CHALLENGES IN SUSTAINING A COMPUTER EMERGENCY RESPONSE TEAM: MALAYSIA CERT EXPERIENCE

SHARIFAH ROZIAH MOHD KASSIM
MYCERT
CYBERSECURITY MALAYSIA
Agenda

• Brief Introduction About MyCERT
• Our Services and Achievements
• Challenges in Sustaining our Team
• Lessons Learnt
• Areas of Improvement
• Conclusion
• Q&A
Brief Introduction to MyCERT

Launched in 1997 as a technical reference centre in Malaysia

Parked and funded under the Ministry of Science, Innovation & Technology, to provide Incident Response for the general public and organizations in Malaysia

Operating with 18 staff with two main services, Incident Response (Reactive) and Malware Research (Pro-active)

Audience: Malaysian Internet User

International Affiliation: Deputy Chair of APCERT, Permanent Secretariat of OICCERT. A member of FIRST – active in FIRST Membership sponsor.
## Services

<table>
<thead>
<tr>
<th>Reactive</th>
<th>Proactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Incident Response and Handling</td>
<td>1. Watch and Warn / Threat Monitoring</td>
</tr>
<tr>
<td>2. Security Operation Centre (SOC)</td>
<td>2. Applied Research</td>
</tr>
<tr>
<td></td>
<td>5. Security Advisory &amp; Alerts</td>
</tr>
</tbody>
</table>
Incident Reporting Channels

- Email
  - cyber999@cybersecurity.my

- Phone/Hotline
  - +603 8992 6888
  - 1 300 88 2999

- Fax
  - +603 8945 3442

- SMS
  - 15888 “Cyber999 Report”

- Mobile (24x7)
  - +6019 266 5850


- Walk In - Office Hours: MYT 0900 – 1800

- Mobile application (iOS and Android)

Increasing…
# Incidents Handled by Category (2014)

<table>
<thead>
<tr>
<th>Category</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Related</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Cyber Harassment</td>
<td>57</td>
<td>41</td>
<td>45</td>
<td>44</td>
<td>46</td>
<td>48</td>
<td>52</td>
<td>44</td>
<td>53</td>
<td>36</td>
<td></td>
<td></td>
<td>447</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td></td>
<td></td>
<td>30</td>
</tr>
<tr>
<td>Fraud</td>
<td>250</td>
<td>264</td>
<td>280</td>
<td>399</td>
<td>401</td>
<td>519</td>
<td>406</td>
<td>372</td>
<td>435</td>
<td>366</td>
<td>377</td>
<td>408</td>
<td>4477</td>
</tr>
<tr>
<td>Intrusion</td>
<td>109</td>
<td>78</td>
<td>216</td>
<td>70</td>
<td>13</td>
<td>28</td>
<td>43</td>
<td>47</td>
<td>104</td>
<td>105</td>
<td>173</td>
<td>134</td>
<td>1125</td>
</tr>
<tr>
<td>Intrusion Attempt</td>
<td>3</td>
<td>11</td>
<td>24</td>
<td>157</td>
<td>63</td>
<td>75</td>
<td>21</td>
<td>241</td>
<td>649</td>
<td>12</td>
<td>19</td>
<td>27</td>
<td>1302</td>
</tr>
<tr>
<td>Malicious Codes</td>
<td>251</td>
<td>78</td>
<td>101</td>
<td>55</td>
<td>47</td>
<td>48</td>
<td>29</td>
<td>14</td>
<td>22</td>
<td>13</td>
<td>16</td>
<td>42</td>
<td>716</td>
</tr>
<tr>
<td>Spam</td>
<td>40</td>
<td>23</td>
<td>32</td>
<td>36</td>
<td>61</td>
<td>55</td>
<td>385</td>
<td>530</td>
<td>548</td>
<td>671</td>
<td>735</td>
<td>534</td>
<td>3650</td>
</tr>
<tr>
<td>Vulnerabilities Report</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>717</td>
<td>498</td>
<td>707</td>
<td>773</td>
<td>645</td>
<td>777</td>
<td>943</td>
<td>1258</td>
<td>1822</td>
<td>1216</td>
<td>1376</td>
<td>1186</td>
<td>11918</td>
</tr>
</tbody>
</table>

**Fraud** – phishing, online scam, 419 scam, purchase, impersonation, spoofing

Incidents Handled by Category (2015)

<table>
<thead>
<tr>
<th>Category</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Related</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>Cyber Harassment</td>
<td>30</td>
<td>40</td>
<td>32</td>
<td>51</td>
<td>30</td>
<td></td>
<td>45</td>
<td></td>
<td></td>
<td>166</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>Fraud</td>
<td>276</td>
<td>235</td>
<td>232</td>
<td>313</td>
<td>303</td>
<td>388</td>
<td>253</td>
<td>252</td>
<td>247</td>
<td>2499</td>
</tr>
<tr>
<td>Intrusion</td>
<td>88</td>
<td>508</td>
<td>29</td>
<td>63</td>
<td>21</td>
<td>20</td>
<td>85</td>
<td>233</td>
<td>206</td>
<td>1253</td>
</tr>
<tr>
<td>Intrusion Attempt</td>
<td>28</td>
<td>22</td>
<td>21</td>
<td>21</td>
<td>10</td>
<td>6</td>
<td>13</td>
<td>8</td>
<td>13</td>
<td>142</td>
</tr>
<tr>
<td>Malicious Codes</td>
<td>21</td>
<td>30</td>
<td>26</td>
<td>26</td>
<td>35</td>
<td>51</td>
<td>43</td>
<td>39</td>
<td>220</td>
<td>491</td>
</tr>
<tr>
<td>Spam</td>
<td>389</td>
<td>430</td>
<td>455</td>
<td>434</td>
<td>348</td>
<td>850</td>
<td>338</td>
<td>88</td>
<td>58</td>
<td>3390</td>
</tr>
<tr>
<td>Vulnerabilities Report</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>16</td>
</tr>
</tbody>
</table>


Fraud – phishing, online scam, 419 scam, purchase, impersonation, spoofing
Local News Coverage On MyCERT

**JENAYAH**

**ARXIB : 25/09/2014**

**Hantar virus ke telefon lepaskan wang**

Oleh AZRAI MOHAMMAD
pengsiling@utusan.com.my

---

**Virus Zeus Boleh Serang Maybank2U, CIMB Clicks**

By admin on September 25, 2014

**Nation**

Published: Wednesday August 20, 2014 MYT 12:00:00 AM
Updated: Wednesday August 20, 2014 MYT 1:53:51 PM

**Hacker targets info on MH370 probe**

BY NICHOLAS CHENG

**EXCLUSIVE**: KUALA LUMPUR: The computers of high-ranking officials in agencies involved in the MH370 investigation were hacked and classified information was stolen.

The stolen information was allegedly being sent to a computer in China before CyberSecurity Malaysia – a Ministry of Science, Technology and Innovation agency – had the transmissions blocked and the infected machines shut down.
What we have seen in year 2014

- Mass Web Defacement Incident
- Hoax Message/Malware Attack MH370 Planes missing
- HeartBleed Vulnerabilities
- Spear Phishing Attack related to MH370
- Malware attack on MH17 tragedy
- Speaker Malware
- ‘Is this your photo’ SMS Malware
- DDOS Attack towards FI
- Android Malware – Premium SMS

Jan | Feb | Mar | April | May | Jun | July | Aug | Sept | Oct | Nov | Dec
Malware Research Centre (MRC)

MRC Projects/Activities

Advisories and Alerts

- Software vulnerabilities (Advisories)
  - 0-day vulnerabilities (Java, PDF)
  - Patch / Upgrade
  - Security update for Firefox

- Outbreaks 2015 (Alerts)
  - Circulation of Emails Attached with Malicious Document
  - Attack to .my domains
Advisories and Alerts

MyCERT Advisories

MyCERT Advisories, Alerts and Summaries for the year 2015

- **08/10/2015** MA-525.102015: MyCERT Vulnerability and Threat Summary - September 2015
- **08/10/2015** MA-524.102015: MyCERT Vulnerability and Threat Summary - August 2015
- **04/10/2015** MA-523.092015: MyCERT Alert – New “Ghost Push” Variants Sport Guard Code
- **22/09/2015** MA-520.092015: MyCERT Advisory - Adobe Releases Security Updates for Flash Player

Honeynet - LebahNet

Malware Analysis

Uniq Binaries

Copyright © 2015 CyberSecurity Malaysia
Malware Distribution Sensor

Sensor installed inside the participant network

Further malware processing will be conducted in reporting server

Server to store database of event/binaries processed in reporting server. Dashboard will generate graph/report based on database.

LebahNet Mini Sensor 1
LebahNet Mini Sensor 2
LebahNet Mini Sensor 3
LebahNet Mini Sensor 4

Internet connection encapsulated with SSL-based encryption for report submission * port 443

Malware tries to attack the sensor and sensor will emulate the attacking process as a vulnerable machine to get the sample binaries.

Centralized Reporting Server

DEWS Network

Database Server + Dashboard

Event/binaries will be submitted and processed in reporting server.

Malware Research
Challenges in Sustaining a CERT

- Stakeholder Buy-In
- Cooperation from Various Parties
- Staffing and Skills & Expertise
- Budget
- Quality of service
- Change in Nature of Incident
Stakeholders Buy-In

Challenge to convince the roles of CERTS and its capabilities to a constituency

Stakeholder looks into investment that brings return (ROI). CERTs are non-profit organization.

Must achieve targeted Key Performance Indicators
Cooperation from Various Parties: Local & International

1) Cooperation from Law Enforcement Agencies

2) Cooperation from Service Providers,

3) CERT to CERT cooperation

4) Cross border issues: Language, Culture, Law.
Staffing, Skills and Expertise

- Insufficient staff to meet the growing needs and demands
- Developing/maintaining skills and expertise
- Reduce staff turnover – improve staff benefits
Budget

- Not-self funded
- Affect Resources and operations
- May need to start charge service
- Depends on Economic

Advantages
Quality of Service

1) Consistency & improvement to the quality of current service

2) Introduce more new value-add service for public

3) Customer satisfaction should be a priority

4) Develop new tools to support the operation

5) Incident resolution rate
Nature of Incidents Change

1) Technical vs Non-technical Incidents

2) Challenge to respond to non-technical incidents

3) Victims are aggressive

4) Escalation to Law Enforcement Agencies – incidents sometimes become less priority for Law Enforcement.
Areas of Improvement for CERTS

- Stakeholders buy-in
- Understanding the constituency and its needs
- Resources with necessary skills and expertise
- Effective Communication with all parties
- Efficient Operations and services
Lessons Learnt

• Communication is essential. Need to communicate well on issue faced by the CERT with relevant parties & communication on operational matters.

• Need to ensure the CERTs direction is well understood by all parties in the constituency to avoid misconception on CERT’s roles.

• Selecting right resources with the right skillsets. Always have business contingency plan to address staff turn over issue.

• CERTs need to come up with their own new ideas and solutions to overcome problems and issues related to budget.

• Issues and problems in CERT must not affect the CERTs main functions.
Conclusion

• MyCERT’s presence is needed in our constituency to address the ever-growing cyber incidents.

• Good cooperation and collaboration with the APCERT, OIC CERT, South East Asia countries CERTs and FIRST community has further improved our visibility in the global.

• However, there are still many improvements need to be made in order to sustain our continuity and our visibility.

• Need to immediately address challenges and issues by coming up with effective solutions.
Any Questions
Thank you

Corporate Office
CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.
T : +603 8946 0999
F : +603 8946 0888
H : +61 300 88 2999
www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office
Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia
T: +605 528 2088
F: +605 528 1905
www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy

Copyright © 2015 CyberSecurity Malaysia