Cyber Clean Center Project
- A five year retrospective -

You NAKATSURU
JPCERT Coordination Center
Analysis Center
Agenda

- Background - Japanese situation -
- The Cyber Clean Center
- Seeing the Effect
- Achievement
- Existing Issues
- Current Status
BACKGROUND
- JAPANESE SITUATION -
Internet users in 2005

70.8%

source: MIC "Internet users as a proportion of the population"
http://www.soumu.go.jp/johotsusintokei/english/
Growth of malware until 2005

- Virus
- Worm, Trojan, Backdoor
- Bot

Mischief, Concept code

For Profit (underground)
Infected PCs in 2005

- Targeted "broad-band users"

2.0 ~ 2.5%

400,000 users
Our Decision

- It's easy to reach infected users.
- It's a good idea to develop user literacy.
THE CYBER CLEAN CENTER
Organization Chart

Cyber Clean Center Steering Committee
Ministry of Internal Affairs and Communications/
Ministry of Economy, Trade and Industry

BOT countermeasure system operation group
Telecom-ISAC Japan

BOT program analysis group
JPCERT Coordination Center

Disinfection tool developing business bodies

BOT infection prevention promotion group
Information-Technology Promotion Agency, Japan

Project participating security vendors

Project participating ISPs (Internet service providers)

(about 80 ISPs) (TrendMicro) (7 Anti-Virus Software Vendors)
Operational Framework

Collection → Analysis → Sharing

Notification
SEEING THE EFFECT
User coverage

Partner ISPs

8 large ISPs

2006

2007

2008
Honeypot coverage

/16 block count (Honeypot) 31%

/16 block count (Attack source) 71%
Honeypot improvement

Windows client type (XP + 2000)

Exploit emulation

80 + 30

40
CCC Cleaner enhancement
CCC Cleaner enhancement

IP address type check

Hosts file check

Windows Update

Can not remove

Report the results
Activities of infected users

- TV shows, Newspapers, Magazines
- Events, Presentations
- Improve the site contents
- Deliver direct-mails

<table>
<thead>
<tr>
<th>Activity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access CCC site</td>
<td>70%</td>
</tr>
<tr>
<td>Download CCC cleaner</td>
<td>52%</td>
</tr>
<tr>
<td>Windows Update</td>
<td>44%</td>
</tr>
<tr>
<td>Completion Report</td>
<td>30%</td>
</tr>
</tbody>
</table>

**Access CCC site:** 36%

- TV shows, Newspapers, Magazines
- Events, Presentations
- Improve the site contents
- Deliver direct-mails

**Download CCC cleaner:** 30%

**Windows Update:** 22%

**Completion Report:** 14%
International cooperation

- Information sharing
- Incident response
Human resource development

- anti-Malware engineering WorkShop (MWS)
  - Using "CCC's data" as shared dataset
Human resource development

**IT specialist program to promote Key Engineers as security Specialists (IT Keys)**

ACHIEVEMENTS
Statistics

17,426,320 samples
(1,992,928 unique samples)

30,217 hash-unique unknown samples

206 updates

536,628 emails for 108,726 users
Infected PCs

In **2005**
- **2.0 ~ 2.5%**
- **450,000 users**

In **2008**
- **1.0%**
- **300,000 users**

In **2010**
- **0.6%**
- **190,000 users**
CCC as a best practice

ITU-T Study Group 17

ITU-T X.1205
Overview of cybersecurity
(Approved on 2008-04-18)

ITU-T X.1205
Supplement on best practices against botnet threats
(Approved on 2010-12-17)
EXISTING ISSUES
Attack vector

Not only direct infection via networks

- USB
- Network
- Mail
- Download
- Browser
Countermeasure approach

- Considering other ways to reduce malwares

Diagram:
- Provider
- Herder
- C&C
- Creator
- Reseller
- Spammer
- Affiliater
- Download
- Exploit
- Zombies
CCC as a national project

- a 5 year project

http://www.flickr.com/photos/chaojikazu/5310041917
CURRENT STATUS
Thank You!

Web:  https://www.ccc.go.jp/en_index.html
      https://www.jpcert.or.jp/

Email: aa-info@jpcert.or.jp