Threat Mitigation Strategies for Virus in Japan

AVAR 2003
November 7, 2003

Yasuko Kanno
IT Security Center IPA, Japan

IPA Overview

IPA Information-technology Promotion Agency, Japan
Quasi-governmental organization : Ministry of Economy, Trade and Industry (METI), will be restructured into "Independent Administrative Institution" Established: October, 1970
Mission: Information processing technology promotion Personnel: About 170

- ■ R&D and Support
  - ✧Advanced Software Technology
  - ✧IT Security Technology
  - ✧E-Commerce Technology
  - ✧E-Government Support
- ■ Credit Guarantee
- ■ Education & Training
  - ✧Develop Training Materials
  - ✧Educational Support
- ■ IT Security Enhancement

IPA/ISEC Overview

(ISEC: Information technology SEcurity Center)

- ◆Mission : IT Security Enhancement in Japan
- ◆Established in January, 1997
  - ➢ Had been working on anti-virus activities since October, 1991
- ◆Current Personnel : around 40
  - ➢ Including guest researchers, technical and administrative staffs
- ◆4 Groups
  - ➢ Planning and Research Group
  - ➢ Virus & Unauthorized Access Countermeasures Group
  - ➢ Cryptography Research and Evaluation Group
  - ➢ Security Evaluation & Certification and Information Assurance Group

Today's Agenda

1. Statistics out of IPA surveys and virus detection reports to IPA.
2. Current tendency of virus including fast spreading worms
3. Countermeasures to mitigate virus threat.

PART 1

The Present Virus Status in Japan

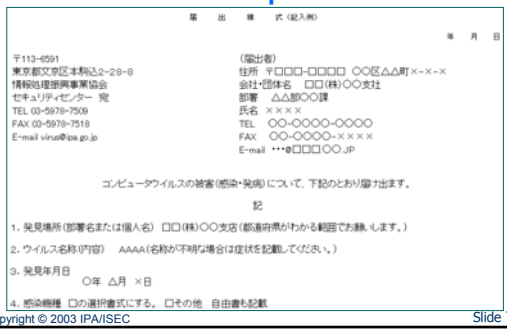
Statistics out of IPA surveys and virus detection reports to IPA.

Data Source

1. Virus Detection Report by E-mail or FAX submitted to IPA everyday
2. Annual Virus Survey by IPA
3. Recent Survey regarding Blaster

Virus Detection Report

Format of the report to IPA



第　出　様　式（記入例）

年　月　日

〒113-6591
東京都文京区本郷3-28-8
情報処理振興事業協会
セキュリティセンター　宛
TEL 03-5978-7509
FAX 03-5978-7518
E-mail virus@ipa.go.jp

（届出者）
住所　〒□□□-□□□□　○○区△△町×-×-×
会社・団体名　□□（株）○○支社
部署　△△部○○課
氏名　××××
TEL　○○-○○○○-○○○○
FAX　○○-○○○○-××××
E-mail　･･･@□□□.○○.JP

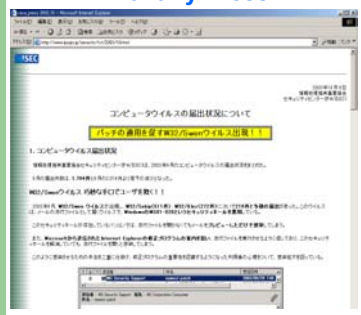
コンピュータウイルスの被害（感染・発病）について、下記のとおり届け出ます。

記

1. 発見場所（部署名または個人名）　□□（株）○○支店（都道府県がわかる範囲でお願いします。）
2. ウイルス名称（内容）　AAAA（名称が不明な場合は症状を記載してください。）
3. 発見年月日
　○年　△月　×日
4. 感染機種　□の選択書式にする。　□その他　自由書も記載

Virus Detection Report - Sep 2003

Monthly Press



コンピュータウイルスの届出状況について

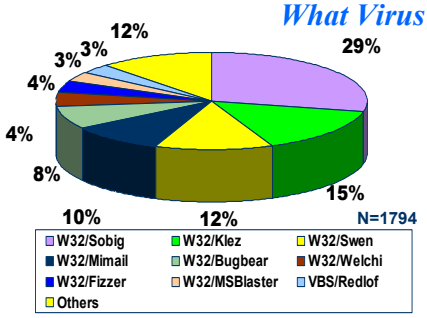
パッチの適用を促すW32/Swenウイルス出現！！

This is an example of monthly virus incident report for September 2003 complied by IPA. IPA made monthly press release to show the virus incident tendency and advice the Best Current Practice to protect against virus.

In September 1,794 reports were submitted and there is a little decrease of the number comparing August repots of 2,014

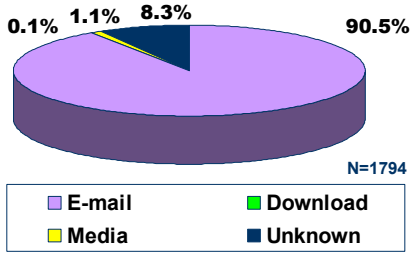
Virus Detection Report - Sep 2003

What Virus?



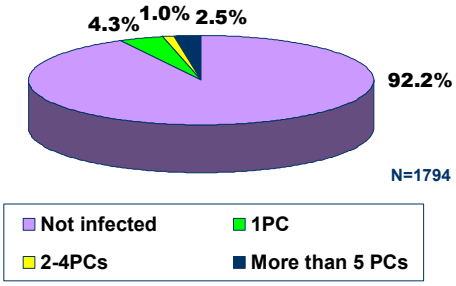
Virus Detection Report - Sep 2003

From Where?

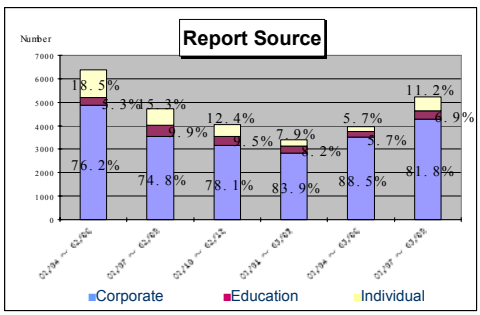


Virus Detection Report - Sep 2003

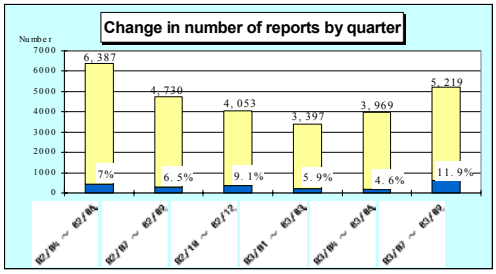
How many PCs are infected?



Virus Detection Report Apr 2002-Sep 2003

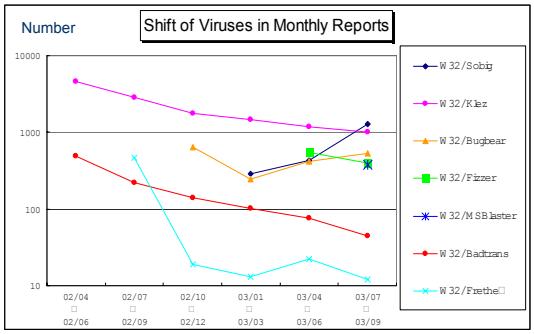


Virus Detection Report Apr 2002-Sep 2003



shows the number of damaged bodies
shows the number of detected cases before infection

Virus Detection Report Apr 2002-Sep 2003



Prevalence Table - Aug. 2003

VB		IPA	
1. Win32/Sobig	66.29%	Win32/Sobig	26.91%
2. Win32/Miami	18.74%	W32/Klez	20.31%
3. Win32/Opaserv	5.54%	W32/MSBlaster…	15.64%
4. Win32/Bugbear	2.30%	W32/Bugbear	7.60%
5. Win32/Klez	1.61%	W32/Miami	5.31%
6. Win32/Nachi	1.28%	W32/Welch…	4.27%
7. Win32/Dupator	1.10%	W32/Fizzer	3.77%
8. Win32/Yaha	0.68%	VBS/Redolf	3.13%
9. Win32/Lovsan	0.51%	W32/Yaha	2.33%
10. Win32/Funlove	0.37%	Wscript/Fortnight	1.54%

… : Win32/Lovsan is also known as W32/MSBlaster
Win32/Nachi is also known as W32/Welch

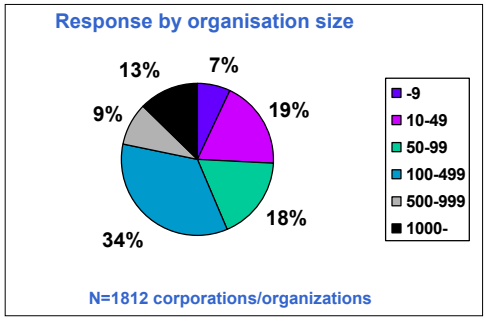
Annual Virus Survey

Questionnaires

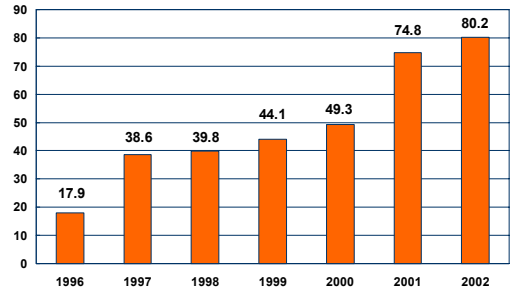
5,000 questionnaires sent to various companies/organizations in Japan

- done every year since 1989
- returned 1,812 responses (36%)
- term: Jan. – Dec. 2002

Annual Virus Survey 2002

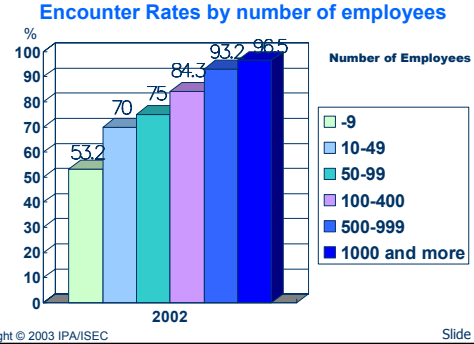


Annual Virus Survey 2002



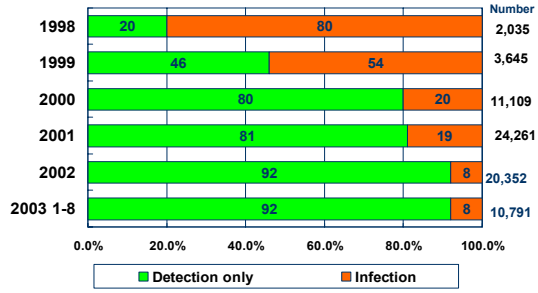
Annual Virus Survey 2002

Encounter Rates by number of employees



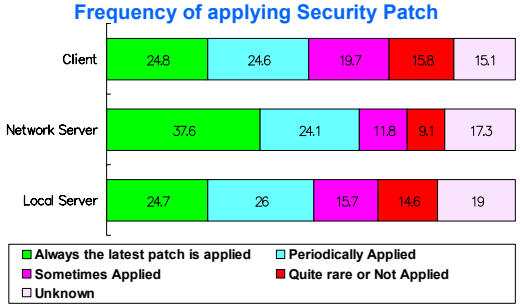
Change of infected rate

"Was your computer already infected or did you find it before infection?"



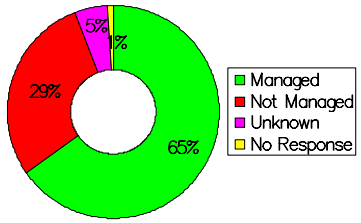
Annual Virus Survey 2002

Frequency of applying Security Patch



Annual Virus Survey 2002

Anti-virus software Update Management



Annual Virus Survey 2002- Overseas

Survey-for U.S.A., Germany, Korea and Taiwan

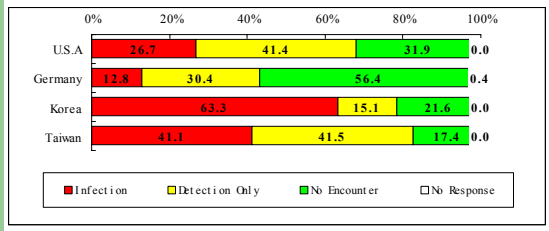
Respondents' ratio classified by number of employee

Country / Number of employee	U.S.A N=502 (%)	Germany N=502 (%)	Korea N=500 (%)	Taiwan N=501 (%)
1 - 9	24.3	35.1	15.4	15.2
10 - 49	18.7	31.3	29.8	28.7
50 - 09	9.8	15.1	23.6	21.6
100 - 499	13.5	15.9	25.8	26.5
500 - 999	18.5	1.6	2.6	4.0
1000 -	15.1	1.2	2.8	4.0
No Answer	0.0	0.0	0.0	0.0

The survey was conducted by visiting companies and got 500 and more of responses for each country.

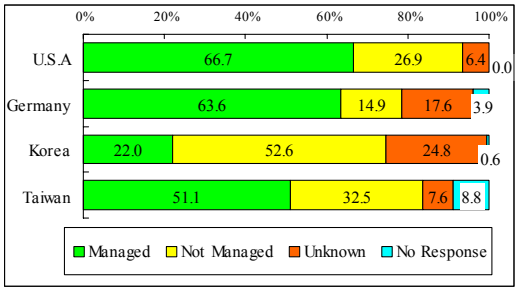
Annual Virus Survey 2002- Overseas

Rate of Infection/Detection



Annual Virus Survey 2002- Overseas

Anti-virus software Update Management



Survey regarding Blaster and Welch

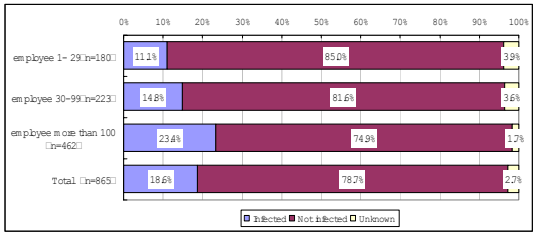
Recent Survey regarding Blaster and Welch

Questionnaire through telephone and fax

- from 28 Aug, 03. - 11 Sep, 03 (2weeks)
- to corporate user (mainly system administrator)
- returned 982 responses

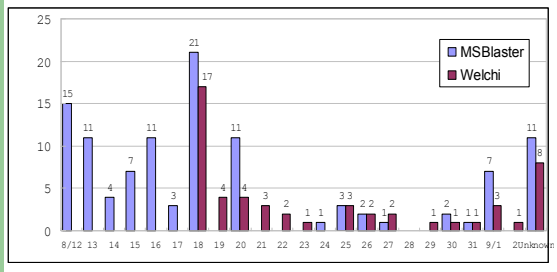
Survey regarding Blaster and Welch

Infected body (percentage) by MSBlaster and Welchi



Survey regarding Blaster and Welch

Infected Date by MSBlaster and Welchi

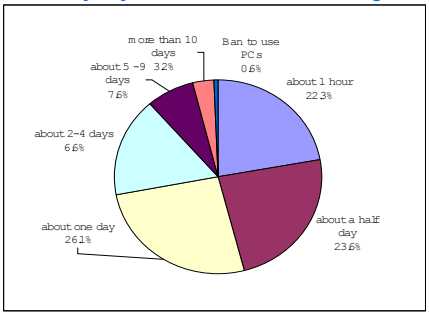


(n=164)

Survey regarding Blaster and Welch

How many days to recover from the damage

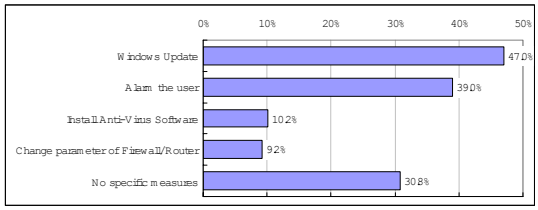
(n=157)



Survey regarding Blaster and Welch

What kinds of taking measures

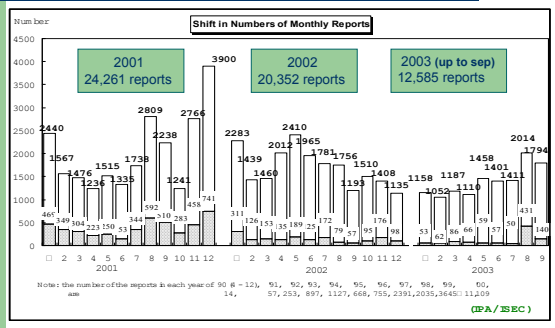
(n=866)



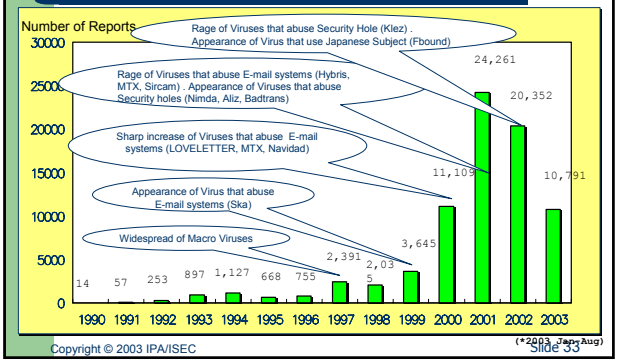
PART 2

Current tendency of virus including fast spreading worms

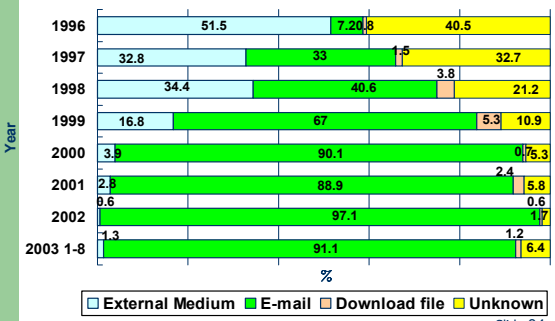
Shift in Numbers of Monthly reports



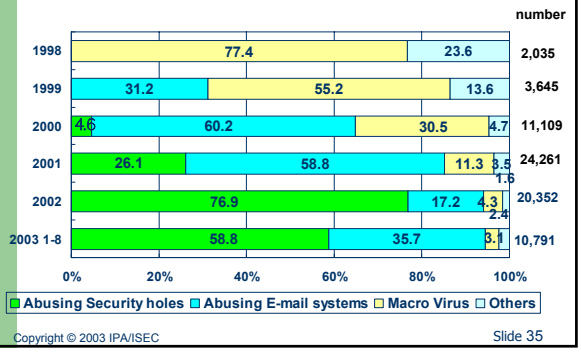
Tendency of Virus from 1990 - 2003



Change of the Method of Infection



Types of Viruses



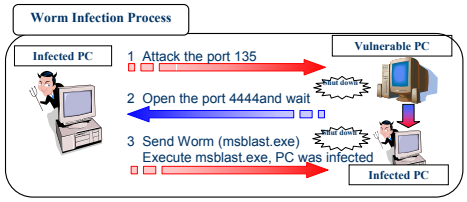
Major Viruses reported from Jan – Aug, 2003

Name of the Virus	Number	First reported	Method of Infection
W32/Klez	3,355	2001/11	Abuse e-mail system & Security Hole
W32/Sobig	1,492	2003/ 1	Abuse e-mail system
W32/Bugbear	1,050	2002/10	Abuse e-mail system & Security Hole
W32/Fizzer	862	2003/ 5	Abuse e-mail system
VBS/Redlof	601	2002/ 5	Abuse e-mail system & Security Hole
W32/Yaha	393	2002/ 8	Abuse e-mail system
W32/MSBlaster	315	2003/ 8	Abuse Security Hole
XM/Laroux	212	1997/ 1	Macro Virus (Excel)
W32/Magistr	209	2001/ 4	Abuse e-mail system
W32/Hybris	205	2000/12	Abuse e-mail system

Outbreak of W32/MSBlaster.

First reported Aug 2003

Abuse RPC Vulnerability of MS03-026



Just connect to the internet, then infected!

Current tendency of Virus

Various Infection Route

* Abuse E-mail system (execute attached file and infected)
* Abuse E-mail and Security Holes (no execution necessary)
  Only preview mails and infected (Klez. Frethem)
  Only see the Web page and infected (Nimda)
* Abuse Security Holes -> fast spreading worms
  (IIS: CodeRed SQL: Slammer RPC: MSBlaster)
* Abuse Shared Folders (Nimda, Bugbear)
* P2P file system (Fizzer)

Use Multiple Infection Method

Current tendency of Virus

Mass infection and long term influence

* Spread Millions of PCs in a twinkle (MSBlaster.Slammer)
* Spoof sender, Delete anti-virus software (Klez, Bugbear)

Attack Computer Network

* Denial of Service Attack
* Back Door
* Falsification of Web page
* Leakage of the information.

Using Cracking Method and Spread rapidly.

PART 3

Countermeasures to mitigate virus threat

Advise on Computer Virus

IPA/ISEC provides advice on virus

- Around 2,000 advices per month via phone and fax
  10:00 – 17:00 Monday – Friday
  emergency such as MSBlaster 24x7
- Publishing FAQ on important advice via IPA/ISEC web site.

Monthly Tips when press release

- September : Be careful about W32/Swen which deceive you in sophisticated way!!
- August : Historical Damage cased by W32/MSBlaster. Did you exterminated the worm?
- July: Invisible virus lurks in the mail. Did you installed the patch for the security hole?

Advise on Computer Virus

Various information of countermeasures

Best Current Practice for IT users in Japan

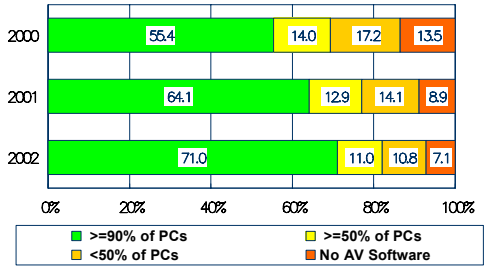
- The Seven Basic Anti-Virus Measures for PC Users
- The Five Instructions When Opening Attachment Files
- The Dangers of Downloading

Various information of countermeasures

- New Virus Information
- Virus DB
- Anti-Virus School (CD-ROM)
- Anti-Virus Movie
- Check list of anti-virus countermeasures
- Investigation and report

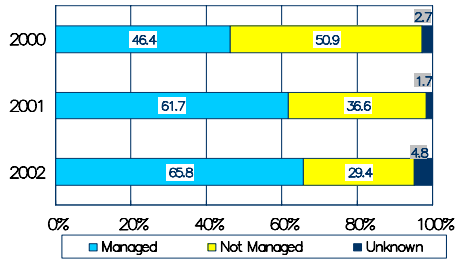
5 millions web page accesses per month

Installation Rate of Anti-Virus Software for Clients



Source: Annual Virus Survey 2000 - 2002

Anti-virus software Update Management



Source: Annual Virus Survey 2000 - 2002

ALERTS

IPA/ISEC provides alerts and information on countermeasures on specific web pages, when new viruses with fast spreading capability or serious vulnerability are found.

Following alerts are issued recently

- W32/Swen (Listed on September 22, 2003)
- Windows RPCSS (Listed on September 18, 2003)
- W32/MSBlaster (Updated on September 11, 2003)
- W32/Sobig (Updated on August 22, 2003)
- Windows RPC vulnerability (Updated on August 13, 2003)
- W32/Bugbear (Updated on June 9, 2003)
- W32/Fizzer (Updated on May 14, 2003)

IT Security Seminar

- From1995 held security seminar every autumn in cooperation with METI
- This autumn only in October more than 1000 attendants in 8 locations
- Around 50 seminars in year
- More than 5000 attendants per year
- Virus demonstration
- Distribute CD-ROM, Videos and Information

IPA Internet Observation System

- Internet traffic monitor using 8 global IP addresses (6 for monitoring, 2 for test)

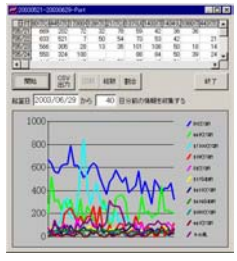
  Mainly monitor ports scan (TCP/UDP)
- Real time logging
- Provide real time visual output
- Database function
- Make various reports from the accumulated data

Background

Massive scanning activity, Random propagation of worms
Flood of vulnerability information
(need information in the wild for appropriate risk analysis)

Internet traffic monitoring

Sample Report - Top 20 port attacked



* Top 20 port attack during 40 days form 2003/06/29
* Accumulated data can be processed using Excel format

IPA Countermeasures against W32/MSBlaster

- On 17th July, Microsoft announced a new vulnerability
- IPA recognized the dangerous character and high risk level of this vulnerability and released emergency alert on our web page.

Since the announcement of this vulnerability, IPA alerted to pay high attention against the appearance of the worm which exploits this vulnerability.
Since then, IPA gathered as much as information from not only domestic but also international sources using IPA Multilingual Information System and also carefully watched internet traffic through IPA Internet Observation System.

12th August

Appearance of the W32/MS Blaster Worm

IPA Countermeasures against W32/MSBlaster

IPA Activities

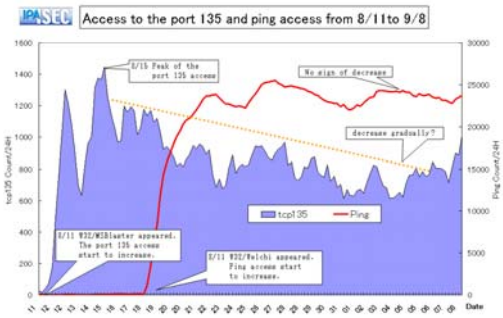
* Consultation over the phone.
* Distribute recovery manual by fax.
* Emergency Level Support of 24 x 7
* Gather and provide information using IPA internet observation system.
* Release alert to users who will return from their summer vacation.

Call/Fax/Mail in this period

	new	total
8/12 (Tue)	70	70
8/13 (Wed)	130	200
8/14 (Thu)	400	600
8/15 (Fri)	600	1200
8/16 (Sat)	500	1700
8/17 (Sun)	130	1830
8/18 (Mon)	310	2140
8/19 (Tue)	90	2230
8/20 (Wed)	100	2330
8/21 (Thu)	40	2370
8/22 (Fri)	30	2400

About 10 days from the worm outbreak, the number of inquiries and phone calls or fax to IPA seeking advice and consultation against the worm showed the tendency to calm down.

Data from IPA Internet Observation System



Anti-Virus Activities

- Receives reports on Computer Virus
- Summarize reports and publicizes statistics/countermeasures monthly basis
- Virus Survey – annually and occasionally
- Virus Alert
- Vulnerability Information
- Provide Best Current Practice Tip
- IT Security Seminar
- Internet Monitoring

IT Security Center(ISEC)

Information-technology Promotion Agency (IPA)

http://www.ipa.go.jp/security/

isec-info@ipa.go.jp