Anti-Bot Countermeasures in Japan

- Introducing Cyber Clean Center -

25 March 2008

Telecom-ISAC Japan
Planning and Coordination Division

K. Arimura

What is Telecom-ISAC Japan?

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

https://www.telecom-isac.jp/

- Japan's first ISAC established in July 2002.
- Members including telecommunications carriers collect, analyze and share information and take timely measures to ensure trouble free and stable operations of services.

Members

- **Cooperative activities and information sharing are centered on working groups.**
- **The color of T-ISAC-J activities are reflected in the WGs.**

Pres. : **KDDI Corp.**
VP's : **NTT Communications Corp., NIFTY Corp.**
Members : NEC Corp., **SOFTBANK TELECOM Corp., Internet Initiative Japan Inc.**, Hitachi, Ltd., **Matsushita Electric Industrial Co., Ltd., Oki Electric Industry Co., Ltd., SOFTBANK BB Corp.**, Yokogawa Electric Corp., Matsushita Electric Works, Ltd., **NIPPON TELEGRAPH AND TELEPHONE EAST Corp., NIPPON TELEGRAPH AND TELEPHONE WEST Corp., NTT VISUAL COMMUNICATIONS Corp., KDDI R&D Laboratories, NEC BIGLOBE, Ltd. NIPPON TELEGRAPH AND TELEPHONE Corp.**, FUJITSU LIMITED
Alliance members: Little eArth Corporation Co., Ltd., Intec NetCore Inc., Trend Micro Inc., IBM Japan Co., Ltd./ISS
Observers : Ministry of Internal Affairs and Communications, National Institute of Information and Communications Technology, etc.

The companies in green are ISPs and carriers.

Main activities of WGs

- Responses to DDoS attacks
- Wide area monitoring
- Monitoring of BGP routing information
- Measures to counter Antinny
- ✓ Research and Investigation of infection by botnets in Japan
- ✓ Measures to counter bot programs / Operation of the website CCC etc.

Anti-bot Measures

The Anti-bot Measures Project was launched in December 2006.

- **Our portal site: Cyber Clean Center**
  https://www.ccc.go.jp/

- **Promotion and collaboration among 2 ministries (MIC and METI).**
- **Organized by Telecom-ISAC Japan, JPCERT/CC and IPA.**
- **Co-operation with 65 ISPs who are ISAC members (currently) and antivirus vendors in the anti-bot measures workflow.**
- **From FY 2006 to 2010**
- **Main objectives:**
  - **To reduce the number of bot-infected users**
  - **To make removal tools that specialize in bots that are widespread in Japan**
  - **To provide specimens to security vendors participating in the project.**

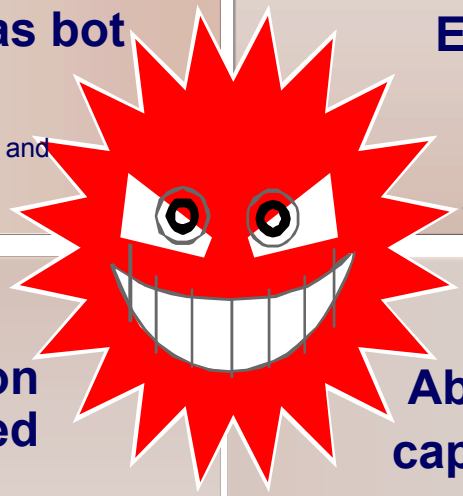
Bots in Japan: Survey Results

About 80% of malware programs observed on Japanese telecom networks are classified as bot programs

【Estimate from the results of studies by T-ISAC-J and JPCERT/CC in 2005】

The estimated infection rate is 2%-2.5%
Equivalent to 400k - 500k people (computers)

【Estimate from the results of studies by T-ISAC-J and JPCERT/CC in 2005】



It takes about 4 minutes on average for an unprotected PC to be infected when connected to the Internet.

【From experiments conducted by T-ISAC-J and JPCERT/CC in 2005】

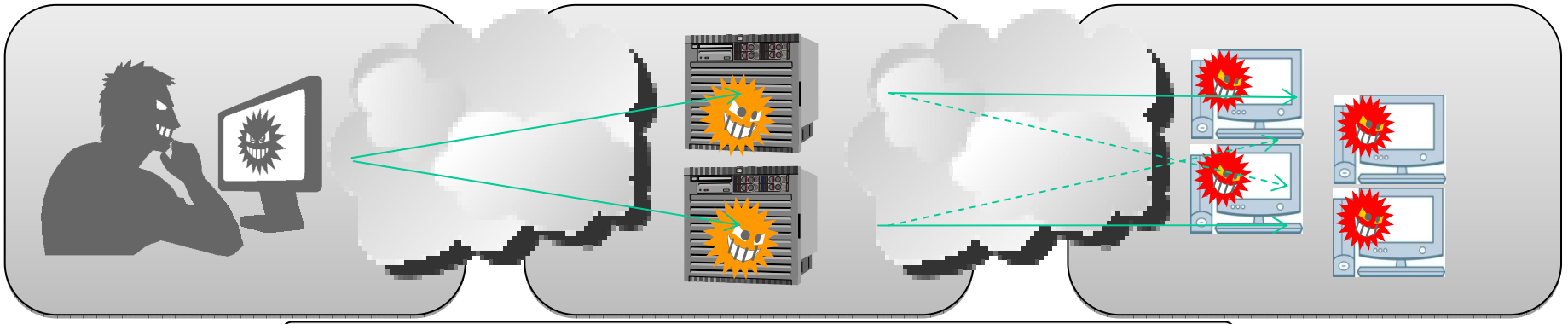
About 100 types of bots are captured in our honey-pot as unknown types per day.

【Number of bot programs with unique hash capturing by CCC】

And

- **It was revealed that traffic caused by botnets or viruses tops 300Mbps per IP.**
- **A total of around 10Gbps of traffic from Japanese IP addresses are wasted by botnets. (SPAM mail traffic via botnets are not included.)**

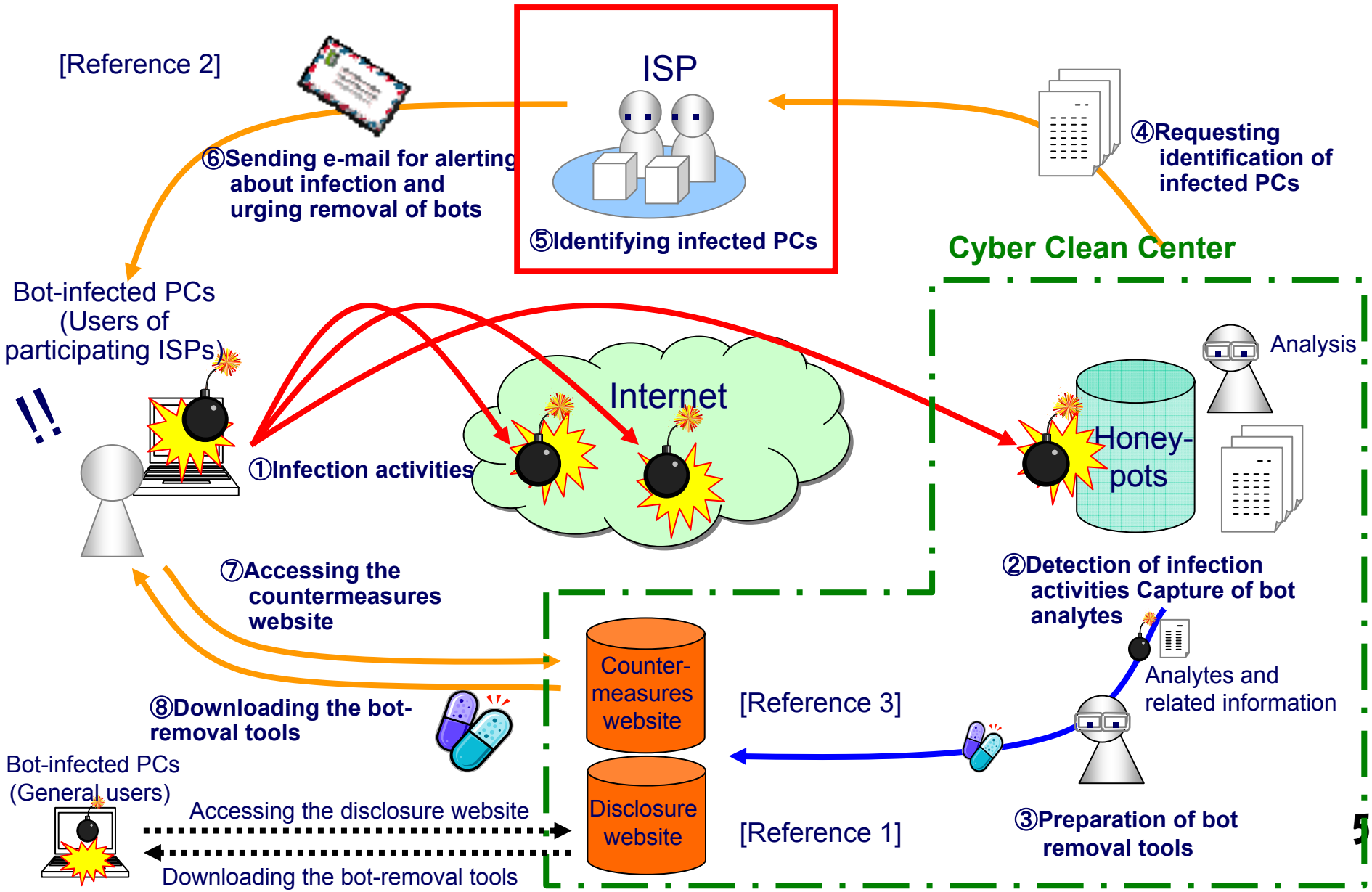
Why Countermeasures against Bot-infected Users?



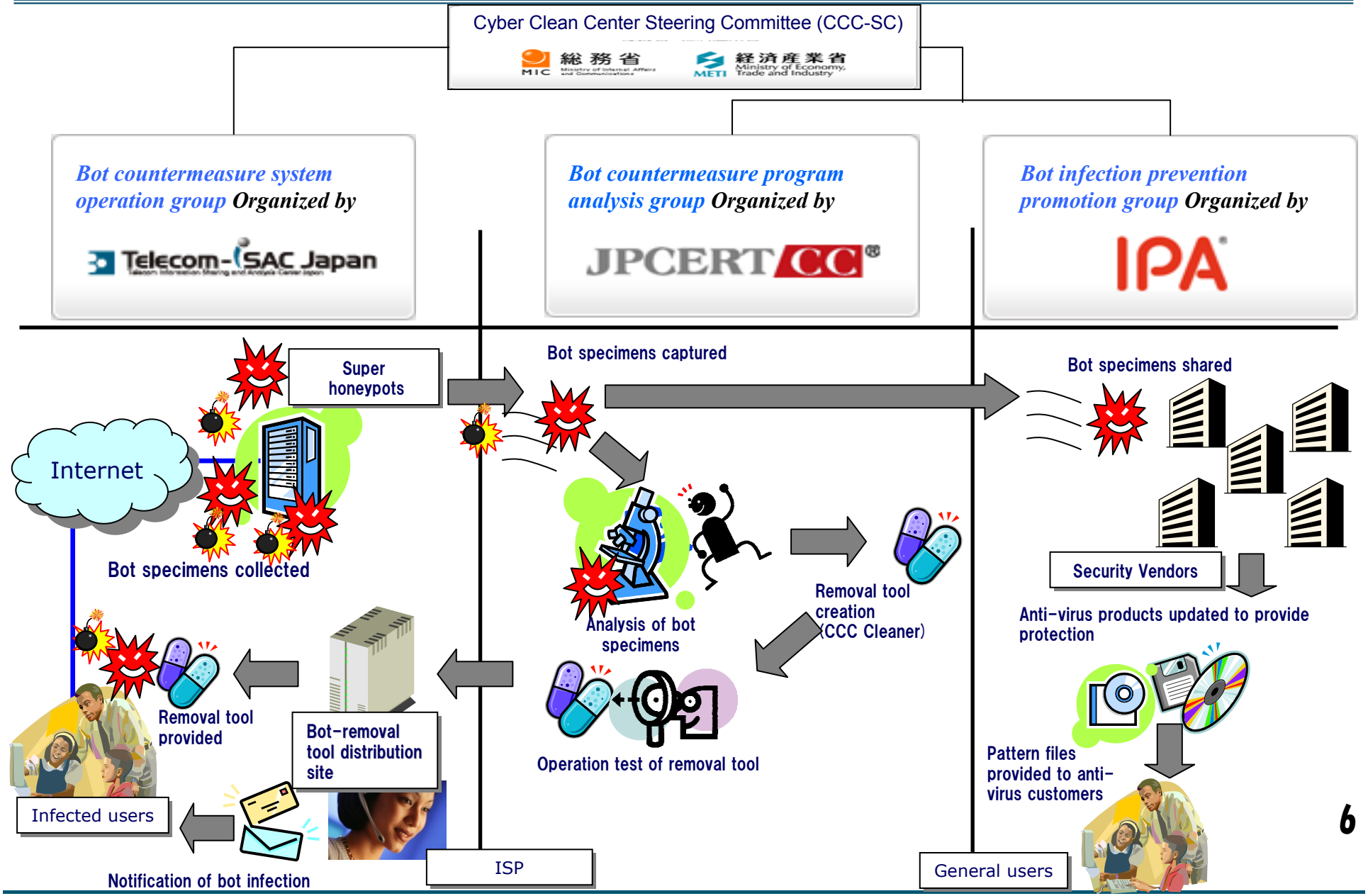
What should countermeasures target?

×	×	○
●Herders are difficult to Yes, It is LEA's Job!	● Servers are located mainly The reason we are here! are eliminated. ● Nevertheless, we want to eliminate C&C servers in Japan.	● Detect bot-infected PCs in Yes, WE can take care of this! ● HoneyPots to collect bots and locate infected PCs!

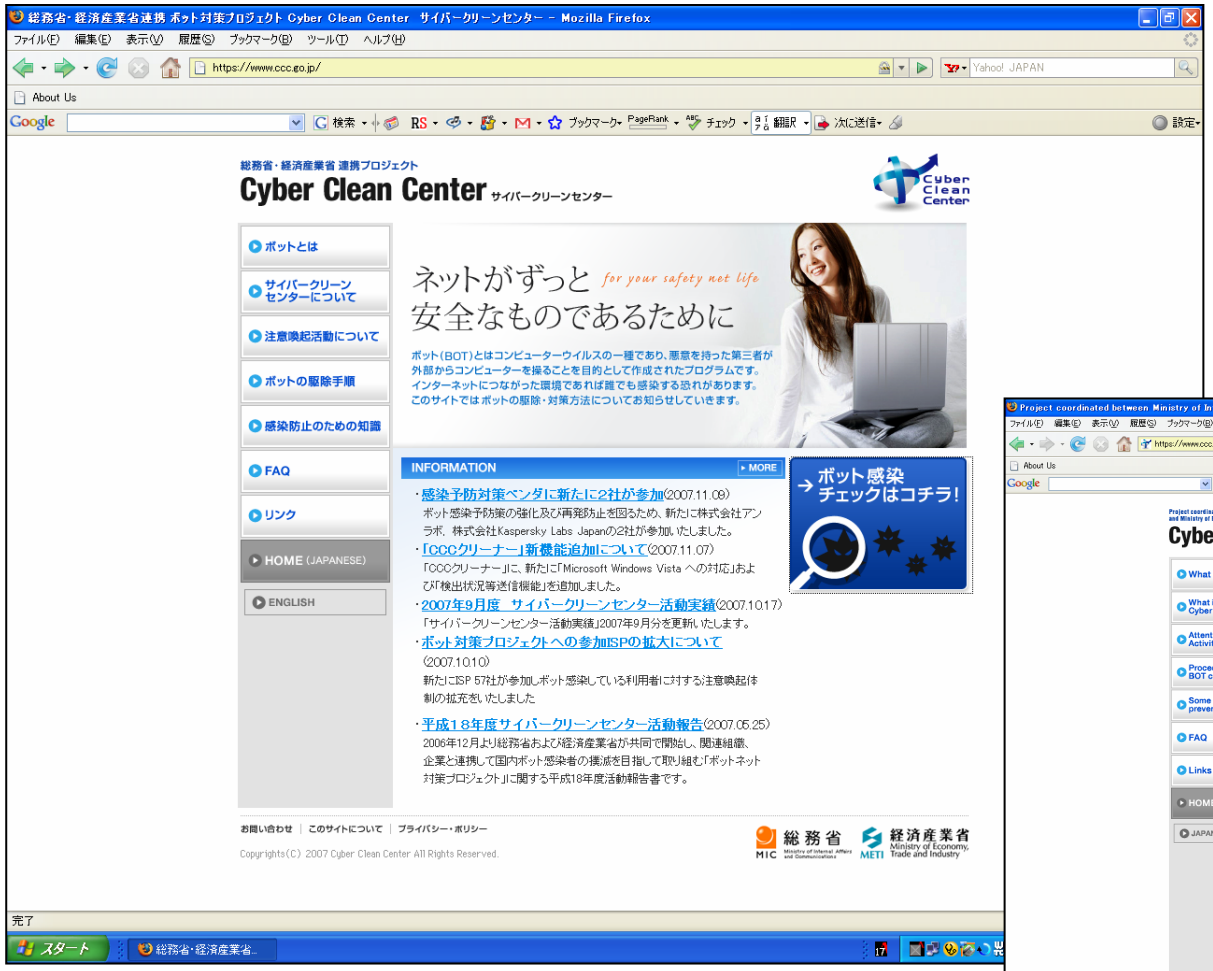
Workflow for Countermeasures against Bot-infected Users



Roles of Three Organizations



CCC Public Site (Image) [Reference 1]



Japanese Version

http://www.ccc.go.jp/

Website for the public

English Version

Security Alert E-mail Text (Image) [Reference 2]

Subject: 【重要】悪性プログラム（BOT）駆除のお願い

あんしん太郎様

平素はAnshin-Netをご利用いただき誠にありがとうございます。
セキュリティ担当　○○と申します。

総務省・経済産業省の連携プロジェクトである「サイバークリーンセンター
（以下、CCC）」より、ボット（BOT）※1感染者からの感染活動に伴う通信が検出
されたため、感染者に対しBOTの駆除を案内して欲しいとの連絡が弊社に寄せられました。

そのため、弊社においてCCCからの情報をもとに感染活動を実施しているOCN回線
を確認したところ、ご契約の回線（お客さま番号「${ISP_CUSTOMER_ID}」）であ
ることが判明いたしました。

ボットは他のお客様に感染を広げるだけではなくお客様のパソコン内の情報を外
部に流出させる恐れもある非常に悪質なウイルスです。

きましては、下記のボット対策サイトへアクセス後、サイト内の手順に従って
ット駆除の実施や再発防止の実施をお願い申し上げます。
応が完了しましたら、サイト内に設置された対策完了ボタンを押して頂くこと
弊社でもお客様の対策実施状況が確認できますので、ご協力お願い申し上げ
す。

■ボット（BOT）対策サイト
https://taisaku.ccc.go.jp/7a4ckxkk3nakf2mf77t

CLICK

| 対策後は必ずサイト上で完了連絡をしていただきますようお願いいたします。
| なお完了連絡がない場合は再度ご案内させていただくことがございます。

～以下省略～

Tracking ID given to each user

To Counter-measures site

CCC Countermeasures Site [Reference 3]

From the alert e-mail

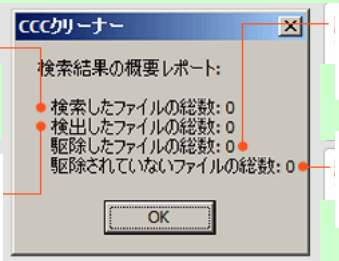
The Tracking ID

[Step3] Results of running cleaner are displayed and sent to CCC

＋ ①Survey

Number of files searched

Number of files cleaned



number of files infected by viruses

Number of files not cleaned

＋ ②Bot-removal status

③ List of malware causing infection

[Sending Results of Running CCC Cleaner]

Results of CCC's Activities

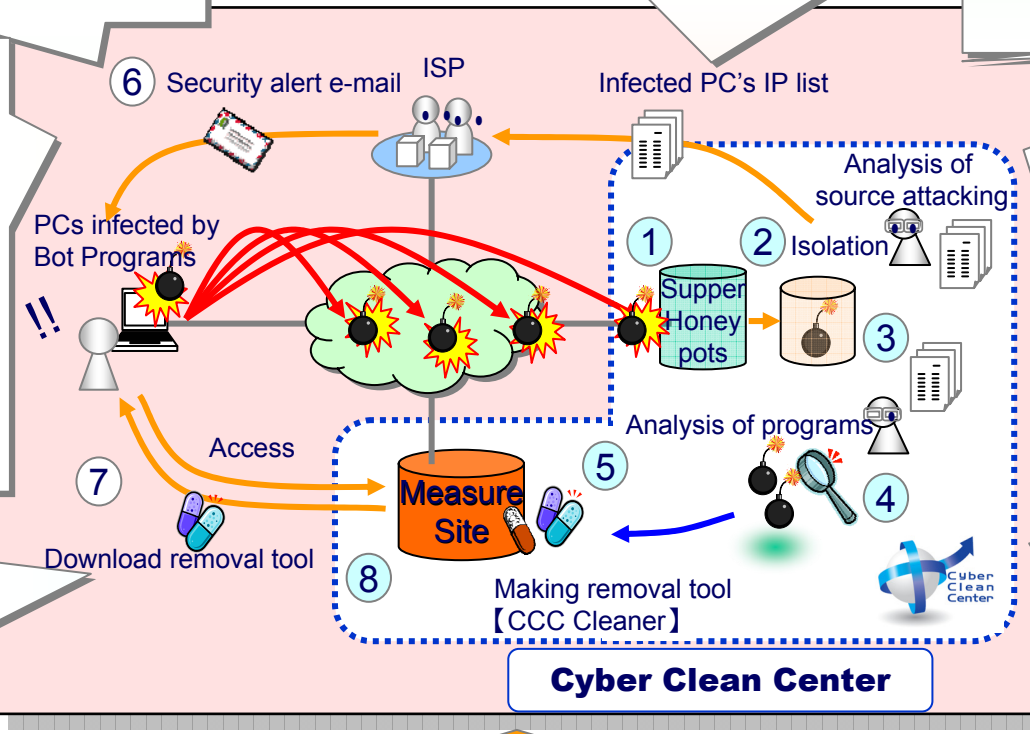
Dec. 2006 - Jan. 2008
(except for some data)

Telecom ISAC Japan

① Total number of specimens collected: **6,534,844**
[Specimens, such as bot programs (binary files) are collected from among the countless attacks on the "honey-pot."]

②Number of unique specimens：**159,683**
[Since a number of the specimens collected are the same, those that are identical in size and external characteristics are removed to separate unique specimens (binary files).]

③ Number of unknown specimens：**8,377**
[Unique specimens are examined using commercial anti-virus software, then those that are undetectable are separated.]



⑥ Security alerts: **197,035** times
[This is the number of security alerts that cooperating ISPs provided to infected users.]

Number of recipients: **48,391**

④Number of specimens reflected in removal tools: **6,915**
[Unknown specimens are analyzed to create bot-removal tools for those that are high-risk and currently infecting many PCs.]

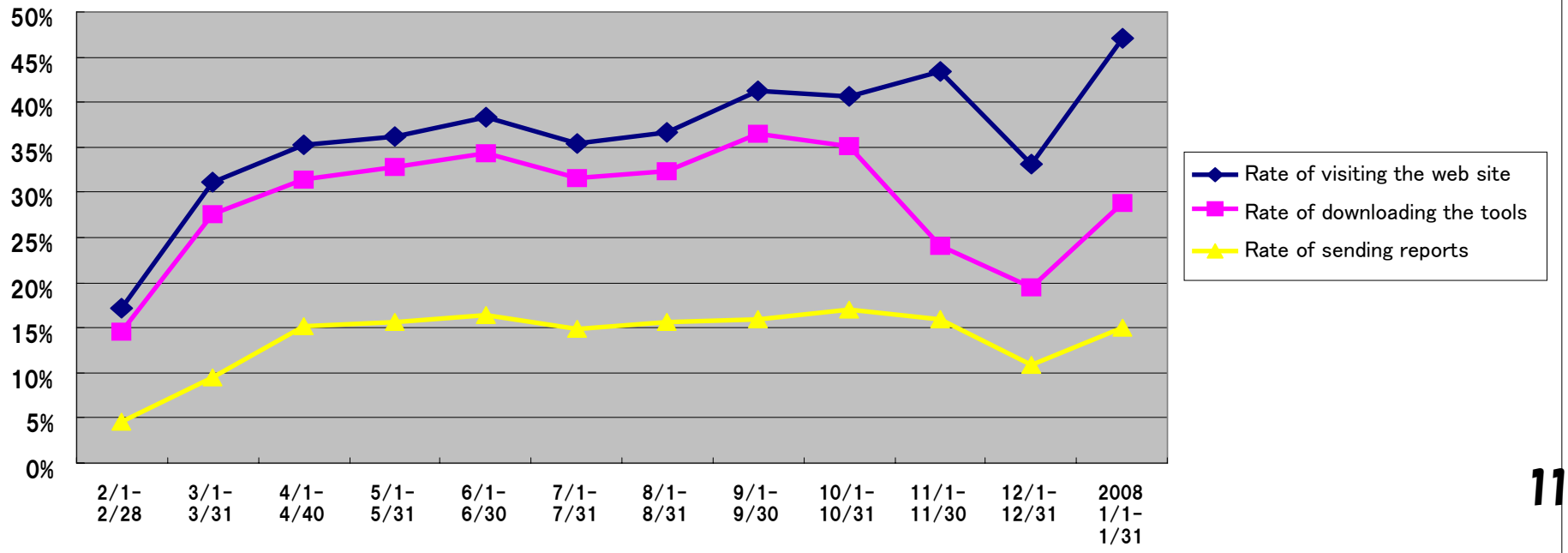
⑦ Ratio of security alert recipients who download bot-removal tools: 30%

⑤Bot-removal tools Updated: 53 times
[Bot-removal tools are updated every week.]

Total Downloads of Removal Tools: **284,100**

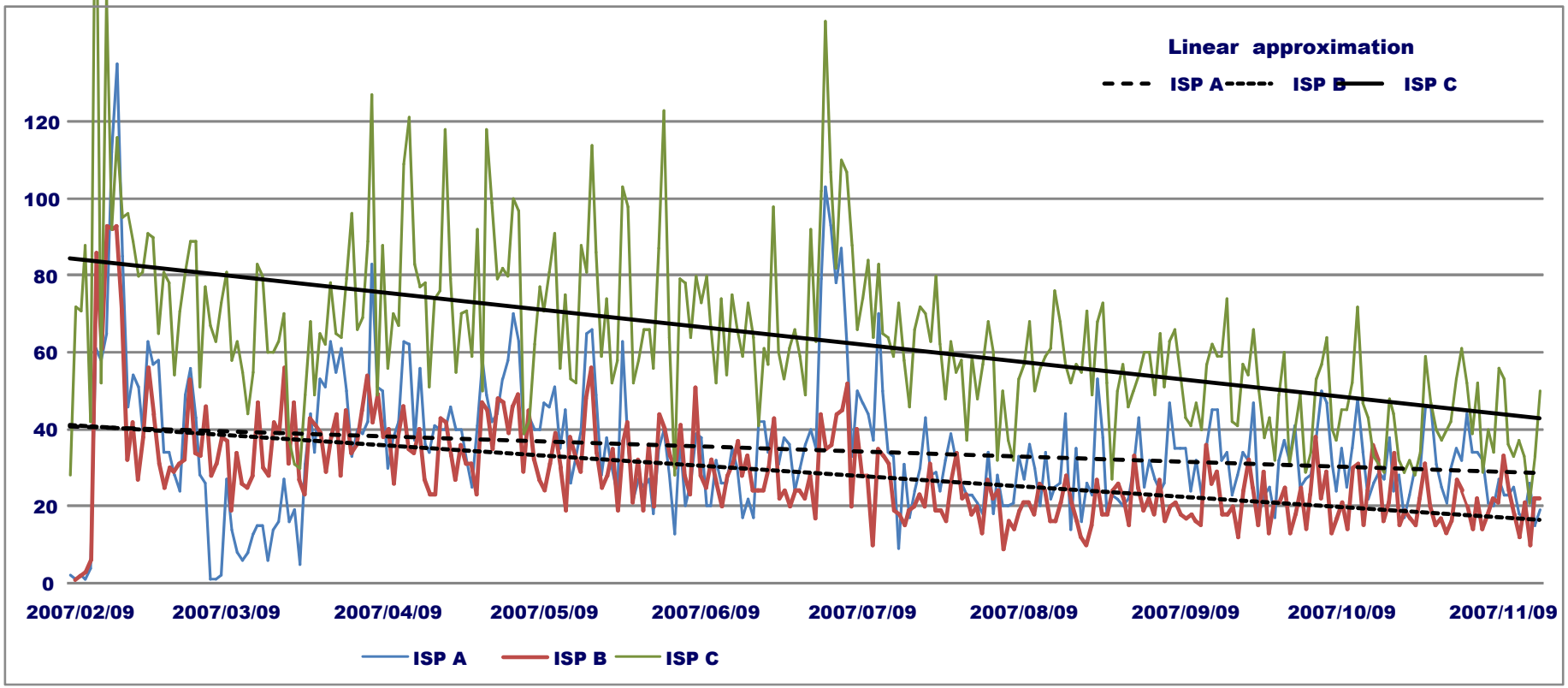
Status of Responses by Users

- The user response rate from e-mail notification is excellent
- The ratio of site visitors is gradually rising but seems to have peeked
- The download rate fell in November due to a change in procedures (Windows Update required before downloading the tools)



Effect of CCC Activities [1]

Changes in Number of New Infections by ISP

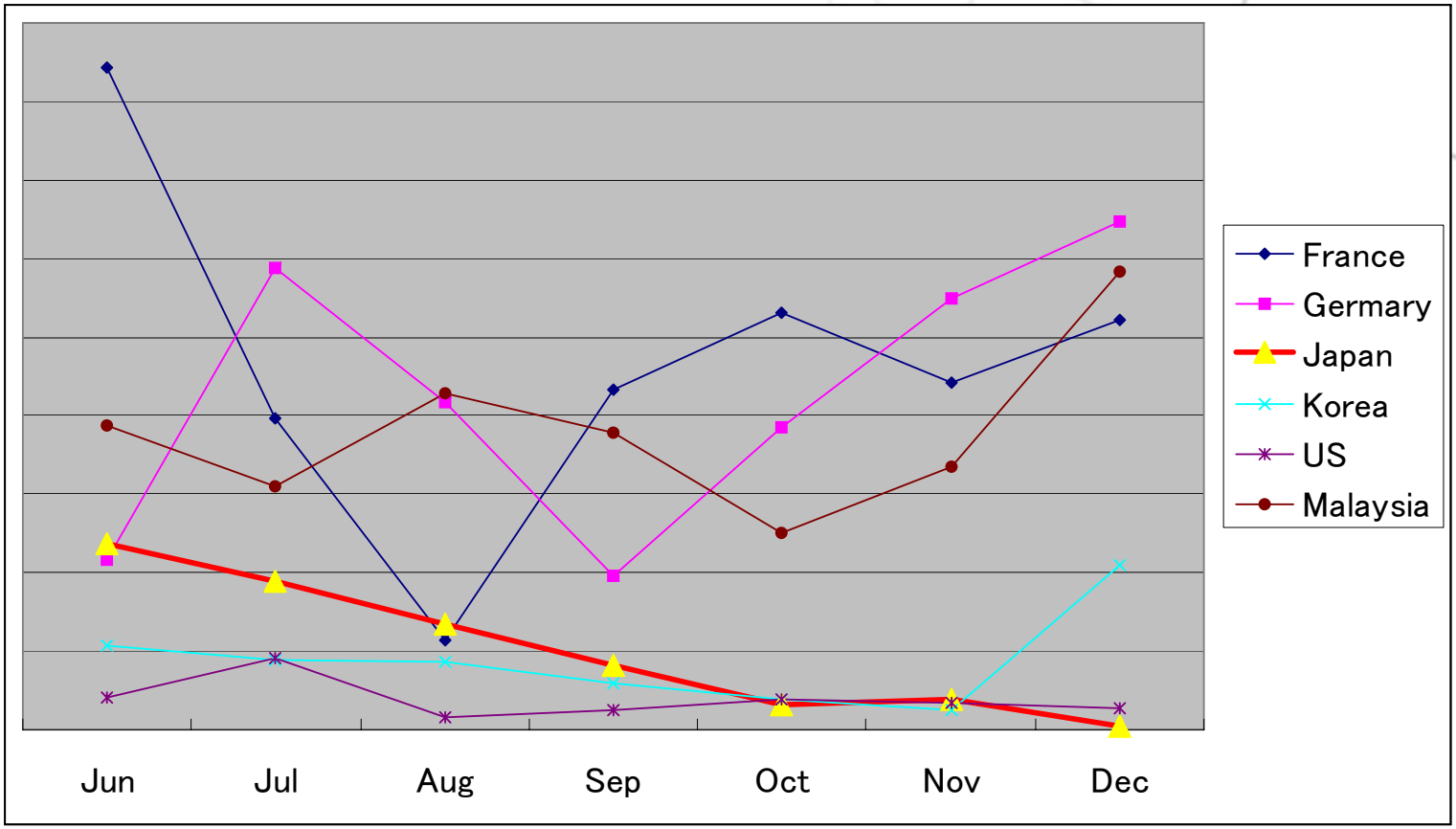


There is a trend of a decline in the number of new users infected by malware

Effect of CCC Activities [2]

安心を、ひとつ上のステージへ。
TREND MICRO

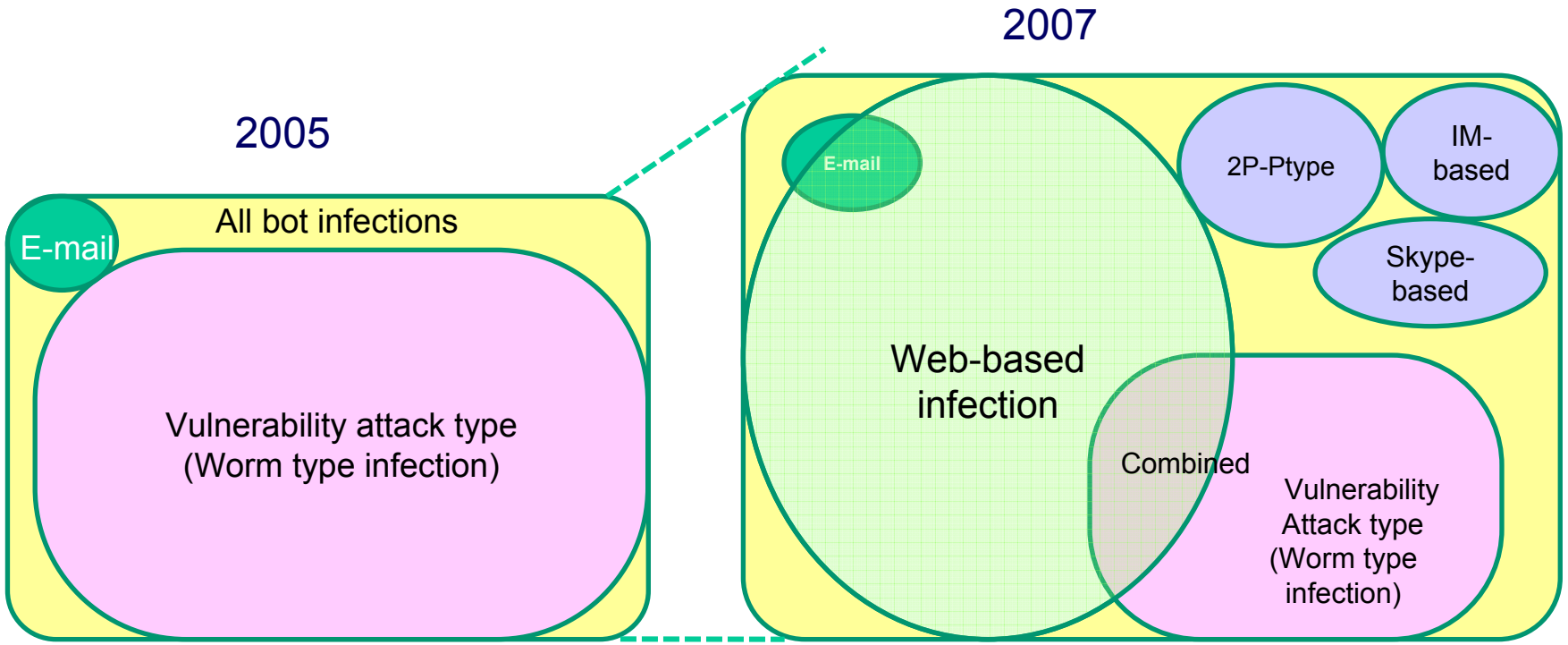
Malware samples collected by bot honeypots worldwide (2007)
（Courtesy Trend Micro Inc.）



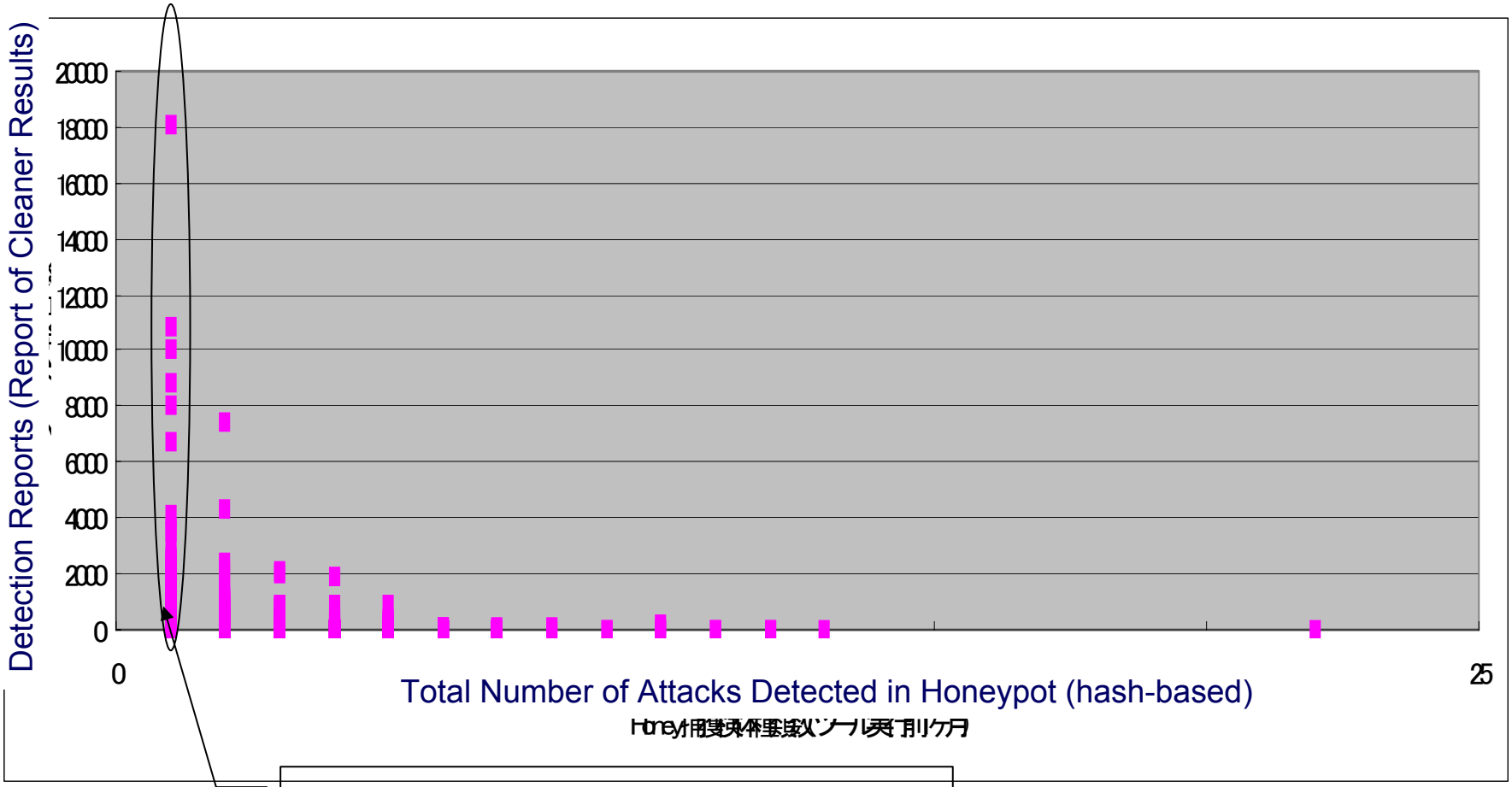
In Japan, vulnerability attacks (worm type infections) tend to be on the decline

Anticipated New Threats Related to Bots

The mode of infection is shifting from vulnerability attack type to other modes, and the threat of bots themselves is increasing (estimate).



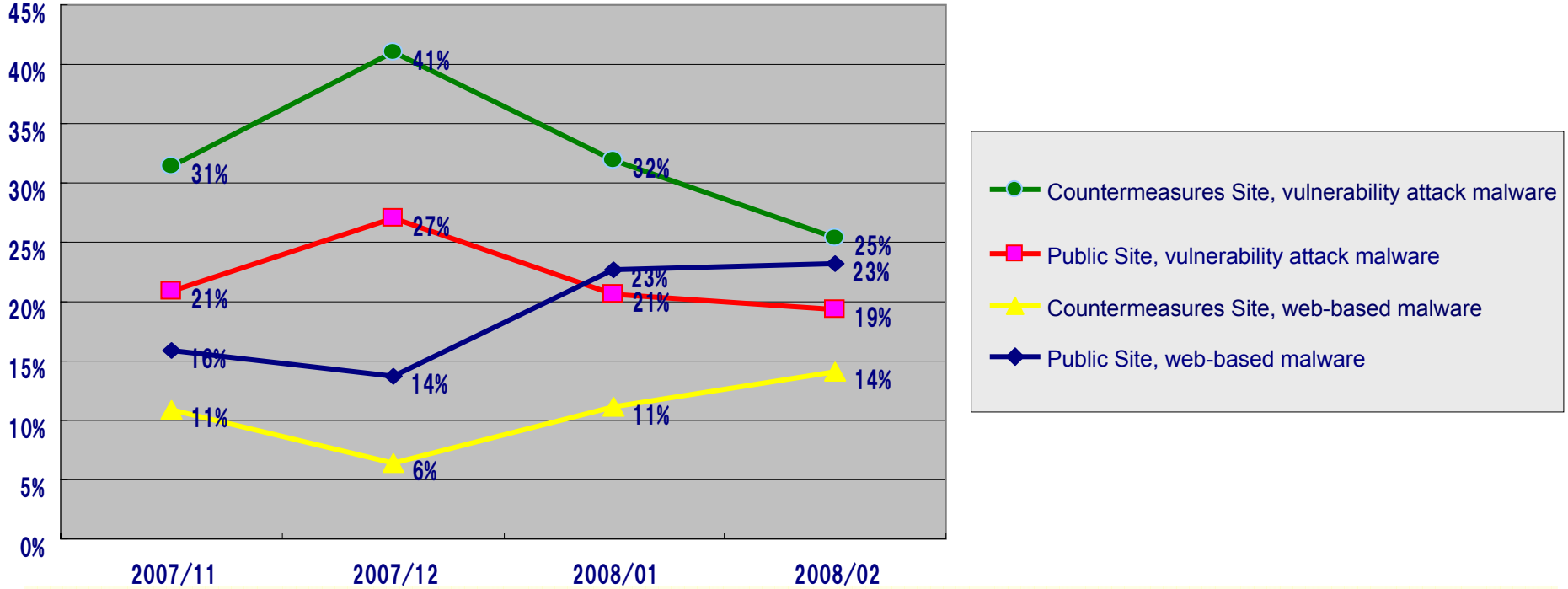
State of Multiple Infections of Bot-infected PCs



There is one type of sample that a PC attacks once the CCC honey-pot , but the PCs are infected by an average of 200.4 malwares.

Used as a topic in user education

From Vulnerability Attacks to Web-based Infection



1. Data
   "Bot infection list" sent using the reporting function after running CCC Cleaner
2. Data analysis
   The content of the list has been classified into web-based infections and vulnerability attacks. The number of types are tabulated on a monthly basis.
3. Trend estimation
   The type of bots using web-based infections are on the increase. The types of bots using vulnerabilities are on the decline.

The number of infections based on the monthly tabulation results shows a similar trend. However, further analysis of monthly trends is required.

The Next Step in Enhancing the CCC Project

- **Change the composition of honeypots**
- **Consider modes of infection other than vulnerability attacks**
  - **Field surveys of malware using web-based infection**
  - **Consider and implement countermeasures against malware using web-based infection**
- **Broaden the reach of ISPs (Increase number of partners)**
- **Build a closer relationship with global partners**
- **Inform the public about anti-malware measures**