Technology, Media, and Telecommunications (TMT) and Transport Industry Groups were Singapore's Top Cyber Targets in 2021: Ensign InfoSecurity Report

Ransomware, multi-modal attacks, and cyber supply chain compromises emerge as key cyber threat trends impacting organisations in 2022

Singapore, 21 July 2022 – Ensign InfoSecurity (Ensign), Asia's largest pure-play end-to-end cybersecurity services provider, today unveiled the findings of its Cyber Threat Landscape 2022 report, which found that the Technology, Media, and Telecommunications (TMT) and Transport industry groups were the top targets for cyber threats in Singapore in 2021.

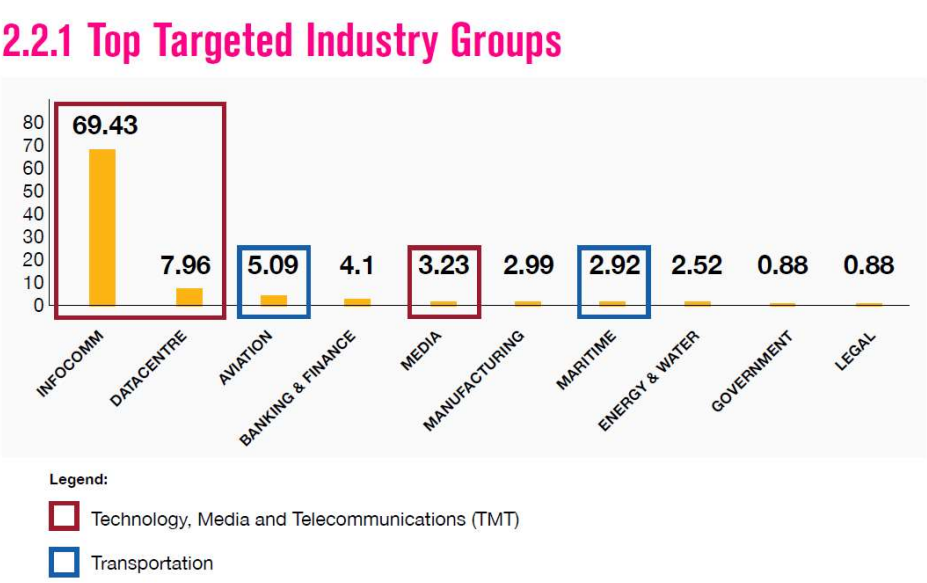
The latest edition of Ensign's report provides insights and analysis into the cyber threat landscape in Singapore and key Asia Pacific markets such as Hong Kong, Malaysia, and South Korea. It also explores emerging cyber threats that will impact organisations in 2022 and beyond.

Here are some of the key findings from the report:

Singapore: TMT and Transport Emerged as Top Targeted Industry Groups in 2021

The Technology, Media, and Telecommunications (TMT) industry group, comprising infocommunications[1], data centre and media sectors, was the top target for threat actors in 2021. Ensign found that nearly **70% of malicious traffic** observed in Singapore in 2021 was directed at the infocommunications sector.

Percentage of malicious traffic observed targeting Singapore industries in 2021



Threat actors targeted TMT organisations to covet these firms' bandwidth and computing resources, which can be used to build botnets or compromise other connected organisations. Additionally, many TMT organisations also support other businesses by providing services such as processing and storing sensitive data. This gives malicious actors

[1] **Infocommunications** companies specialise in network connectivity and infocommunication technology products and services. Some examples include telecommunications companies, internet service providers, and network operators.

an easy access pathway to target and access downstream customers via cyber supply chain compromise.

“Infocommunications companies are lucrative targets for malicious actors as their services penetrate and power almost every aspect of our society and digital economy. We need to constantly elevate our cyber defence capabilities to prevent cyber threats from derailing our nation’s digital ambition and undermining our position as a regional technology hub. This would require public and private stakeholders to work closely together to build a vibrant cybersecurity ecosystem conducive to nurturing skilled cyber talents and driving innovation,” said Steven Ng, CIO and EVP of Managed Security Services, Ensign.

In addition, threat actors were targeting media organisations following the cyberattack campaigns outside Singapore. Media companies saw cyberattacks designed to cause business disruptions, including ransomware campaigns. A key driver behind these attacks was to prevent facts from being disseminated to the public. The intention was to distort or disrupt the public’s understanding of the situation.

The Transportation industry group, comprising the Aviation and Maritime sectors, became increasingly attractive targets due to their global and regional connectivity. This is fuelled by the collection of personal identifiable information (PII) for cross-border travel, which may include medical information for COVID-19 tracking purposes.

The Maritime sector continues to see ransomware attacks targeting shipping lines and maritime support services. This further exacerbates supply chain challenges caused by COVID-19. Ransomware operators are likely exploiting the already-strained business operations to pressure organisations to pay the ransom.

Singapore: Rise in Opportunistic Cyberattacks due to COVID-19

In 2021, Ensign observed an increase in opportunistic cyber incidents using stolen credentials in Singapore. It revealed that **80% of these incidents were traced to** “hands on keyboard” intrusions against remote access portals such as VPN and Virtual Desktop Interfaces. In these attacks, threat actors manually log into an infected system using leaked credentials.

These attacks can be attributed to COVID-19 where companies were forced to swiftly establish emergency remote working arrangements. However, some of these systems are not adequately secured. As a result, past credential leaks and bad cyber hygiene, such as reusing leaked passwords, led to a number of these opportunistic cyber breaches.

Global trends: Ransomware attacks and cyber supply chain disruptions are growing globally

1. Increasingly Sophisticated Ransomware Tactics

Ransomware remains a prominent and prevalent threat globally. This is exacerbated by increasingly sophisticated methods, such as multi-extortion attacks ransomware attacks.

Ransomware operators most typically leverage a mix of the following extortion threats:

1. Disrupting business operations;
2. Leaking exfiltrated data;
3. Reporting to regulators;
4. Reporting to stock exchange for public listed victims;
5. Rallying key customers to force the victim to pay the ransom by threatening to leak their personal or sensitive information;
6. Buying online advertisements to publicise the compromised victims; and
7. Disrupting Internet-facing services via Distributed Denial-of-Service (DDoS) attacks.

Threat actors are highly selective of their victims. Their criteria are typically based on the target victims' ability to pay a high ransom amount. These organisations usually provide high-availability services required for uninterrupted downstream operations.

Ransomware operators are also prioritising more lucrative regions and markets in their attacks. According to the data that Ensign gathered from ransomware data leak sites and active ransoms in 2021, almost half of the ransomware incidents occurred in companies operating in the US (49%), followed by Europe (22%) and Asia (9%).

Furthermore, Ensign found a 133% increase in Singapore-based companies being mentioned on ransomware leak sites. The financial sector is the top target for ransomware attacks. The maritime and aviation are the next most targeted sectors.

2. Multi-modal Attacks, incorporating Misinformation, Disinformation and Malinformation (MDM), on the Rise

Multi-modal attacks have risen in prominence as threat actors attempt to increase their success rate. As these types of attacks come from multiple fronts, they can result in greater confusion among the victims and require more resources to tackle. In particular, MDM techniques have been incorporated in multi-modal attacks to support phishing or perform influence campaigns.

MDM techniques employed for phishing typically leverage misleading information or distorted facts to trigger the victims' urgency of response or action. This increases the threat actors' chances of successfully gaining access to the targets. Such techniques have been observed in the COVID-19 themed phishing attacks and election-related attacks.

Threat actors also leverage MDM techniques in extortionist attacks. This includes using false information to cause negative hype or sharing illegally exfiltrated sensitive information to influence a large-scale outcome.

3. Threat Actors Compromising the Cyber Supply Chain Upstream

Cyberattacks through compromised cyber supply chains serve as effective and less secured backdoors for threat actors, giving them a higher probability of success with a minimum investment of efforts and resources. As threat actors move upstream in the cyber supply chain, there are more significant implications, affecting more victims downstream.

The cyber supply chain comprises hardware, software, and vendors, and each element presents unique security complexity. A key challenge organisations face across the cyber supply chain is the imperfect inventory of assets. This allows threat actors to slip through an organisation's security blind spots and compromise their digital environment.

Furthermore, the report highlighted that threat actors can compromise all stages of the software development chain:

- Threat actors can attack and compromise open-source libraries. This can expose organisations to risks such as code injections when their developers leverage commercial reusable code libraries.
- During a software's building and test phase, threat actors can attack code repositories, leading to exposed credentials and certificates and malicious code injected with automated commit.
- Threat actors also exploit zero-day vulnerabilities when new software is launched, or updates are implemented.

The next category of cyber supply chain compromises relates to hardware. This category is the hardest for cyber defenders to address and increasingly involves firmware and

microcode. Sophisticated attackers continue to exploit them as firmware patches can be complex to implement. Hence, remediation may only be possible in 6 to 9 months.

Furthermore, hardware-related vulnerabilities provide the threat actor access to privileges higher than the operating system. This means that the threat actor can potentially infect the system with malware and maintain persistence without being detected by conventional anti-malware solutions or even modern endpoint detection and response solutions. Due to the nature of such vulnerabilities, the implications are much more severe than application-level vulnerabilities.

END

About Ensign InfoSecurity

Ensign InfoSecurity is the largest, pure-play end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Their core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is in-house research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

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

Media Contacts

Ms Wendy Ong
Ensign InfoSecurity
+65 9247 9506
wendy_ong@ensigninfosecurity.com

Mr Goh Wee Gin
IN.FOM (On behalf of Ensign InfoSecurity)
+65 94570207
ensignpr@infom.asia