Technology, Manufacturing, and Banking and Finance were Threat Actors' Top Targeted Sectors in Asia Pacific in 2020: Ensign InfoSecurity Report

The report also found that opportunistic threat actors sought to exploit people's emotions and uncertainties during the pandemic by using Covid-19 topics to anchor their phishing campaigns

Singapore, 14 June 2021 – Ensign InfoSecurity (Ensign), Asia's largest, pure-play cybersecurity firm, today unveiled the findings of its **Cyber Threat Landscape 2021** report, which found that the **technology**, **manufacturing,** and **banking and finance** industries were the top targets in Asia Pacific for threat actors in 2020.

Ensign's latest report provides insights into the cyber risks and threats that surfaced across four Asia Pacific markets – Hong Kong, Malaysia, Singapore, and South Korea – as the pandemic dramatically reshaped the business landscape. It also explores cyber threat trends that are emerging or will persist in 2021.

Here are the key findings and insights from the report:

Sector analysis: Threat actors targeted the technology sector to achieve economies of scale

Technology service providers were attractive targets for threat actors as many organisations have engaged their services during the pandemic to ensure business continuity. A successful cyber attack would allow the threat actors to obtain the credentials of these service providers' clients, gaining them illicit access to a wide range of companies.

Threat actors also targeted technology hardware and software vendors to breach and implant malicious codes and components into the vendors' product development systems. This enabled the perpetrators to rapidly develop zero-day exploits or create backdoors to compromise the integrity of the products, allowing them to readily reach a larger pool of targets.

The threat actors' focus on these sectors is a concern as organisations continue to invest in digital technologies. According to IDC, digital transformation investments in Asia Pacific including Japan and China (APJC) are poised to hit an estimated US$921 billion by 2024, compared to US$430 billion in 2019[1]. Additionally, IDC estimates that by the end of 2023, 80% of enterprises in Asia Pacific will put mechanisms in place that will enable them to shift to cloud-centric infrastructure and applications twice as fast as before the pandemic[2].

"Technology suppliers and service providers will continue to be lucrative targets for threat actors as organisations become increasingly reliant on digital technologies to support their business operations and position themselves for the future. If threat actors can successfully compromise just one of these companies' systems, it can create a ripple effect that will impact large groups of organisations across industries and geographies," said Steven Ng, CIO and EVP of Managed Security Services, Ensign.

"Organisations need to recognise that as their cyber supply chain ecosystem expands and diversifies, they will also need to take additional steps to mitigate the elevated cyber risks that come with it. This includes increasing the organisation's situational awareness by maintaining

[1] IDC Worldwide Digital Transformation Spending Guide - Technology Forecast 2021

[2] IDC FutureScape: Worldwide IT Industry 2021 Predictions — Asia/Pacific (Excluding Japan) Implications

a complete inventory of the software, hardware, and information assets that are within their network, and those managed by their partners and vendors," added Steven.

Sector Analysis: Threat actors exploited Covid-19-induced disruptions and set their sights on trade secrets

Ensign highlighted that in 2020, threat actors attacked manufacturing companies with ransomware. The perpetrators understood that these companies' production capabilities were already strained due to the pandemic-induced supply chain disruptions. This made manufacturers more willing to pay the ransom to resume operations quickly and avoid further production disruption.

Cyber adversaries also targeted manufacturing companies to steal their trade secrets, including industrial design, operational knowledge, as well as source materials and suppliers. These types of information are particularly valuable as they can significantly undermine the victims' competitive edge while boosting the capabilities of their competitors.

Sector Analysis: Threat actors intensified social engineering attacks and sought to exploit remote working arrangements in the banking and finance sector

As the country went into lockdown during the pandemic in 2020, there was increased usage of online banking services. This led threat actors to ramp up their social engineering attacks by faking banking websites and mobile applications to deceive bank customers into disclosing their credentials.

The report also revealed a greater increase in threat activities in this sector due to the widespread adoption of remote working arrangements. More exploit attempts were targeting remote solutions used in this sector compared to other industries. Threat actors were particularly interested in getting credentials to gain access to banks and other financial institutions. They could sell this information to ransomware operators and other sophisticated threat groups that can find their way into these organisations' core network.

Emotet and TrickBot were Top Malware Detected Across Asia Pacific

Ensign found that **Emotet** and **TrickBot** were the top malware observed across the region in 2020, constituting the bulk of Command & Control (C2)[3] threat activities detected, especially in Hong Kong, Malaysia, and Singapore.

Threat actors commonly use Emotet and TrickBot as they are versatile in design, allowing the perpetrators to steal credentials, obtain information to move deeper into the infiltrated network, and inject additional malicious payloads into the compromised digital environment.

Threat actors frequently target technology service providers with these two malware families due to their capabilities to download more malware into the infected systems. Both Emotet and Trickbot were also observed to be used in phishing campaigns worldwide.

Opportunistic Threat Actors Exploited Covid-19 in Phishing Campaigns

The report revealed that threat actors sought to exploit individuals' anxiety, fear, and curiosity caused by the pandemic through phishing attacks. Ensign uncovered that **99% of the phishing campaigns** detected in Singapore in 2020 were centred on Covid-19 subjects, and that the market's Circuit Breaker period provided an opportune timeframe for threat actors to launch phishing attacks.

---

[3] Command and Control is a set of techniques that threat actors use to communicate and commander devices that have been compromised by malware. Threat actors can issue instructions to the compromised devices, including downloading additional malicious payloads or transferring stolen data back to the threat actors.

Similarly, in South Korea, most phishing emails also took advantage of the pandemic situation. One of the top threat actor groups in Asia Pacific, Lazarus Group, also impersonated the South Korean government to announce fake additional Covid-19 payouts and shopping vouchers in their phishing campaign in June 2020. The attacks were targeted at 700,000 email addresses they have illicitly obtained from previous breaches.

Moreover, Ensign found that Covid-19-themed phishing attacks are more effective. In an exercise Ensign conducted to test a client's cybersecurity measures, 35% of the organisation's employees clicked on the simulated malicious link included in Ensign's mock Covid-19-related phishing email and provided their personal information. This is 10% higher than the average result of past exercises, demonstrating the effectiveness of customised, well-timed phishing campaigns.

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:

Sherin Y Lee
Head of Marketing
Ensign InfoSecurity
marketing@ensigninfosecurity.com

Ashleigh Ow
IN.FOM (on behalf of Ensign InfoSecurity)
+65 6440 0122
ensignpr@infom.asia