

Are the Internet users safe ? The unknown enemy ?

India, 23.1.2006, SANOG event

F-Secure Corporation

Jari Heinonen

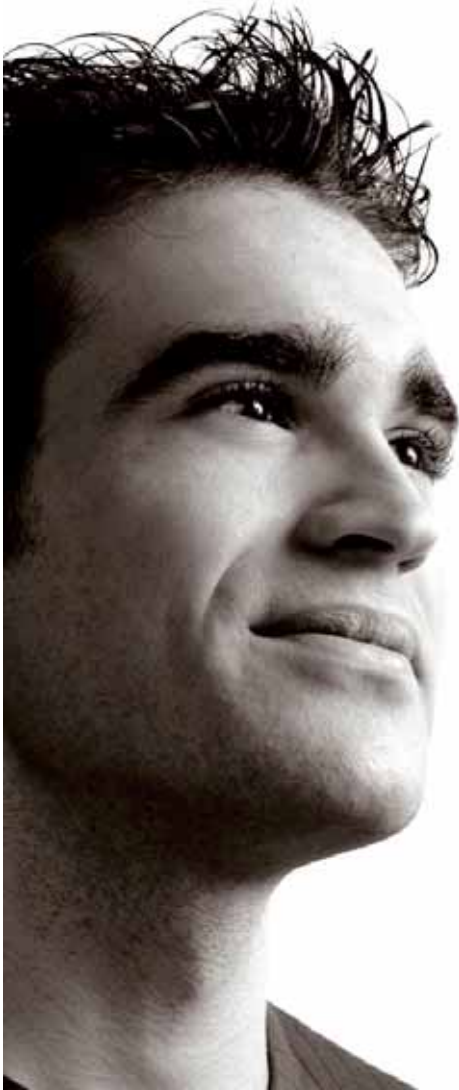
Director, Asia Pacific Region

jari.heinonen@f-secure.com



Topics

1. Virus threats
2. Damage caused by the viruses
3. eMail threats
4. Spam problem
5. Why security through ISP's ?
6. Future outlook





Our shared challenge:

New threats take many forms, appear faster and are developed by organized criminals

F-SECURE®



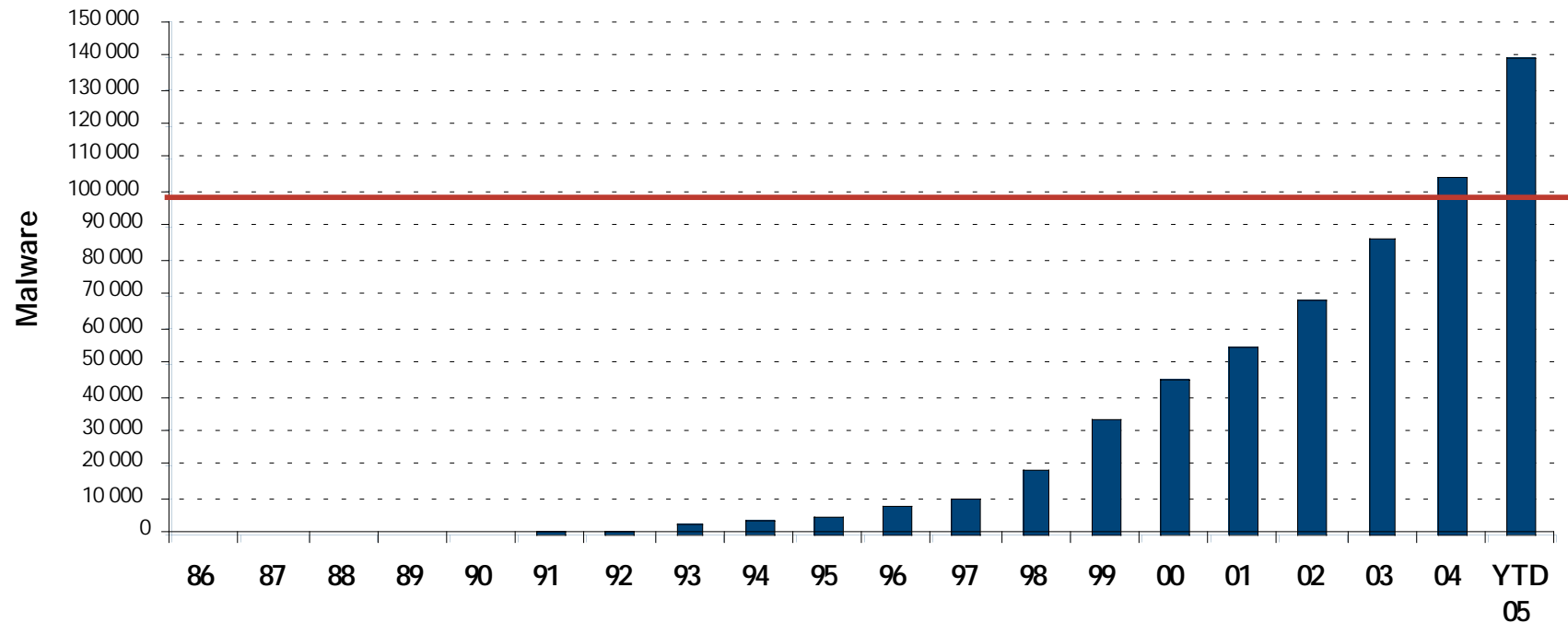
BE SURE.



Virus Eras 1986-

Years	Virus type	Outbreak speed
1986-1995	Boot virus	One year
1995-1999	Macro virus	One month
1999-	Email worm	One day
2001-	Network worm	One hour

The volume growth of malware in the wild shows no sign of slowing down

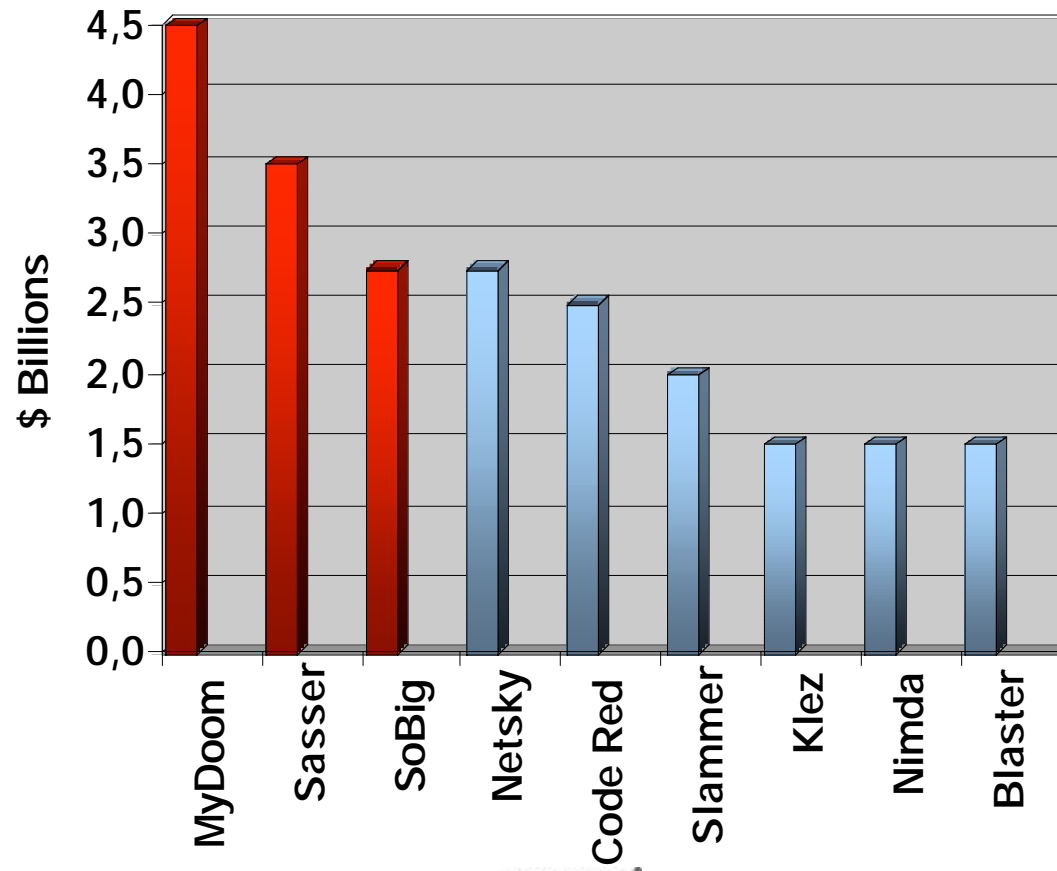


Data source: F-Secure

What did they cause?

Name	Transportation	Power	Infrastructure	Banks
Slammer	Air traffic control problems in USA	Infected a nuclear power plant in Ohio	911 phone services down in Seattle	Bank of America's ATM network down
Blaster	Air Canada flights grounded, CSX trains stopped	NY ISO power operator's network infected	Numerous RPC-based SCADA networks down	Several Windows-based ATM networks infected
Sasser	Railcorp trains stopped in Australia, Delta flight problems, delays with British Airways flights	Hong Kong government's department of energy networks infected	Infected: Two hospitals in Sweden, EU commission, Heathrow airport, Coastguard UK	Several banks shutting down offices because of internal infections

Top 9 financial damage of malicious code attacks 2001-2004



Data source: CEI

What are the threats?

Viruses, worms

Phishing scams

Online data theft, identity theft

Spying

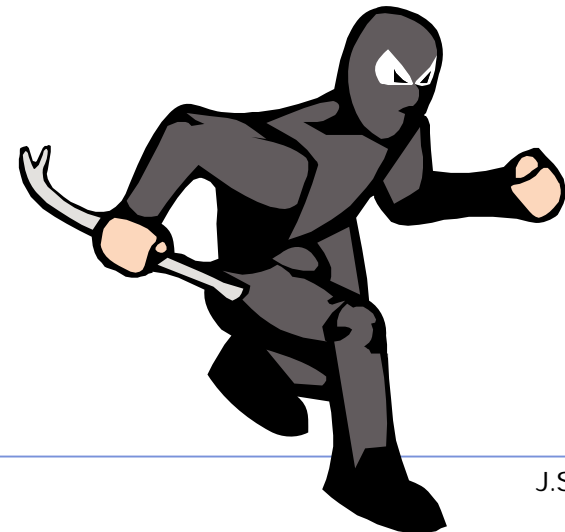
Who's behind them?

Kids, teenagers

Activist, anarchists

Criminal organizations

Spies



We used to be fighting these...



Chen-Ing Hau
Author of
the CIH virus



Joseph McElroy
Hacked the Fermi lab
network



Benny
Ex-29A



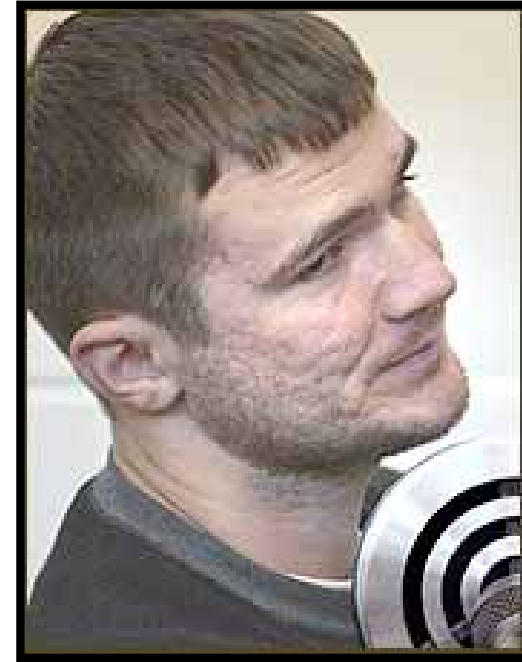
Today we are fighting these!



Jeremy Jaynes
Millionaire,
and a spammer



Jay Echouafni
CEO,
and a DDoS attacker



Andrew Schwarmkoff
Member of Russian mob,
and a phisher





MONOCULTURE



Windows
& TCP/IP



Windows
& TCP/IP



Windows
& TCP/IP

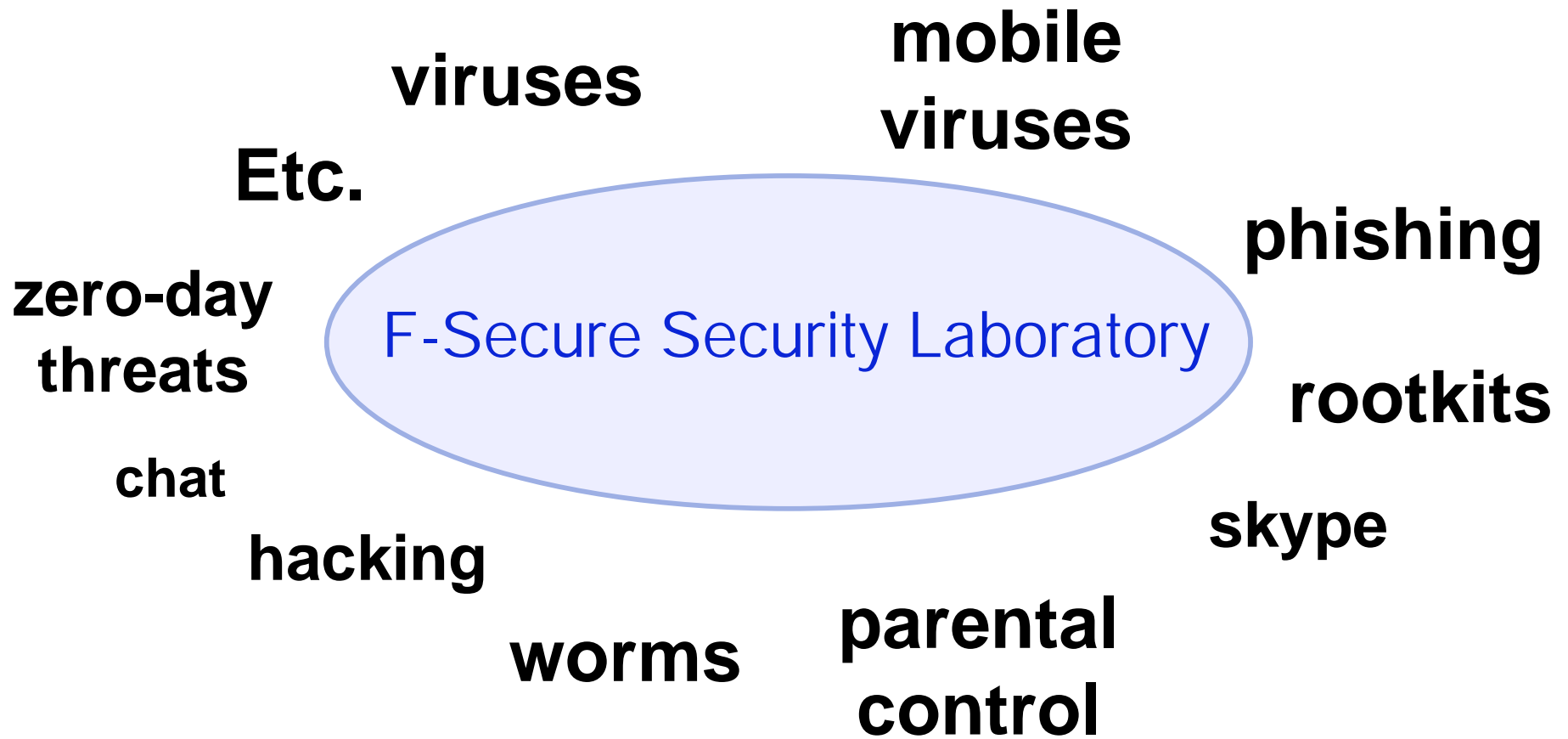


Windows
& TCP/IP

Windows
& TCP/IP



Broader picture of security











WORLDMAP LIVE

(c) F-Secure Corporation

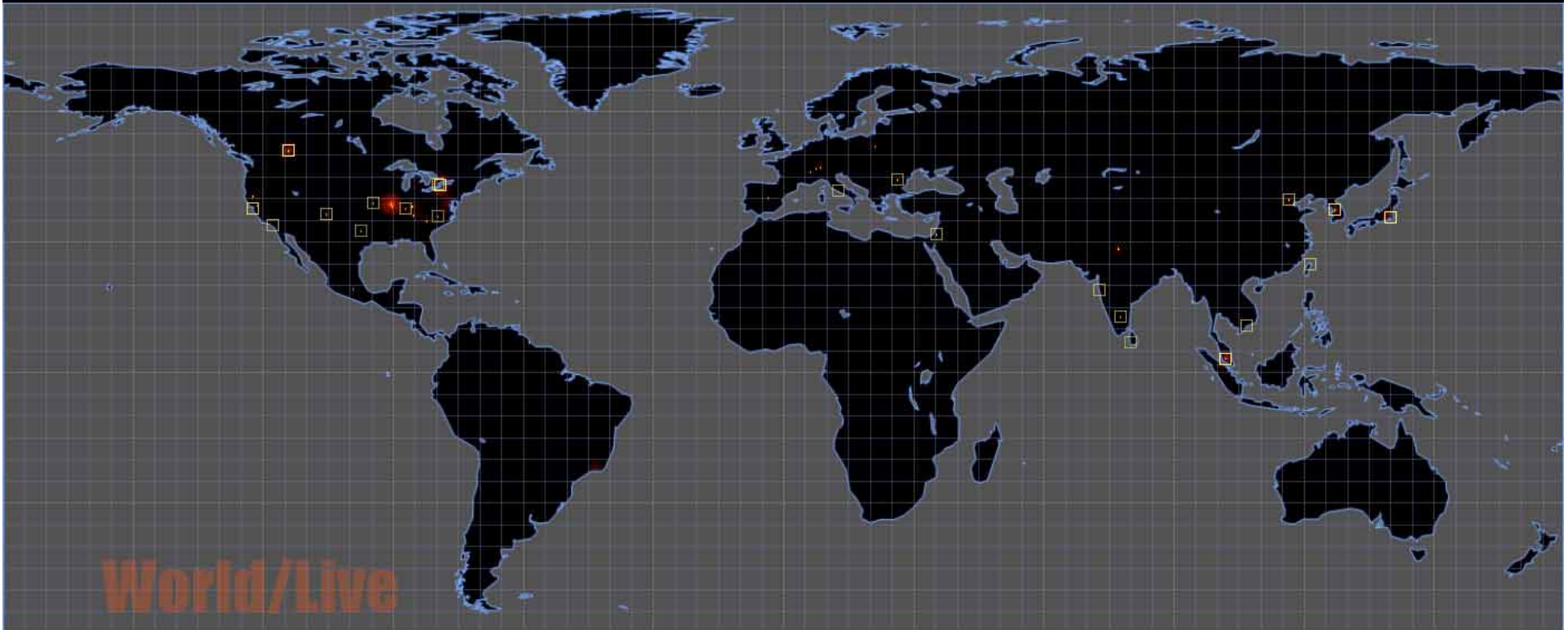
Exit Status >>

INFECTION: ALL COMBINED
RUNNING COUNT: 443
CURRENT RATE: 203 / h
>LIVE FEED >PLAYBACK [1x]

Thursday, 19.01.2006

05:26:11

GMT Standard Time



	[TIME]	[INFECTION]	[LOCATION]
	05:19:43	Trojan-PSW.Win32.Lineage.sr	TAIWAN / TAIPEI
Epidemic	05:20:08	[Not named yet]	INDIA / MUMBAI
High	05:20:09	Net-worm.Win32.MytoB.T	CHINA
	05:20:40	Net-Worm.Win32.MytoB.ab	VIET NAM / HO CHI MINH CIT
Medium	05:23:29	Trojan-downloader.Win32.Istbar.Gen	USA / ANAHEIM, CA
Low	05:24:45	Net-worm.Win32.MytoB.Bi	KOREA
Quiet	05:25:17	Net-Worm.Win32.MytoB.c	MALAYSIA



VIRUS WORLDMAP LIVE
(c) F-Secure Corporation

SCENARIO NAME: Global/Dec 2,2004
VIRUS NAME: ALL COMBINED
SCOPE: GLOBAL

RADAR LEVEL: N/A

Stop >>



>LIVE FEED

>ARCHIVE PLAYBACK 2.0 h/s

Sunday, 05-22-2005
23:09:30 CET

TRACE STARTED: 05-16-2005
TOTAL VIRUS COUNT: 38599
CURRENT RATE: 229 / h


SIM TIME: 6 DAYS 22 HOURS
LATEST ALERT: W32/Mytob.D
LOCATION: CHINA / XI LOJING!!





A photograph of a laboratory door. The door is closed and has a large white warning sign with black text. To the right of the door, there is a red emergency light hanging from the ceiling. The walls are a light blue color. A yellow and black striped caution tape is visible on the wall below the door.

WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING
IN PROGRESS

 RESTRICTED AREA



F-SECURE WORLD MAP

1.1.105

[Previous Hour](#) |
 [Previous Day](#) |
 [This Month](#) |
 [Previous Month](#) |
 [This Year](#) |
 [Previous Year](#)

Alert level: **Quiet**

Time period: 2005-01-01 00:00:00 to 2005-12-31 23:59:59 GMT

Infection(s): All Viruses

Area: [Globe](#) > [Asia](#) > [India](#)

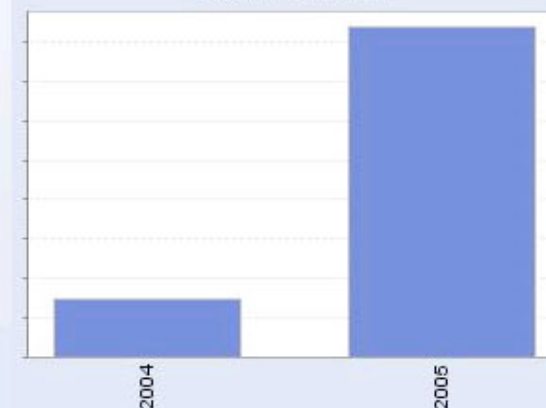


No data
 Quiet
 Low
 Medium
 High
 Epidemic

[Top Viruses](#) |
 [Top Families](#) |
 [Top Variants](#)

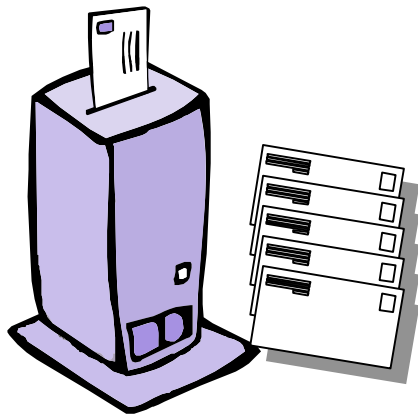
Viruses	Percentage
All Viruses	100.0%
W32/Netsky.Q@mm	↑ 14.5%
W32/MytoB.U	↓ 7.1%
Html/iframe@expl	→ 6.3%
Net-worm.Win32.MytoB.U	→ 6.3%
Email-worm.Win32.Netsky.Q	→ 5.8%
Email-Worm.Win32.DoomBot.b	↑ 5.4%
Net-worm.Win32.MytoB.Y	→ 5.4%
W32/MytoB.Y	↓ 5.3%

All Viruses, India





Direct spam



Viagra Inc.
(Spammer)

?#%\$!?



Ed

?#%\$!?



Bob

?#%\$!?



Lisa

?#%\$!?



Jack

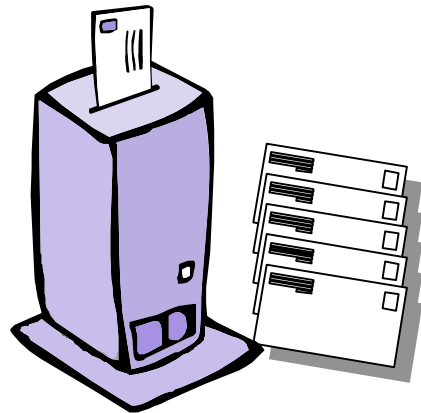
?#%\$!?



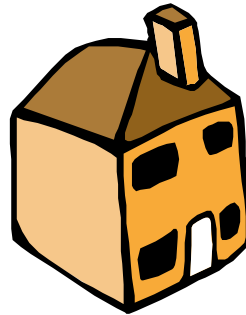
Mary



Spam through Proxy



Viagra Inc.
(Spammer)



Peter
(Zombie / Proxy)

?#%\$!?



Ed

?#%\$!?



Bob

?#%\$!?



Lisa

?#%\$!?



Jack

?#%\$!?



Mary



Sober.Y

1 in 13 e-mails infected

Postini has blocked 218+ million copies

Still 35% of all reports globally

50% of all blocked viruses in HK are Sober.Y



Image Copyright © F-Secure Corporation



Image Copyright © F-Secure Corporation



Spam

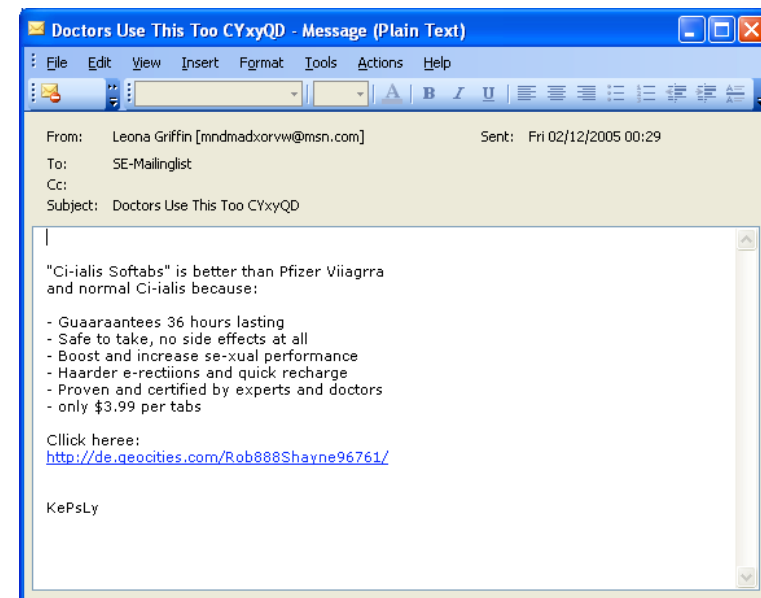
Globally, 68.8% of all messages are spam
(2004: 72.1%)

US: 77.0%

Hong Kong: 61.6%

UK: 59.9%

China: 44.7%



Source: MessageLabs

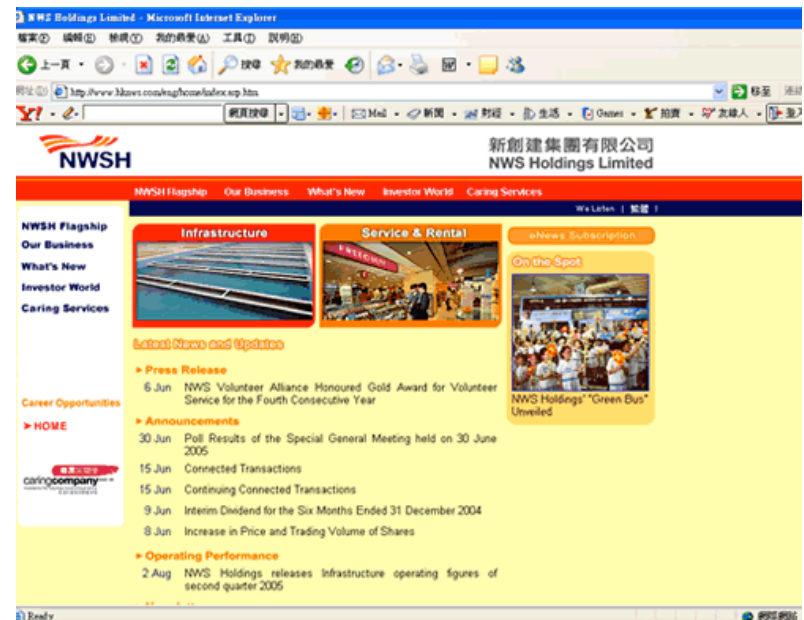
Phishing

Increase globally: 1/120 messages, increase by 95% from 2004

US still hosting most sites; 31.22%

China: 12.13%

Republic of Korea: 10.91%



What are Rootkits?

- A rootkit is a program that hides things
- First Unix rootkit appeared in the early 90s
 - In the beginning rootkits were mainly replacements for system tools: For example, "ls" tool that is used to list directory contents would be replaced with a version that will not print out certain filenames
 - File integrity checking tools such as Tripwire were designed to detect these first generation rootkits.
- Windows rootkits appeared in 2000



SONY  **BMG**

MUSIC ENTERTAINMENT



 **player**
_ □ ×

Van Zant
 Get Right With The Man


? ×

MUSIC **BONUS** ○○○○○○

 → 
  → 



⏪ □ ⏩ ⏮ ⏭ off ⏴ ⏵ 📶

Takin' Up Space	02:45
Nobody Gonna Tell Me What To Do	03:25
Sweet Mama	03:33
Help Somebody	04:13
Things I Miss The Most	03:54
I Know My History	03:03
I Can't Help Myself	04:10
I'm Doin' Alright	03:17
Lovin' You	04:01
Plain Jane	03:27
Been There Done That	04:19

⏪ □ ⏩ ⏮ ⏭ off ⏴ ⏵ 📶

Takin' Up Space 00:00








[NEWS](#) > [Technology](#)

[SAVE](#) | [EMAIL](#) | [PRINT](#) | [SUBSCRIBE TO MONEY](#) | [RSS](#)

Sony BMG recalls copy-protected CDs

Computer viruses had emerged that took advantage of security holes in the copy protection software.

November 16, 2005: 12:08 PM EST

BARCELONA, Spain (Reuters) - Music company Sony BMG, yielding to consumer concern, said Wednesday it was recalling music CDs containing copy-protection software that acts like virus software and hides deep inside a computer.

Sony BMG has used the XCP copy-protection software on 49 titles from artists such as Celine Dion and Sarah McLachlan and produced an estimated 4.7 million music CDs. Around 2.1 million units have been sold on to consumers.

The software, developed by British software makers First4Internet, installs itself on a personal computer used to play the CD in order to guard against copying, but it leaves the back door open for malicious hackers.



 **Technology**
[+ See more stories](#)

advertiser links [what's this?](#)

Succeed with CCTV. Net
DVR and NVR software for

To
Of
W
P
we
B
O
sk

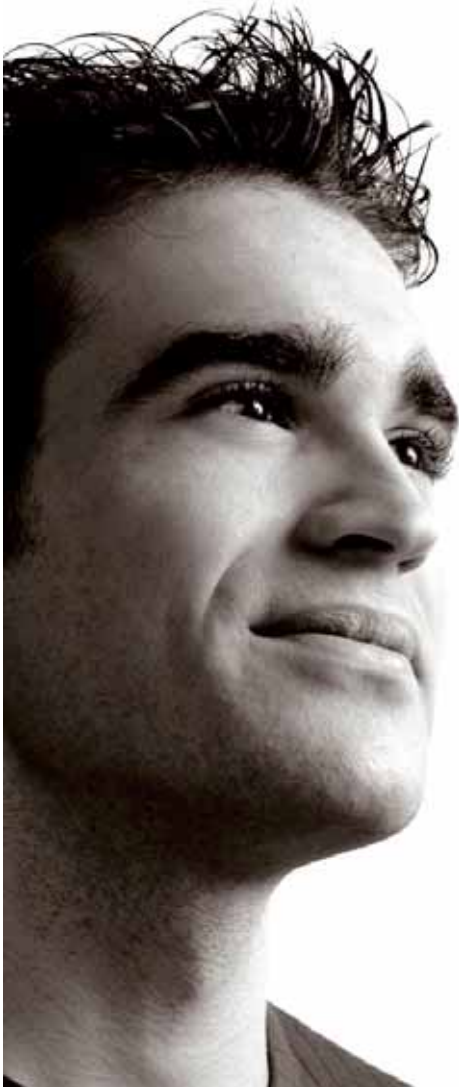


Why it is important for ISP's to offer security solutions as a part of the access services ?



1. Responsible player

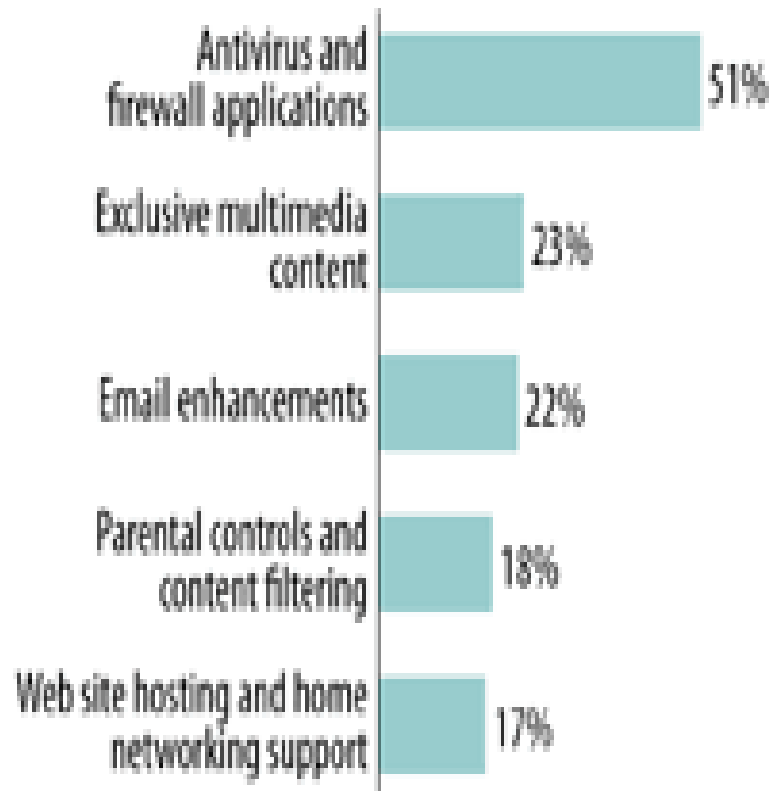
- ISPs are being held responsible to create a **positive Internet experience** among their customers
- The customer **demands** Internet security
 - Willingness to pay more on top of their regular access product to provide additional services
 - Two thirds of US and Canadian households indicate a willingness to pay for security services (Park Associates, 2005)
 - 66% would switch to an ISP who offered a security service



2. Additional source of revenues

Few Consumers Want To Pay For Services

Only security services command a premium



- Customers **are willing** to pay for antivirus and firewall applications (Forrester Research)
- **Willingness to pay more** on top of their regular access product



3. Decrease costs through security

The more users are protected against viruses and spam ...

- The less viruses are received and sent out
- The less spam will go around
- The less unnecessary network load will be created.

The less computers will be infected by viruses, spyware ...

- The less computers will slow down, the less consumer annoyance will be created
- The less incoming support calls.



4. Increases customer retention

The customer will become more loyal to the Service Provider

- Has the access + security = two crucial Internet services = more value
- Has invested more time in ordering these services
- Larger barrier for the customer to change to another provider
- A more positive Internet experience



ISP vs. the retailer

How did you obtain the Anti-Virus on your computer?

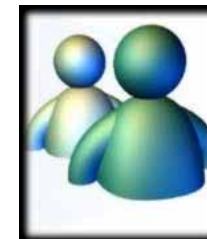
- ✓ Self = 44%
- ✓ Came with computer = 50 %
- ✓ **Included with ISP = 3 %**
- ✓ Other = 3 %



FUTURE DEVELOPMENT



What about 2006???



Summary

Viruses are still the most common problem

With network attacks it's easy to cripple the internet

But crashing a network doesn't crash our society

Anti-virus programs and firewalls provide practical security

But for critical infrastructure, you have to isolate your system from public networks

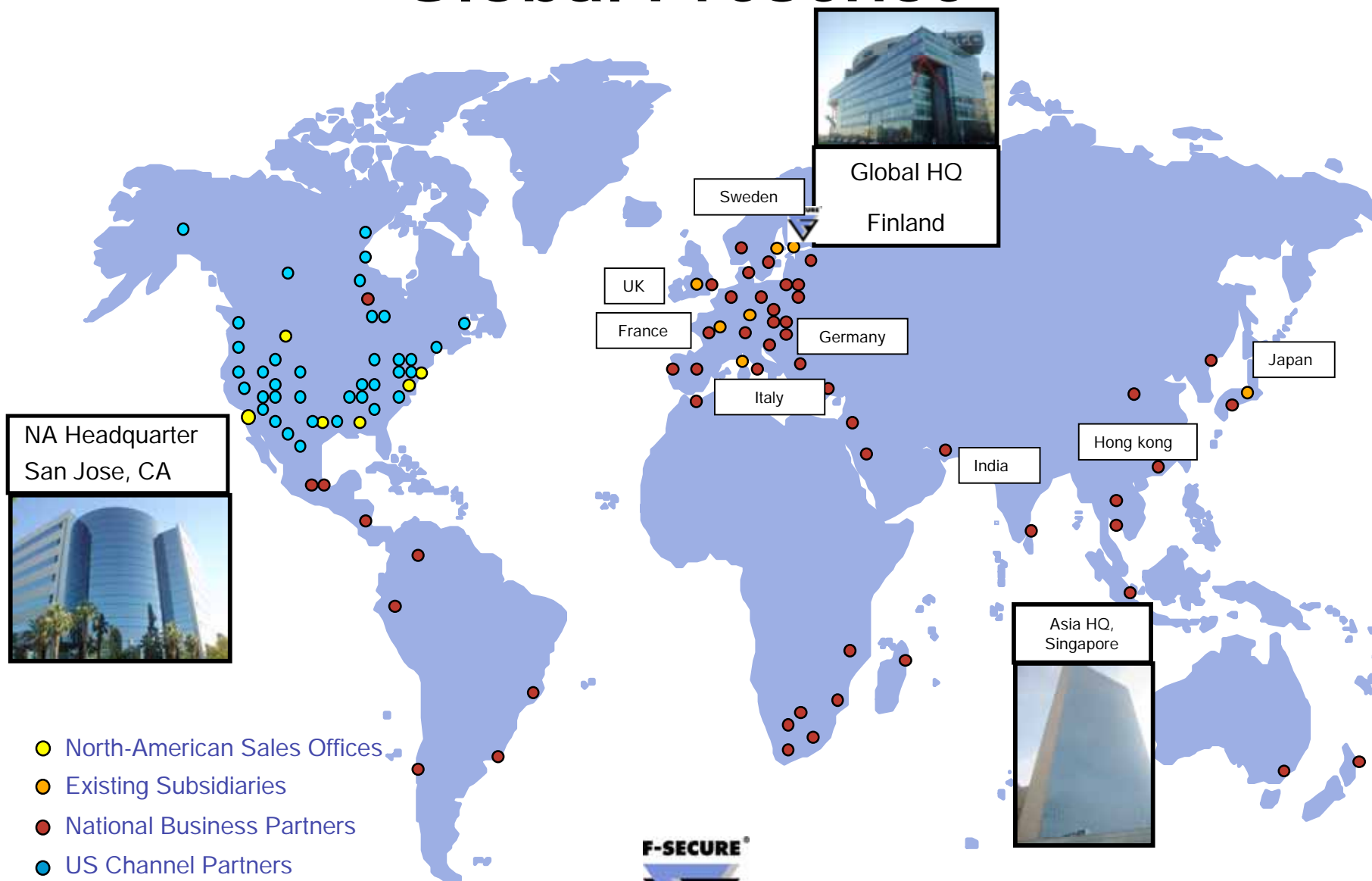


F-Secure Corporation - Overview

- ❑ Security solutions for handheld devices, laptops, desktops, servers and gateways
- ❑ Established in 1988 and Public since 1999 (HEX:FSC)
- ❑ 13 offices worldwide, partners in 70 countries
 - Europe, Home market – leading player in Service provider business
 - US, Canada, South America – Growing business
 - Asia – Growing, establishing new channels, present 10 years
- ❑ Growing anti-virus business with a high service component
- ❑ Strong channel strategy
- ❑ About 400 Employees,
- ❑ Healthy basis for the growth



Global Presence



For further queries:

www.f-secure.com

jari.heinonen@f-secure.com

paul.simon@f-secure.com



**BE
SURE.**

