Security Predictions 2018

by StarHub Cyber Security

Data breaches continues to be an issue

2017 saw a few major data leaks from big companies like **Yahoo**, **Uber** and **Equifax**.

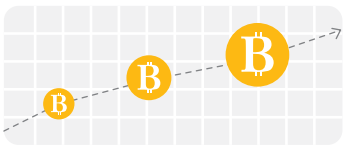
Even the National Security Agency (NSA) was not spared, with a suite of government hacking tools exposed in April.

Hackers will increasingly target Enterprises and Government agencies using **social engineering** and **exploitation techniques**. With the **leakage of NSA hacking tools** like the EternalBlue, hackers are **better equipped** to continue their attacks in 2018.

Rise of cyber criminal interest in Bitcoin

Thanks to its anonymous nature, **Bitcoin is a preferred payment method** of choice for **shady or illegal transactions**.

In December, **Bitcoin's value hit an all-time high of $19,850.** At the same time, hackers stole from several cryptocurrency exchanges (YouBit, NiceHash etc.).



A UK bitcoin exchange senior executive was also **kidnapped** and **ransomed for more than $1 million worth of Bitcoin**. These incidents show **an aggressive criminal interest in Bitcoin** and points to an escalation of such attacks in 2018.

Increase in IoT Malware variants and prevalence

As IoT devices increase, so too does hacker interest in controlling them for nefarious purposes.

Recently, **StarHub Cyber Security** detected an uptick in **malicious IoT-related activities** in Singapore.

The release of the Mirai source code and leakage of exploits and hacking tools are risks that **IoT device makers must acknowledge**.

This development means 2018 will see manufacturers address these exploits, and raise the bar regarding threat prevention.

Ransomware continues to gain momentum

2018 will continue to see Ransomware attacks, in conjunction with the rise of Bitcoin, the preferred payment method of cyber criminals.

With the **rise of Ransomware-as-a-Service (RaaS)** on the dark web, almost anyone can launch a crippling ransomware attack.

Organisations need to work extra hard in 2018 to defend against such attacks.

Security awareness, as well as security prudence, will also **play a big part in mitigating** these threats.

Advanced Persistent Threats (APT) – Supply Chain Threats and State Sponsored Attacks

In 2017, supply chains across the globe saw two instances of APT attacks — **NotPetya and CCleaner**. Intended targets were not affected directly.

However, commonly used software such as **accounting tools were infected** and **exploited**. Experts expect this vector to be used well into 2018.

Another threat that **remains a concern is state-sponsored attacks**. On-going **geopolitical tension** among certain countries (US, China, N.Korea, Russia, etc.) means its risk continue in 2018.

1800 888 8888 starhub.com/cybersecurity enterprise@starhub.com

StarHub