RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 013 – 26 January 2018

Cyber Threats: 2018 and Beyond

By Foo Siang-tse and Shashi Jayakumar

Synopsis

How are cyber threats evolving? What can be done to mitigate these threats? Are the solutions technical ones, or do they lie in human instinct and response?

Commentary

2017 WAS a watershed year with an unprecedented number of cyber hacks, leaks and data breaches. We believe 2018 will be worse, as attackers become increasingly creative with attack methods and increasingly destructive payloads that better target system vulnerabilities. Why is this so?

Asymmetric Threat Landscape

First, the threat landscape will continue to be asymmetrical. Threat actors have an edge over enterprises that are hard-pressed to staff up internal cyber security teams.

State-sponsored actors and, increasingly, organised crime groups are well-funded, organised and resourced. They can afford to take their time to do research on their target, create the right malware and tailor their attacks to their targets. Even if they were to fail the first time, they can persist to try again and again at very little marginal cost.

These entities are aided by the breathtaking rate of technological advancement. But attackers have also begun to acquire an increasingly deep understanding of human nature. This has manifest itself in more nuanced attacks that make use of social engineering and behavioural insights.

What we have seen in recent years is the continued evolution of (and preference for)

very complex and precise spear phishing campaigns, unlike spam or phishing e-mails which are mass attacks. A spear phishing campaign targets specific individuals, organisations or businesses, to collect sensitive information.

It may take the form of a professional-sounding, personalised e-mail that makes use of personal data collected from public posts on social media sites and blogs to target subjects to lower their guard – to entice them to click on suspicious links or open documents that may be virus-contaminated.

Hacking and Shadow Economy

Hacking has created a shadow economy where data is bought and sold on the dark Web to organised cybercriminal syndicates. Data is the new oil. It is what threat actors are after, and what needs the most protection.

This has birthed a booming shadow economy. On top of personal data, zero-day exploits (targeting vulnerabilities that the target has no awareness of) are also available for sale. Large botnets are available for rent, and so are services such as ransomware-as-a-service and DDoS-as-a-service. DDoS attacks – distributed denial of service -- flood a target system with more traffic than it can handle, bringing it down.

There is a market for exploits, which are attacks on computer systems made through a particular vulnerability of the system, and for trading these exploits. There is a growing number of actors trading such exploits which drives up supply.

An iOS zero-day – an attack mechanism targeting previously unknown vulnerabilities in Apple mobile operating systems – can cost as much as US$1.5 million (S$2 million). It is no wonder that technically gifted programmers see the attraction of providing such services.

Healthcare Industry Exposed

In 2018, we will see an increasing number of extortionist attacks around the world targeting critical infrastructure. Transportation, energy and medical institutions are choice targets as a service outage can cause severe public backlash and, therefore, increases the possibility of a payout.

In recent months, the healthcare industry has been a victim of more attacks. This is because of the value of healthcare data – such as medical histories – which can be used for a variety of cyber fraud.

Cyber attacks will cost American hospitals more than US$305 billion over five years and one in 13 patients will have their data compromised by a hack, according to industry consultancy Accenture in a 2015 report. A 2015 study by Brookings showed that, since late 2009, the medical information of more than 155 million Americans has been exposed without their permission through about 1,500 breaches.

Healthcare institutions are vulnerable partly because government regulations forced healthcare operators to adopt electronic health records and other advances even if they weren't ready to adequately invest in security.

Would-be smart nations should take note that mass adoptions of digital solutions do create a security nightmare, giving hackers an endless attack surface to target.

Evolve to Stay Ahead

So how should organisations respond? For swift detection and mitigation of threats, what is critical is round-the-clock monitoring of networks, applications and devices, through an in-house security operation centre or outsourced service. The next generation of security operations centres also need to incorporate big data analytics and deep machine learning capabilities to keep on top of the massive amount of data generated.

At the operational level, the overall incident response framework must be routinely audited and strengthened. The incident response team must be drilled through specific skills training, table top scenarios, and full-fledged, realistic, red team-blue team exercises (blue team being the defenders; red team the simulated attackers). External assistance should be sought if there is a lack of internal skillsets or personnel.

Singapore organisations especially need to take the threat of cyber attacks more seriously. A survey conducted by managed security services provider Quann and research firm IDC in June last year covered 150 senior IT professionals from medium to large companies based in Singapore, Hong Kong and Malaysia.

The results showed that 40 per cent of the respondents do not have incident response plans for when they are being attacked and 67 per cent do not practise their incident response plans.

Need for Comprehensive Strategy

Cyber security requires a comprehensive approach that goes beyond the chief information security officer or head of information technology. The executive leadership must not see cyber security as a cost centre and an IT issue, but as an integral part of corporate risk management.

Senior management and the board must understand the threat landscape and data protection strategies.

Beyond the board and management, every employee matters. A Cyber Security Agency of Singapore 2017 survey showed that Singaporeans display risky behaviour that jeopardises their own and their company's cyber security. It does not matter how advanced the corporate anti-virus is if employees indiscriminately download free but potentially malware-laden software from dubious sources. Every careless employee is an open door for hackers to exploit.

With the number and complexity of attacks rising, enterprises need to stay on top of their cyber security preparedness.

Effective cyber security is not about keeping up with the cyber security products arms race. Instead, it is about ensuring that seemingly mundane tasks, such as keeping

patches up-to-date, ensuring that security hardware is maintained and managed well, and ensuring compliance with user policies and procedures, are performed well by human beings.

Even with the best technology, the human factor plays a critical role in ensuring enterprises stay cyber secure. Firewalls must be kept up-to-date but the most important firewall is still the human one.

Foo Siang-tse is managing director of Quann, a managed security services provider. Shashi Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.

This commentary is written in memory of Mr Chng Ho Kiat, Director, Cyber Security and Resilience Division, Ministry of Communications and Information, who passed away on 24 January 2018.

A version of this commentary first appeared in The Straits Times 26 Jan 2018.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg