technology/cybersecurity/lockbit-cybercrime-gang-says-it-is-back-online-following-global-police-bust-2024-02-26/

J. Taylor. HWL Ebsworth hack: 65 Australian government agencies affected by cyber-attack. (18 September 2023). The Guardian. Retrieved from: https://www.theguardian.com/australia-news/2023/sep/18/hwl-ebsworth-hack-65-australian-government-agencies-affected-by-cyber-attack

K

K. Alspach. CISA Breached Via Ivanti VPN Vulnerabilities: Report. (8 March 2024). CRN. Retrieved from: https://www.crn.com/news/security/2024/cisa-breached-via-ivanti-vpn-vulnerabilities-report

K. Meegan-Vickers. The LockBit takedown Law enforcement 'trolls' ransomware gang. (4 April 2024). Global Initiative. Retrieved from: https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/

K. Poireault. DragonForce Ransomware Group Uses LockBit's Leaked Builder. (25 April 2024). Infosecurity Magazine. Retrieved from: https://www.infosecurity-magazine.com/news/dragonforce-ransomware-lockbit/

Kirin 9000. Hisilicon. Retrieved from: https://www.hisilicon.com/en/products/Kirin/Kirin-flagship-chips/Kirin-9000

L

L. Tang. Billion-dollar money laundering case: Singapore police began 'comprehensive intelligence probe' in early 2022. (3 October 2023). Channel News Asia. Retrieved from: https://www.channelnewsasia.com/singapore/billion-dollar-money-laundering-police-intelligence-probe-2022-3816371

L. Yulisman. Indonesia hunts for Bjorka, hacker selling 1.3b SIM card users' data, taunting officials. (19 September 2022). Bleeping Computer. Retrieved from: https://www.straitstimes.com/asia/se-asia/indonesia-hunts-for-bjorka-hacker-selling-13b-sim-card-users-data-taunting-officials

Loongson releases next-generation CPU; new breakthrough in domestic design. (28 November 2023). Global Times. Retrieved from: https://www.globaltimes.cn/page/202311/1302643.shtml

M

M. Burgess. Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. (27 February 2022). Wired. Retrieved from: https://www.wired.com/story/ukraine-it-army-russia-war-cyber-attacks-ddos/

M. Harjani. Are US export controls making China's chip industry more innovative? (22 April 2024). Lowly Institute. Retrieved from: https://www.lowyinstitute.org/the-interpreter/are-us-export-controls-making-china-s-chip-industry-more-innovative

M. Lim. China launches its first open-source desktop operating system as it moves to cut use of US tech. (15 July 2023). Retrieved from: https://www.straitstimes.com/asia/east-asia/china-launches-its-first-open-source-desktop-operating-system-as-it-moves-to-cut-use-of-us-tech

MA-1027.022024: MyCERT Advisory - Recent Cyber Incidents Launched by TA ROOTK1T ISC Team to Malaysia Organisations. (6 February 2024). Malaysia Computer Emergency Response Team. Retrieved from: https://www.mycert.org.my/portal/advisory?id=MA-1027.022024

Microsoft Threat Intelligence. The many lives of BlackCat ransomware. (13 June 2022). Microsoft. Retrieved from: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

N

N. Eddy. DragonForce Malaysia Releases LPE Exploit, Threatens Ransomware. (1 July 2022). Dark Reading. Retrieved from: https://www.darkreading.com/vulnerabilities-threats/dragonforce-malaysia-releases-lpe-exploit-threatens-ransomware

N. Gisonna. Great Fitrewall Chinese Internet Policy. Britannica. Retrieved from: https://www.britannica.com/topic/Great-Firewall

N. Nelson. GPT-4 Can Exploit Most Vulns Just by Reading Threat Advisories. (19 April 2024). Dark Reading. Retrieved from: https://www.darkreading.com/threat-intelligence/gpt-4-can-exploit-most-vulns-just-by-reading-threat-advisories

O

O. Yoachimik & J. Pacheco. DDoS threat report for 2023 Q3. (26 October 2023). Cloudflare. Retrieved from: https://blog.cloudflare.com/ddos-threat-report-2023-q3/

P

P. Verma. AI deepfakes threaten to upend global elections. No one can stop them. (23 April 2024). The Washington Post. Retrieved from: https://www.washingtonpost.com/technology/2024/04/23/ai-deepfake-election-2024-us-india/

PJSC Rostelecom. Retrieved from: https://www.rst-com.ru/b2b/aurora/

R

R. Daws. GitHub suffers from over 100K infected repos. (29 February 2024). Developer. Retrieved from: https://www.developer-tech.com/news/2024/feb/29/github-suffers-over-100k-infected-repos/

R. Lakshmanan. New COSMICENERGY Malware Exploits ICS Protocol to Sabotage Power Grids. (26 May 2023). The Hacker News. Retrieved from: https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html

S

S. Contorno & D. O'Sullivan. DeSantis campaign posts fake images of Trump hugging Fauci in social media video. (8 June 2023). CNN. Retrieved from: https://edition.cnn.com/2023/06/08/politics/desantis-campaign-video-fake-ai-image/index.html

S. Gatlan. MITRE says state hackers breached its network via Ivanti zero-days. (19 April 2024). BleepingComputer. Retrieved from: https://www.bleepingcomputer.com/news/security/mitre-says-state-hackers-breached-its-network-via-ivanti-zero-days/

S. Ryohtaroh & T. Cheng. Japan's chip reboot: TSMC, Samsung, Micron pave way for silicon revival. (28 February 2024). Nikkei Asia. Retrieved from: https://asia.nikkei.com/Spotlight/The-Big-Story/Japan-s-chip-reboot-TSMC-Samsung-Micron-pave-way-for-silicon-revival

S. Sharwood. MongoDB to terminate Russian SaaS accounts. (15 March 2022). The Register. Retrieved from: https://www.theregister.com/2022/03/15/mongodb_terminates_russian_saas/

Samsung. Retrieved from: https://semiconductor.samsung.com/processor/

Security Asset Management Statistics to Know in 2023. (18 May 2023). Noetic Cyber. Retrieved from: https://noeticcyber.com/security-asset-management-statistics-to-know-2023/

T

T. Broderick. Russia Is Trying to Leave the Internet and Build Its Own. (12 July 2023). Scientific American. Retrieved from: https://www.scientificamerican.com/article/russia-is-trying-to-leave-the-internet-and-build-its-own/

Tizen. Retrieved from: https://docs.tizen.org/platform/what-is-tizen/overview/

V

V. Insinna & Z. Siddiqui. Boeing says 'cyber incident' hit parts business. (3 November 2023). IT News. Retrieved from: https://www.itnews.com.au/news/boeing-says-cyber-incident-hit-parts-business-601999

Vx-underground. X. (4 March 2024). Retrieved from: https://twitter.com/vxunderground/status/1764676460113994220

W

W. Knight. The US Throws $52 Billion at Chips—but Needs to Spend It Wisely. (28 July 2022). Wired. Retrieved from: https://www.wired.com/story/chips-act-52-billion-semiconductor-production/

X

XZ Utils Backdoor — Everything You Need to Know, and What You Can Do. (1 April 2024). Akamai. Retrieved from: https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know