If you were under-attack, would you ever know?
September 2016
Dung Nguyen Bui
Senior Manager, IT Risk & Assurance Services, EY Vietnam
Agenda

1. Cyber security overview
2. Live Demo on security risks using mobile devices
3. How to defend? What is the approach for security practices?
4. Q&A
Cyber security overview
Cyber Security risks and incidents, are they for real?
Vietnam is placed 7th in Asia in Internet usage (Asia has 44.8% of total global internet users)

About 50% of Vietnamese enterprises are using e-commerce

100% of companies use the Internet for their business

- 30% Banking websites have security vulnerabilities
- 220 websites in Vietnam had been attacked by Chinese hackers
- 85% of computers have virus infection via USB

In Vietnam, 2,045 agencies and business websites were hacked this year, but the number of cyber security experts was too low to cope with all of these incidents.

Vietnam has become the TARGET

2015 and 2016

10,000 websites .vn hacked

70,83% computers infected

39,95% leaking codes

ASEAN Government, State-owned Organizations | High risk of cyber attack

200 Dangerous cyber codes installed in 10 years

Vietnam government, State-owned Organizations | Become THE TARGET

100 Dangerous codes attack Vietnam internet

56 websites .gov attacked

Social media: Facebook, Twitter, LinkedIn, etc. used to be hacked

Confidential information unsecured

Cybersecurity in Vietnam is IN DANGER

Source: IT threat evolution, Securelist.com
In 2013, a group of Iranian hackers attacked the Bowman Avenue Dam near Rye Brook, New York, which is used to control water flow when it rains to prevent flooding.

“The incident represented a known intrusion on critical infrastructure. A stroke of good fortune prevented the hackers from obtaining operational control of the flood gates because the dam had been manually disconnected for routine maintenance” – Reuters.

Our client: Access to Hydropower Plant Controller System was compromised

Missed a security patch in OS server. This vulnerability allows malicious people to take full control of the server which can be used as a launching point to compromise the Plant Controller System.

Malicious people can compromise other servers/workstations in Plant Controller System network to perform unauthorized actions, e.g. control the dam gates.
LESSON LEARNED: Every weakness can turn into disasters, and **Security is only as strong as the weakest link**.
National Infrastructure
Hacker targeted a leading airline in Vietnam

In July 2016, a group of hackers attacked the web portal of a leading airline in Vietnam. Besides, the hackers also illegally accessed and modified the content of advertisement displays at the airports.

Consequences:
- User interface and contents of the website were illegally modified.
- Personal information of 400,000 customers was leaked.
- Significantly impacted the security operations of the airports; dozens of flights were delayed.
National Infrastructure
Hacker targeted a leading airline in Vietnam

In July 2016, a group of hackers attacked the web portal of a leading airline in Vietnam. Besides, the hackers also illegally accessed advertisement websites. Consequently, significantly impacted the security operations of the airports; dozens of flights were delayed.

LESSON LEARNED:
► Perform Information security assessment
► Establish the Incident Handling and Response Processes
March 2016 - Malwares injected in customers’ smartphone of 20 banks in Australia, New Zealand & Turkey, stole login details and intercepted two-factor authentication codes, transaction information.

Reason:
Vulnerability in updating Adobe Flash Player

Malware hijacks big four Australian banks' apps, steals two-factor SMS codes

COMMERCIAl BANKs in Vietnam | Affected systems: E-banking systems

Illegal money transferring from bank account without victim’s acknowledge
LESSON LEARNED: New applied technology and its associated risks should be understood and assessed fully and regularly to ensure information security.
Banking & Finance
No such thing as a ‘trusted network’

Bangladesh Bank hackers compromised SWIFT software, warning issued

Vietcombank loses 4tn dong after its customer encounters 500m dong online fraud

Over the weekend, all people have been paying attention to the phishing scam in which a cardholder of the Commercial Joint Stock Bank for Foreign Trade of Vietnam (Vietcombank) has complained having lost of 500 million dong in her account. According to explanation of Vietcombank, the customer followed a link to a malicious website and provided her account information. Vietcombank has timely froze 300 million dong, and the remaining 200 million dong was withdrawn by the hackers via ATM in Malaysia.
Banking & Finance
No such thing as a ‘trusted network’

LESSON LEARNED:
- End-point security and users awareness on information security
- Security controls effectiveness
Every can and will be a target
No such thing as a ‘small fish’...

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>TOTAL</th>
<th>SMALL</th>
<th>LARGE</th>
<th>UNKNOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72)</td>
<td>368</td>
<td>181</td>
<td>90</td>
<td>97</td>
</tr>
<tr>
<td>Administrative (56)</td>
<td>205</td>
<td>11</td>
<td>13</td>
<td>181</td>
</tr>
<tr>
<td>Agriculture (11)</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Construction (23)</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Educational (61)</td>
<td>165</td>
<td>18</td>
<td>17</td>
<td>130</td>
</tr>
<tr>
<td>Entertainment (71)</td>
<td>27</td>
<td>17</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Financial Services (52)</td>
<td>642</td>
<td>44</td>
<td>177</td>
<td>421</td>
</tr>
<tr>
<td>Healthcare (62)</td>
<td>234</td>
<td>51</td>
<td>38</td>
<td>145</td>
</tr>
<tr>
<td>Information (51)</td>
<td>1,496</td>
<td>36</td>
<td>34</td>
<td>1,426</td>
</tr>
<tr>
<td>Management (55)</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Manufacturing (31-33)</td>
<td>525</td>
<td>18</td>
<td>43</td>
<td>464</td>
</tr>
<tr>
<td>Mining (21)</td>
<td>22</td>
<td>1</td>
<td>12</td>
<td>9</td>
</tr>
<tr>
<td>Other Services (81)</td>
<td>263</td>
<td>12</td>
<td>2</td>
<td>249</td>
</tr>
<tr>
<td>Professional (54)</td>
<td>347</td>
<td>27</td>
<td>11</td>
<td>309</td>
</tr>
<tr>
<td>Public (92)</td>
<td>50,315</td>
<td>19</td>
<td>49,596</td>
<td>700</td>
</tr>
<tr>
<td>Real Estate (53)</td>
<td>14</td>
<td>2</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Retail (44-45)</td>
<td>523</td>
<td>99</td>
<td>30</td>
<td>394</td>
</tr>
<tr>
<td>Trade (42)</td>
<td>14</td>
<td>10</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Transportation (48-49)</td>
<td>44</td>
<td>2</td>
<td>9</td>
<td>33</td>
</tr>
<tr>
<td>Utilities (22)</td>
<td>73</td>
<td>1</td>
<td>2</td>
<td>70</td>
</tr>
<tr>
<td>Unknown</td>
<td>24,504</td>
<td>144</td>
<td>1</td>
<td>24,359</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>79,790</td>
<td>694</td>
<td>50,081</td>
<td>29,015</td>
</tr>
</tbody>
</table>

Every can and will be a target
No such thing as a ‘small fish’...

LESSON LEARNED:
- That won’t happen to me!
E-commerce

Amazon Suffers Security Breach; 80,000 Login Credentials Leaked (Updated)

By Agan Uzunovic on July 10, 2016

A hacker going by the online handle of 0x2Taylor has claimed to breach the servers of e-commerce giant Amazon ending up leaking login credentials of 80,000 users.

The 597.4 MB leaked data includes usernames and encrypted passwords of Amazon users. The hacker states he targeted Amazon as the firm did not reply or pay any attention at critical security flaws in their server. Earlier, 0x2Taylor also claimed responsibility for conducting a cyber attack on Baton Rouge police department when Alton Sterling was killed by two of the city’s police officers.
LESSON LEARNED:
Constant cyber-war between attackers and defenders, with the question of current protection effectiveness.
International manufacturing companies in Vietnam:

In 2015, 2016, many leading companies in these industries experienced information security incidents. Serious consequences:
- All data **DELETED**
- Manufacturing system shut down
- Corporate Confidential Information **LEAKED**.

Trump Hotels attacked by hackers -- again

Luxury Hotel leaks thousands of guest details

Hackers also target healthcare, hotels, law, security, pizza company, and…

Panama Papers case:
Records of 12 country leaders leaked
LESSON LEARNED:
- Knowing **what to protect** – Information classification
- Design and apply proper controls
Credit card details on 20 million South Koreans stolen

Credit card details from almost half of all South Koreans have been stolen and sold to marketing firms.

The data was stolen by a computer contractor working for a company called the Korea Credit Bureau that produces credit scores.

The names, social security numbers and credit card details of 20 million South Koreans were copied by the IT worker.

The scale of the theft became apparent after the contractor at the centre of the breach was arrested.
Vendors, suppliers and contractors can be your weak link

LESSON LEARNED:
Conduct **IT risk & cybersecurity assessment** before/during working with vendors, suppliers, contractors
Malicious links, Phishing websites are sent to trick users to click in via Facebook posts, Facebook messages, Facebook ads, Viber messages, Gmail, ...

Làm gì là Vikya Nguyễn được lên báo thành niên đó hong dạy. quay video được bảo đăng luôn hay the Vikya Nguyễn. Gần trở nối tiếp rói đố nhá https://www.facebook.com/.../6276.../67899967/1685601025052733/...
LESSON LEARNED: Work/Corporate and Personal Information could easily be leaked with low security awareness ... and the impact is unmeasurable.