

Internet Threats Today and Tomorrow



Agenda

- Intro about AVERT
- Threat count and growth rate
- Threats using the known system vulnerabilities
- Noteworthy viruses overview
- Threats during 2004 and beyond
- Defense against the new threats
- Q&A



AVERT at-a-glance

- Customer Support/Services
 - Work With ALL PC Users To Provide Answers On Real & Potential Threats
- Virus Analysis/Anti-Virus Research
 - · Global Team Provides Local & International Coverage
- Advanced Software/Detection Research
 - Develops Solutions For Tomorrows Virus & Security Threats
- Web Based Solutions and Services
 - Web Programs Give Customers Easy Access To VIL and Our Technology



AVERT 20 Cities Worldwide

Asia & PacRim

North America

Beaverton*
Santa Clara*
Los Angeles*
Vancouver*
Dallas

Bangalore*
Singapore*

Hong Kong*

Tokyo*

Sydney

Beijing

South America

Mexico City San Paolo

U.K. & Europe

Aylesbury*

Hamburg*

Amsterdam*

Paris*

Stockholm

Madrid

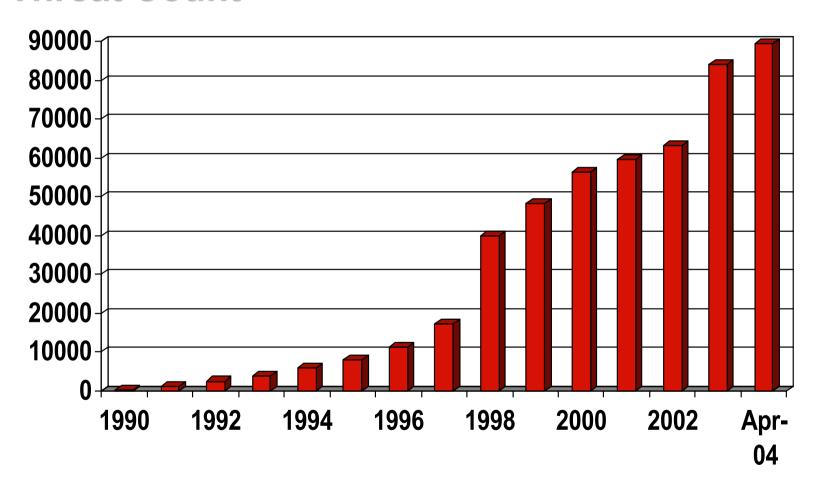
Johannesburg



Threat count and growth rate



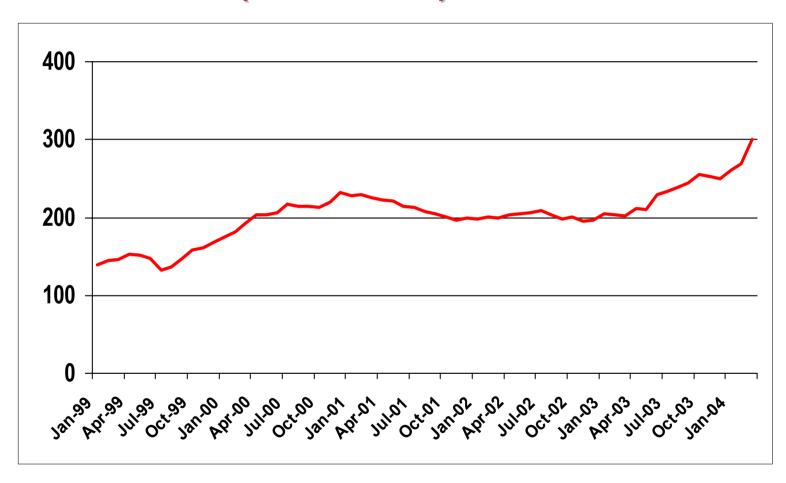
Threat Count



Source: McAfee's VirusScan statistics



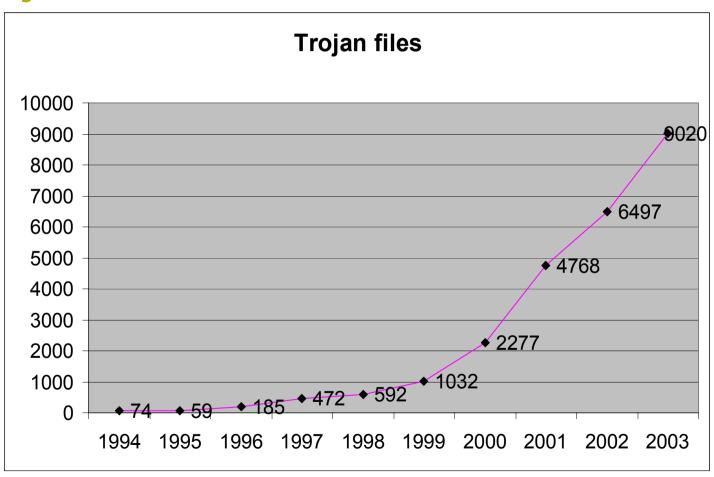
The WildList (Worldwide)



Source: WildList Org.

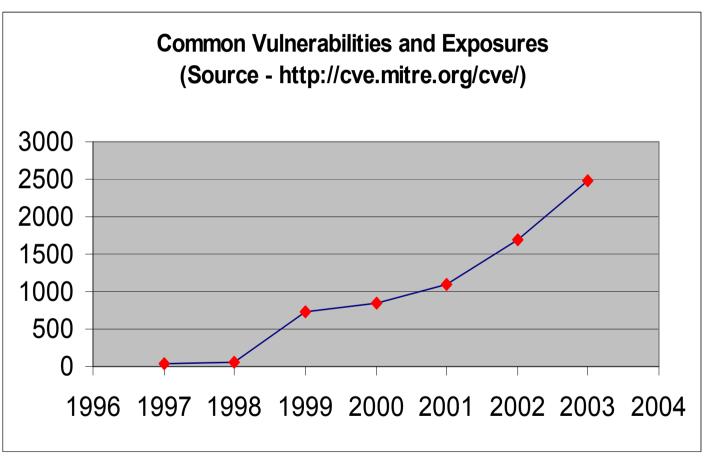


Trojan Threats Continue to Grow





System exploits . . . not just Microsoft



Source: National Infrastructure Protection Center - 2001



Example of bulletins and the worms that followed

	CVE Reference	MS Reference	Worm Name	Patch Date	Worm Date
•	CVE-1999-0668	MS99-032	VBS/BubbleBoy@MM	08/31/1999	11/08/1999
•	CVE-1999-0018	-	Linux/Ramen.worm	11/24/1997	01/17/2001
	CVE-1999-0997	-	Linux/Ramen.worm	12/20/1999	01/17/2001
•	CVE-2000-0917	-	Linux/Ramen.worm	09/25/2000	01/17/2001
•	CVE-2001-0010	-	Linux/Lion.worm	01/29/2001	03/23/2001
	CVE-1999-0977	-	SunOS/BoxPoison.worm	12/29/1999	05/09/2001
•	CVE-2000-0884	MS00-078	SunOS/BoxPoison.worm	10/17/2000	05/09/2001
•	CVE-2001-0500	MS01-033	W32/CodeRed.worm	06/18/2001	07/17/2001
	CVE-2000-0884	MS00-078	W32/Nimda.gen@MM	10/17/2000	09/18/2001
•	CVE-2001-0154	MS01-020	W32/Nimda.gen@MM	03/29/2001	09/18/2001
•	CVE-2001-0154	MS01-020	W32/Aliz@MM	03/29/2001	05/22/2001
	CVE-2001-0154	MS01-020	W32/Klez.a@MM	03/29/2001	10/26/2001
•	CAN-2002-0656	-	Linux/Slapper.worm	07/31/2002	09/13/2002
	CAN-2002-0649	MS02-039	W32/SQLSlammer.worm	07/24/2002	01/25/2003
	CAN-2003-0352	MS03-026	W32/Blaster.worm	07/16/2003	08/11/2003
•	CAN-2003-0352	MS03-026	W32/Nachi.worm.a	07/16/2003	08/18/2003
•	CAN-2003-0109	MS03-007	W32/Nachi.worm.a	03/17/2003	08/18/2003
	CAN-2003-0352	MS03-026	W32/Nachi.worm.b	07/16/2003	02/11/2004
•	CAN-2003-0109	MS03-007	W32/Nachi.worm.b	03/17/2003	02/11/2004
	CAN-2003-0812	MS03-049	W32/Nachi.worm.b	11/11/2003	02/11/2004
•	CAN-2003-0003	MS03-001	W32/Nachi.worm.b	01/22/2003	02/11/2004
•	CAN-2004-0362	-	W32/Witty.worm	03/18/2004	03/20/2004
	CAN-2003-0533	MS04-011	W32/Sasser.worm	04/13/2004	04/30/2004

(Source - http://cve.mitre.org/cve/)



Some noteworthy worms and viruses



	Bagle ■ .A 1/18/04		<u>Netsky</u>		<u>Mydoom</u>	
			Most viral emails ever	A .	1/26/04	
			Same author	■ .B	1/28/04	
			Source code distributed, now different authors	■ .D	2/12/04	
				■ .E	2/13/04	
■ .B	.B 2/17/04	. A.	2/16/04 Announces s	elf as Skynet.c	ZZ	
		■ .B	2/18/04 "Skynet, not N	Vetsky"		
				■ .F	2/19/04	
■ .C	2/27/04	. C	2/25/04 Calls Mydoon	n.F a thief of io	deas	



<u>Bagle</u>		<u>Netsk</u>	<u>(Y</u>		Mydo	<u>om</u>
■ .D	2/28/04					
■ .E	2/28/04					
■ .F	2/29/04 Int	roduces password	ded ZIP files			
■ .G	2/29/04					
■ .H	3/1/04	. D	3/1/04	Reiterates Skynet.c	Z	
		■ .E	3/1/04			
■ .l	3/2/04				■ .G	3/2/04
■ .J	3/2/04 "Hey,N don't r	Netsky, fuck off yuine our bussines	you bitch, ss, wanna start a v	war?''		
■ .K	3/3/04	■ .F	3/3/04		■ .H	3/3/04
		■ .G	3/4/04			
		■ .H	3/5/04			



Bagle		<u>Netsky</u>		
		■ .I	3/7/04	
		■ .J	3/8/04	
		■ .K	3/8/04	Mentions texas and "last one"
■ .L	3/9/04			
		■ .L	3/10/04	•
■ .M	3/11/04	■ .M	3/11/04	•
■ .N	3/13/04 ZIP	password now §	given via an image	file
■ .0	3/15/04	■ .N	3/15/04	Hand off of source to another set of programmers Mentions Fanaticon.
■ .P	3/15/04			Montons i unuticon.
		■ .0	3/17/04	•



Bagle

Netsky

■ .Q 3/18/04 Uses 590 internet infected machines to infect through

R 3/18/04

■ .S 3/18/04

■ .T 3/18/04

■ .P 3/21/04

■ .U 3/26/04

■ .Q 3/28/04 Mentions Russia; no backdoors

■ .V 3/29/04

■ .R 3/31/04 Mentions Bruce Schneider, cz, and Russia

■ .W 4/5/04

■ .S 4/5/04 Inse

Inserts backdoor

■ .T 4/6/04

■ .X 4/8/04

■ .U 4/7/04

Network Associates®



W32/Sasser.worm.b

Highlights:

- Self-executing worm exploits Microsoft Windows vulnerability (MS04-011) (CAN-2003-533)
- Gaobot.worm.ali led up to the discovery of Sasser, by exploiting this vulnerability on a smaller scale
- Evidence shows that many Sasser infected systems were also infected with Gaobot, suggesting Sasser was seeded via Gaobot
- Sasser requires no user intervention. It's completely transparent.
- Scans local subnets, class A & B along with other completely random subnets, looking for systems responding to TCP port 445 SYN requests.
- Threat could have been much worse if scanning algorithm was more logical.
- Instructs compromised PC to download and execute viral code.
- Creates a remote shell via port 9996 and FTP server via 5554 FTP server contains bug, which other viruses are exploiting



Other noteworthy virus (summary)

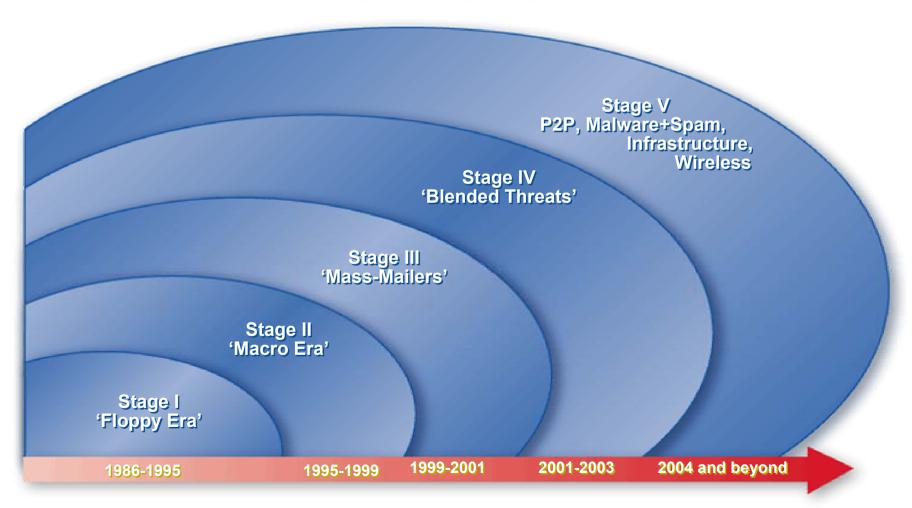
- W32/Sobig.a@MM (1/09/2003)
 - Used MX Lookup bringing down mail servers due to load
- W32/SQLSlammer.worm (1/25/2003)
 - First worm that does not have a actual file infection
- W32/Blaster.worm.a (8/11/2003)
 - Was originally named W32/Lovsan.worm.a
- W32/MyDoom@MM (1/26/2004)
 - Ability to guess email addresses and mail servers



2004 and Beyond



Evolution of the Threats





Potential attacks

IRC

Peer-to-Peer

Linux

Win32 Viruses

Script viruses

Macros

Root Kits & Drivers

Dialers

Buffer Overflows

Unwanted Apps

XML

.NET

Instant Messenger

2 Years

Cell phones

Immediate and Continuing High **Immediate and Continuing** Medium **Immediate and Continuing** High **Immediate and Continuing** High **Immediate and Continuing** High **Immediate and Continuing** High 6 Months Medium 1 Year Low 1 Year Medium

Low



Future Unix Threats

- More Unix machines, bigger impact of malware.
- Mobile phones running Unix
- Malware written in .NET
- Cross Platform infectors:
- Java Script malware for Windows & Unix
- Binary files running on both Windows and Unix : Mono project



Defense Against New Threats

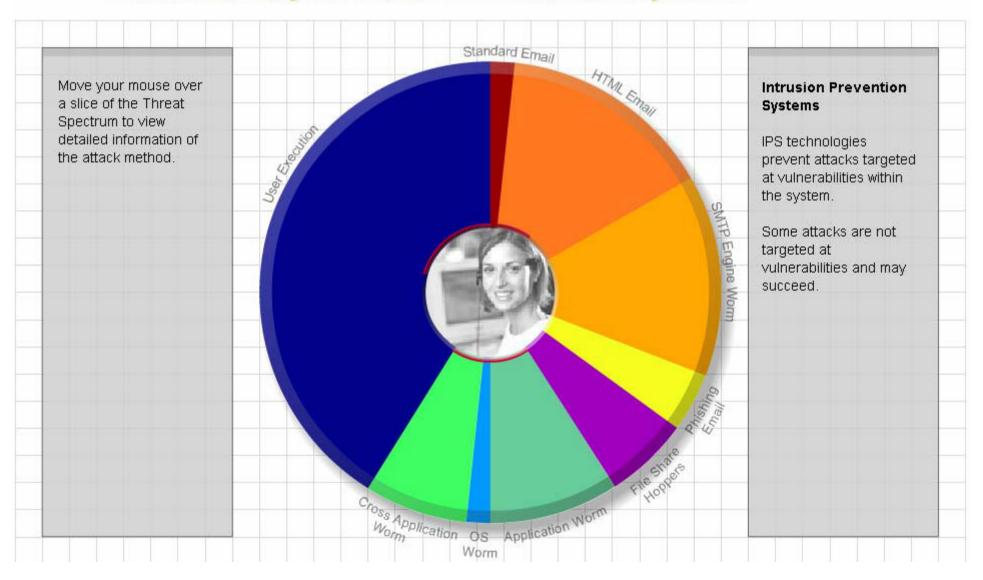
Leo Chan

Regional Engineering Manager – McAfee Security

email: leo_chan@nai.com

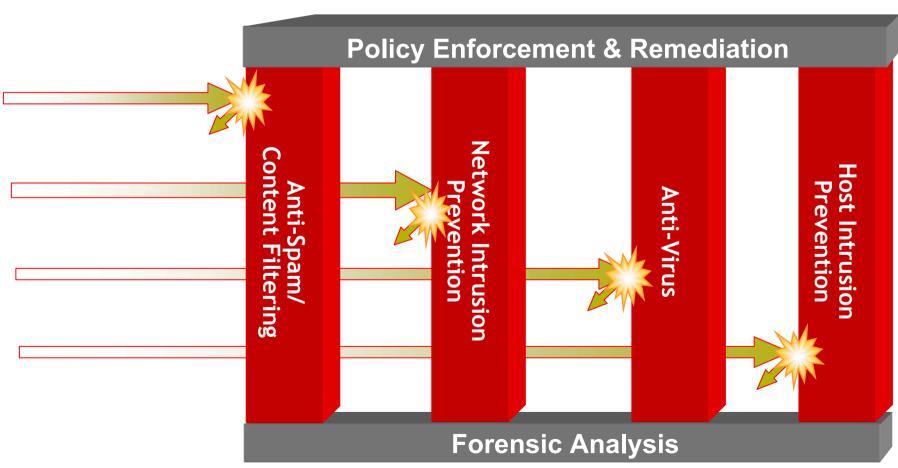


Protection Layer - Intrusion Prevention Systems





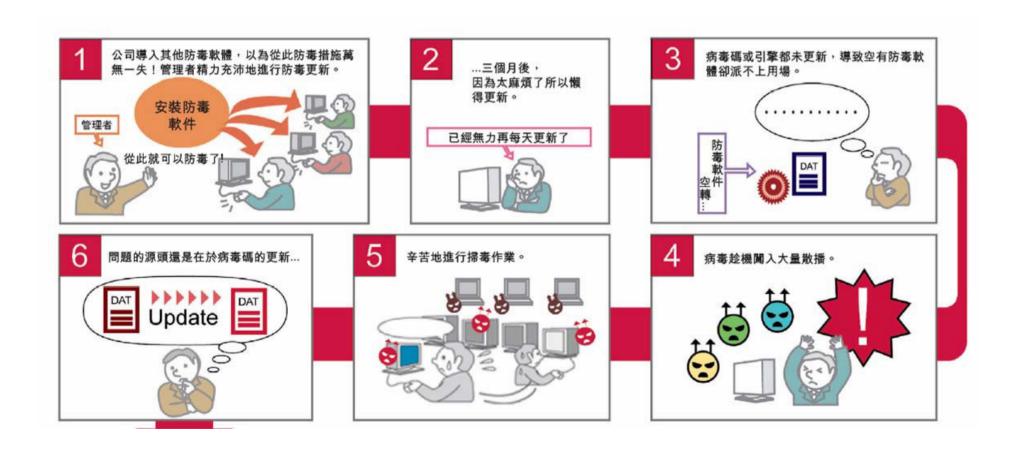
Strategy for Large Enterprises



McAfee® Protection-in-Depth Strategy



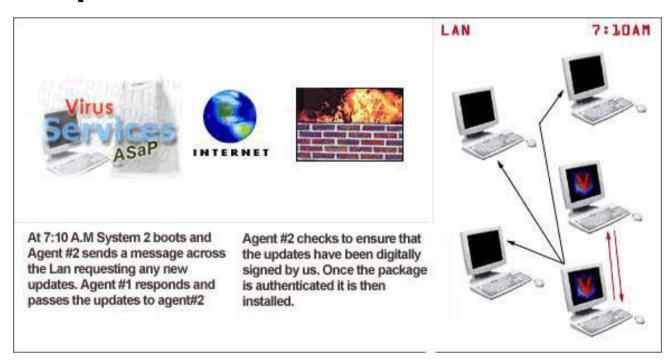
Issues for SMB





Technology to Ensure update

Requirement no human attention





Managed Service for ensuring security

- Provide Security News and Updates
- Report Security status for the company
- Monitor and alert security problems

