Lessons from targeted cyber attacks

Know your environment
Know your attacker
By 2020, worldwide financial losses due to cybercrimes may rise to over US$12 trillion. Organizations need to be on constant alert to the ever-evoluting cyber threat landscape and future-proof their cyber defenses in averting and limiting the damage inflicted by cyber attackers.

Adopting cyber security resilience around the principles of Detect, Protect and React is more critical now than ever before.

Jason Yuen
Malaysia Cybersecurity Leader, EY
Background of cyber attacks

The proliferation of cyber attacks in a number of financial services organizations across several emerging markets points to the growing sophistication of cyber thefts. Cyber criminals appear to have long-term strategies and plans to interfere with large-scale financial transactions using custom Malware and Advanced Persistent Threat (APT) techniques (e.g., Carbanak). They are well-organized, with the patience to infiltrate an organization’s security system over time.

In the financial services sector, regulatory response has now shifted to mitigating systemic cyber risks and gaps across the financial system. Current focus is on the enhancement of the security of financial messaging services such as the SWIFT global payments system. SWIFT has recently initiated the Customer Security Program (CSP) which involves customer inspections and disclosures of non-compliance against 16 mandatory controls and 11 voluntary controls.

This alert attempts to discuss lessons from targeted cyber attacks to-date (e.g., bank infrastructure that connects to the SWIFT network) and provide some guidance in setting security control policies and measures to avert and/or mitigate potential financial losses to cyber criminals.

In preparation for future cyber attacks, organizations need to adopt high vigilance in evaluating their organizations’ readiness towards imminent cyber attacks to their systems and financial assets.

Note:
SWIFT = Society for Worldwide Interbank Financial Telecommunication

Take 5: Lessons from targeted cyber attacks
Key characteristics of cyber attacks

The first step for organizations seeking to enhance their cybersecurity ability is to develop a better understanding of the nature of the threats to them, both their internal environment (“Know Your Environment”) and their external threats (“Know Your Attacker”).

Set out below are some key characteristics of targeted “vulnerable” environments and tactics pursued by cyber attackers.

Chart 2: Key characteristics of cyber attacks

- Privileged accounts which are not adequately monitored
- Weak network segmentation allowing easy lateral movement
- Lack of timely, comprehensive patching of technologies
- Credentials which are stored in unprotected files on computer systems
- Depth and quality of security event monitoring which lag behind evolving attack vectors
Know your attacker

- Has access to a comprehensive cyber attack ecosystem
- Operates like a business-for-hire
- Covers tracks to hinder investigation
- Knows specifically which application to attack
- Chains multiple exploits to achieve full-system compromise
Mitigating cyber attacks - 5 proactive steps

When evaluating your organization's resilience to cyber attacks, the following five steps serve as a guideline:

1. **Proactive cyber assessment**
   Perform proactive, structured and “context-aware” cyber assessment with knowledge of:
   - Business processes
   - Applications in use
   - Underlying infrastructure
   - Traffic patterns
   - User activity (e.g., traceability tests: system logins to statement reconciliations)

2. **Prepare for breaches**
   Create or improve a cyber attack response plan:
   - Document updated escalation points and incident response contacts
   - Develop “dos and don'ts” post-breach detection
   - Test incident response process (e.g., cyber incident response plans, vulnerability mitigation programs)
   - Document dispute management process

3. **Realign cyber protection**
   Protection at all levels:
   - Board and management understand current security posture of the cyber security environment
   - Granular controls for hosts, network and end-point parts of the cyber security infrastructure
   - Security monitoring of the cyber security environment (e.g. when and what were the recent changes to the cyber security system / Electronic Fund Transfer (EFT) activities?)

4. **Refresh controls**
   Adopt more stringent control processes:
   - Cyber security audit to cover all components of the cyber security environment – beyond application and general controls
   - Increased frequency of cyber security reviews and to include pen-testing and detailed technical reviews
   - Outsource cyber security IT operations to enhance on-premise security
   - Enhance security log data collection and storage process e.g. commit all cyber security logs to another server
   - Start building baseline for behavioural anomaly detection
   - Use payment analytics for fraud detection

5. **Consider independent review and reporting**
   Engage an external team with strong business and security expertise to:
   - Identify weaknesses in cyber security controls and security (e.g. compromise assessments)
   - Provide an objective opinion on the security posture
EY contacts

Chow Sang Hoe
Malaysia Advisory Leader, EY
EY Asean Advisory Leader
Tel: +603 7495 8696
sang-hoe.chow@my.ey.com

Susanna Lim
Malaysia Advisory - Risk, EY
Tel: +603 7495 8773
susanna.lim@my.ey.com

Jason Yuen
Malaysia Cybersecurity Leader, EY
Tel: +603 7495 8789
jason.yuen@my.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

©2018 Ernst & Young Advisory Services Sdn. Bhd.
All Rights Reserved.

APAC no. 07001269

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/my