Anti-bot Countermeasures in Japan: Cyber Clean Center Update

Chris Horsley / Takashi Manabe
JPCERT/CC
Japan’s online environment
The Cyber Clean Center
CCC Operation
Challenges
127 M
340 /km²

31 /km²
2.5 /km²
Japan’s online environment

Broadband users

~80%
Average connection:

93.6 Mbps

$34.21 USD per month
E-banking penetration: 45.9%
OS share

5% MS Windows 95%
Threats

• Regional specialties
  – Winnie (P2P) data disclosure

• The usual
  – Malicious email attachments
    • Bots
  – SQL injection / malicious web sites
  – Targeted
Intro to the

Cyber Clean Center

(CCC)

A tool for cleaning botnet infections
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

 Project participating ISPs
(Internet service providers)

 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
For your safety net life

BOT is a type of computer viruses and a program that a third party has developed with malicious intent to control your computer externally. Any computer could be infected by BOT once connected to the Internet. This site is to provide you information on how to clean BOT, as well as how to protect your computer from BOT.

INFORMATION

- Activity Report 2008-10
- Activity Report 2008-09
- Activity Report 2008-06

- Fiscal Year 2007 Activity Report on Cyber Clean Center (2008.10.07)
  This is the FY 2007 activity report on “anti-bot measures project,” jointly conducted by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) since December 2006, aiming to eliminate bot infection/bot-infected PCs in Japan through collaborative efforts by related organizations and companies.

- Activity Report 2008-07
- Fiscal Year 2006 Activity Report on Cyber Clean Center (2007.05.25)
  This is the FY 2006 activity report on “anti-bot measures project,” jointly conducted by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) since December 2006, aiming to eliminate bot infection/bot-infected PCs in Japan through collaborative efforts by related organizations and companies.
Collection
Analysis

- Attack reports, samples
- CCC Operations Group
- AV check
- CCC Analysis Group
- Develop detection pattern
- CCC Prevention Group
- Vendors
Analysis

AV Scan
AV vendor notification
Surface analysis
Runtime analysis
Static analysis
Analysis

Goals:
• Trend prediction
• Countermeasure improvement
  – via sharing samples
• Identify supporting infrastructure
  – Secondary malware hosts, C&Cs, config files
Notification

- Attack reports, samples
  - CCC Operations Group
  - ISP 1
  - ISP 2
  - ISP 3
Monthly collection average until now:

- 55k unique samples
- 54k detected by AV
- 1k not detected by AV
- 512k non-unique samples

* Subject to significant variance each month
Results of alert activities in January of FY 2009

1. Total number of collected samples
   - This month: 432,184
   - Cumulative sum: 12,866,088
   - Number of samples of BOT viruses, etc., collected from myriads of attacks on "doocy machines" [binary files]

2. Number of identified, unique samples
   - This month: 36,196
   - Cumulative sum: 827,687
   - As many of the same samples may be collected, this process treats the samples with the same size and external features as one sample. This is the number of identified, unique samples derived from the process (binary files)

3. Number of unknown samples
   - This month: 314
   - Cumulative sum: 21,827
   - The number of samples that cannot be detected by commercially available anti-virus software after isolating and searching for collected samples

4. Number of alerts
   - Number of emails
     - This month: 11,034
     - Cumulative sum: 352,616
   - Number of recipients
     - This month: 4,926 (2,442 new recipients)
     - Cumulative sum: 75,531
   - The number of infected users and the number of alert mails sent to them by Project Participating ISPs

5. Rate of downloading disinfection tools by alerted users
   - 30% (cumulative)

6. Number of samples for which disinfection tools have been developed
   - This month: 337
   - Cumulative sum: 17,750
   - Number of samples that are highly dangerous and transmit infections to many users and for which disinfection tools have been developed

7. Total of disinfection tool downloads from the public opening site
   - Multiple downloads in the same timeslot are counted as one download
   - This month: 18,809
   - Cumulative sum: 554,684
   - Disinfection tools are updated weekly
CCC Cleaner

Copyright 2007-2008, Trend Micro, Inc JPCERT/CC
https://www.ccc.jp

本ドキュメントは、CCCクリーナーの使用上の注意点などを記載したReadme.txtです。
本製品をご利用になる前に、必ずご一読ください。

なお、下記URLに記載されている「駆除ツール」の使用についても十分にご理解いただき、同意してからご使用ください。

ファイル検索オプション
○ すべてのローカルドライブを検索する（A）
○ 選択したフォルダを検索する（C）
CCC features

• Check:
  – Windows Update on?
  – Broadband router?
  – Hosts file

• Explain:
  – Risk of running Win 9x
  – What to do if malware can’t be removed

• Report (optional)
  – Summary of scan results
  – Send to CCC for statistical purposes
363,559 notification emails sent to 77,601 recipients. Around 47% of notifications are for re-infections.
Of 77601 email recipients, 65% go to CCC website. 38% download CCC cleaner. 21% file finish report.
1: Why don’t people download the tool?

Multi-page explanation was too long and technical.

Use single page
Use simple language
Improving user acceptance

2. Engaging education

http://botkujo.jp
Improving user acceptance

3. Security software confusion

- Anti-virus
- Personal firewall
- Anti-spyware
- Security suites

What does what?
4. ISP security services misunderstood

“I’m sure my ISP will protect me.”
Challenges

• Currently honeypots only
  – Honeypots + mail scanning + web site monitoring etc offer better coverage

• CCC only checks for Windows Update
  – Doesn’t check 3rd party apps

• Can’t repair infected system files
  – Current suggestion to users: format

• Bot countermeasures
  – Download site takedown work complex
  – Difficult dealing with “bullet-proof” hosting
Thank you!
office@jpcert.or.jp