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.
<table>
<thead>
<tr>
<th>Years</th>
<th>Virus type</th>
<th>Outbreak speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1986-1995</td>
<td>Boot virus</td>
<td>One year</td>
</tr>
<tr>
<td>1995-1999</td>
<td>Macro virus</td>
<td>One month</td>
</tr>
<tr>
<td>1999-</td>
<td>Email worm</td>
<td>One day</td>
</tr>
<tr>
<td>2001-</td>
<td>Network worm</td>
<td>One hour</td>
</tr>
</tbody>
</table>
The volume growth of malware in the wild shows no sign of slowing down.

Data source: F-Secure
### What did they cause?

<table>
<thead>
<tr>
<th>Name</th>
<th>Transportation</th>
<th>Power</th>
<th>Infrastructure</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Slammer</strong></td>
<td>Air traffic control problems in USA</td>
<td>Infected a nuclear power plant in Ohio</td>
<td>911 phone services down in Seattle</td>
<td>Bank of America's ATM network down</td>
</tr>
<tr>
<td><strong>Blaster</strong></td>
<td>Air Canada flights grounded, CSX trains stopped</td>
<td>NY ISO power operator's network infected</td>
<td>Numerous RPC-based SCADA networks down</td>
<td>Several Windows-based ATM networks infected</td>
</tr>
<tr>
<td><strong>Sasser</strong></td>
<td>Railcorp trains stopped in Australia, Delta flight problems, delays with British Airways flights</td>
<td>Hong Kong government's department of energy networks infected</td>
<td>Infected: Two hospitals in Sweden, EU commission, Heathrow airport, Coastguard UK</td>
<td>Several banks shutting down offices because of internal infections</td>
</tr>
</tbody>
</table>
Top 9 financial damage of malicious code attacks 2001-2004
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

viruses

mobile viruses

phishing

rootkits

skype

parental control

F-Secure Security Laboratory

due to

J.S. 13
WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING IN PROGRESS
Direct spam

Viagra Inc. (Spammer)

Ed
Bob
Lisa
Jack
Mary
Spam through Proxy

Viagra Inc. (Spammer)

Peter (Zombie / Proxy)

Bob

Ed

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
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 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 KCP 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.
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

- 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%

Source: AOL/NCSA Online Safety Study, October 2004
FUTURE DEVELOPMENT
What about 2006???
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
For further queries:

www.f-secure.com

jari.heinonen@f-secure.com

paul.simon@f-secure.com
BE
SURE.