The Digitisation of Banking: Threats and Opportunities

Tony Jarvis
Chief Strategist, Threat Prevention
APAC, Middle East & Africa
History of Online Banking

1983: First Internet service using television

1994: First online banking website

1998: Eight US banks have at least 1 million users each

2001: PayPal reinvents online payments

2007: iPhone redefines smartphones forever

2011: 400 million people are banking online

2013: Facebook targets financial services
FinTech

Threat or opportunity?

Usage and growth

Obstacles
Blockchain

Infinite possibilities

Attacks have already begun

Adoption in the planning phase

Challenges ahead
ATM Attacks

- Attacks making headlines
- ATM fraud on the rise
- Chip-enabled machines should help
- Credit cards leading debit cards

Chip Surge
Percentage of MasterCard-branded cards with security chip

Credit cards: 88%
Debit cards: 33%
Whaling – A Growing Threat

Threats have evolved from phishing, to spear-phishing, to whaling

AFGlobal Corporation tricked out of $480,000, attackers tried for an additional $18 million

Costs $2.3 billion, 17,642 victims
Dridex

Began as a **Banking Trojan**

Developed it’s own **Botnet**

Also used for **Locky**

Dridex **creators** behind Locky?
Flash Banker
EXISTING THREATS AND NEW ENTRANTS

MALWARE

RANSOMWARE
Locky is a ransomware Trojan that targets the Windows platform. This malware sends out system information to a remote server and receives an encryption key to encrypt files on the infected system. The malware demands that the payment to be made in the form of Bitcoins digital currency.
Why Ransomware?

Easier
- Social engineering
- Exploit kits
- Broad audience

Profit
- Faster payment
- Bitcoin benefits

Obstacles
- Simple attacks
- Onus on victim
WHAT ARE THE IMPLICATIONS?
Budgets on the Rise

Getting customers on board with good cyber security hygiene

Defining an acceptable level of risk

Lack of understanding among stakeholders

The more I build, the more holes I discover

“Blame the victim” mentality

Attracting and retaining the right talent

Time spent remediating things not done properly in the past

Lack of consensus from regulators

Threats from malicious insiders
The financial impact **GROWS** dramatically with **TIME**.

- **Direct loss:** $162,000,000
- **Estimated indirect loss:** >$1 Billion

**Cost over Time:**

- **Recon**
- **Weapon**
- **Deliver**
- **Exploit**
- **Install**
- **C&C**
- **Act On**

 Weeks After Infection

**Contractor Infection**

**Initial Target Infection**

**POS Infection**

[Restricted] ONLY for designated groups and individuals
Compliance

Supply & Demand
High demand, short supply

Scope
From individual function to enterprise-wide role

Evolution of Role
From advisory to:
- Projects
- Product development
- Thought leadership

High demand, short supply
Opportunities and Threats

Payments

IOT

DDoS

Whaling
Where to Invest?

**Actionable Intelligence**
Big data and analytics

**Innovation**
Field trips, labs, fusion centres

**Training**
War-gaming, red-teaming
## Opportunities Are Everywhere

<table>
<thead>
<tr>
<th>Year</th>
<th>Location</th>
<th>Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>SINGAPORE</td>
<td>MAS working with Polytechnics</td>
</tr>
<tr>
<td>2016</td>
<td>SINGAPORE</td>
<td>SMART Nation Platform</td>
</tr>
<tr>
<td>2015</td>
<td>SINGAPORE</td>
<td>The FinTech and Innovation Group (FIG)</td>
</tr>
<tr>
<td>2015</td>
<td>SINGAPORE</td>
<td>Financial Sector Technology and Innovation Group</td>
</tr>
<tr>
<td>2015</td>
<td>HONG KONG</td>
<td>FinTech Steering Group</td>
</tr>
<tr>
<td>2015</td>
<td>HONG KONG</td>
<td>Injection into Innovation and Technology Fund</td>
</tr>
<tr>
<td>2014</td>
<td>HONG KONG</td>
<td>FinTech HK</td>
</tr>
<tr>
<td>2013</td>
<td>HONG KONG</td>
<td>The Bitcoin Association Hong Kong</td>
</tr>
</tbody>
</table>
Bangladesh Central Bank
It Takes More Than Technology
The Cyber Kill Chain

Reconnaissance
Identify the target and exploitable weaknesses

Weaponization
Create/select attack vector

Delivery
Deliver the malicious payload to the victim

Exploitation
Gain execution privileges

Installation
Install the malware on infected host

Command & Control
Establish a channel of communication

Act on Objectives
Data collection or corruption, Lateral movement and exfiltration

[Restricted] ONLY for designated groups and individuals
IS IT POSSIBLE?

PREVENTION

IS IT POSSIBLE?
WHAT ABOUT INCIDENT RESPONSE?
WHAT ABOUT...
OFFENSIVE SECURITY?
Have a Plan

“Malcolm Turnbull launches $230m cyber security strategy”
– Australia, 21st April 2016

“Public servants’ computers to have no Net access”
– Singapore, 8th June 2016

“CyberSecurity Malaysia to continue emergency response role in Asia Pacific” – Malaysia, 31st October 2016
Others Have Responded

G7 sets forth guidelines

Encourages
• Risk management framework
• Assess and update defences

Goals
• Common approach, language
• Disclosure and sharing

Three annexes
• Baseline requirements
• Running a SOC
• Reporting incidents

Key takeaways
• Involve the board
• Risk management approach
• Emphasises prevention
Multi-Layered Security

Pre-Compromise

- Reconnaissance
  - IPS
  - Firewall
  - DLP
  - Document Security
- Weaponization
  - Threat Intelligence
- Delivery
  - Firewall
  - Anti-Spam
  - URL Filtering
  - Threat Emulation
  - Threat Extraction
  - Mobile Threat Prevention

Compromise

- Exploitation
  - Anti-Virus
  - IPS
  - Threat Emulation
- Installation
  - Anti-Bot
  - Endpoint Security

Post-Compromise

- Command & Control
  - Anti-Bot
  - Endpoint Security
  - Forensics
  - Mobile Threat Prevention
- Act on Objectives
  - DLP
  - Document Security
  - Firewall
  - IPS

BETTER SECURITY, TOGETHER

[Restricted] ONLY for Check Point authorized personnel.
You Have the Advantage

USE IT
AND REAP THE BENEFITS
Recommendations for the ROAD AHEAD

ADOPT
Solutions to proactively address adversaries

ESTABLISH
Real-time monitoring systems

AUTOMATE
Processes to address technology challenges

CREATE
Awareness and encourage education

MAKE
Security a boardroom agenda
Let’s stay in touch
THANK YOU

Please contact me directly with any questions or comments

tjarvis@checkpoint.com
+65 9724 6221