

Combined Protection: F-Secure Anti-Virus and Distributed Firewall

F-SECURE®



Topi Hautanen

Product Marketing Manager, F-Secure Corporation

Fabrizio Cassoni

Content Security Manager, Symbolic S.p.a.

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. The text is positioned above a stylized, purple and black shield-like graphic that resembles a shield with a large, white, stylized letter 'F' inside.

Agenda

- Threats of the modern world:
 - hackers
 - viruses, worms
- Virus & worm case studies
- Future threats
- Protection against future threats
- Security solutions as business enabler

The logo features the text "F-SECURE" in a bold, black, sans-serif font, with a registered trademark symbol (®) to its upper right. Below the text is a stylized, three-dimensional shield-like shape composed of overlapping purple and black geometric forms, resembling a shield with a large 'F' cutout.

F-SECURE®

F-Secure Corporation

F-Secure enables enterprises and people to work securely and be more productive while they extend their business practices.

We provide high-quality, easy to use software based security solutions to protect against complex information security attacks.





F-SECURE[®]

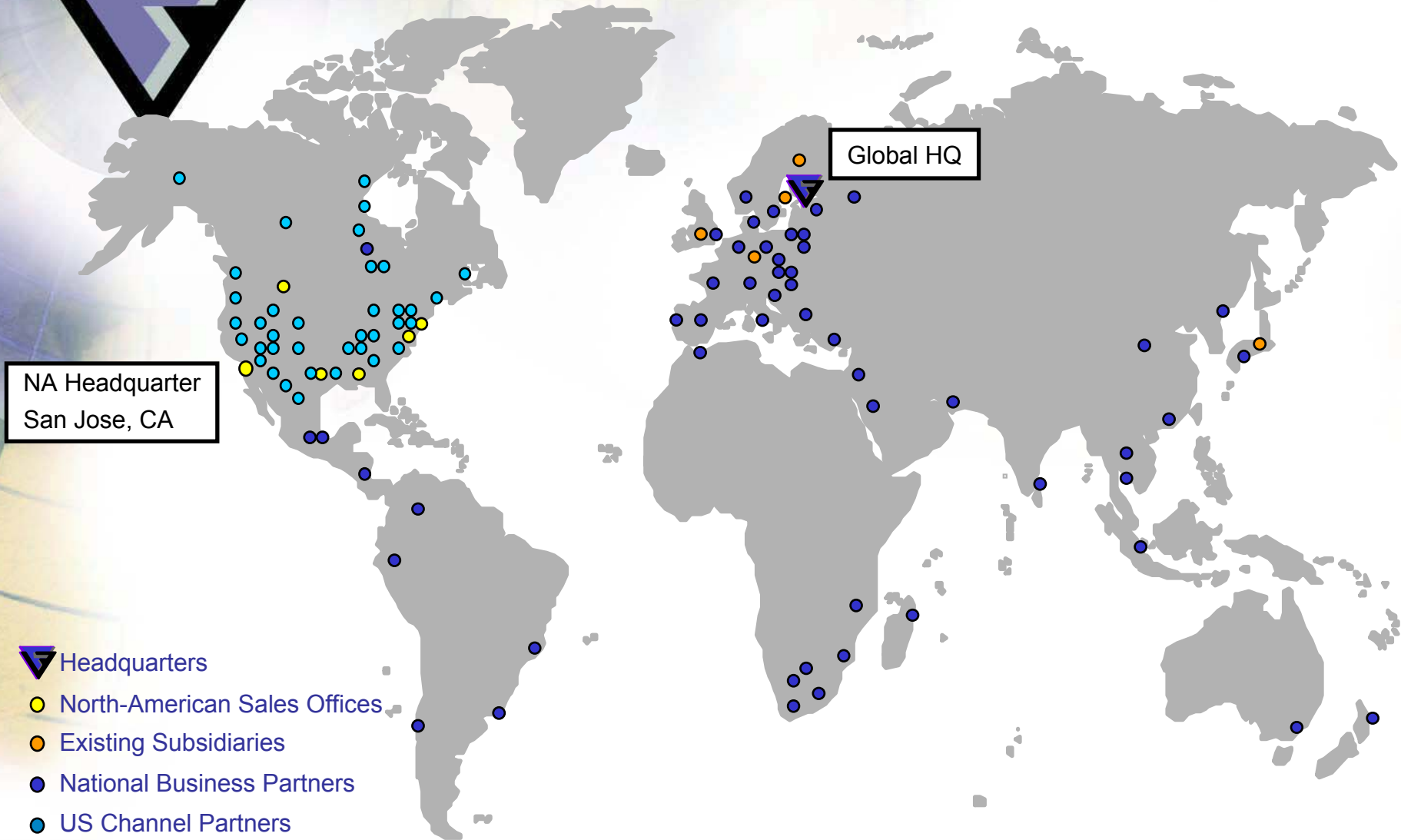
F-Secure Corporation

- **Security solutions for handheld devices, laptops, desktops, servers and gateways**
 - Stopping hostile code and hackers
 - Ensuring confidentiality through encryption
- **14 offices worldwide, partners in 100 countries**
 - Net sales of € 38.5m in 2002, >300 employees
- **Growing anti-virus business**
 - Seven consecutive quarters of over 20% growth per quarter in subscription services through service providers
 - Europe's two largest ISPs (DT and FT) offer F-Secure solutions
- **Established in 1988 and Public since 1999 (HEX:FSC)**
- **Strong channels and partnerships, e.g.**
 - Compaq/HP, Deutsche Telekom, EDS, Fujitsu Siemens, NEC BNS, Nokia, Siemens ICN, Symbian...

F-SECURE®



Global Presence

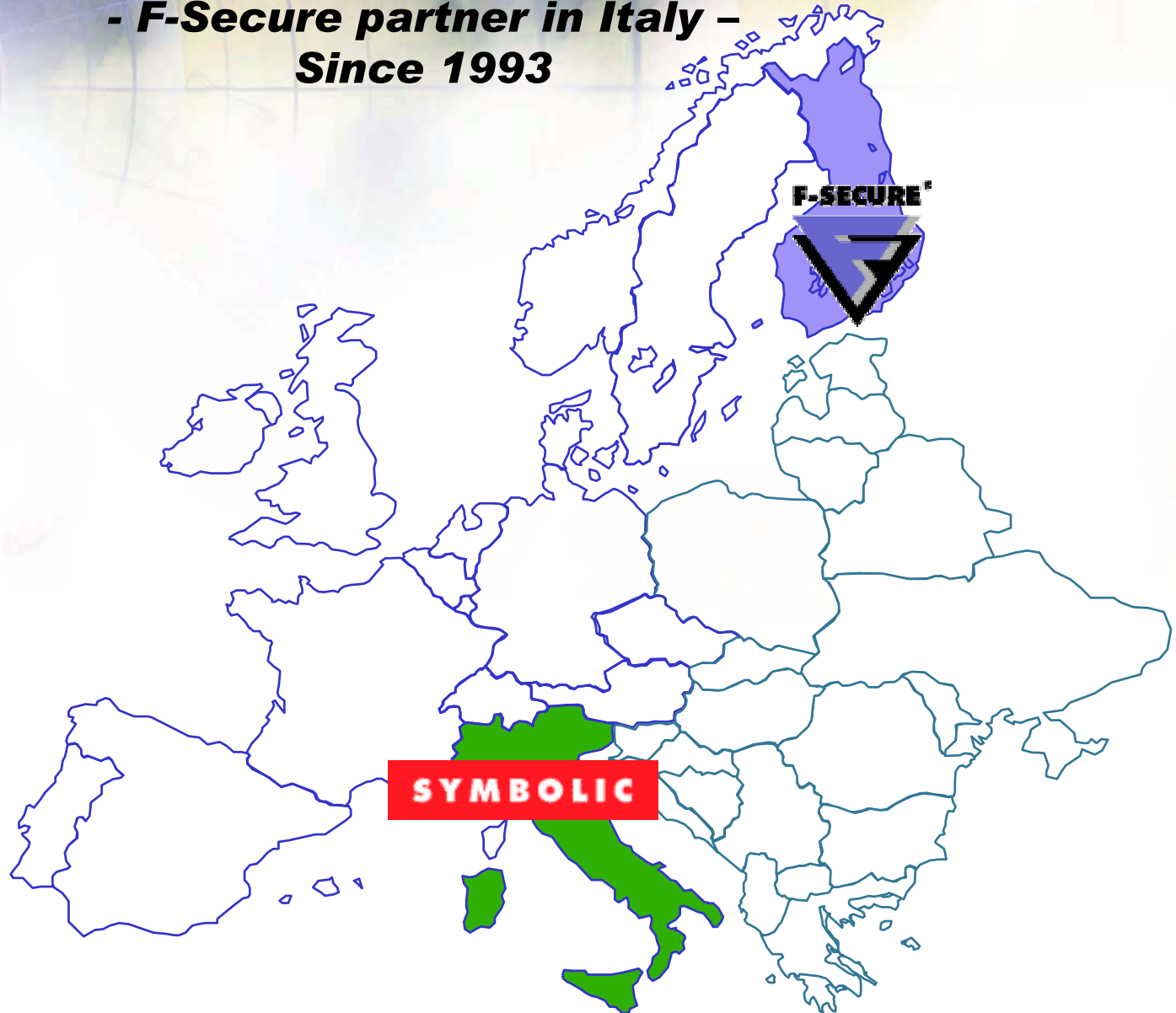


F-SECURE®



Symbolic S.p.A.

**- F-Secure partner in Italy -
Since 1993**





Symbolic

- Presente sul mercato da circa 10 anni
- Specializzata in Network Security
- Partner e distributore italiano di F-Secure Corp.

“La nostra mission è di rendere disponibili soluzioni avanzate per la sicurezza dei computer e delle comunicazioni. La strategia adottata si basa sull'analisi della sicurezza di un sistema informativo, l'offerta di soluzioni pratiche e affidabili, l'informazione e la ricerca.”

Martino Traversa, Founder e CEO

F-SECURE®



Ambiti Operativi

SYMBOLIC

- Anti-Virus
- IT Risk Mgmt
- PKI
- Content Security
- HSM
- Firewall

{ INTRINSIC

- Security Services
- Area Didattica: Informare

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the upper right. Below the text is a stylized, three-dimensional shield or triangle shape composed of overlapping purple and black geometric forms.

F-SECURE[®]

World Today

- 'Always on' broadband access is gaining popularity
 - Easy unprotected targets for networked hacking
- Work is being done outside corporate premises:
 - Confidential data is created and stored outside the corporate gateway firewall
 - Laptops are connected to home and hotel networks

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the right. Below the text is a stylized, purple and black shield-like graphic with a white 'F' shape inside.

World Today

"Honeypot project"

- Average hacking density per connected host:
 - >200 port scans a month
 - 17 netbios scans a day
 - the number is increasing rapidly
- Standard Win98 machine was hacked 5 times within 4 days when connected to Internet
- Standard RedHat Linux machine was hacked in 72 hours when connected to Internet
- Fastest manual hacking in 15 minutes, 92 seconds with worm

F-SECURE®



Many faces of the computer criminal

- Hobbyists - Script Kiddies
- Activists / Terrorists
- Thieves - 'Soldiers of fortune'
- Industrial espionage / Spying



F-SECURE®



Hacking/cracking for fun

- The net is full of kids scanning thousands of machines, looking for vulnerable ones
- Usually, the motive is not to spy on your data, but to use your computers resources
- Typical misuses: chat servers, file servers for MP3s, pirate software or porno...



```
:Co0lWoRx :ok?  
:Ricky :ii have 2 cards i will trade  
:[Agent] :yo  
:[Agent] :is a master card a 16 digit or 13 ?  
:NPN :16  
:darius :?  
:NPN :1234/5678/9102/3456
```

F-SECURE®



Easy access to hacking tools

SuperScan 3.00 Hostname Lookup Configuration

IP: 127.0.0.1
Resolved: FSIBM310.FI.F-Secure.com

Scan type: Only scan responsive pings, Show host responses

Scan: Pinging 127.0.0.1 0, Scanning 127.0.0.1 0, Resolving 127.0.0.1 0

WlDcaak Password Recovery Software For MS Word (C) Copyright by John E. Kurlich 1997 Ver. 1.0

File Password

Select A File

Recover File Password

Password Length

Document Protections

Text Decode Window... Click on bad characters and correct them, then recover password

Mem o M a n a g e r S m i
t h T o s e c r e a t a r y
V i r t a n e X M e x t m
o n t h , l e t s f i r e
B o b . A n d l e t s g i
v e L i s a a r a i s e .
. . .
F - S e c u r e
O y j S u o m a l a i n
e n F - S e c u r e o y

LC3 - [demo.lcs]

User Name	LM Password	<8	NTLM Password	NTLM Hash	Challenge	Audit Time
BillG	??????A			C04E842B9F5B114C86921C4163AE85B1		
Administrator	??????S			C7E2622D76D3F001CF08B07536468BCC		
fredc	CRACKPOT		crackpot	80030E356D15FB194272DCFD7DD3234		0d 0h 0m 15s
twoa	AA	x	aa	C566344F963BE79C8FD99F535E7AAD8		0d 0h 0m 12s
william	IMPUNITY		impunity	686E0FB2ED246885B98586C73B5BF77		0d 0h 0m 13s
threea	AAA	x	aaa	E24106342BF38BCF57A6A4B29016EFF6		0d 0h 0m 12s
foura	AAAA	x	aaaa	FA5664875FFAD0A6F1ABF9B097FA46F		0d 0h 0m 12s

Dictionary Status: words_total 137893, words_done 235007, % done 58.676+

Brute Force: time_elapsed 0d 0h 0m 0s, time_left, % done, current test, keyrate

SMS Messenger

Message Text (160 characters maximum) 127

8AA9F9D9E9F9A5A8D76F9E68AA9F9D9E9F9A5A8D76F9E68AA9
F9D9E9F9A5A8D76F9E68AA9F9D9E9F9A5A8D76F9E68AA9
6F9E68AA9F9D9E9F9A5A8D76F9E

Destination(s) +358400648180

Submit Type Standard Extended

Received Messages

Status	Coding	Class	Origin / Destination	Date	Time
--------	--------	-------	----------------------	------	------

Received Message Text

Standard Retrieve Extended Retrieve



send fake mail.com

[Compose](#) | [Join](#) | [Login](#) | [Resources](#) | [Open Relay List](#) | [Chat](#) | [Contact Us](#)

Compose

From



To



CC BCC

Subject

Message Body

Hello people, it's that time of the year again: we need to change all network passwords.

Please e-mail your old passwords to passwordchange@hotmail.com and we'll mail your new password to you right away.

Thanks,
Security Team

Features:

- Industrial Strength Anonymous Emailing
- Fake Emails
- Attachments
- CC & BCC recipients
- Plain Text & HTML
- Fast Emailing

F-SECURE®



Hacking for profit / idealism

- Terrorists
- Activists
- Information warfare
- The professionals (spies/espionage) rarely get caught





search: **This site contains nothing worthily to search for ;p**

[WinMX](#)
[KaZaA Lite](#)
[eDonkey](#)
[iSONEWS](#)
[Emule](#)
[Shareaza](#)

news

- RIAA - Own3d by.... ;p
- oohh riaa want's to hack Filesharing Users / Servers ? - better lern to secure your own server...
- Sorry Admin - had to deactivate ur accounts - they'll be reactivated after 2 hours
- greetz : Rage_X, BRAiNBUG, SyzL0rd, BSJ, PsychoD + all the others who want to stay anonymous :]
- wanna contact ? h4x0r0815@mail.ru

Recommended File Sharing Tool - selected by Riaa.org

#	Program Name	OS	Rating
	<p><u>Emule</u> eMule is a open source filesharing client which is based on the eDonkey2000 network but offers more features than the standard client.</p>		1 2 3 4 5 Overall XXXXX Content XXXXX Users XXXXX Speed XXXXX
1	<p>Features - Download resume</p>	Win32	

Aldrich H. Ames



Life without parole

David S. Boone



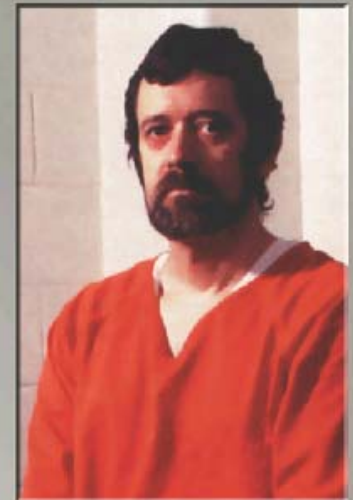
24 Years

Jonathan J. Pollard



Life

Earl E. Pitts



27 Years

Roderick J. Ramsay



36 Years

Christopher J. Boyce



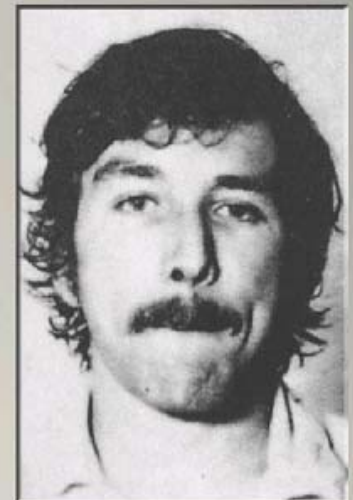
68 Years

Harold J. Nicholson



23 Years and 7 Months

Andrew D. Lee



Life

F-SECURE®



Kevin Mitnick damages 1993-1994

- Sun, USA; Solaris source code: **\$80M**
- NEC, Japan; Mobile phone sources: **\$1.75M**
- Nokia, Finland; HD760 project: **420kEUR**
- Nokia, UK; "Mobile software": **\$135M**
- Novell, USA; Netware sources: **\$75M**
- Fujitsu, USA; PCX phone sources: **\$2.1M**
- **Sentenced on August 9th, 1999**
- **Total damage: \$296,000,000**
- **Mitnick ordered to pay: \$4,125**
- **And to serve 46 months in prison**
- **Just released from prison**

Source: <http://www.hackernews.com/orig/letters.html>



NBC News

The logo for F-SECURE, featuring the text 'F-SECURE' in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized graphic consisting of a purple triangle pointing downwards, with a white 'F' shape inside it, all enclosed within a black outline.

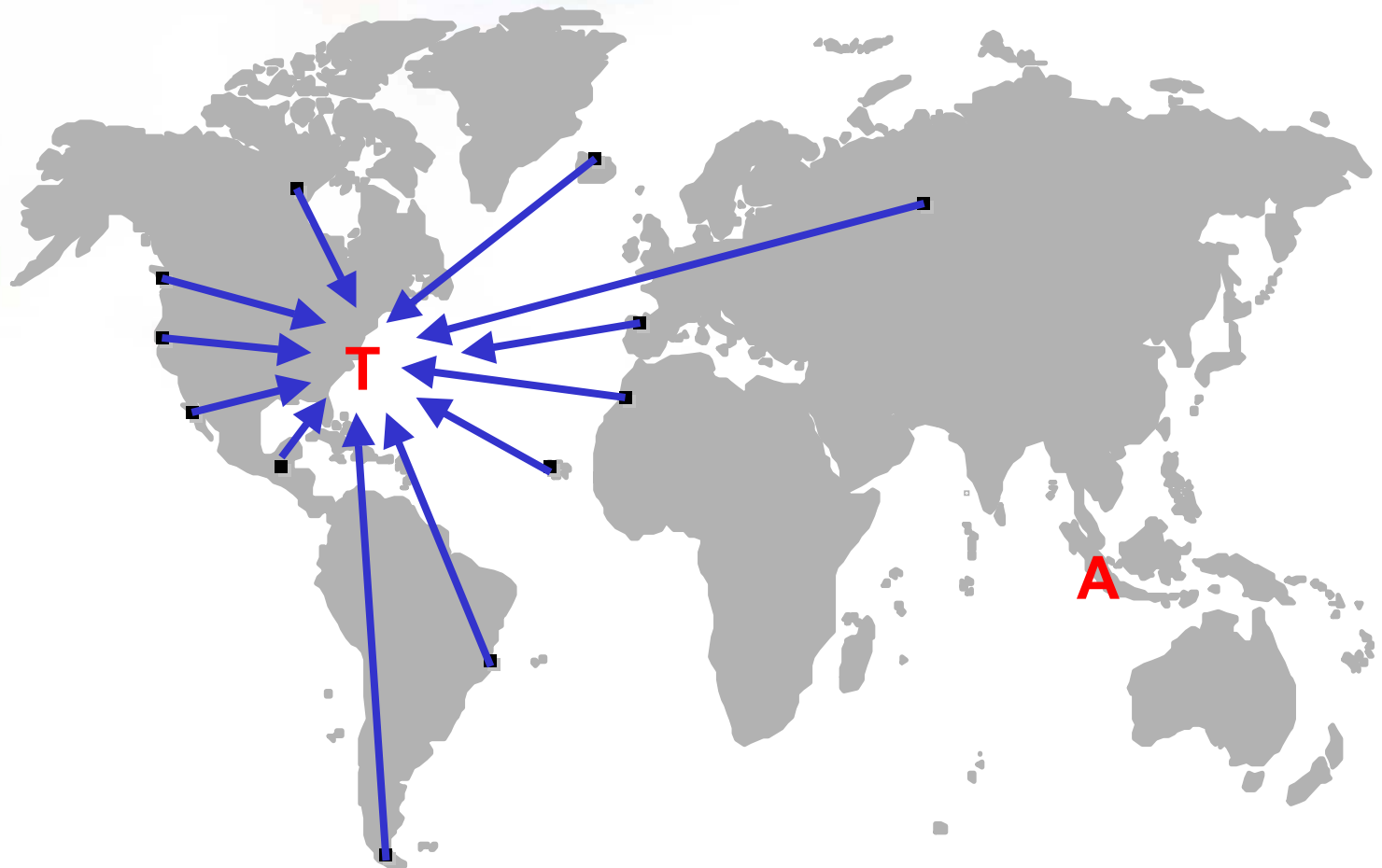
Denial of Service (DoS) attacks

- 'Denial of Service' (DoS): Intentional network attack or exploit that prevents users to use the targetted network service
- As a result of DoS the service is partly or totally stopped
- Example: www.whitehouse.gov becomes unavailable

F-SECURE[®]



Distributed Denial of Service (DDoS)



F-SECURE®



Case Code Red

- First web worm
- First DDoS worm
- Jumps from www site to another
- Three phases
 - Spreading
 - Attack
 - Sleeping
- Infected 340,000 machines in July 2001

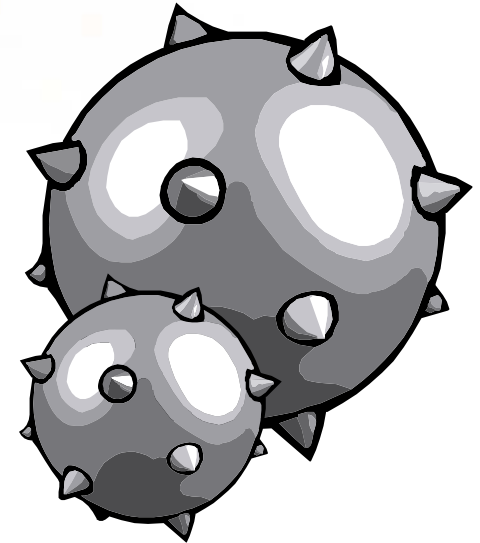


F-SECURE®



Virus – Definition

Virus is a piece of software that has been programmed to spread further by infecting other programs.

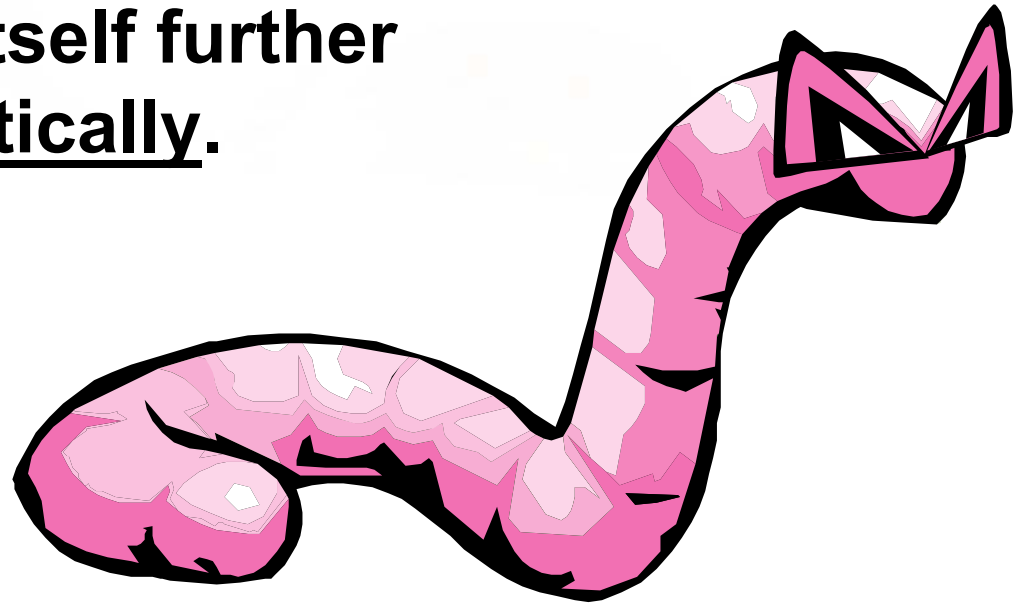


F-SECURE®



Worm – Definition

Worm is a standalone virus – it does not infect existing programs, just sends itself further automatically.



F-SECURE®



Worm types

Email

- Melissa
- Klez
- Bugbear

Network

- Morris worm
- Code Red
- Slapper

...
...smtp..
...http...
...



The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the upper right. Below the text is a stylized, geometric logo consisting of a large, dark purple triangle pointing downwards, with a smaller, lighter purple triangle nested inside it, and a black outline.

Worm – What it does?

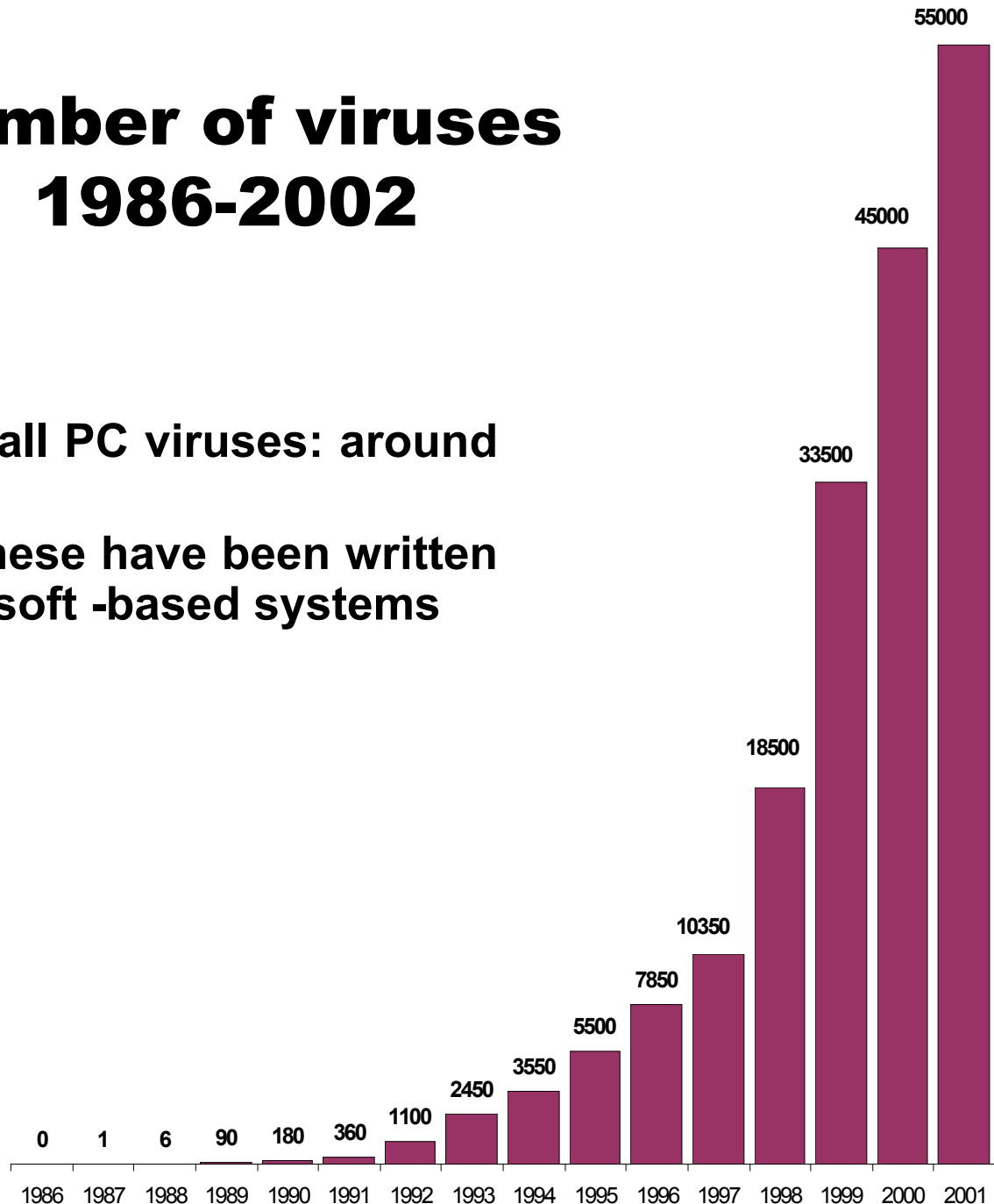
- Email worms rely on users to spread further
 - Send emails with infected attachments around
- Network worms do not need human intervention
 - Exploit vulnerabilities in networked systems

F-SECURE®



Number of viruses 1986-2002

- Total count of all PC viruses: around 60 000
- Almost all of these have been written to target Microsoft -based systems
 - DOS
 - Windows
 - IIS
 - Exchange
 - Internet Explorer
 - Outlook
 - Office
 - Word
 - Excel
 - Powerpoint



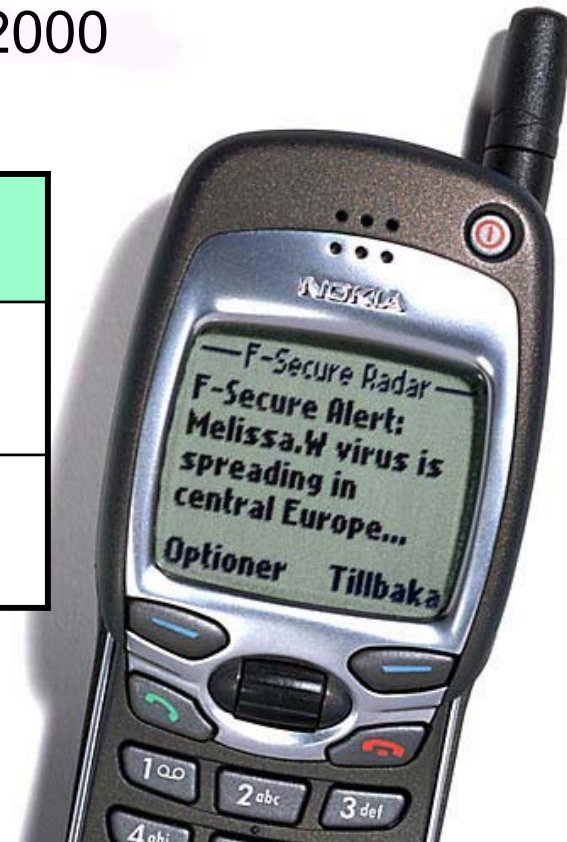
F-SECURE®



Was 2002 been a quiet virus year?

- 2001 was the worst year ever
- 2002 has been roughly as bad as 2000

	Year 2001	Year 2002	Year 2003
F-Secure Radar Level 1 Alerts	9	2	0
F-Secure Radar Level 2 Alerts	31	27	5



F-SECURE®





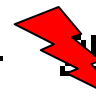
**Year
2003**

- Lirva.A
- ExploreZip.E
- Lirva.B
- Sobig
- Slammer/Sapphire

Date

tammikuu

2003

M	T	K	T	P	L	S
		1	2	3	4	5
6	7			10	11	12
13	14	15	16	17	18	19
20	21	22	23	24		26
27	28	29	30	31		

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a purple triangle pointing downwards, with a black outline and a white 'F' shape inside it.

What is a combined threat?

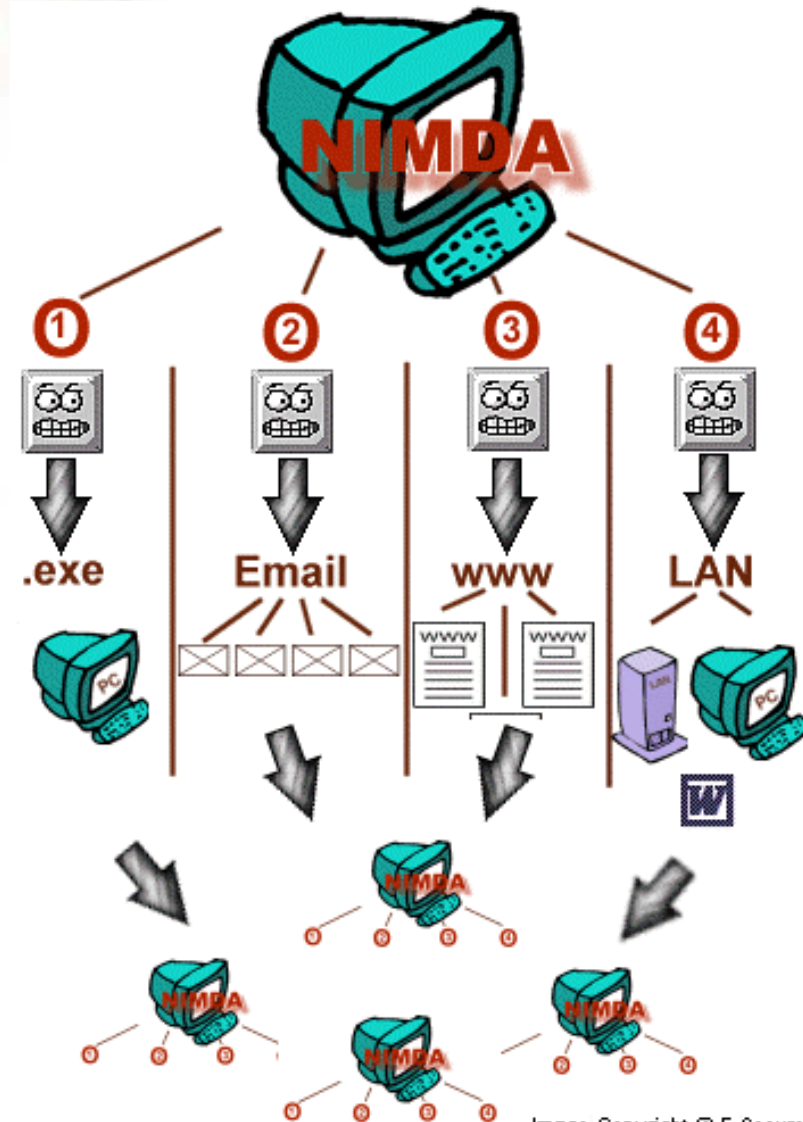
- **Virus** or worm that spreads using known vulnerabilities, "*virus using hacker mechanisms to spread*"
 - **Spreads rapidly** using multiple propagation methods (email, HTTP, direct connection...)
 - **Spreads automatically** using known vulnerabilities
 - Attacks from **multiple points**: infects .exe's, creates network shares, HTML pages

F-SECURE®



Case Nimda

- Four different viruses in one
- Infected 2.2 million machines in a day
- Network traffic jams
- Shares your drives
- Who made it?
- This was version 0.5...



F-SECURE®



Case Sircam

- Most widespread data stealing virus
- Locates recently used documents
- ...and sends them away

Date: Wed, 05 Sep 2001 11:28:30 +0300
To: Mikko.Hypponen@F-Secure.com
From: John Doe <John@Doe.com>
Subject: New salaries for the development team.doc

Hi! How are you?

I send you this file in order to have your advice

See you later. Thanks



[New salaries for the development team.doc](#)

The F-Secure logo consists of the text "F-SECURE" in a bold, black, sans-serif font, with a registered trademark symbol (®) to its upper right. Below the text is a stylized, three-dimensional shield-like shape. The top part of the shield is purple, and the bottom part is black, with a white outline. The shield is set against a circular background that resembles a globe with latitude and longitude lines.

Case: Slapper

- Detected on Saturday 14th of September 2002
- Linux / Apache / OpenSSL worm
- Much like Code Red – and Scalper
- Spreads in C source code format
- Creates a peer-to-peer attack network of infected machines
- The attack network can be controlled by virus writer to launch DDoS attacks

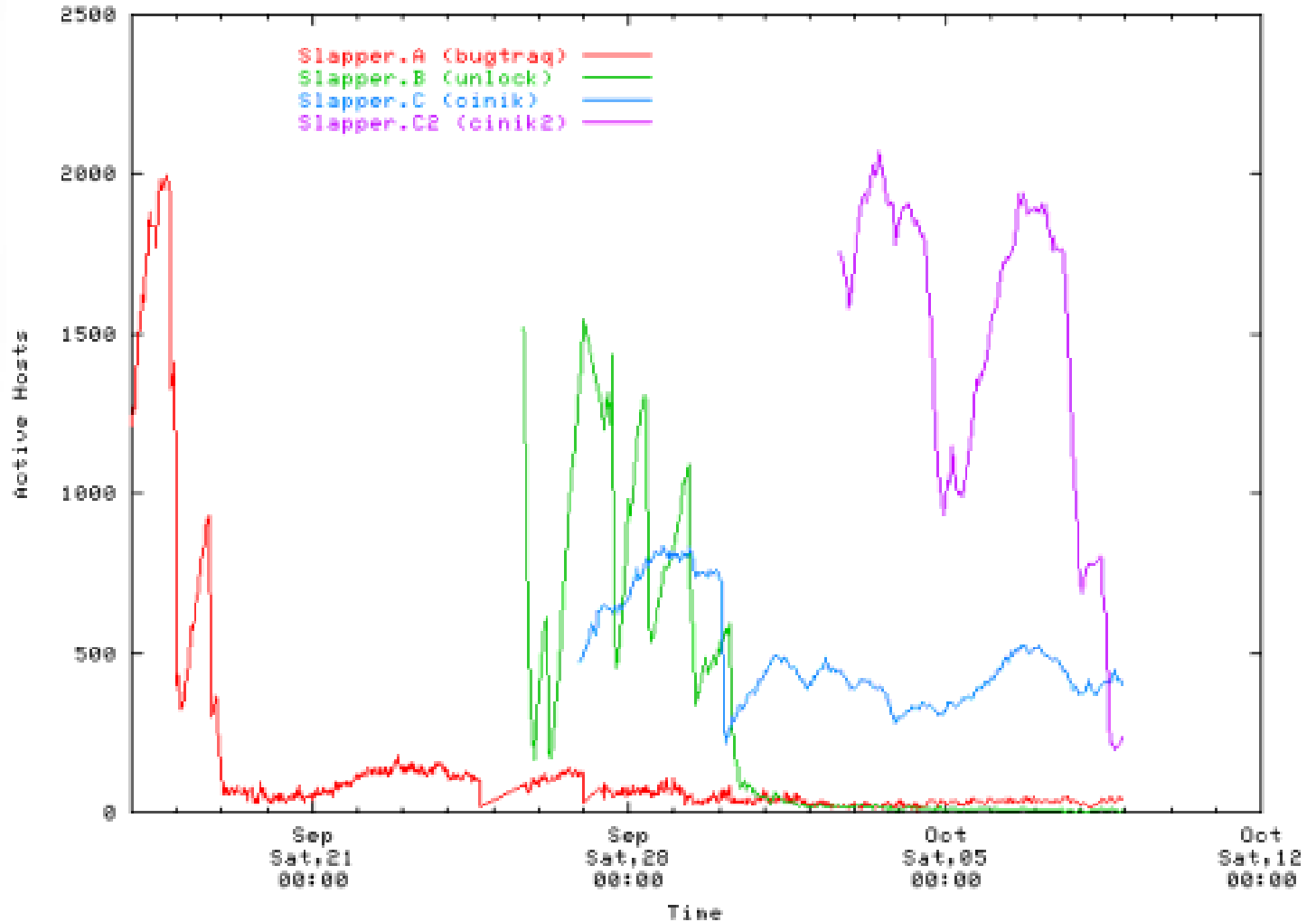


F-SECURE®



Slapper active hosts

Slapper spreading numbers.

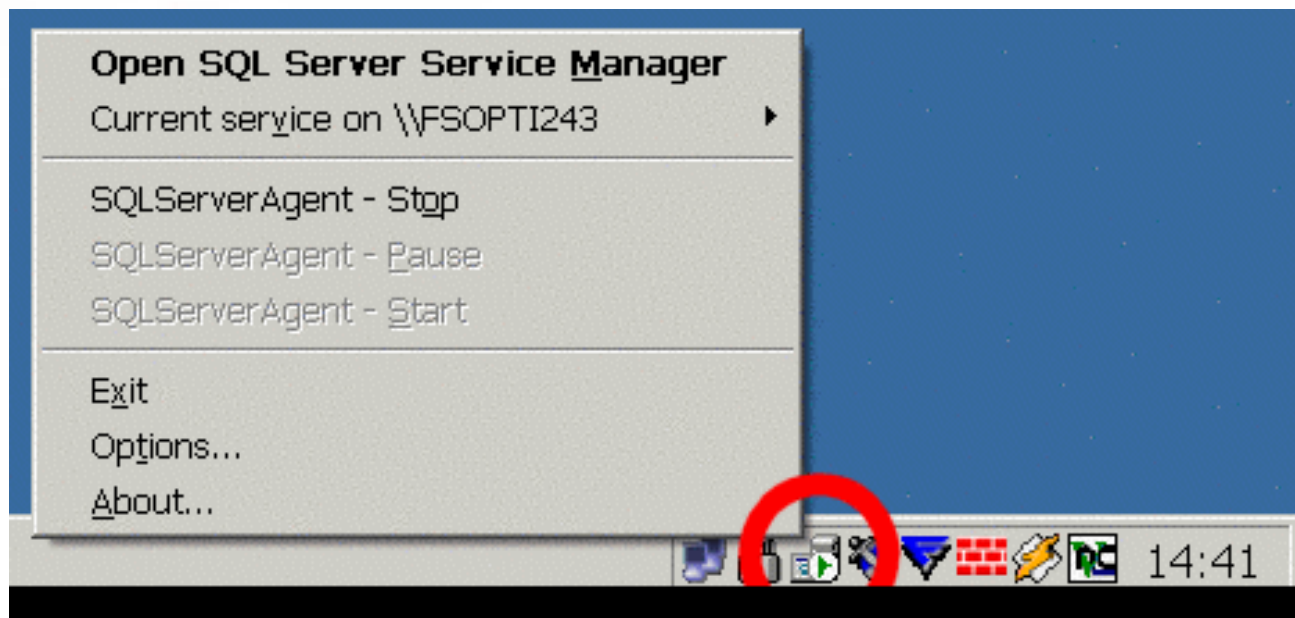


F-SECURE®



Case Slammer

- Also known as Sapphire
- Started on saturday 25.1.2003 at 07:31
- Exploited a known buffer overflow in Microsoft SQL Server / MSDE 2000



The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized graphic consisting of a large, black-outlined letter 'F' that is partially filled with a purple-to-blue gradient. The background of the entire slide is a faint, light-colored globe with a grid of latitude and longitude lines.

Who runs SQL Server?

- Not that many
- But many Microsoft apps includes MSDE 2000

.NET Framework SDK

ASP.NET Web Matrix

BizTalk® Server 2002 Partner Edition

Host Integration Server 2000

Office XP Premium, Professional, Developer

Project Server 2002

Retail Management System headquarters 1.0

Small Business Server 2000

SQL Server 2000, Enterprise Edition, Developer Edition, Personal Edition (RTM, SP1, SP2)

Visio Enterprise Network Tools

Visual FoxPro® 7.0 and 8.0 beta

Visual Studio .NET 2002 Professional, Enterprise Developer, and Enterprise Architect editions

Visual Basic .NET Standard 2002 ,

Visual C++ .NET Standard 2002 ,

Visual C# .NET Standard 2002

Windows Enterprise Server 2003 RC1, only if UDDI is enabled

Windows Server 2003 RC1, only if UDDI is enabled

Application Center 2000 RTM, SP1, SP2 Encarta Class Server 1.0

Host Integration Server 2000

Microsoft Business Solutions Customer Relationship Manager

Microsoft Class Server 2.0

Operations Manager 2000 RTM, SP1

Retail Management System Store Operations 1.0

SharePoint™ Team Services 2.0 beta 1

Small Business Manager 6.0 , 6.2, and 7.0

Windows XP Embedded Tools

Windows Enterprise Server 2003 RC2

Windows Server 2003 RC2

...

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol. Below the text is a stylized graphic consisting of a large, dark blue triangle pointing downwards, with a smaller, lighter blue triangle nested inside it, creating a sense of depth and a shield-like appearance.

F-SECURE[®]

3rd party apps running MSDE (more than 150)

Acuity 2.0

Adage ERP

Adonis

Aelita Enterprise Directory
Manager

Affymetrix Microarray

AllFusion Component Modeler 4.1

Altiris Deployment Server

Altris/Spescom Deployment Server

AMS

ARCserveIT (MSSQL is optional)

AscentCapture 5.51

ASP.NET Web Matrix Tool

ASSET v1.01 - NIST

assetOutlook

Backup Exec 9.0

BioLink ver 1.5

Biomek FX

BizTracker

BlackBerry Enterprise Server

Blackboard Transaction System

bv-control and bv-admin products

Byggsafe

Centennial Discovery

Centreware web

Chaperon 2000

Cisco Building Broadband ServiceExpress Metrix

Cisco CallManager 3.3(x)

Cisco E-Mail Manager (CeM)

Cisco Intelligent Contact

Cisco Unity 3.x, 4.x

Citrix Nfuse Elite

CommVault Galaxy

Compaq Insight Manager

Compaq Insight Manager v7

Connected TLM

ControlCenter ST

Crystal Reports Enterprise 8.5

Davilex Account

Dell OpenManage IT Assistant

Directory Sizer (franzo.com)

EdWeb

Elron IM Web Inspector Internet

Enterprise Security Reporter 2

ePolicy Orchestrator

Exact Compact 2000

Exact Globe 2000

Exchange Migrator

Exchange Migrator

Exec View 3.0

ExecView v3.x for Backup Exec

Fazzam 2000

Firehouse Software

FlipFactory

Genifax

GFI S.E.L.M

GiftWrap

JD Edwards OneWorld

Journyx Timesheet

Kaseya VSA

KeepTalking

LanDesk

LANDesk Management Suite

Lexware Warenwirtschaft

Lyris Listmanager

Mail Max 5

MailSweeper

Map Info Discovery

Marshal Software MailMarshal

Marshal Software WebMarshal

Marvin

MAS 500

McAfee ePolicy Orchestrator

Trend Micro Control Manager 2.5

Trend Micro Damage Cleanup Server

...

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a purple triangle pointing downwards, with a black outline and a white 'F' shape inside it.

What did Slammer do?

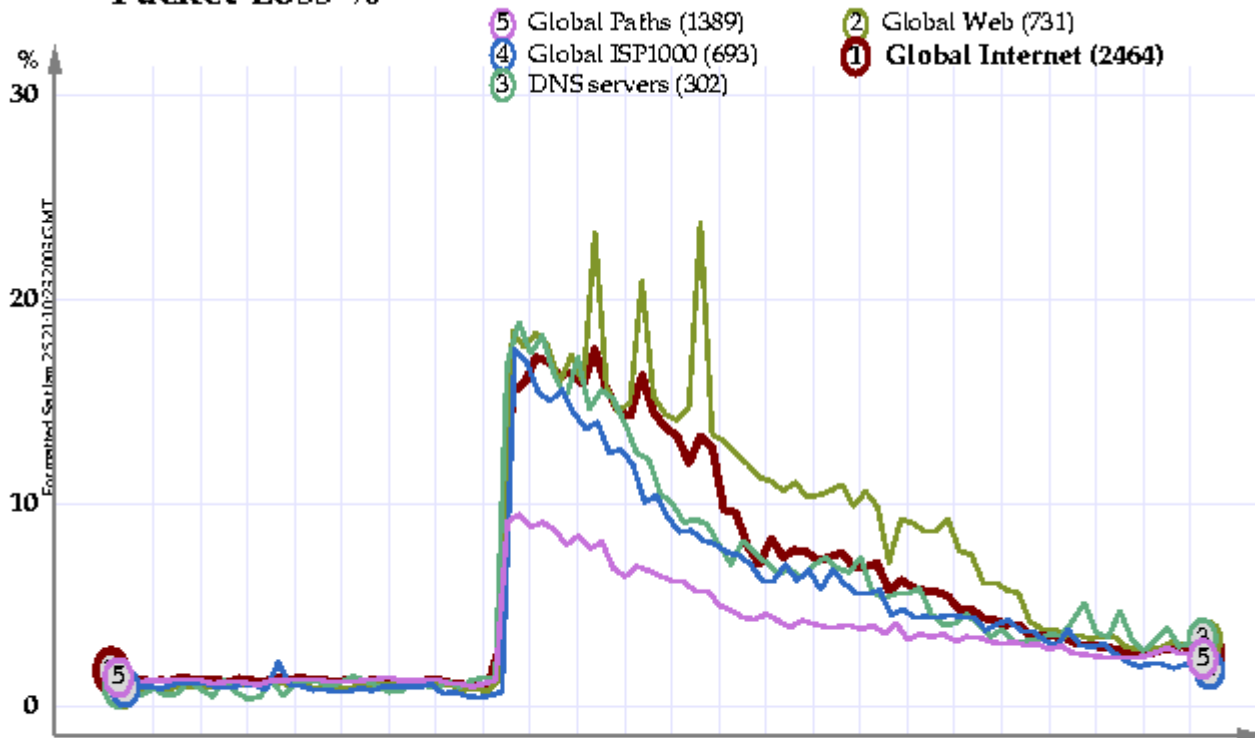
- Infected around 100,000 computers
- Peaked in 10 minutes
- Doubled in size every 8.5 seconds
- Created massive amounts of network traffic
 - A Finnish county reported that their main switch saw 80Mb/s traffic to the Internet from their library's SQL server
- One machine could do more than 30,000 infection attempts per second

F-SECURE®



Saturday 24.1.2003, 07:31

Packet Loss %



Timezone () (c) Copyright 2003 Matrix NetSystems, Inc. www.matrixnetsystems.com
GMT Jan 24 Jan 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00
EST Jan 24 7 PM 9 PM 11 PM Jan 25 3 AM 5 AM 7 AM 9 AM 11 AM 1 PM 3 PM

F-SECURE®



What did Slammer cause?

- Internet traffic slowed down globally
- Bank of America's ATM terminal network down more than 2 days
- Seattle area's 911 emergency services down for 14 hours
- Houston's Bush Intercontinental, Newark and Cleveland airport air traffic control was unavailable for some time
- South Korea and Slovenia disconnected from Internet
- Microsoft itself got infected internally (XP Registration Center down)
- Traffic peaked again on Monday when people turned their workstations on

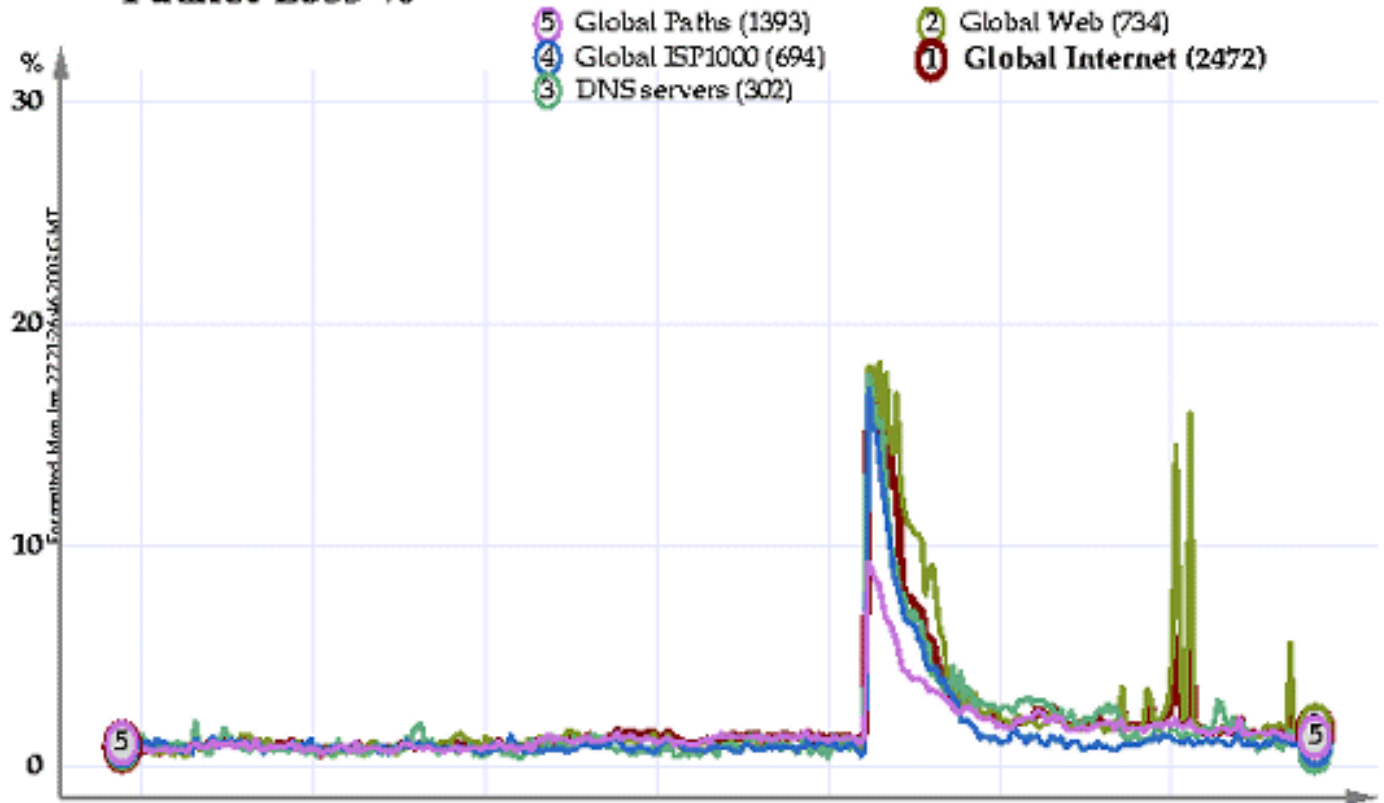


F-SECURE®



Monday 26.1.2003

Packet Loss %



Timezone 0
GMT Jan 1/22 1/23 1/24 1/25 1/26 1/27
EST Jan 20 Jan 21 Jan 22 Jan 23 Jan 24 Jan 25 Jan 26

(c) Copyright 2003 Matrix NetSystems, Inc. www.matrixnetsystems.com

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a purple triangle pointing downwards, with a black outline and a white 'F' shape inside it.

F-SECURE[®]

Who wrote it?

- Exploit by David Litchfield / NGS
- Tests by Lion / CNHonker
- We don't really know



CNHONKER.COM

· 红客联盟 ·

· HUE ·

- [About](#)
- [Advisories](#)
- [Beginner](#)
- [Chat](#)
- [Checklist](#)
- [Documents](#)
- [Exploits](#)
- [Forums](#)
- [Projects](#)
- [Standard](#)
- [Tools](#)

红客联盟公告



- Merry Christmas! 圣诞节快乐! 12-24 红客联盟
- 关于论坛最近遭受拒绝服务攻击的公告 11-17 lion
- 某国内知名安全公司招聘信息 11-11 lion
- 红客联盟论坛重新开放 10-17 lion
- 红客联盟严正声明 10-05 红客联盟
- 关于中国红客网络技术联盟 10-05 红客联盟
- 关于红客联盟邮件列表 09-23 lion
- 红客联盟网站更新脚本全部完成,今天将开始更新! 09-23 lion

[更多公告>>>](#)

最新文档更新

▶ [开放项目]	Win32 ISAPI/Filter BackDoo...	01-27	lion
▶ [文档资料]	Perl的安全性监测	01-23	墨斗鱼
▶ [新手上路]	Netbios详谈	01-18	孤单的人
▶ [新手上路]	NT/2000提升权限的方法小谈	01-18	孤单的人
▶ [安全公告]	Windows SMB implementation...	01-11	Marke(转)
▶ [安全公告]	a.shopKart Shopping Cart r...	01-11	Marke(转)
▶ [安全公告]	tanne 0.6.17远程格式串漏洞	01-11	Marke(转)
▶ [安全公告]	Remote (and local) root vu...	01-11	Marke(转)
▶ [文档资料]	delphi单一文件实现密码窃取	01-23	微程
▶ [新手上路]	一次透过SNIFF有目的性的入...	01-04	龟仙人(Ainby)

[提交文章>>>](#) [更多文档>>>](#)

邮件列表

邮箱地址

联盟IRC

host: irc.sunnet.org
port: 6667
#cnhonker
Web入口
download: HIRC

合作站点

[www.ccAnn.com](#)

最新软件更新

▶ [后门木马]	HFilter V0.10	01-28	lion
▶ [扫描工具]	Infoscan.exe	01-27	uhhuhy
▶ [攻击工具]	HGod V0.51	01-16	lion
▶ [扫描工具]	HScan v1.01	01-06	uhhuhy
▶ [扫描工具]	HScan v1.00	01-01	uhhuhy
▶ [文档下载]	phrack60.tar.gz	12-29	lion

F-SECURE®



The Packet

WinHex - [dump]

File Edit Search Position Window Extra Options File Manager Help Tab

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	04	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000010	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000040	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000050	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000060	01	DC	C9	B0	42	EB	0E	01	01	01	01	01	01	01	70	AE	.ÜÉ*Bè.....p@
00000070	42	01	70	AE	42	90	90	90	90	90	90	90	90	68	DC	C9	B.p@B hÜÉ
00000080	B0	42	B8	01	01	01	01	31	C9	B1	18	50	E2	FD	35	01	*B,....1É±.Páy5.
00000090	01	01	05	50	89	E5	51	68	2E	64	6C	6C	68	65	6C	33	...P áQh.dllhel3
000000A0	32	68	6B	65	72	6E	51	68	6F	75	6E	74	68	69	63	6B	2hkernQhounthick
000000B0	43	68	47	65	74	54	66	B9	6C	6C	51	68	33	32	2E	64	ChGetTf'1lQh32.d
000000C0	68	77	73	32	5F	66	B9	65	74	51	68	73	6F	63	6B	66	hws2_f'etQhsockf
000000D0	B9	74	6F	51	68	73	65	6E	64	BE	18	10	AE	42	8D	45	'toQhsend%. @B E
000000E0	D4	50	FF	16	50	8D	45	E0	50	8D	45	F0	50	FF	16	50	ÔPÿ.P EàP EÏPÿ.P
000000F0	BE	10	10	AE	42	8B	1E	8B	03	3D	55	8B	EC	51	74	05	%. @B ..=U iQt.
00000100	BE	1C	10	AE	42	FF	16	FF	D0	31	C9	51	51	50	81	F1	%. @Bÿ.ÿÐ1ÉQQP Ë
00000110	03	01	04	9B	81	F1	01	01	01	01	51	8D	45	CC	50	8B	... Ë...Q E P
00000120	45	C0	50	FF	16	6A	11	6A	02	6A	02	FF	D0	50	8D	45	EÀPÿ.j.j.j.ÿDP E
00000130	C4	50	62	6C	61	68	20	68	6F	70	73	DB	81	F3	3C	61	ÀPblah hopsÛ ó<a
00000140	D9	FF	8B	45	B4	8D	6E	6F	6E	76	69	72	61	6C	01	C2	Ûÿ E' nonviral.À
00000150	C1	E2	08	29	C2	8D	04	90	01	D8	89	45	B4	6A	10	8D	Áá.)Á ..@ E'j.
00000160	45	B0	50	31	C9	51	66	81	F1	78	01	51	8D	45	03	50	E*P1ÉQf Ëx.Q E.P
00000170	8B	45	AC	50	FF	D6	EB	CA									E-PÿÖeÉ

Page 1 of 1 Offset: 0 = 4

F-SECURE[®]



Future

- Warhol worms?
- Flash worms?
- PDA viruses?
- Infected mobile phones?



The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside. The background of the slide is a faint, colorful globe with latitude and longitude lines.

F-SECURE[®]

How long does it take to scan the full internet?

- Assume full IPv4 address space (aaa.bbb.ccc.ddd)
- $255*255*255*255 = 4,228,250,625$
- Assume 1 second per machine
- $4,228,250,625s = 48,938$ days
- $48,938$ days = 134 years

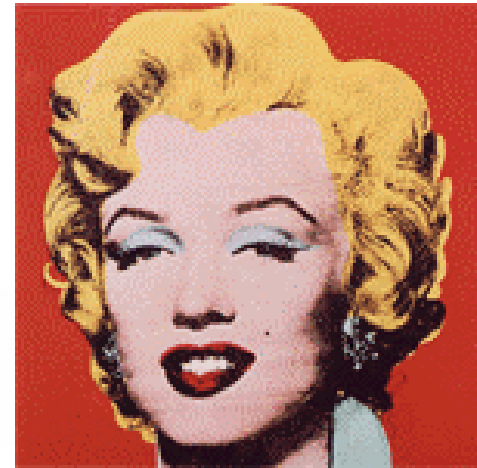
F-SECURE®



Warhol Worm – 15 minutes of "Fame"

**"In the future,
everybody will
have 15 minutes
of fame"**


– Andy Warhol



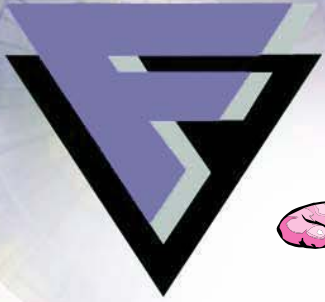
F-SECURE[®]



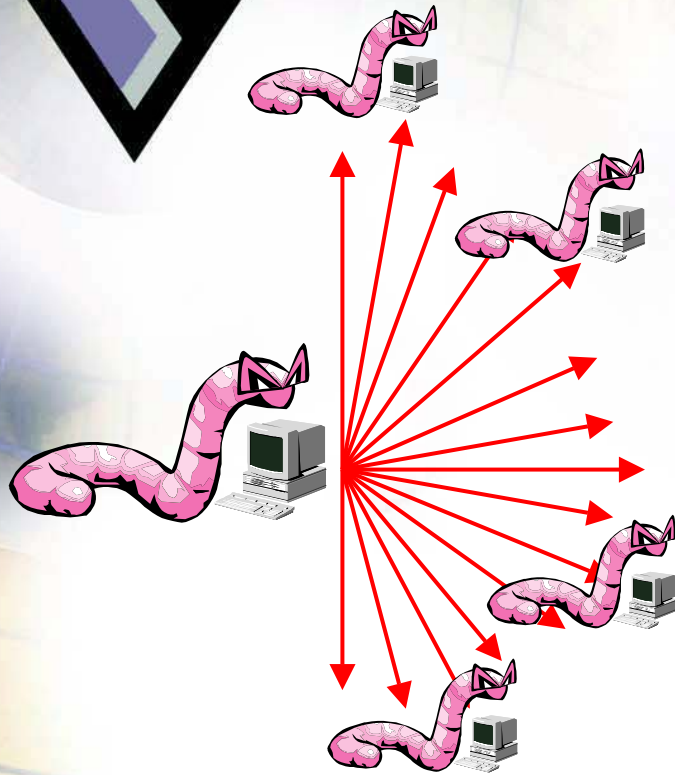
Warhol Worm – How would it work?

- 
- Hitlist scanning for initial propagation
 - List of 10 000 to 50 000 likely vulnerable machines is prepared beforehand
 - Upon infection hitlist is divided in half
 - Optimized routines
 - Permutation scan (block cipher of 32 bits with a preselected key)
 - Scan (Is the target vulnerable?)
 - Probe (Infect the target)

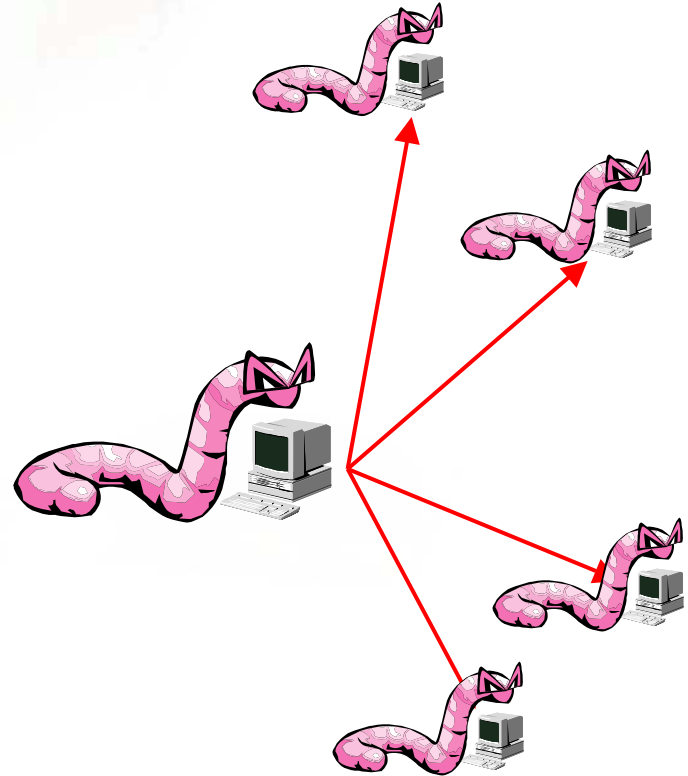
F-SECURE®



Network Worm



Warhol Worm



15 hours

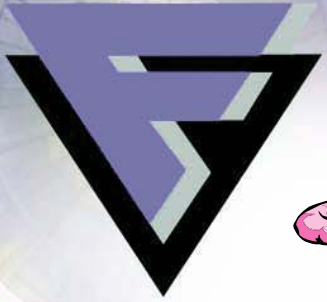
15 minutes

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

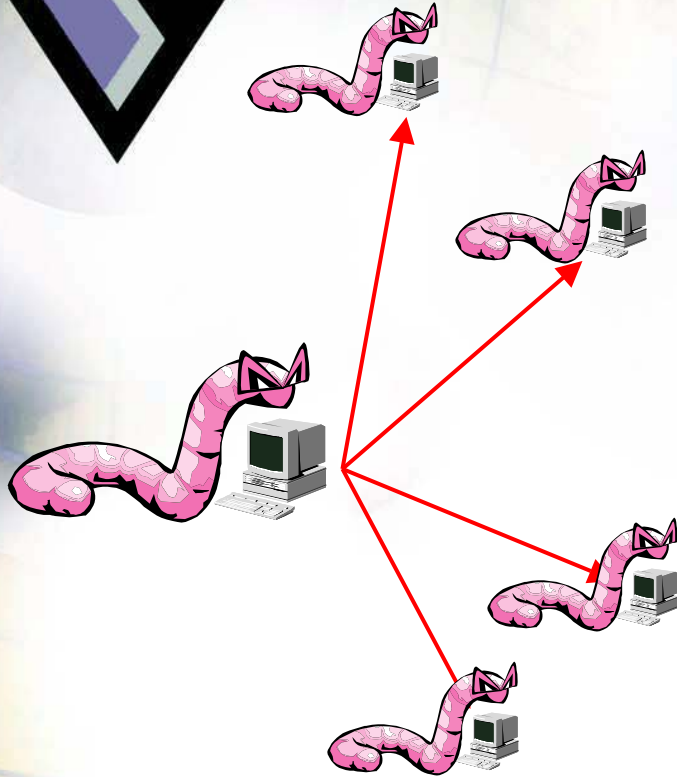
Flash Worms – 30 secs to Infect the Internet

- Hitlist scanning for initial propagation
 - List of all likely vulnerable machines is prepared beforehand
 - Starting from machines with good network connections
- Highly optimized routines
 - Scan is performed beforehand
 - 99,9% of infections are succesful

F-SECURE®

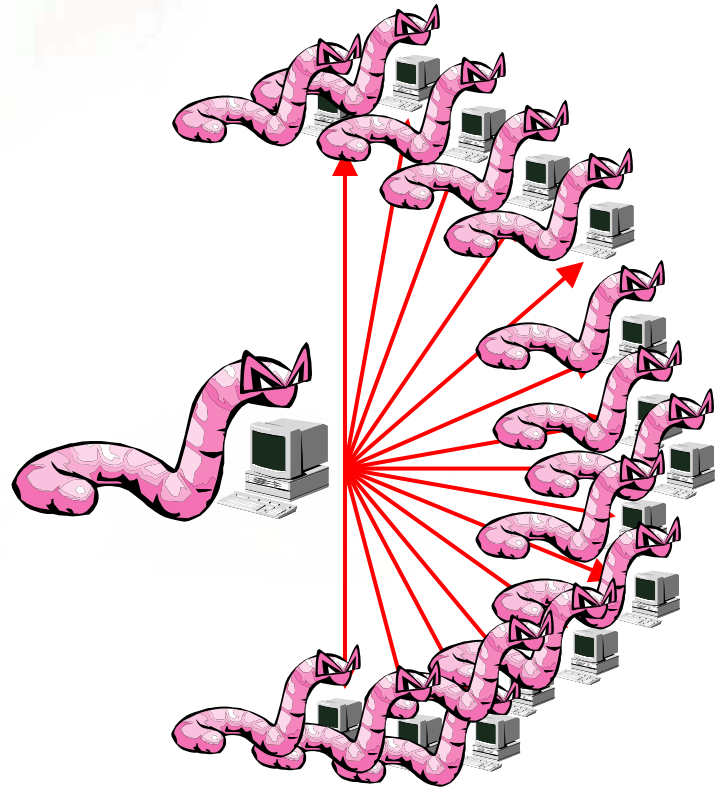


Warhol Worm



15 minutes

Flash Worm



15 seconds

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a purple triangle pointing downwards, with a white and black shape inside that resembles a shield or a stylized letter 'F'. The entire logo is set against a circular background with a grid pattern, suggesting a globe.

F-SECURE®

Reasons why anti-virus is not enough

- Even the virus definition updates are fast, new worms spread even faster
- Heuristics in anti-virus products can be fooled and new worms can be tested against existing heuristic products
- New worms may not be detected by plain anti-virus since the worm may operate only in RAM memory (e.g. Slammer)

=> You will need firewall and anti-virus products to work together!

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the upper right. Below the text is a stylized, three-dimensional shield or triangle shape composed of overlapping purple and black geometric shapes.

F-SECURE®

How to protect against combined threats?

- Early warning
- Proactive defense (firewall)
- Active defense (anti-virus)
- Fast and automatic definition updates

F-SECURE®

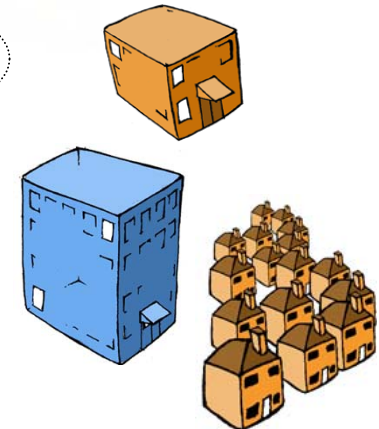


Early Warning: F-Secure Radar

- Provides instant critical security alerts straight from our labs 24 X 7 X 365.
- Sends those alerts to a wide variety of devices, so you definitely get the message (phones, pagers, faxes, SMS, etc)
- Works around the globe!



Getting the Right
Information



Wherever You Are



On Your
Preferred Device

The logo features the text "F-SECURE" in a bold, black, sans-serif font, with a registered trademark symbol (®) to its upper right. Below the text is a stylized shield emblem composed of overlapping geometric shapes in shades of purple and blue, all contained within a circular border that has a grid pattern.

F-SECURE®

Proactive defense: F-Secure Distributed Firewall

- F-Secure Distributed Firewall protects your PC and confidential information against hackers and worms
- F-Secure Distributed Firewall includes:
 - Intrusion Prevention
 - Application Control
 - Security Alerts... in single easy-to-use program.

F-SECURE®



Proactive defense: F-Secure Distributed Firewall

- Easy-to-use interface for changing security levels with built-in rules
- Immediate protection after installation!

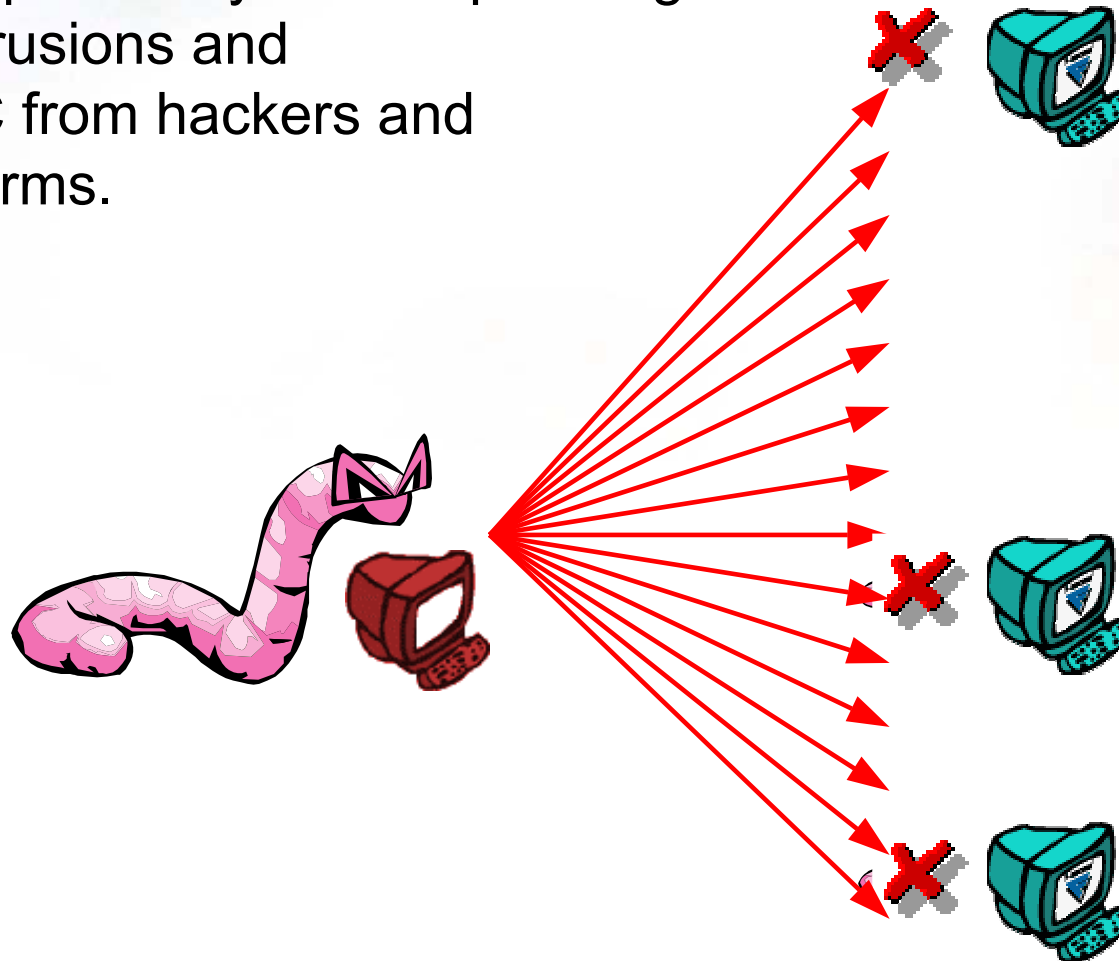


F-SECURE®



Proactive defense: F-Secure Distributed Firewall / Intrusion Prevention

- Automatically protects your computer against networked intrusions and hides your PC from hackers and networked worms.



F-SECURE®



Proactive defense: F-Secure Distributed Firewall / Application Control

- Gives you the possibility to control what programs are accessing the network
- Trojans, spyware and other malicious applications cannot transfer your confidential information, such as credit card numbers, to the Internet hackers

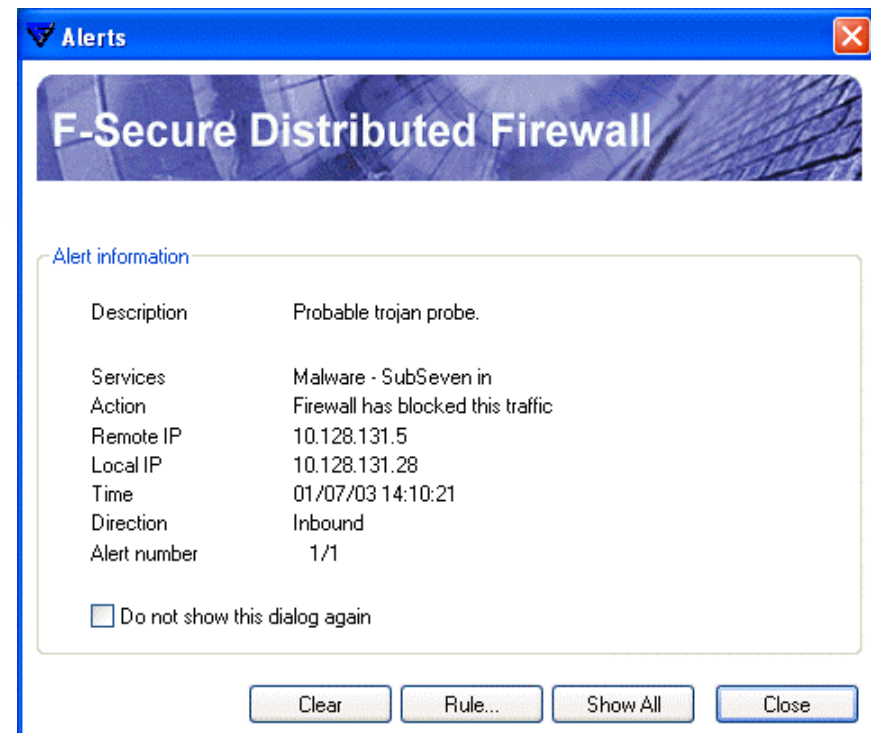


F-SECURE®



Proactive defense: F-Secure Distributed Firewall / Alerts

- F-Secure Distributed Firewall monitors both outgoing and incoming Internet traffic.
- Security alert is given if suspicious activity is blocked.



The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, three-dimensional shield or triangle shape composed of overlapping purple and black geometric forms.

F-SECURE®

Active Defense: F-Secure Anti-Virus

- Easy-to-use solution for keeping customers rapidly and automatically protected against fast-spreading Internet-borne viruses and other malicious code
- F-Secure Anti-Virus protects both office workstations, home and mobile workers, ensuring system availability and data integrity every minute of every day, everywhere in the world

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, three-dimensional shield or triangle shape composed of overlapping purple and black geometric forms.

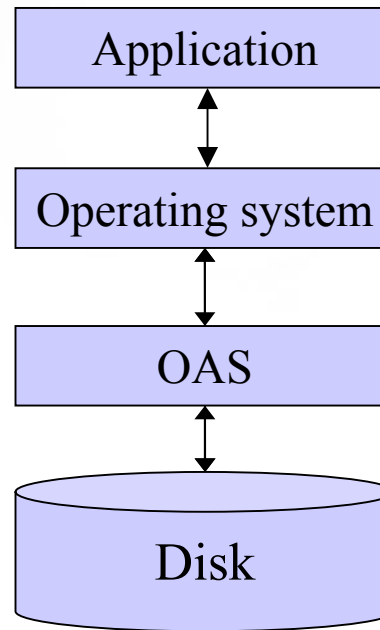
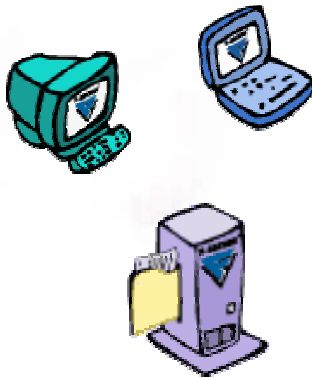
F-Secure Anti-Virus

- IT administrator can install the software to every desktop and laptop computers from a single console without needing to visit them
- Automatic virus signature delivery from F-Secure using advanced incremental transfer mechanisms
- Automatic reporting on (product) status, even if there's nothing wrong to let you know that protection is alive & updated with the newest cure from F-Secure Virus Research Lab.
- Advanced delivery of virus definition updates to corporate remote offices using F-Secure Anti-Virus Proxy

F-SECURE®



Always-on protection for Workstations and File Servers



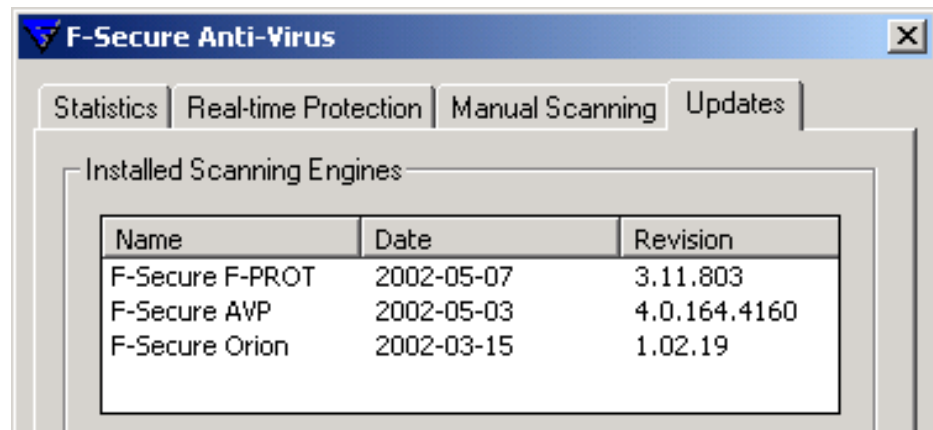
- **Totally transparent and automatic**
- **Hard to bypass**

F-SECURE®



100% virus detection

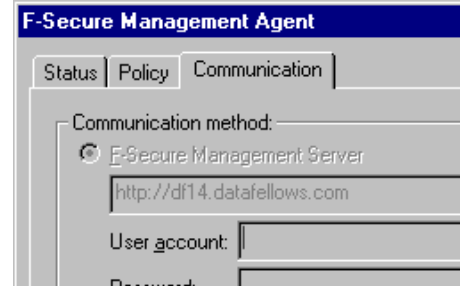
- Using multiple independent virus scanners:
 - F-Prot: Macro, file and boot sector virus detection and removal
 - AVP: Polymorphic and macro virus detection and removal
 - Orion: Heuristic scanner for unknown viruses



The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol. Below the text is a stylized, purple and black shield-like graphic with a white 'F' shape inside.

Centralized Management

- Reduce bypassing of security settings!
- Keep end-users focused on their work, not on the utilities in their computers!
- How?
 - Hide the whole user interface, if feasible.
 - Use F-Secure's centralized management to restrict end-user access to critical settings
 - Use F-Secure Policy Manager to monitor settings changed by end-users



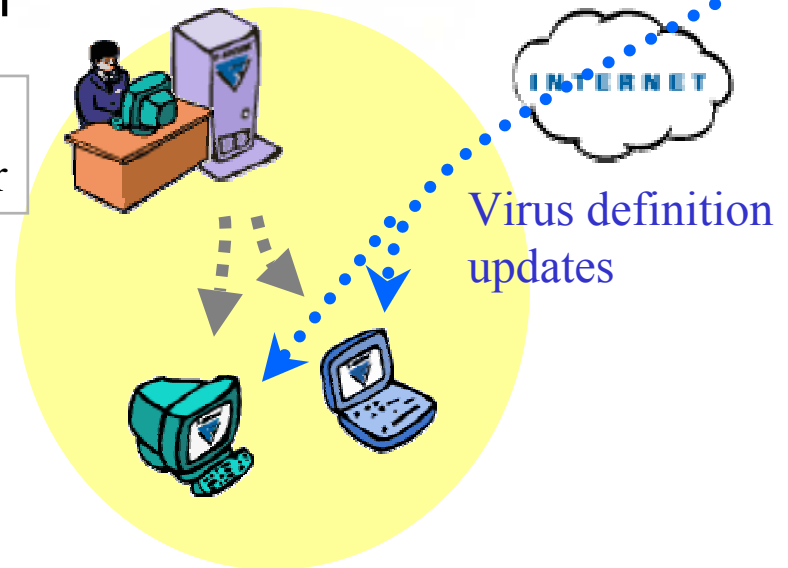
F-SECURE®



Automatic Daily Updates

- F-Secure Virus Research Lab produces definition updates daily, or immediately if needed
- Several different distribution channels available both for standalone computers, traveling users and workstations in a LAN
- Updates can be fully automated or initiated by the administrator or end-user

F-Secure
Policy Manager

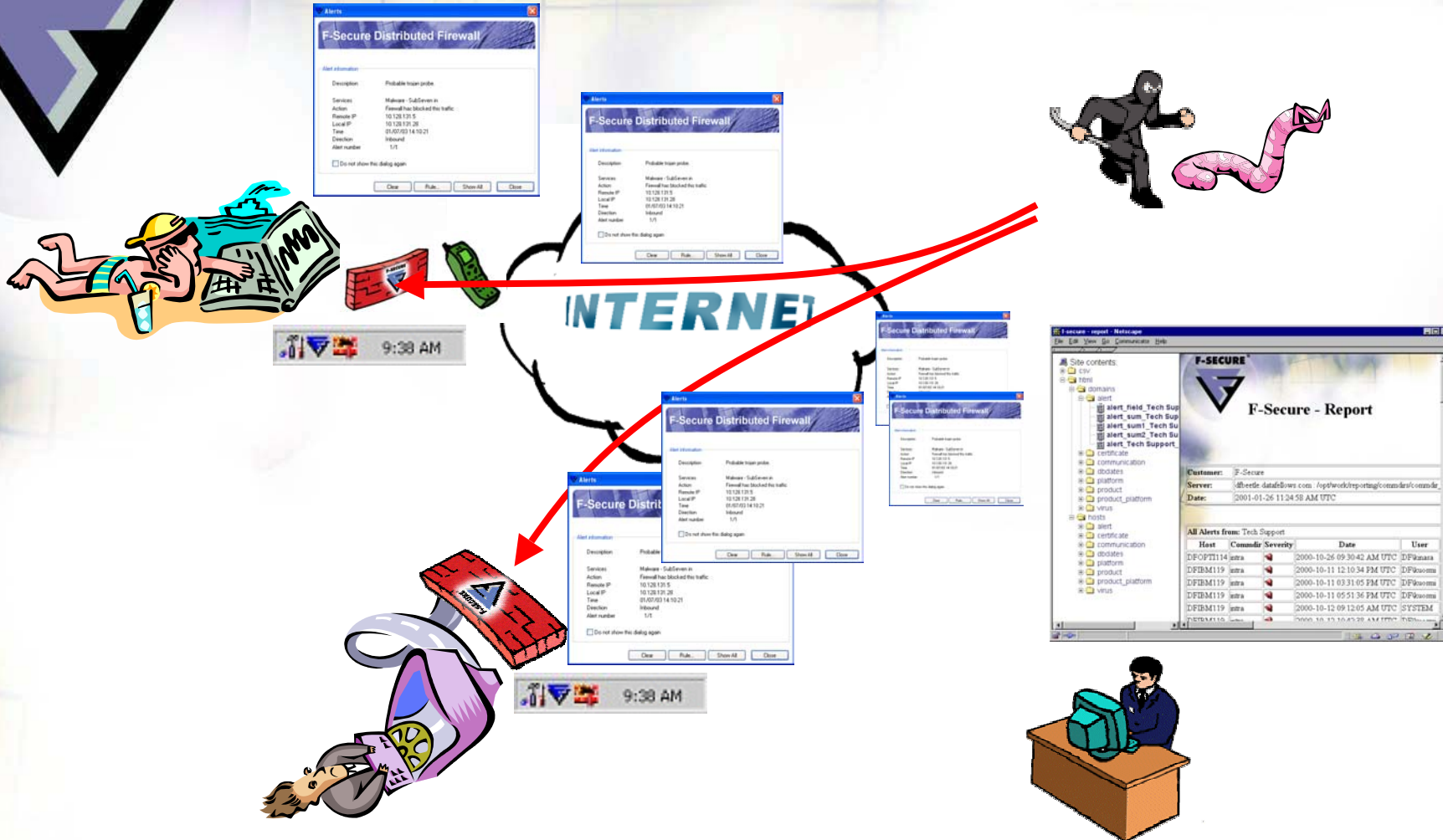


Virus Research
Laboratory

F-SECURE®



Centralized alerts



Corporate Network Administrator

F-SECURE®



Comprehensive Alerting and Reporting

- Alerts can be forwarded to...:
 - To F-Secure Policy Manager Console
 - To Local User Interface
 - To Local log file
 - As e-mail messages
 - To NT's event log
 - As SNMP traps
- Custom reports can be created and viewed
 - in F-Secure Policy Manager Console
 - with standard web-browser,
 - exported to Microsoft Excel
- F-Secure Policy Manager Reporting Option can create custom reports automatically in the background, to be viewed or exported for further analysis

F-Secure - Report

Customer: F-Secure
Servers: example_commdir:C:\DATA\Policy-Manager\PM5.10\RPOS.10\Build 17\example\demo\Commdir1\
Date: 2001-10-17 17:54:23 UTC

Virus alerts from /

Severity	Name	Count
	Security Alert	27
	Fatal Error	24
	Error	35
	Warning	0
	Informational	0

Host	Commdir	Security Alert	Fatal Error	Error	Warning	Informational
Host\WinName2	example_commdir	3	0	5	0	0
Host\WinName3	example_commdir	8	6	10	0	0
Host\WinName4	example_commdir	8	9	10	0	0
Host\WinName5	example_commdir	8	9	10	0	0

All virus alerts from /

Host	Commdir	Severity	Date	User	Message
Host\WinName2	example_commdir		2000-07-28 20:25:14 UTC	user4	Malicious code found in file H:\user4\Prylar\Eicar\leicar.com. Infect
Host\WinName2	example_commdir		2000-08-01 15:21:04 UTC	user4	Manual scanning was finished - workstation was found infected!
Host\WinName2	example_commdir		2000-08-11 09:54:22 UTC	user4	Malicious code found in file C:\WINNT\Profiles\user4\Local Settings
Host\WinName3	example_commdir		2000-07-08 18:15:42 UTC	user4	Malicious code found in file C:\vob\leicar.com. Infection: EICAR_T

F-SECURE®

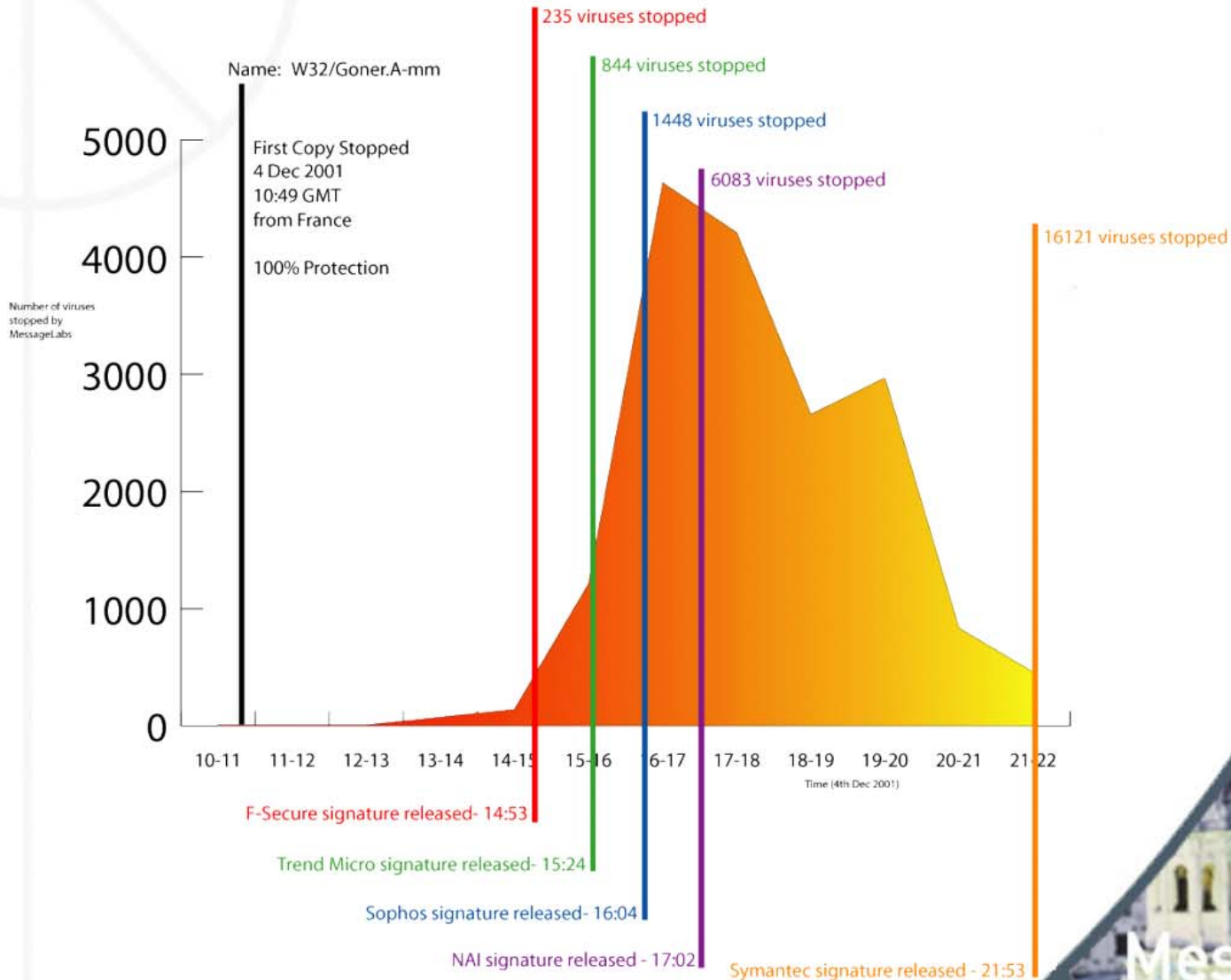


Fast Updates: F-Secure Anti-Virus Research Lab

- Typical reaction time around 2.5 hours
 - Melissa 1999: 3h 15min
 - Loveletter 2000: 1h 40min
 - Anna Kournikova 2001: 2h 5min
 - Sircam 2001: 1h 50min
 - Nimda 2001: 1h 57min
 - Slapper 2002: 4h 10min
 - Bugbear 2002: 2h 47min



Rapid signature updates





F-SECURE[®]

From risk management to business enabler

- Historically the role of security solutions has been concentrating on risk management
- We believe that by using the right security solutions enable corporations to do business more efficiently:
 - More flexible and productive ways to do work
 - Enable corporations to focus on their core business
 - Enable corporations to grow their business and productivity
 - Reduce commercial and legal risks due to protection against combined threats

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Summary

- Network intrusions are here to stay
- Viruses and Worms are getting faster and smarter
- Protection against combined threats is build on:
 - Early warning
 - F-Secure Distributed Firewall
 - F-Secure Anti-Virus
 - Fast virus definition updates
- With efficient protection you can concentrate on your business without worrying about Internet threats

Certifications

F-SECURE®



- F-Secure Anti-Virus for Internet Mail Verified Interoperability with Cisco PIX 500 Firewall
- F-Secure SSH for Unix and Windows Verified Interoperability with Cisco IOS Release 12.1(1)T and Cisco PIX 5.2
- F-Secure Anti-Virus for Firewall 6.01, Windows version OPSEC Certified and Interoperable with Check Point FireWall-1
- The cryptographic library of F-Secure FileCrypto for Pocket PC is the only FIPS 140-2 certified cryptographic module in the market.
- F-Secure SSH Client for Windows Containing FIPS 140-1 Certified Cryptographic Components
- Nokia OK for F-Secure FileCrypto, F-Secure SSH and F-Secure Anti-Virus for Nokia 9200 Communicator Series
- In addition, close co-operation with the following technology partners:

CISCO SYSTEMS
Verified



Microsoft
CERTIFIED
Partner



CYBERGARD
WORLDWIDE
DEFEND YOUR DOMAIN

rockliffe
ROCK SOLID INTERNET SOFTWARE™

symbian
Technology
Partner

Compaq Solutions Alliance
Member
COMPAQ

jsa

BALTIMORE
www.baltimore.com

CLEARSWIFT

F-SECURE®

Awards & Acknowledgements

- F-Secure Anti-Virus for Workstations SC Magazine Recommended (January 2003)
- F-Secure Anti-Virus 5.40 Obtains the Prestigious "VB100%" award (Virus Bulletin Magazine, June & November 2002)
- F-Secure AV 5.40 Receives Checkmark Levels 1 and 2 (August 2002)
- F-Secure Anti-Virus Named the Editor's Choice (Finnish IT Magazine Tietokone – February 2002)
- F-Secure Anti-Virus for Microsoft Exchange Pick of the 2001 (SC Magazine – 2001)
- F-Secure Anti-Virus 5.30 Received the Full Score of 100 % for Full-Zoo Virus Recognition (AV-Test.org/PC Welt - November 2001)
- F-Secure Named One of Europe's 50 Hottest Tech Firms (Time Magazine – June 2000)



INFORMATIONWEEK



TIME.com



F-SECURE[®]



Thanks!