Current Conditions and Challenges of Cybersecurity in Taiwan

Chou, Chih-Ho (周智禾)
Section Chief,
Department of Cyber Security,
Executive Yuan, Taiwan (ROC)
9/12/2017
Outline

• Cybersecurity Overview of Taiwan Government
• Cyber Attack Trends
• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche
• Conclusions
Introduction of NICST

• National Information and Communication Security Taskforce (NICST)

• Established since January 2001
  • Convened by Vice Premier, Executive Yuan
  • Steering Committee comprised of central government CISOs/Municipality CISOs/Deputy Director of NSB/Experts
  • Secretariat by Department of Cyber Security (DCS), Executive Yuan
  • 8 major working groups for cyber security related tasks execution and coordination among agencies
  • One service center (National Center for Cyber Security Technology, NCCST) plays the role of National CSIRT
PDCA Cycle of Government Sector Information Security Management System

- **Cybersecurity Management Act (Draft)**
- **National Strategy for Cybersecurity Development Program (2017~2020)**
- **National Cyber Security Whitepaper**
- **Directives for Agencies**
  - Agency Responsibility Ranking Criteria
  - Agency To-Do List (TDL)
  - IT System To-Do List
  - Incident Report Guideline

- **Agencies**
  - Implement Agency TDL (ISMS/Defense-in-Depth/24x7 Monitoring/Dedicated Staff)
  - Implement IT System TDL
  - Deploy Agency-wide GCB
  - Incident Report and Handling...

- **NCCST**
  - G-ISMS Services (Early Warning/Incident Response/System Security/Mgmt Process/Awareness Training)
  - Public-Private Partnership (G-SOC/G-ISAC)
  - International Cooperation...

- **Competent Authorities**
  - Cyber Crime Investigation
  - Content Security
  - Human Resources Development
  - Personal Information Protection
  - Mobile App Test

- **Cyber Offensive and Defensive Exercise**
- **Annual Audit (1st Party/3rd Party)**
- **Cyber Health Check, VA, PT**
- **Incident Report and Social Engineering Drills**
- **Agency Governance Maturity and Protection Capability Level Assessment**
- **National Cyber Security Indicators**
- **Domestics/Intl. Contests**

- **NICST Committee Meeting**
- **NICST Consulting Committee Meeting**
- **NICST Working Group Meeting**
- **CIO and CISO Meeting**
- **Quarterly Workshop for IT Personnel**
• Cyber Security Overview of Taiwan Government

• Cyber Attack Trends

• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche

• Conclusions
International Cybersecurity Trends

Cyber criminals steal personal data to affect the operations of e-commerce and finance.

Information and security providers have been hacked to lead to damage the trusted supply chain.

Organized hackers use Advanced Persistent Threat (APT) attacks to steal the confidential data of official, national defense and business.

The open systems and the Internet are used in critical infrastructures increasingly. That results in the growing of the risks.

Cyber-warfare and DDoS paralyzed national network operations.
International Cybersecurity Trends

• Ransomware expands
  • Almost 10% of organizations detected ransomware activity last quarter

• Automatic attacks
  • 80% of organizations reported high-or critical-severity exploits

• More mobile malwares
  • The total malware volume jumped from 1.7%(in Q4 2016) to 8.7%(in Q1 2017)

• Build botnets out of IoT(Internet of Thing) devices to launch the DDoS attack – e.g. Mirai

Source: Fortinet (Taiwan Security View: IOT Threats on Rise)
APT Hackers Around the Globe

• Over 20 APT hacker teams (2014~2015)
  • US, UK, China, Russia, and Israel
  • North Korea and Middle East

Source: https://apt.securelist.com/
APT Attacks

• APT Attack Analysis
  • 91% of APT Attacks started from a spear phishing e-mail
  • 94% of spear phishing e-mails have attachment files
  • Most common file types are .doc, .exe, .scr, .au3, .jpg, .pdf

<table>
<thead>
<tr>
<th>File Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>.doc</td>
<td>39%</td>
</tr>
<tr>
<td>.exe</td>
<td>23%</td>
</tr>
<tr>
<td>.scr</td>
<td>9%</td>
</tr>
<tr>
<td>.au3</td>
<td>8%</td>
</tr>
<tr>
<td>.jpg</td>
<td>5%</td>
</tr>
</tbody>
</table>

Spear-Phishing Emails Used in Targeted Attacks

Source: 2015 Symantec Internet Security Threat Report
Hard to Detect

How Compromises Are Being Detected

- 31% victims discovered the breach internally
- 69% victims notified by an external entity

Time from Earliest Evidence of Compromise to Discovery of Compromise

- Median number of days that threat groups were present on a victim’s network before detection: 205 days
- 24 days less than 2013
- Longest Presence: 2,982 days

APT Phishing

- 78% of observed phishing emails were IT or security related, often attempting to impersonate the targeted company’s IT department or an anti-virus vendor
- 72% of phishing emails were sent on weekdays

Source: 2015 Mandiant Annual Threat Report
Problems with Website Vulnerabilities

• So far, most websites around the globe still have vulnerabilities

Source: 2015 Symantec Internet Security Threat Report
• Cyber Security Overview of Taiwan Government
• Cyber Attack Trends
• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche
• Conclusions
Network Equipment at Risk

• Network equipment are hard to manage, and very easily get hacked

• Hacking network equipment is old news, but hackers continue to do so because it relatively easy

• We were collecting phishing mails and analyzed them

• We traced this C&C IP, and found it was located in a civilian household
It is a Wireless Router

- The C&C actually is a wireless router
  - default password
  - built-in VPN function
Transfer Data

• Router transferred packets automatically
  • Transfer all packets came from port 80, 443 to 192.168.10.2
  • 192.168.10.2 is the VPN IP
  • The hacker would continuously receive victims' reporting packets sending through port 80, 443
Looking at the Log

• From the router log we could find the record of the hacker activities

```
Jul 23 08:13:31 pptp[3533]: CTRL: Starting call (launching pppd, opening GRE)
Jul 23 08:13:31 pptp[3534]: Plugin pptp.so loaded.
Jul 23 08:13:31 pptp[3534]: PPTP plugin version 0.8.5 compiled for pppd-2.4.5, linux-2.6.22.19
Jul 23 08:13:31 pptp[3534]: pppd 2.4.5 started by admin, uid 0
Jul 23 08:13:31 pptp[3534]: Using interface ppp10
Jul 23 08:13:31 pptp[3534]: Connect: ppp10 <-> pptp (111.175. )
Jul 23 08:13:34 pptp[3533]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
Jul 23 08:13:35 pptp[3534]: MPPC/MPPE 128-bit stateless compression enabled
Jul 23 08:13:35 pptp[3534]: Cannot determine ethernet address for proxy ARP
Jul 23 08:13:35 pptp[3534]: local IP address 192.168.1.1
Jul 23 08:13:35 pptp[3534]: remote IP address 192.168.10.2
```
Hacker Collect Victim Data via C&C

• This wireless router was set to transfer packets automatically
  • The hacker only needed to connect to the VPN service, then it will receive all packets automatically
  • After further investigation, victims were not only the Taiwan government agencies, there are other countries IP such as U.S., France, U.K., and Germany, reported to this C&C
  • We have sent alert info to CERTs of these countries
• Cyber Security Overview of Taiwan Government
• Cyber Attack Trends
• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche
• Conclusions
Mobile Botnet

2014/6/3
APNIC noticed Dropbox to remove the malicious files

2014/6/7
TWNCERT received this intelligence from APNIC

2014/6/9
TWNCERT cooperated to trace the Botnet with MJIB

2014/6/19~2014/7/10
Sniffing the network traffic from the victims

2014/7/18
MJIB starts investigating this case
## C&C Server

<table>
<thead>
<tr>
<th>ID</th>
<th>ID</th>
<th>电话</th>
<th>运营商</th>
<th>备注1</th>
<th>备注2</th>
<th>型号</th>
<th>更新时间</th>
<th>创建时间</th>
<th>拥有者</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>D5756050320638</td>
<td>092395501</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>302</td>
<td>D576950594818098</td>
<td>0919907589</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>303</td>
<td>D55154262639287172</td>
<td>0919850981</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>304</td>
<td>D511273705020</td>
<td>0112870226</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>305</td>
<td>D551969057424140</td>
<td>0122312222</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>306</td>
<td>D558460024972006</td>
<td>01190095340</td>
<td>Digi</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>307</td>
<td>D55555850522703806</td>
<td>03558550502072360</td>
<td>Soo</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>308</td>
<td>D553346056039176</td>
<td>0134779893</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>309</td>
<td>D553446024945554</td>
<td>01293645571</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>310</td>
<td>D5148751894</td>
<td>0129751894</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>311</td>
<td>D533568706392476</td>
<td>0123450565</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>312</td>
<td>D553056052508776</td>
<td>0197220363</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>313</td>
<td>D593363520201654</td>
<td>0134387964</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>314</td>
<td>D555587054383156</td>
<td>0199972159</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>315</td>
<td>D5186668575</td>
<td>018668575</td>
<td>U Mobile</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>316</td>
<td>D555555260810987</td>
<td>0197484422</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>317</td>
<td>D5112566798</td>
<td>01126468789</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>318</td>
<td>D535437202322609</td>
<td>01198549988</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>319</td>
<td>D55496505404660826</td>
<td>0193720574</td>
<td>Celcom</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>320</td>
<td>D555495054046608826</td>
<td>0126895708</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>321</td>
<td>D555245035053536</td>
<td>0355245035053536</td>
<td>Soo</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
<tr>
<td>322</td>
<td>D55575050122845</td>
<td>0175867209</td>
<td>Maxis</td>
<td></td>
<td></td>
<td>SF-300017</td>
<td>06-28 16:18</td>
<td>06-14 16:15</td>
<td>8375</td>
</tr>
</tbody>
</table>
C&C Server

SMS message with malicious URL

one-to-many mode

cell phone number / devices ID
### C&C Server

<table>
<thead>
<tr>
<th>Cell Phone Numbers</th>
<th>Devices ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0146737929, 012654093, 0112552486, d352167058472284, d359188047219845, d35655605991554, d354802050870139, d356508055137535, 0176351318, d35589050272061, d860205024068177, d358048043880795, d357138050746152, 0137603565, d354832053532428, d35772905948721, d357189056971484, d358654051292490, d358095054727191,</td>
<td>28886, 36555</td>
</tr>
</tbody>
</table>

### SMS Message

<table>
<thead>
<tr>
<th>Many-to-One Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOL3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Many-to-One Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOL7</td>
</tr>
</tbody>
</table>
Hackers swindle money about $144,148 USD ($4,324,440 NTD)
• We discovered 43,899 Bots IPs, The 98% Bots IPs located in Malaysia.
• We also found 393,471 contact information from packets (About 1% of the total population in Malaysia)
<table>
<thead>
<tr>
<th>No.</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MCMC</td>
</tr>
<tr>
<td>2</td>
<td>MyCERT</td>
</tr>
<tr>
<td>3</td>
<td>SingCERT</td>
</tr>
<tr>
<td>4</td>
<td>US-CERT</td>
</tr>
<tr>
<td>5</td>
<td>AusCERT</td>
</tr>
<tr>
<td>6</td>
<td>ID-SIRTII/CC</td>
</tr>
<tr>
<td>7</td>
<td>ThaiCERT</td>
</tr>
<tr>
<td>8</td>
<td>JPCERT/CC</td>
</tr>
<tr>
<td>9</td>
<td>HKCERT</td>
</tr>
<tr>
<td>10</td>
<td>KrCERT/CC</td>
</tr>
<tr>
<td>11</td>
<td>CNCERT/CC</td>
</tr>
</tbody>
</table>
• Cyber Security Overview of Taiwan Government
• Cyber Attack Trends
• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche
• Conclusions
Avalanche

• On Nov. 30th, 2016, Avalanche, a large global network hosting infrastructure used by cyber criminals was dismantled.

• Crimeware-as-a-service (CaaS)

• Targeting over 40 major financial institutions
  • Sensitive personal information stolen
  • Victims’ compromised systems might also have been used to conduct other malicious activities.

• Money mule

“We invite you to work in the home assistant offer.

This job takes 2-3 hours a week and requires absolutely no investment. The essence of this work for incoming client requests in your city. The starting income is about ~2000 Euro per month + bonuses.

You get paid your money every 2 weeks and your bonuses after finish each task!

We promise work for every person. But we accept applications this week only! Therefore, you should send email a request right now. And you will start earning money, starting from next week.”

行政院資通安全處
Malware families

- Corebot
  - stealing banking and credential information
- Matsnu
  - Malware dropper
- Nymaim
  - multipurpose malware family
  - Gozi + Nymaim = Goznym
- Ranbyus (use DGA to generate .tw domain)
  - Banking Trojan
- Rovnix
  - Banking Trojan with bootkit
- Tinba
  - Tiny banking trojan
- URLZone/Beblohol
  - Banking trojan
Double Fast Flux

<table>
<thead>
<tr>
<th>DN</th>
<th>Period</th>
<th>Type</th>
<th>Malicious IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.b.com</td>
<td>100</td>
<td>IN A</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>a.b.com</td>
<td>100</td>
<td>IN A</td>
<td>5.6.7.8</td>
</tr>
<tr>
<td>a.b.com</td>
<td>100</td>
<td>IN A</td>
<td>11.12.13.14</td>
</tr>
<tr>
<td>a.b.com</td>
<td>100</td>
<td>IN A</td>
<td>15.16.17.18.19</td>
</tr>
<tr>
<td>a.b.com</td>
<td>100</td>
<td>IN A</td>
<td>20.21.22.23</td>
</tr>
<tr>
<td>b.com</td>
<td>1000</td>
<td>IN NS</td>
<td>Ns1.a.tw.</td>
</tr>
<tr>
<td>b.com</td>
<td>1000</td>
<td>IN NS</td>
<td>Ns2.a.tw.</td>
</tr>
<tr>
<td>b.com</td>
<td>1000</td>
<td>IN NS</td>
<td>Ns3.a.tw.</td>
</tr>
<tr>
<td>b.com</td>
<td>1000</td>
<td>IN NS</td>
<td>Ns4.a.tw.</td>
</tr>
<tr>
<td>Ns1.a.tw</td>
<td>200</td>
<td>IN A</td>
<td>24.25.26.27</td>
</tr>
<tr>
<td>Ns2.a.tw</td>
<td>200</td>
<td>IN A</td>
<td>28.29.30.31</td>
</tr>
<tr>
<td>Ns3.a.tw</td>
<td>200</td>
<td>IN A</td>
<td>32.33.34.35</td>
</tr>
<tr>
<td>Ns4.a.tw</td>
<td>200</td>
<td>IN A</td>
<td>36.37.38.39</td>
</tr>
</tbody>
</table>
The actions in Taiwan

- MJIB cooperated with TWNIC (Taiwan Network Information Center)
  - 27,987 .tw domain names generated by Domain Generation Algorithm (DGA)
  - Those domain names had not been registered in TWNIC
  - Takedown operation was executed at 13:30 UTC on Nov. 30th, 2016
- Shadowserver worked with partners to build the sinkholing infrastructure and coordinate the international DNS Registry/Registrar activities
Results

• MJIB in Taiwan collaborated with investigators from 30 countries, including the FBI, the United States Department of Homeland Security (DHS), Europol and Eurojust
  • Crucial support of prosecutors and investigators from 30 countries
  • 5 individuals were arrested
  • 37 premises were searched
  • 39 servers were seized
  • Victims of malware infections were identified in over 180 countries
  • 221 servers were put offline through abuse notifications sent to the hosting providers
  • Over 800,000 domains seized, sinkholed or blocked.
• Cyber Security Overview of Taiwan Government
• Cyber Attack Trends
• Cases Studies
  • Attack via Network Equipment
  • Mobile Botnet
  • Avalanche
• Conclusions
Challenges

• Lack of timeliness in terms of information sharing of criminal intelligence

• Crime investigation mode overemphasize on individual case basis

• The issues about the protection of personal data

• It is hard to trace the origins of attacks
  • TOR (The Onion Router) network

• Changes in technology - Cloud Computing
  • Where the data resides
  • What law applies
  • The data obtained from suspect’s computer may have little meaning
Suggestions

• Facilitate trans-border law enforcement exchange visitors

• NICs may
  • establish a platform to record the malicious domains or IPs
  • provide the query records of Root DNS Server
  • help law enforcement agencies block malicious domains or IPs

• Establish contact window for intelligence exchanges
Contact information

- **TWNCERT**
  - +886-2-27339922; twncert@twncert.org.tw

- **TWCERT/CC**
  - [https://www.twcert.org.tw/](https://www.twcert.org.tw/)
  - +886-2-23776418; twcert@cert.org.tw

- **MJIB**
  - +886-2-29112241ext2971; safenet@mjib.gov.tw

- **CIB**
  - [https://www.cib.gov.tw/English/](https://www.cib.gov.tw/English/)
  - +886-2-27652111~5; https://www.cib.gov.tw/Service/EMail
Thanks for your attentions