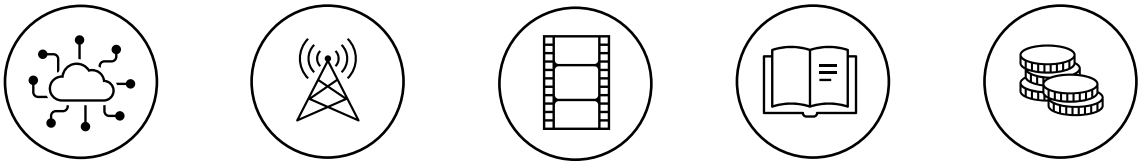
Waterhole Attacks and Phishing Identified as Singapore's Top Cyber Threat Vectors in 2019, Contributing to 84% of Cyberattacks: Ensign InfoSecurity Report

The report also uncovered a surge in activities from the threat actor group, APT32, in Singapore and identified the Emotet malware as a rising threat in 2019

Singapore, 18 May 2020 – Ensign InfoSecurity (Ensign), one of Asia Pacific's largest pure-play cybersecurity firms, today unveiled the findings of its **Singapore Threat Landscape 2019** report, which identified **waterhole attacks**, a strategic website compromise attack, and **phishing** as the nation's top threat vectors in 2019, accounting for **84%** of all cyberattacks detected.

The report also revealed that the **high technology**[1] industry in Singapore is the top target for threat actors in 2019. Companies in this sector are attractive targets as threat actors want to exploit their data centre infrastructure to expand their botnet activities as well as target other organisations whose servers are being hosted there.

In 2019, the top five most targeted sectors in Singapore are:



1. High Technology
2. Info-communications[2]
3. Media
4. Institutes of Higher Learning
5. Financial Services

This report was generated using Ensign's proprietary tools and data models, including Ensign Singapore-centric Cyber Threat Intelligence, Cyber Threat Detection & Analytics engine, and the Ensign IP360 platform which profiles activities and behaviours of anonymous IPs in enterprise network traffic.

"Relevance and context are the most important elements when analysing cyber threat intelligence as threats and trends can differ across geographies, sectors and companies," said Dr. Lim Woo Lip, Executive Vice President, Ensign Labs, Ensign InfoSecurity. "Only by combining different global and local cyber threat intelligence sources are we able to derive accurate and deep information about Singapore-specific threats and help organisations bolster their cybersecurity posture by providing contextulised, actionable insights."

Singapore's Top Two Threat Vectors in 2019

Waterhole attacks are the most prevalent threat vector of 2019, contributing to **nearly half (47%)** of all detected cyberattacks in Singapore. Waterhole attacks occur when an attacker compromises a website and replaces its content with malicious payloads. Unsuspecting victims who then download content from these websites will infect their machines with malware.

This method enables threat actors to execute supply chain attacks where they infect servers

[1]For **high technology** companies, technological innovations and advanced systems, applications, and devices play a central role in their core business offerings and services. Some examples include cloud, data centre, and web hosting service providers.
[2] For **info-communications** companies, they specialise in network connectivity and info-communication technology products and services. Some examples include telecommunications companies, internet service providers, and network operators.

containing updates of popular software and replace these updates with malicious codes to spread malware. This allows threat actors to achieve mass infection, especially when the vulnerable web server is popular and trusted by end users.

The other top threat vector in Singapore is **phishing** (also known as malspam), and almost **two out of five (37%)** of the detected cyberattacks in 2019 can be attributed to it. Phishing is an effective social engineering technique and a popular tactic for threat actors as it is easy to execute and able to target a wide pool of victims.

APT32 – Threat Actor Group with Highest Cyberattack Footprint in 2019

Both waterhole attacks and phishing are the favoured techniques of the threat actor group, **APT32**. The report uncovered that the increase in activities associated with APT32, also known as Oceanlotus, is higher than any other threat actor groups in Singapore in 2019.

APT32, which has been active since 2014, concentrates its activities in Southeast Asia and has targeted multiple private sectors and governments across the region.

In 2019, Ensign detected APT32 associated activities in **23 out of 34 sectors (68%)** in Singapore. The spread of cyberattacks across diverse sectors aligns with APT32's strategy of running opportunistic phishing email campaigns throughout the year.

From April to May 2019, Ensign detected a **500%** spike in APT32 activities in Singapore's manufacturing sector. From October to December 2019, Ensign found an **800%** increase in APT32 activities, which is the result of seasonal phishing campaigns that this threat actor group was running during the shopping and festival seasons.

Emotet – A Rising Threat in 2019

The report also found that Emotet was the most prominent malware in Singapore. Ensign detected Emotet activities in **27 out of 34 (79%)** sectors in 2019, impacting more than **1,200 companies**. The widespread attacks across a broad spectrum of sectors indicates the attacks were likely opportunistic and in the form of spam campaigns.

In the first half of 2019, especially from February to April, Ensign detected high volumes of probing activities on port 445, which is a vulnerable port targeted by Emotet. It is likely that threat actors were scanning for vulnerable targets as part of their reconnaissance.

In Q4 of 2019 (1 October to 31 December), Emotet phishing detections spiked by **nine times** compared to Q3 of 2019 (1 July to 30 September). This can be attributed to the launch of phishing email campaigns by various threat actor groups.

In the same period, there was an 11 times increase in outgoing Emotet C2 (command and control) detections compared to Q3 of 2019. The increase in outgoing traffic with Emotet indicators-of-compromise (IoCs) can be attributed to servers being infected by phishing spam campaigns.

"Conventional and reactionary signature-based threat detection is inadequate in today's cyber threat landscape as modular, polymorphic malware, such as Emotet, are emerging faster than ever. Organisations need to have a proactive cybersecurity posture, and this not only requires access to hyperlocalised, actionable threat intelligence, but also behaviour-based security capabilities that can detect changes in adversary tactics and techniques based on the MITRE ATT&CK® framework,[3]" added Dr. Lim.

[3] **MITRE ATT&CK®** (Adversarial Tactics, Techniques, and Common Knowledge) framework is a knowledge base of cyber threat tactics and technique which allows cybersecurity researchers, cyber threat hunters and red teamers to better understand cyber threats and assess an organisation's cyber risks.

END

About Ensign InfoSecurity

Ensign InfoSecurity is the largest pure-play cybersecurity service provider in Asia with an extensive footprint within the region. The company is headquartered in Singapore, and has offices in Malaysia, Hong Kong and South Korea. It has a workforce of over 500 cybersecurity professionals with skills in the provision of comprehensive cybersecurity services. Its core competencies include security advisory and assurance, architecture design, implementation, validation and management of advanced security controls, threat hunting, and incident response services. Underpinning these competencies is in-house research and development in cybersecurity.

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

Jaclyn Phan
IN.FOM (on the behalf of Ensign InfoSecurity)
ensignpr@infom.asia