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 30 Jun 2019
Emotet activities were detected in 1 out of 2 organisations in Singapore

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

1. MANUFACTURING
2. FINANCIAL SERVICES
3. MEDIA
4. AVIATION
5. HEALTHCARE

The combination of Singapore-centric insights and global intelligence found that:
Emotet activities have increased by more than 300% compared to the same period last year.

WHAT CAN EMOTET DO?

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

POLYMORPHIC
It alters itself to evade signature-based detection.

DATA EXFILTRATION
It steals personal data and financial information.

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

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