Ensign InfoSecurity Unveils New Cyber Threat Detection & Analytics Engine that Provides Unique Singapore-centric, Sectoral Insights on Emerging Cybersecurity Threats

Emotet is identified as one of the key emerging cyber threats in Singapore; its activities were detected in the networks of 1 out of 2 organisations

SINGAPORE. 16 September 2019 **–** Ensign InfoSecurity (Ensign), one of the largest pure-play cybersecurity companies in Asia Pacific, unveiled today its proprietary, first of its kind, **Cyber Threat Detection & Analytics** engine. It is capable of providing highly localised cyber threat intelligence by analysing Singapore-centric network data, which is then correlated and corroborated with global cyber threat intelligence.

This provides organisations with highly contextualised and actionable information to preempt and defend against emerging threats.

The **Ensign Cyber Threat Detection & Analytics** engine was unveiled in conjunction with the official opening of Ensign's global headquarters and its new Security Operations Centre. Senior Minister and Coordinating Minister for National Security, Mr Teo Chee Hean, was the Guest-of-Honour of the event.

Singapore's Senior Minister and Coordinating Minister for National Security, Mr Teo Chee Hean, giving a speech at the official opening of Ensign's global headquarters.

"Cyber threat actors today are constantly evolving their tactics, techniques and procedures (TTPs) that allow them to target new attack vectors and vulnerabilities, while staying undetected in an organisation's network," said Dr. Lim Woo Lip, Executive Vice President, Technology & Capabilities, Ensign InfoSecurity.

"The amalgamation of global and local threat intelligence enables Ensign to provide unique cyber threat insights that fuel effective and holistic cybersecurity strategies. This allows us to identify emerging threats and key vulnerabilities, and proactively implement a multidimensional cyber defence plan, hours or even days, before an attack," Dr Lim elaborated.

Providing Highly Contextualised, Actionable Cyber Threat Intelligence by Leveraging Local Insights and Global Sources

Ensign’s proprietary **Cyber Threat Detection & Analytics** engine leverages big data analytics and advanced artificial intelligence (AI) to detect suspicious activities, and identify threats found in the networks of locally-based organisations.

One of the engine’s key capabilities is real-time behavioural profiling of network data. This function allows Ensign to stay ahead of threat actors’ fast evolving TTPs by examining anomalies in an organisation’s network, such as malicious behaviours or patterns associated with different types of cyber threats.

Ensign also collaborates with its cybersecurity partners in gathering global threat intelligence to complement its local threat data sources.

The combination of local and global intelligence enables the Ensign Cyber Threat Detection & Analytics engine to provide real-time, highly contextualised, Singapore-centric threat insights that focus on attacks targeting local networks. It can also identify threats that are unique to different sectors.

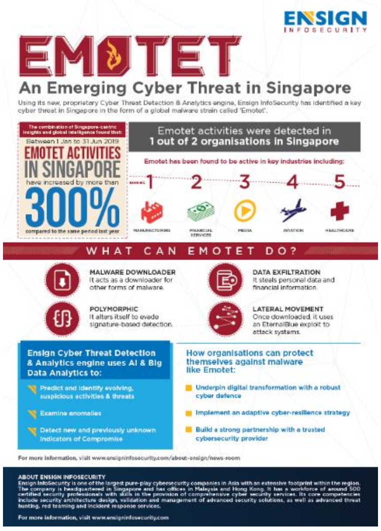
This empowers critical information infrastructure providers, government institutions and enterprises with actionable, sector-specific information, giving them the ability to identify, detect and protect against emerging threats, such as Emotet, with higher confidence and greater accuracy.

Emotet – A Key Emerging Threat in Singapore

Emotet is one of the key cyber threats that Ensign has identified through its **Cyber Threat Detection & Analytics** engine.

First detected by cybersecurity researchers in 2014, Emotet was created as a Trojan virus to steal financial data for illicit monetary gain. Today, Emotet is becoming a significant threat as cyber threat actors have modified the malware to download and deliver other malicious variants.

Between 1 January 2019 to 31 June 2019, Ensign found that Emotet activities in Singapore have increased by more than 300% compared to the same period last year. It has also detected activities from this malware in 50% of local organisations’ network.



ENSIGN INFOSECURITY

EMOTET

An Emerging Cyber Threat in Singapore

Using its new, proprietary Cyber Threat Detection & Analytics engine, Ensign InfoSecurity has identified a key cyber threat in Singapore in the form of a global malware strain called ‘Emotet’.

The combination of Singapore-centric insights and global intelligence found that:

Between 1 Jan to 31 Jun 2019

EMOTET ACTIVITIES IN SINGAPORE have increased by more than 300% compared to the same period last year

Emotet activities were detected in 1 out of 2 organisations in Singapore

Emotet has been found to be active in key industries including:

WHAT CAN EMOTET DO?

MALWARE DOWNLOADER
It acts as a downloader for other forms of malware.

DATA EXFILTRATION
It steals personal data and financial information.

POLYMORPHIC
It alters itself to evade signature-based detection.

LATERAL MOVEMENT
Once downloaded, it uses an EternalBlue exploit to attack systems.

Ensign Cyber Threat Detection & Analytics engine uses AI & Big Data Analytics to:

- Predict and identify evolving, suspicious activities & threats
- Examine anomalies
- Detect new and previously unknown Indicators of Compromise

How organisations can protect themselves against malware like Emotet:

- Underpin digital transformation with a robust cyber defence
- Implement an adaptive cyber-resilience strategy
- Build a strong partnership with a trusted cybersecurity provider

For more information, visit www.ensigninfosecurity.com/about-ensign/news-room

ABOUT ENSIGN INFOSECURITY
Ensign InfoSecurity is one of the largest pure-play cybersecurity companies in Asia with an extensive footprint within the region. The company is headquartered in Singapore and has offices in Malaysia and Hong Kong. It has a workforce of around 500 certified security professionals with skills in the provision of comprehensive cyber security services. Its core competencies include security architecture design, validation and management of advanced security solutions, as well as advanced threat hunting, red teaming and incident response services.

For more information, visit www.ensigninfosecurity.com

Traditionally used to target the financial services sector, Emotet has been modified to target other industries.

In Singapore, Ensign uncovered that the top five sectors with the highest regularity of observed Emotet activities in the first half of 2019 were:

Ranking	Sector
1	Manufacturing
2	Financial Services
3	Media
4	Aviation
5	Healthcare

“Due to its modular and polymorphic composition, Emotet is almost invisible to conventional signature-based cybersecurity solutions, explain Dr Lim.

“By tapping on advanced analytics and deep learning to tackle sophisticated threats, cybersecurity teams will not only be able to detect and respond to an attack in a timely and effective manner, but also analyse and decipher valuable intelligence that can be used to devise preemptive measures to stop future attacks,” concluded Dr Lim.

About Ensign InfoSecurity
Ensign InfoSecurity is one of the largest pure-play cybersecurity companies in Asia with an extensive footprint within the region. The company is headquartered in Singapore and has offices in Malaysia and Hong Kong. It has a workforce of around 500 certified security professionals with skills in the provision of comprehensive cyber security services. Its core competencies include security architecture design, validation and management of advanced security solutions, as well as advanced threat hunting, red teaming and incident response services.

For more information, visit www.ensigninfosecurity.com.

Media Contacts:

Chuang Bing Han
Manager, Marketing, Brand & Communications
Ensign InfoSecurity
marketing@ensigninfosecurity.com

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