



Internet Security Threat Report



- ▶ *Oliver Friedrichs, Senior Manager*
- ▶ *Symantec Security Response*
- ▶ *March 2005*



Agenda

- ▶ Internet Security Threat Report
 - What is the Internet Security Threat Report?
 - What Makes the Internet Security Threat Report Unique?
 - Attack Trend Highlights
 - Vulnerability Trend Highlights
 - Malicious Code Trend Highlights
 - Addition Security Risks Highlights
 - Future Watch

What Is the Internet Security Threat Report?

- ▶ The Symantec Internet Security Threat Report, compiled every six months by Symantec analysts, is the most comprehensive analysis of current Internet security trends.
- ▶ The Internet Security Threat Report provides analysis and discussion of current trends in Internet attacks, vulnerabilities, and malicious code activity, as well as predictions on future threats.



What Makes The Internet Security Threat Report Unique?

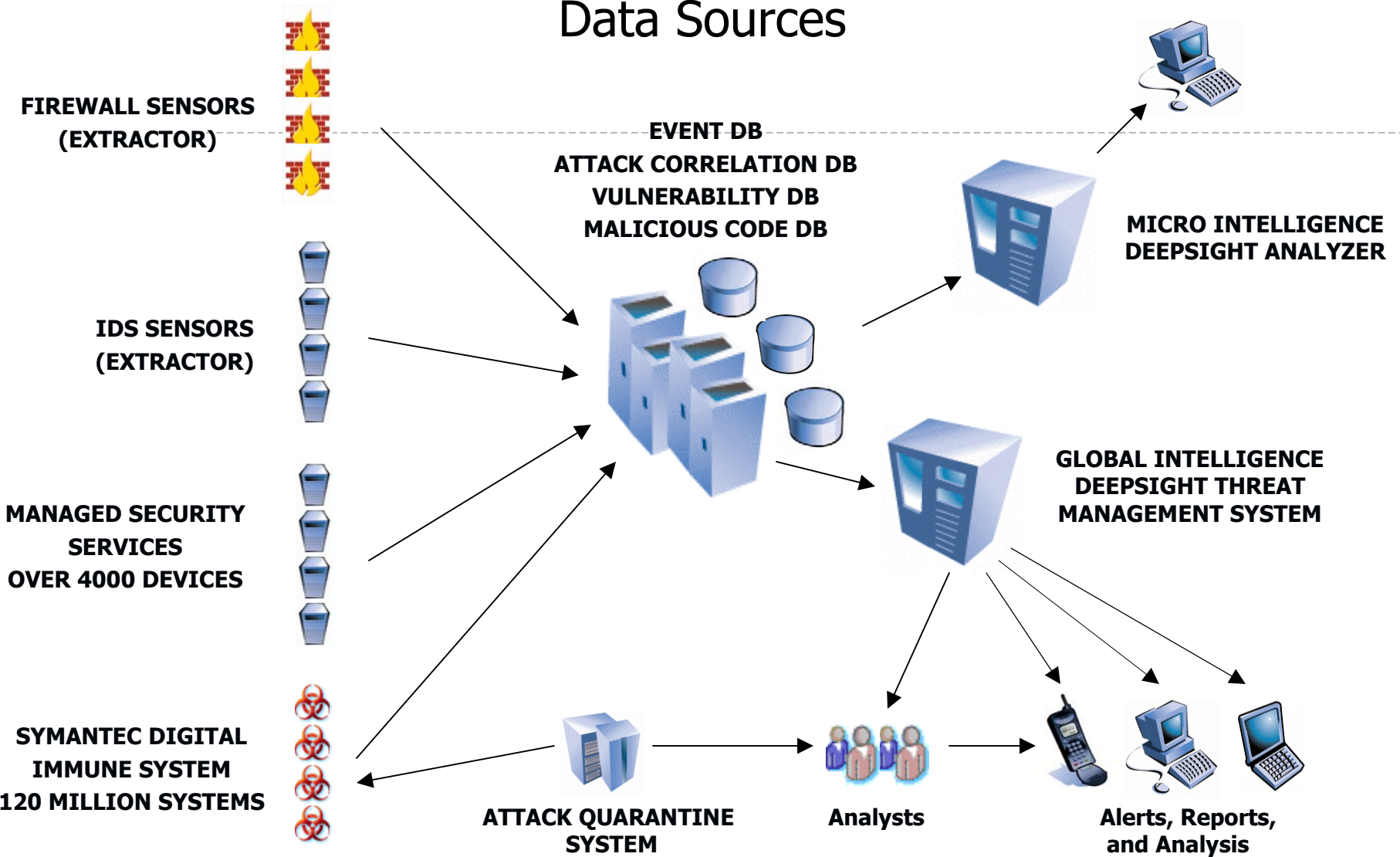
- ▶ Based on one of the world's largest sources of security data.
 - 500 Symantec Managed Security Services customers
 - 20,000 sensors worldwide monitoring network activity in 180 countries
 - 120 million client, server, and gateway antivirus systems
 - 11,000-entry vulnerability database
 - Symantec Probe Network with over 2,000,000 decoy accounts attracting spam and phishing email from 20 different countries around the world.
 - Provides a comprehensive view of what the state of Internet security looks like today.



Attack Trends



Data Sources



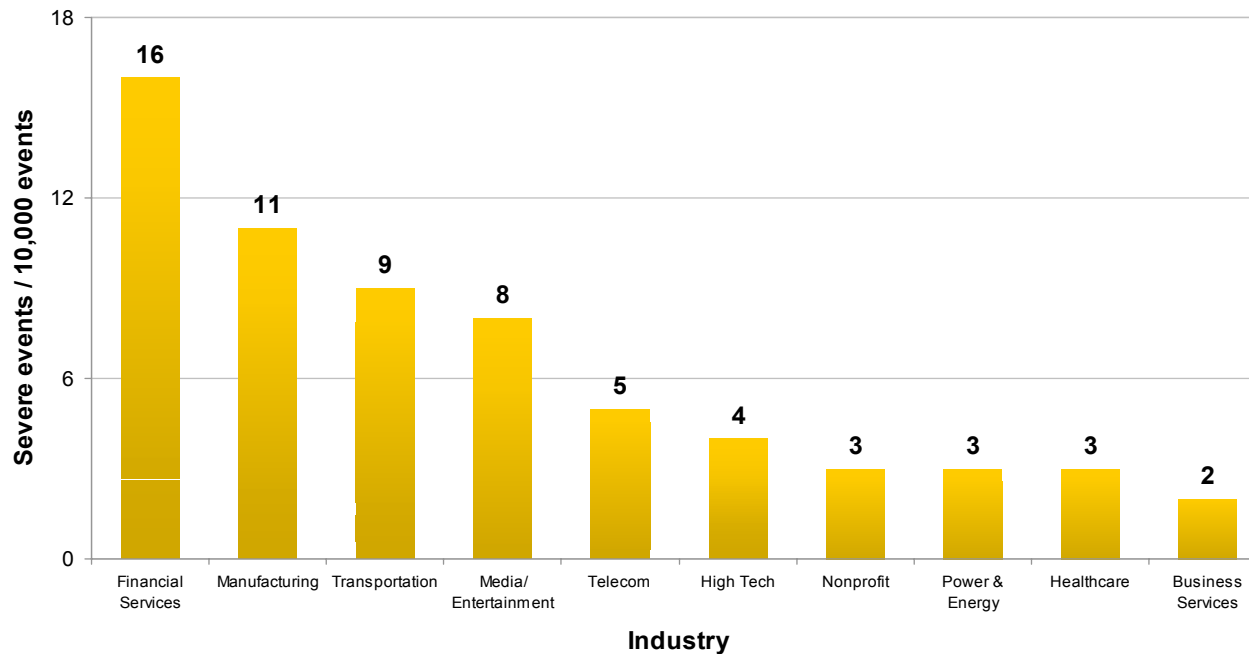
Attack Trends – Bot Infection Statistics

- Statistics are based on the number of computers worldwide that are known to be infected with bots and what percentage are situated in each country.
- The rapid growth of broadband connections in the U.K. along with associated increase in infrastructure and support costs may slow the response of ISPs to reports of network abuse and infection.

Rank	Country	Percent of bot infected computers
1	United Kingdom	25.2%
2	United States	24.6%
3	China	7.8%
4	Canada	4.9%
5	Spain	3.8%
6	France	3.6%
7	Germany	3.5%
8	Taiwan	3.1%
9	South Korea	3.0%
10	Japan	2.6%

Attack Trends - Severe Events By Industry

- Severe attacks pose the greatest threat to organizations as they can result in serious damage and compromise of the targeted network and as such, may indicate the risk to which that industry is exposed.
- With the growth in phishing and other financial motivated attacks, the rise in severe events in financial services is inline with our current and future predictions.



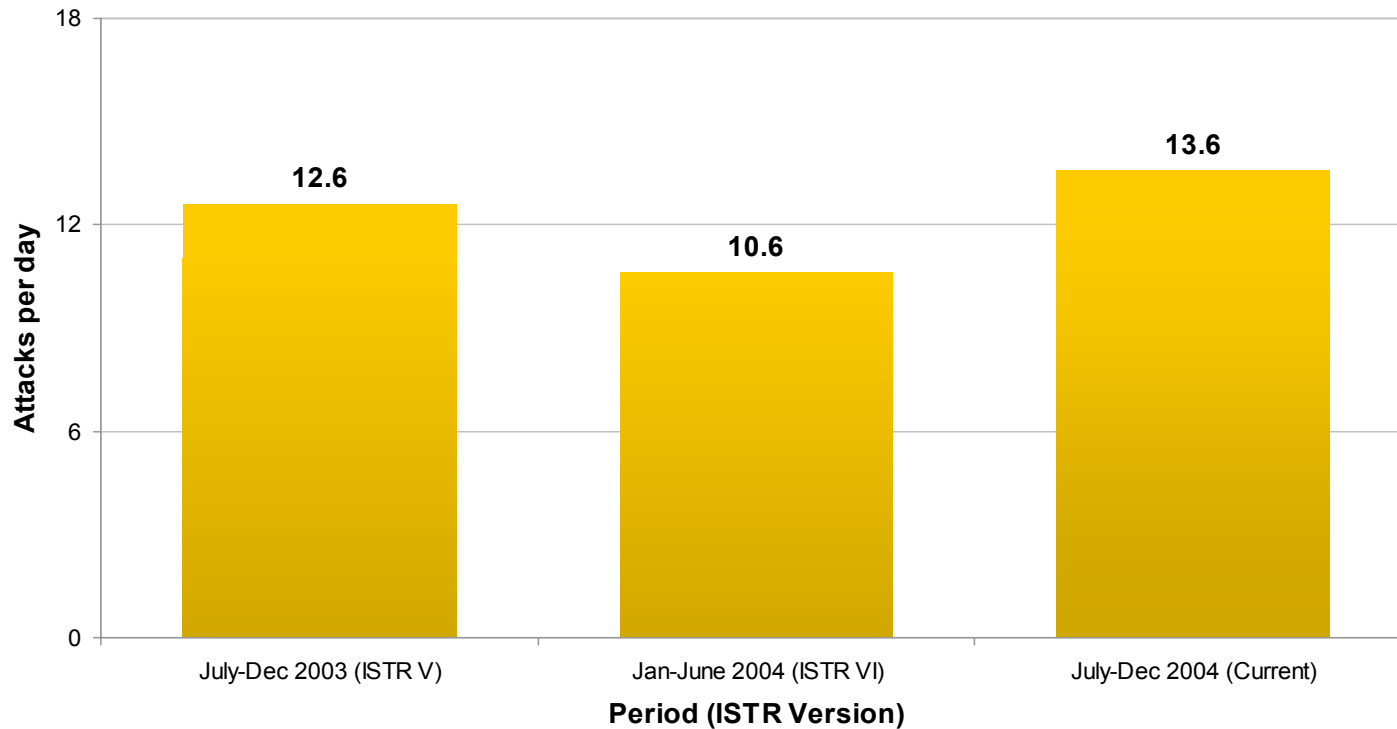
Attack Trends – Top Attacks

- For the 3rd reporting period in a row, the MS SQL Server Resolution Stack Overflow attack remains number 1.
- The Generic TCP Syn Flood Denial of Service Attack is a new entry and is tied to a possible return to an 'older' method of DoS.

Current Rank Jul-Dec 2004	Previous Rank Jan-Jun 2004	Attack	Current Percent of Attackers Jun – Dec 2004	Previous Percent of Attackers Jan – June 2004
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	22%	15%
2	Not Ranked (NR)	Generic TCP Syn Flood Denial of Service Attack	12%	NA
3	10	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	7%	1%
4	6	Generic SMTP Malformed Command/Header Attack	5%	2%
5	2	W32.HLLW.Gaobot Attack	4%	4%
6	NR	Generic Invalid HTTP Version String Attack	4%	NA
7	7	Generic ICMP Flood Attack	3%	2%
8	3	Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack	2%	4%
9	9	Generic HTTP Directory Traversal Attack	2%	1%
10	NR	Generic UTF8 Encoding in URL Attack	2%	NA

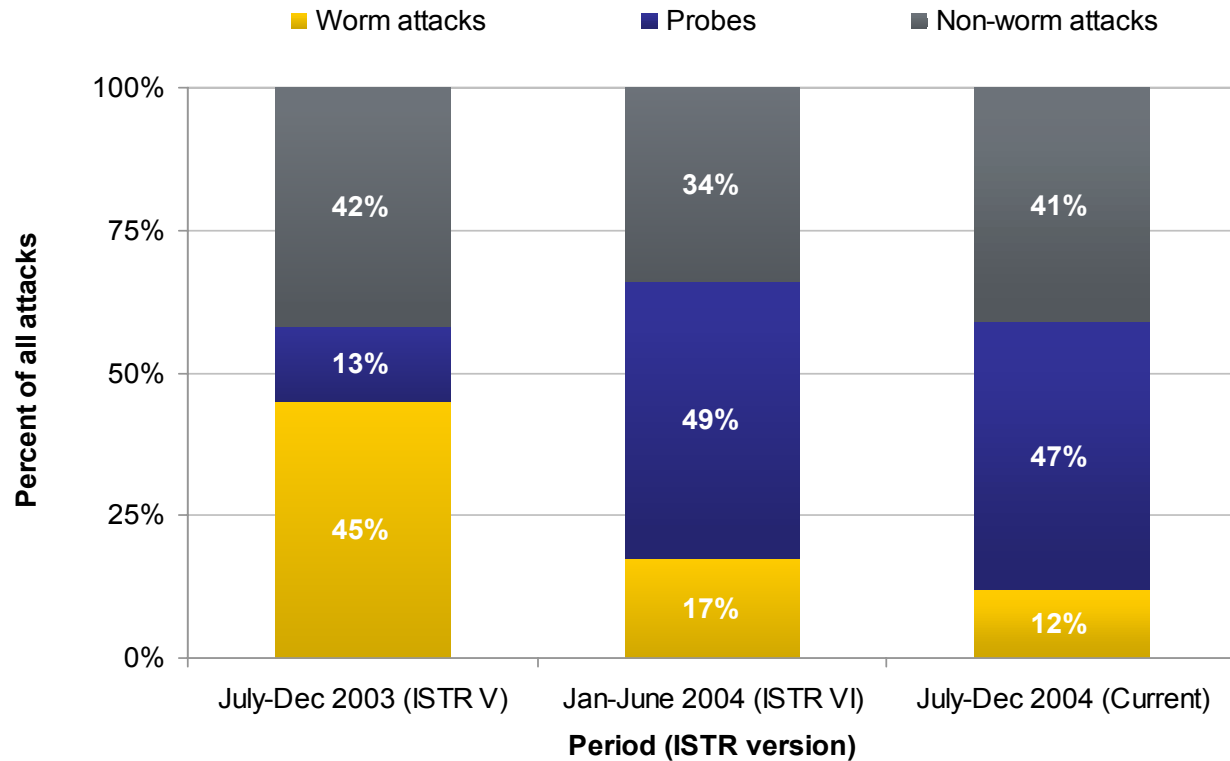
Attack Trends – Daily Attack Rate

- Daily attack rates have risen due to an increase in the volume of probes and non-worm based attacks.



Attack Trends – Attack Type

- Worms attacks continue to decline from a high of 59% in the first half of 2003.
- Probe activity remains high as scanning for back door services on high-level ports increases.



Attack Trends – Top Attacked Ports

Rank Jul-Dec 2004	Rank Jan-Jun 2004	Port	Service Description	Percent of Total Attackers Jul – Dec 2004	Percent of Total Attackers Jan – Jun 2004
1	2	445 TCP	CIFS (Microsoft File Sharing)	35%	17%
2	3	135 TCP	DCE-RPC (Remote Microsoft Windows communication)	17%	15%
3	7	1026 UDP	Various dynamic services	8%	3%
4	4	4662 TCP	Edonkey (File-sharing)	6%	7%
5	NR	1027 UDP	Various dynamic services	5%	NA
6	5	6346 TCP	Gnutella (File sharing)	5%	5%
7	NR	139 TCP	SMB (Microsoft File Sharing)	4%	NA
8	10	1025 TCP	Various Backdoors and dynamic services	2%	3%
9	NR	1434 UDP	Microsoft SQL Services	2%	NA
10	NR	25 TCP	SMTP Services	2%	NA

Attack Trends – Top Source Countries

Current Rank	Jan-June 2004 Rank	Country	Current percent of events	Jan-June 2004 percent of events
1	1	United States	30%	37%
2	2	China	8%	6%
3	5	Germany	8%	5%
4	9	South Korea	4%	3%
5	3	Canada	4%	6%
6	6	Great Britain	4%	4%
7	7	France	3%	4%
8	NR	Japan	3%	NA
9	8	Spain	3%	3%
10	NR	Italy	2%	NA

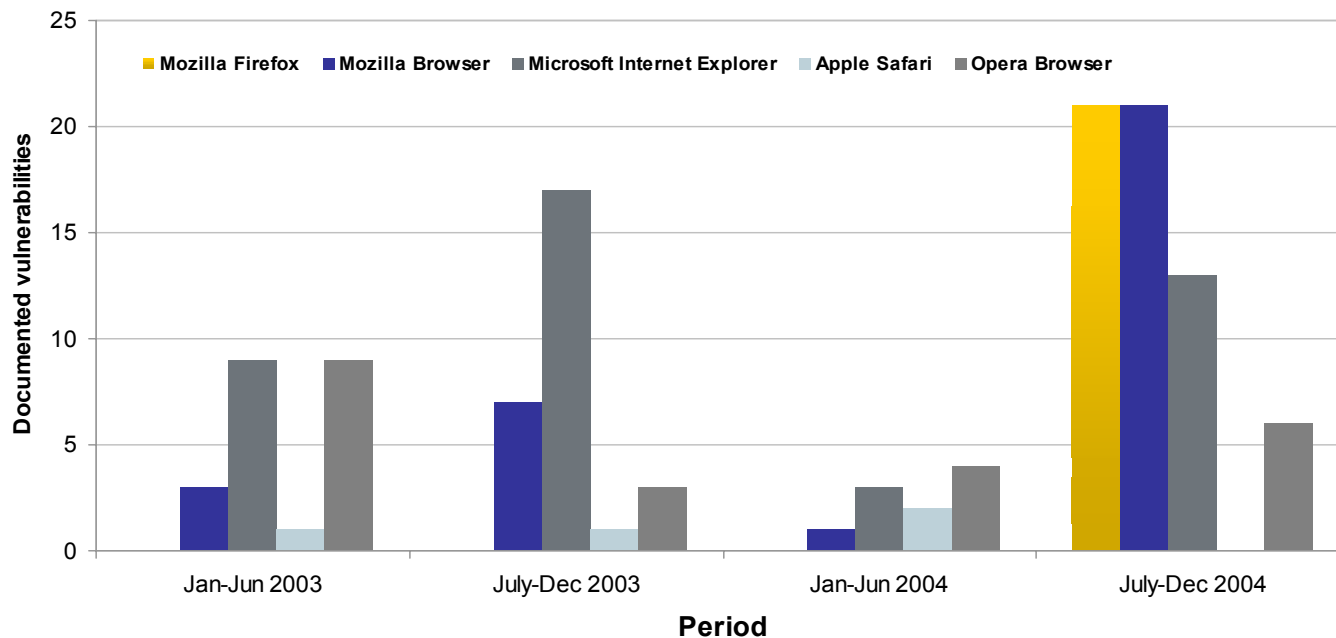


Vulnerability Trends



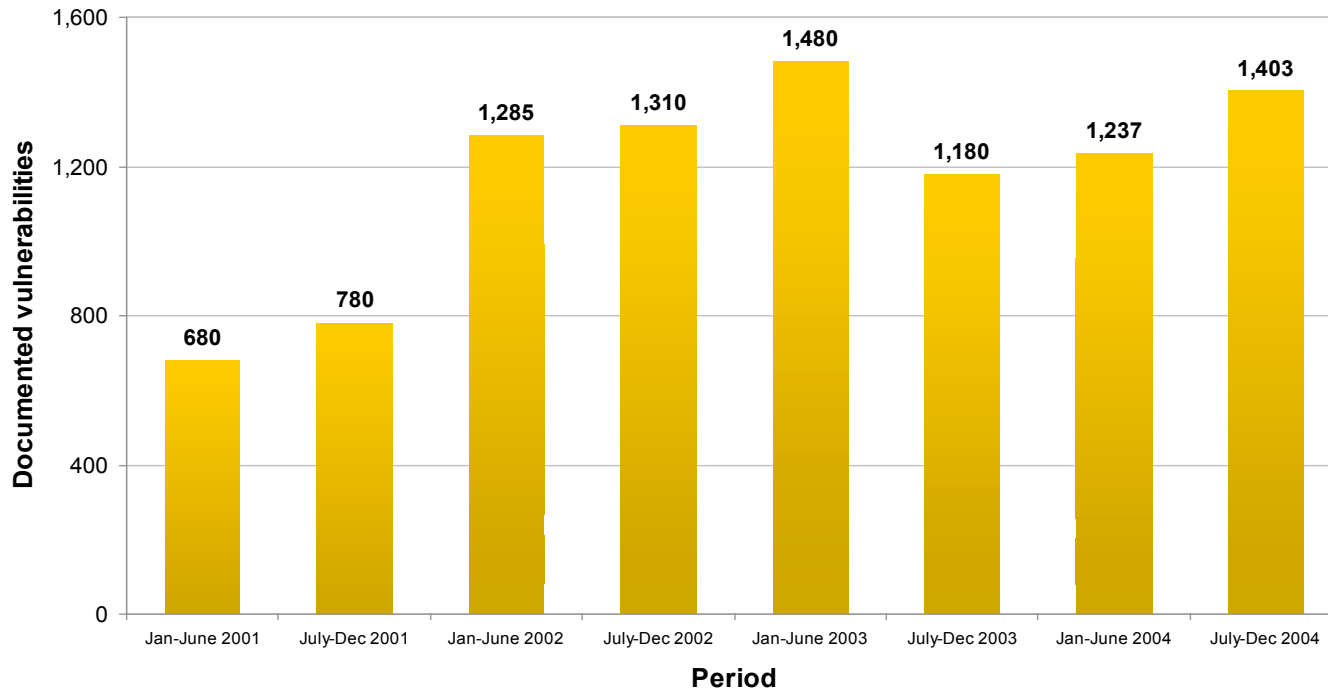
Vulnerability Trends – Web Browsers

- During the current reporting period, Symantec documented 13 vulnerabilities affecting IE and 21 in the Mozilla browsers (Firefox and Mozilla)
- 9 of the 13 IE vulnerabilities were high severity (69%) as compared to 11 of the 21 Mozilla vulnerabilities (52%).



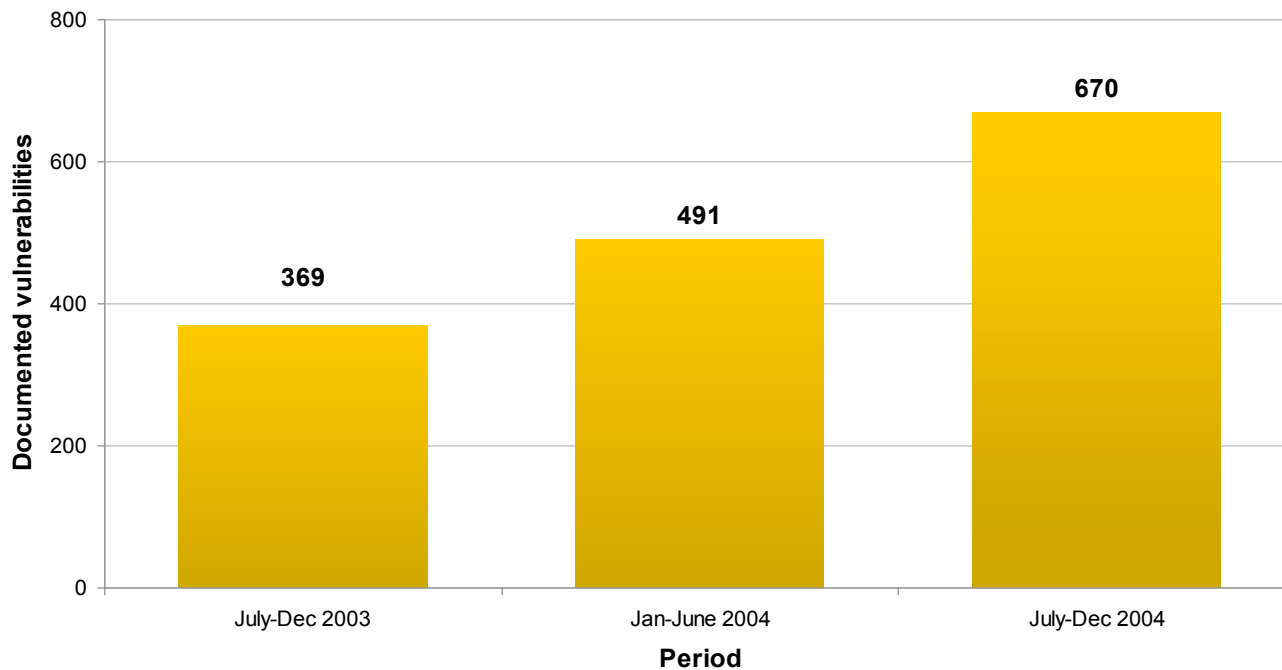
Vulnerability Trends – Total Volume

- Between July 1st and December 31st, 2004 the total number of vulnerabilities grew by 13% over the previous reporting period and is the 3rd consecutive period in which the number of vulnerabilities has increased.



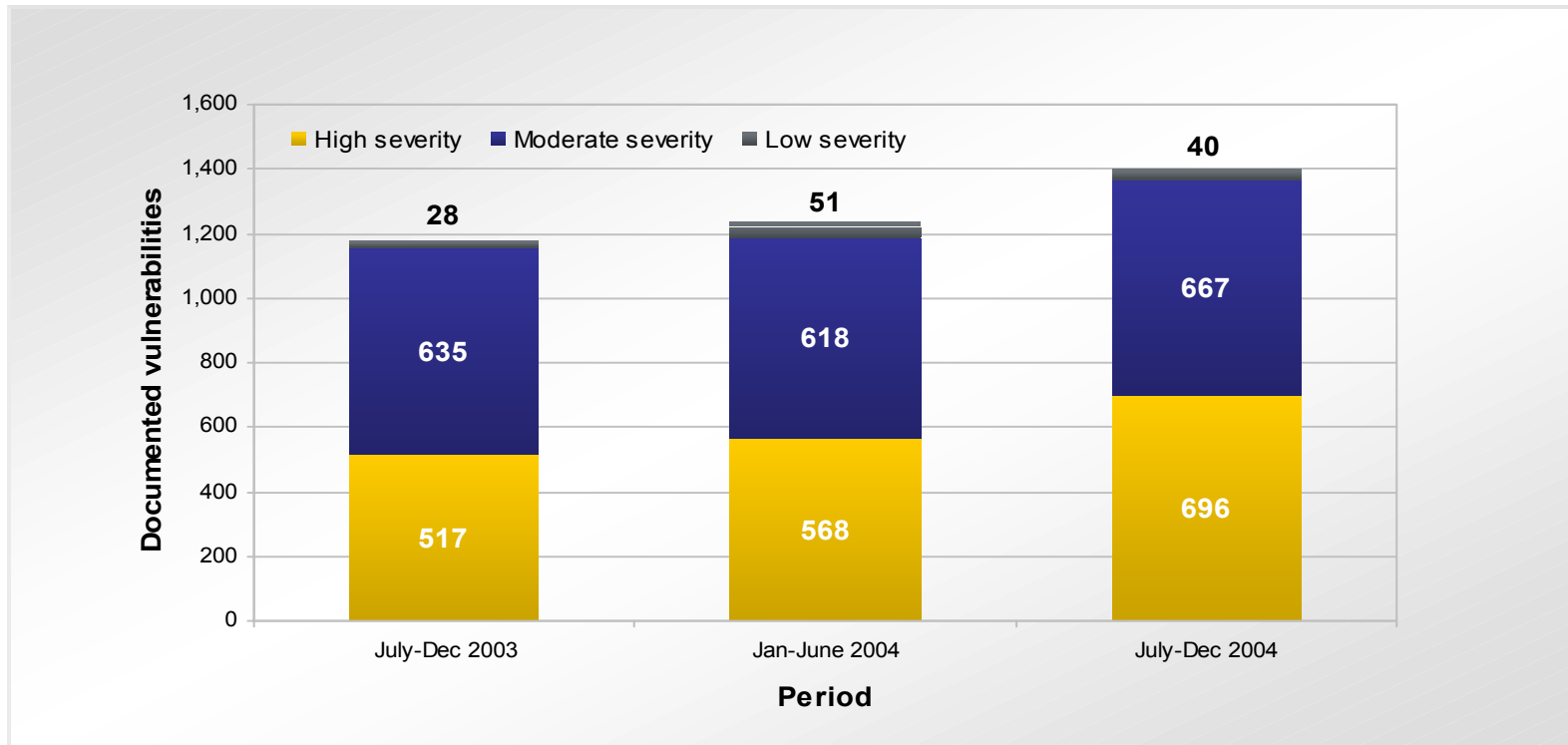
Vulnerability Trends – Web Applications

- 48% of the total number of vulnerabilities disclosed between July 1st and December 31st, 2004 were Web Application vulnerabilities. This is a 16 point increase over the same reporting period in 2003.



Vulnerability Trends - Severity

- High severity vulnerabilities continue to rise representing nearly 50% of the total number of vulnerabilities. When combined with medium severity vulnerabilities, over 97% of the total number of vulnerabilities discovered in this period result in a partial or complete compromise.

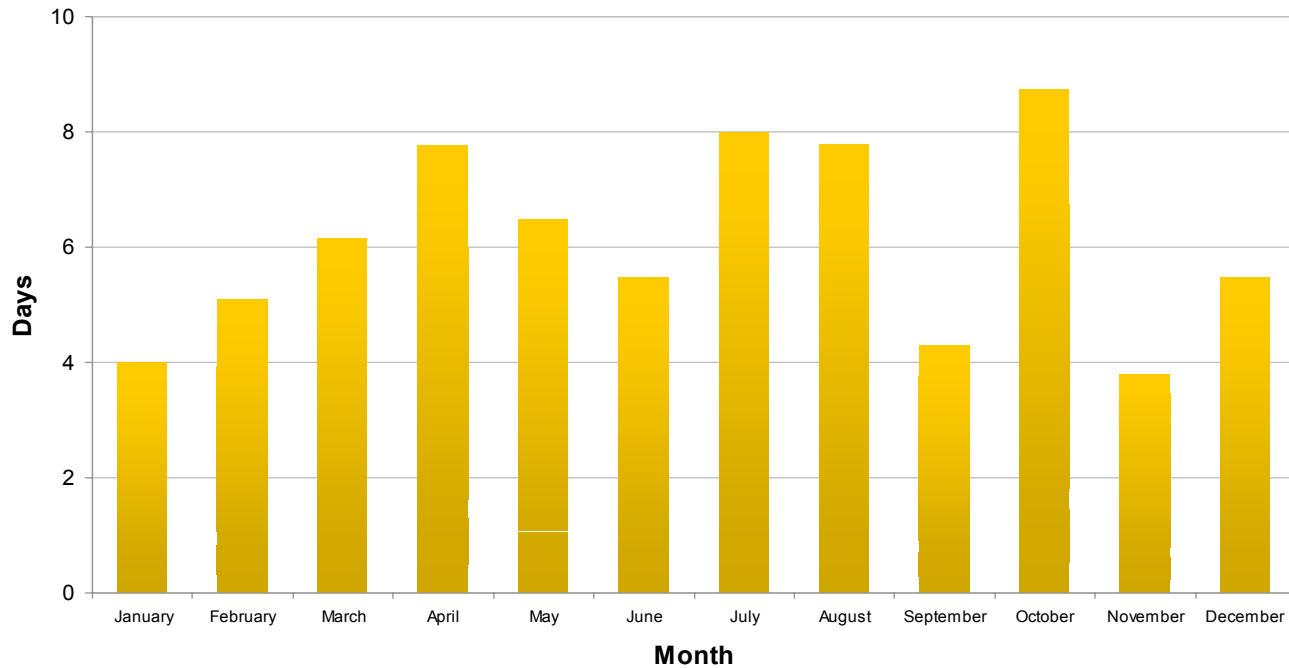


Source: Symantec Corporation



Vulnerability Trends – Exploit Development Time

- Between July 1st and December 31st 2004, the average time between the disclosure of a vulnerability and the publication of its associated exploit was 6.4 days. This represents an increase of less than one day over the previous reporting period.



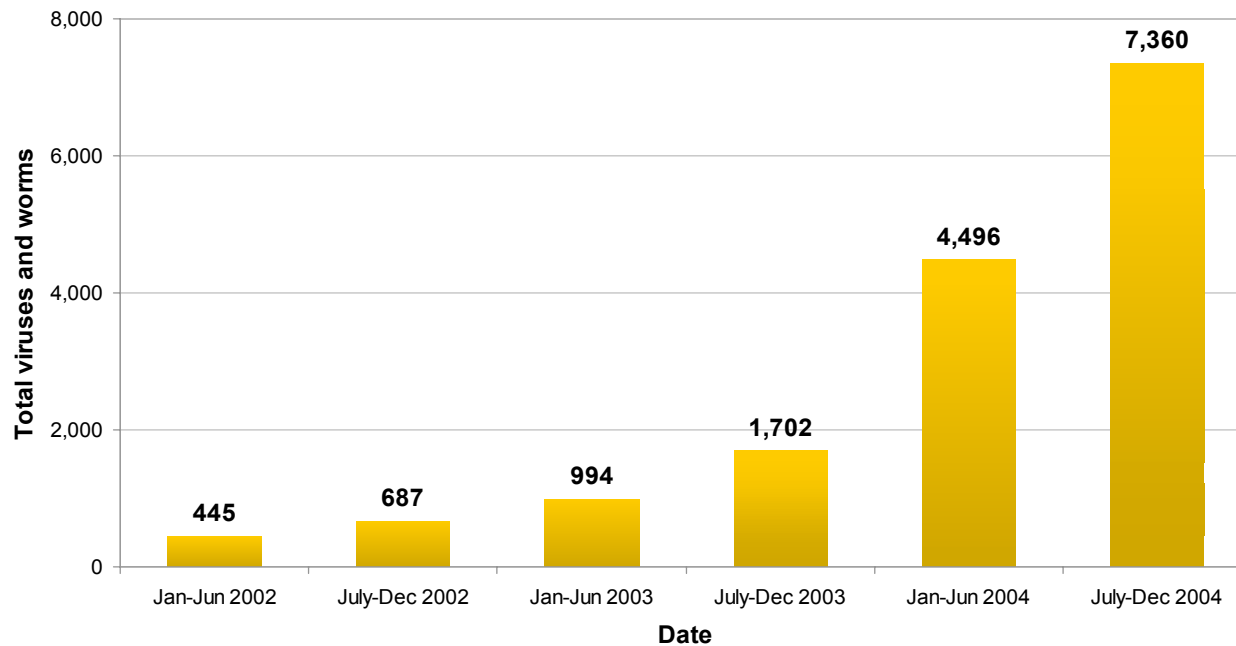


Malicious Code Trends



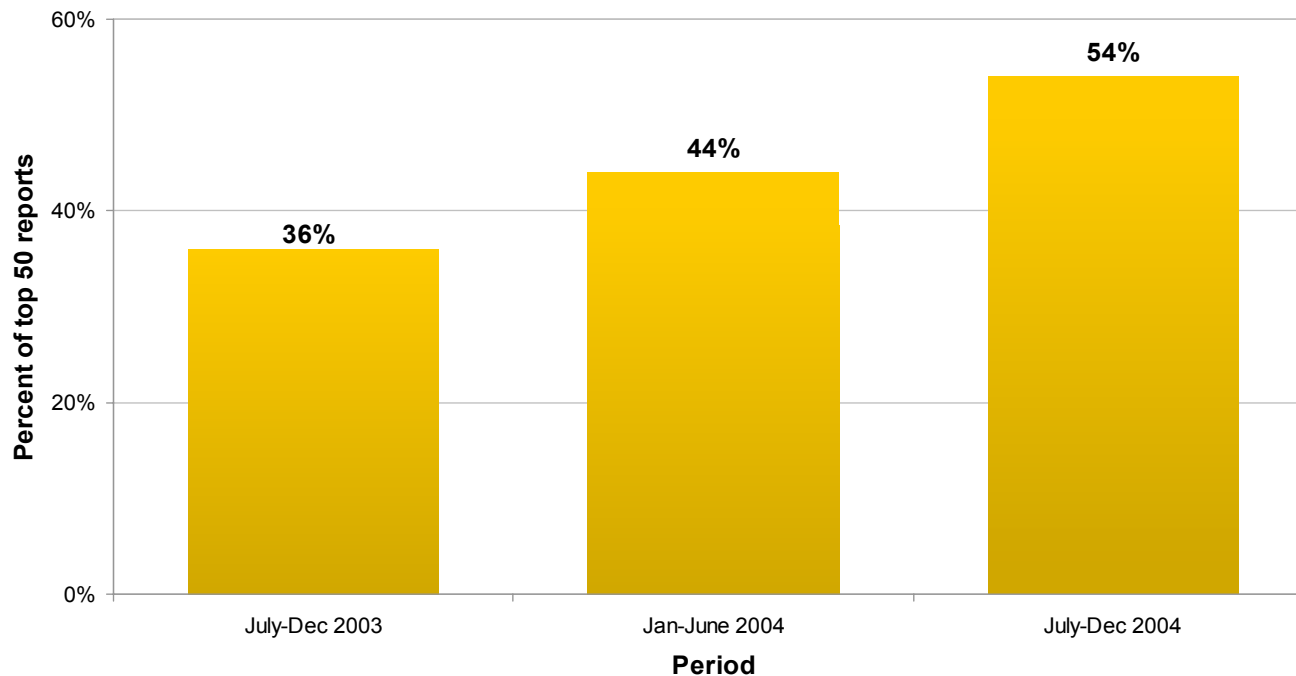
Malicious Code Trends – Win32 Variants

- During the current reporting period more than 7,360 new virus and worm variants were discovered representing a 64% increase over the previous reporting period and a 332% increase over the same period last year.
- As of December 31st, 2004 the total number of Win32 variants is approaching 17,500.



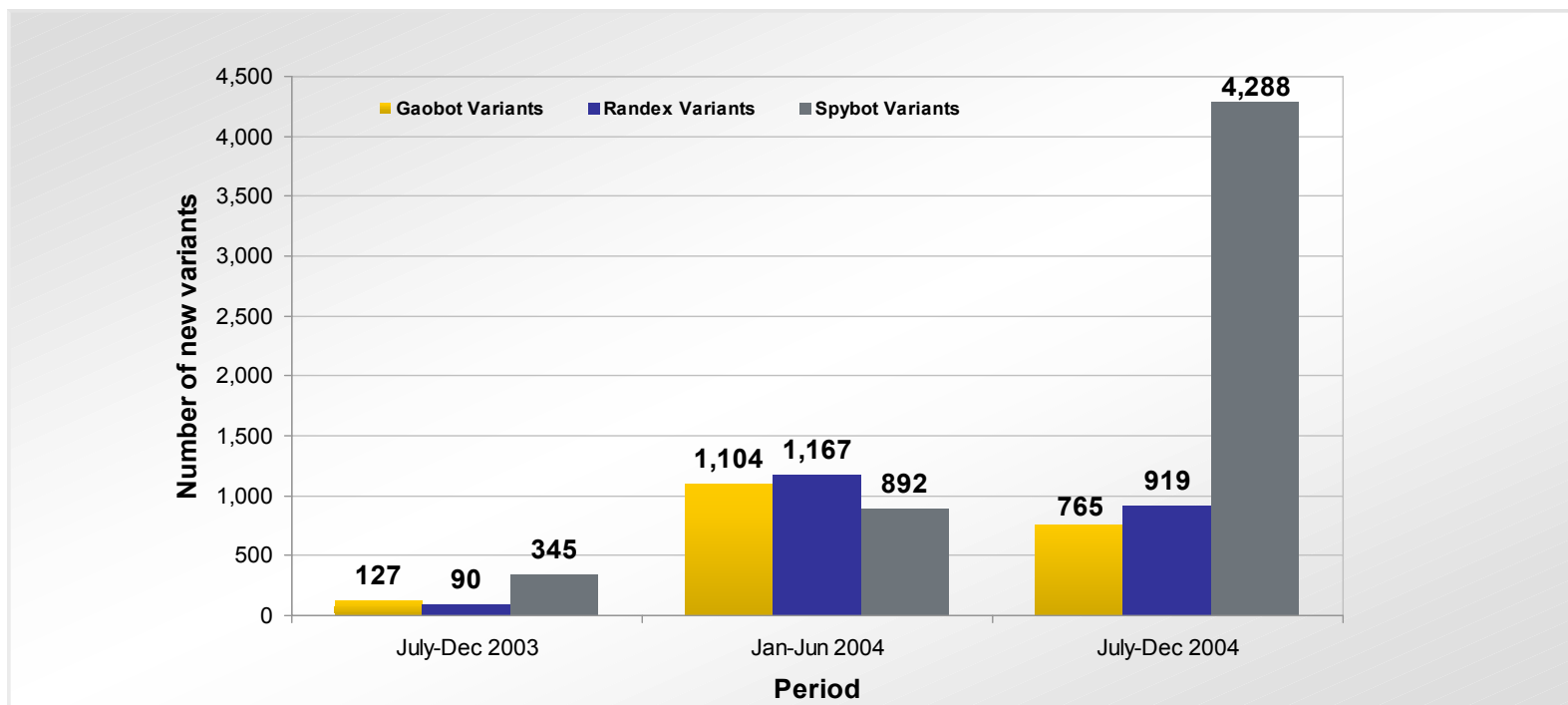
Malicious Code Trends – Confidential Information

- Threats to confidential information continue to increase with 54% of the Top 50 reported malicious code having the potential to expose confidential information.



Malicious Code Trends – Bot Variants

- With close to 4300 new variants between July 1st and December 31st, 2004, Spybot variants have increased by 180% over the previous reporting period.
- Randex, Gaobot and Spybot represent a combined total of close to 6,000 new bot variants, a 189% increase over the previous reporting period.



Source: Symantec Corporation

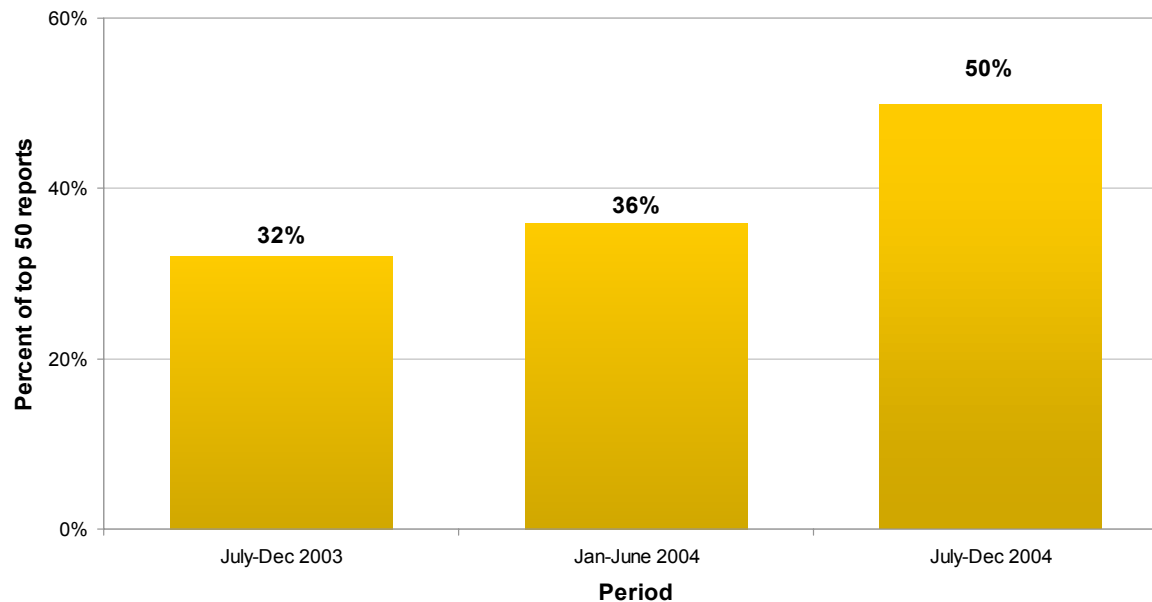
Malicious Code Trends – Top 10 Reports

- Mass-mailing worms dominated the top malicious code reported to Symantec over the last six months of 2004. Eight of the top ten samples reported to Symantec during this period were variants of mass-mailer worms that have been seen in previous reports: Netsky, Sober, Beagle, and MyDoom.

Rank	Sample
1	Netsky.P
2	Sober.I
3	Gaobot
4	Spybot
5	Beagle.AV
6	Beagle.X
7	Mydoom.M
8	Netsky.Z
9	Netsky.D
10	Beagle.AW

Malicious Code Trends – P2P/IM/IRC/CIFS

- The number of threats using P2P, IM, IRC, and CIFS within Symantec's top 50 malicious code reports has increased by 39% over the previous six-month period and currently represent 50% of the Top 50 Threats reported to Symantec.
- Variants of Netsky, Beagle and Mydoom continue to be predominant threats during the current reporting period and all use P2P to spread.



ASR Trends – Top Adware

- The top reported adware program between July 1st and December 31st 2004 – Iefeats – accounted for 36% of the Top 10 reported Adware.
- Adware currently represents 5% of the Top 50 malicious code reported to Symantec.

Rank	Adware Name
1	Iefeats
2	InstantAccess
3	Gator
4	Istbar
5	VirtuMonde
6	Binet
7	CDT
8	MainSearch
9	180Search
10	NetOptimizer

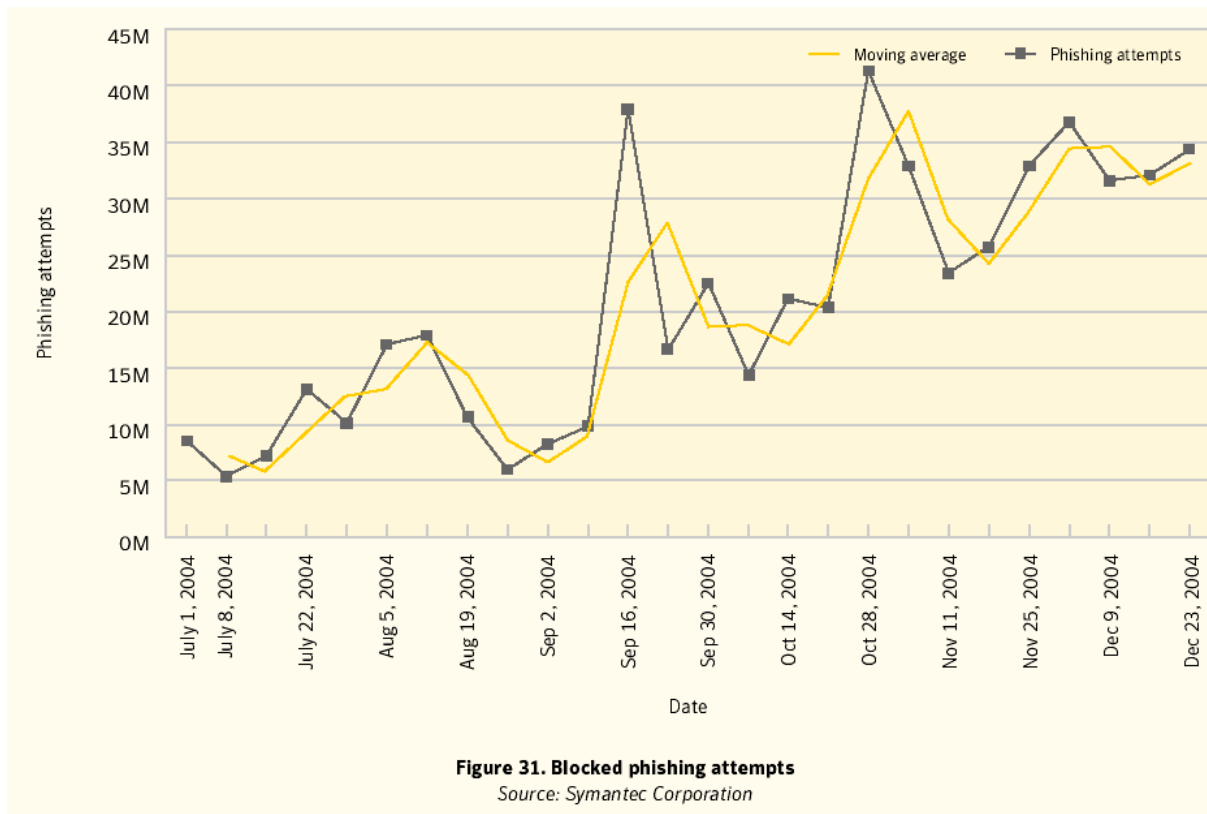
ASR Trends – Top Spyware

- The top reported Spyware program between July 1st and December 31st 2004 – Webhancer – accounted for 38% of the Top 10 reported Spyware.
- The top two reported Spyware account for 68% of the Top 10 reported Spyware.

Rank	Spyware Name
1	Webhancer
2	E2give
3	Apropos
4	Look2Me
5	2020search
6	Dotcomtoolbar
7	Iwantsearch
8	ClientMan
9	Perfect
10	Shopnav

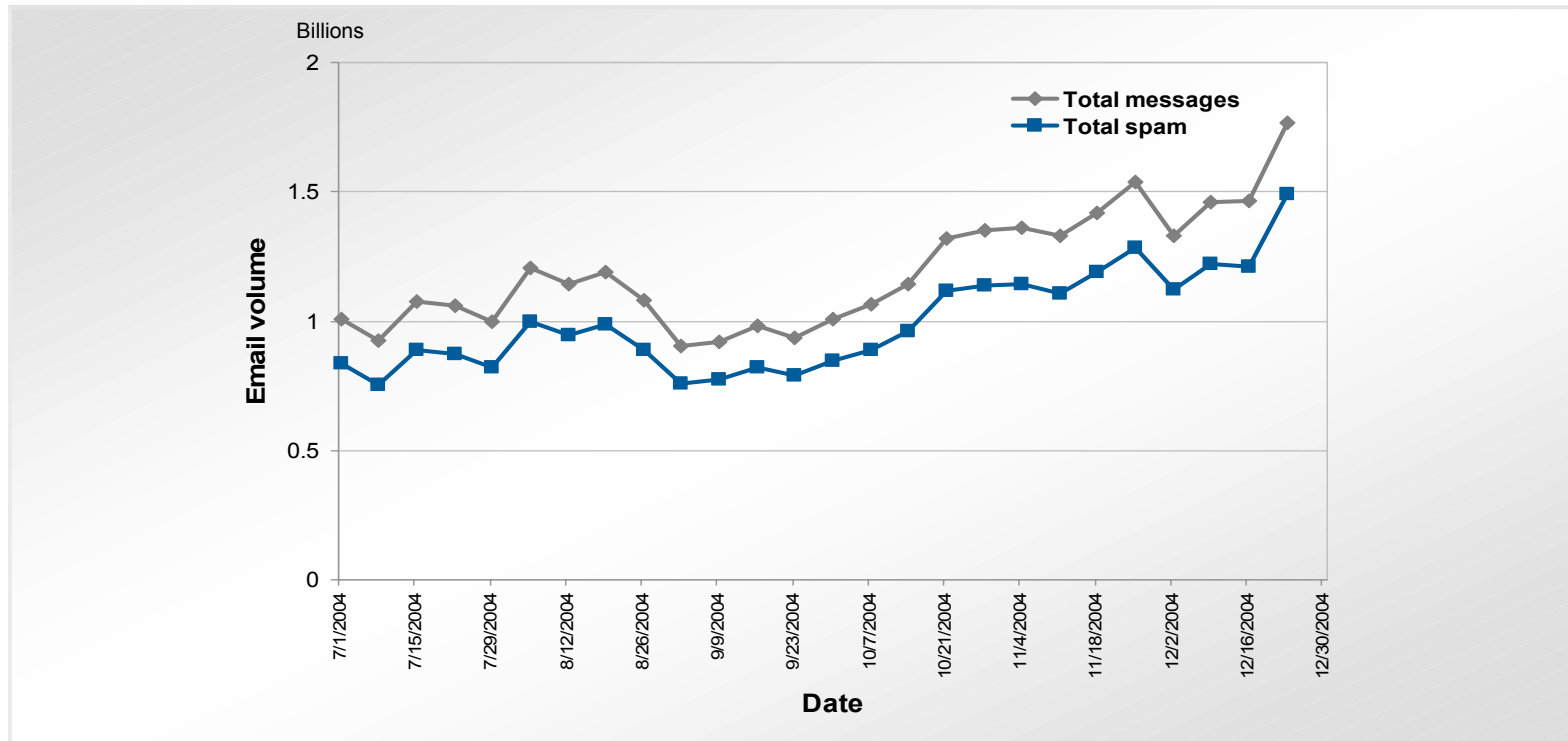
ASR Trends - Phishing Volume

- Between July 1st and December 31st 2004, Phishing emails increased from 9 million per week to 33 million per week over the last half of 2004.



ASR Trends - Spam Growth

- Over 60% of all email traffic between July 1st and December 31st 2004 was considered Spam.
- There was a 77% growth in the amount of Spam that Symantec saw in the companies it monitored.
- Weekly Spam increased from 800 million messages per week to well over 1.2 billion



Source: Symantec Corporation

Quick Hits – Additional Statistics

- **Mobile Malicious Code** - During the current reporting period there were 21 known samples of malicious code for mobile applications, up from one in the previous reporting period.
- **Anti-Fraud Filters** – By the end of the current reporting period, Symantec Anti-Fraud filters were blocking over 33 million phishing attempts per week. This is up from the approximate 9 million per week in the beginning of July 2004.
- **Adware\Spyware** – 5 of the Top 10 reported Adware samples were installed via a web browser and 9 of the Top 10 reported Spyware programs were bundled with other software.
- **Regional Statistics:**
 - **APAC** – Beijing is the top bot city. Netsky.P is top malicious code sample. The Generic Malformed HTTP Message Header Attack is the top attack.
 - **EMEA** – London is the top bot city. Netsky.P is the top malicious code sample. The SQLExp Incoming worm attack is the top attack.
 - **Japan** - Tokyo is the top bot city. Netsky.P is the top malicious code sample. The Microsoft Windows LSASS Buffer Overrun attack is the top attack.
 - **LAM** – Sao Paulo is the top bot city. Gaobot is the top malicious code sample. The Microsoft SQL Server 2000 Resolution Service Stack Overflow attack is the top attack.
 - **NAM** – Los Angeles is the top bot city. Netsky.P is the top malicious code sample. The Microsoft SQL Server 2000 Resolution Service Stack Overflow attack is the top attack.



Future Watch



Future Watch

- ▶ **Viruses and Worms targeting Client Side exploits** are expected to increase over the next six months to a year.
- ▶ **Bots and Bot Networks being used for financial gain.** In conjunction with more sophisticated phishing and malicious code attacks Symantec expects to see an increase in the number of reports of bots and bot networks being used for financial gain.
- ▶ **More damaging mobile device malicious code** is expected to appear over the next six months. The release of the Cabir worm source code in December is an indication of things to come.
- ▶ **Emerging security concerns for Mac OS.** Over the past year Symantec documented 37 high-severity vulnerabilities in Mac OS X.
- ▶ **Embedded malicious code in Audio and Video images.** In September Microsoft announced a vulnerability in its implementation of the JFIF image file format that could potentially allow images files displayed on a host system to execute malicious code.

Best Practices -- Enterprise

- ▶ Turn off and remove unneeded services.
- ▶ If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- ▶ Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- ▶ Enforce a password policy.
- ▶ Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
- ▶ Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
- ▶ Train employees to not open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- ▶ Ensure emergency response procedures are in place.
- ▶ Educate management on security budgeting needs.
- ▶ Test security to ensure adequate controls are in place.
- ▶ Both spyware and adware can be automatically installed on systems along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links or attachments in e-mail messages, or via instant messaging clients. Ensure that only applications approved by your organization are deployed on the desktop.

Best Practices -- Consumer

- ▶ Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against blended threats.
- ▶ Ensure that security patches are up-to-date.
- ▶ Ensure that passwords are a mix of letters and numbers. Do not use dictionary words. Change passwords often.
- ▶ Never view, open or execute any e-mail attachment unless the purpose of the attachment is known.
- ▶ Keep virus definitions updated. By deploying the latest virus definitions, corporations and consumers are protected against the latest viruses known to be spreading “in the wild.”
- ▶ Consumers should routinely check to see if their PC or Macintosh system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- ▶ All types of computer users need to know how to recognize computer hoaxes and phishing scams. Hoaxes typically include a bogus email warning to “send this to everyone you know” and improper technical jargon to frighten or mislead users. Phishing scams are much more sophisticated. Often arriving in email, phishing scams appear to come from a legitimate organization. They attempt to entice users to enter credit card or other confidential information into forms on Web site that mimic the legitimate organization’s Web site. Consumers and business professionals also need to consider who is sending the information and determine if it is a reliable source. The best course of action is to simply delete these types of emails.
- ▶ Consumers can get involved in fighting cyber crime by tracking and reporting intruders. With Symantec Security Check’s tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker’s Internet Service Provider or local police.
- ▶ Be aware of the differences between spyware and adware. Spyware has been used to make malicious attacks and further identity theft, while adware is often used to gather data for marketing purposes and has a valid, generally benign purpose.
- ▶ Both spyware and adware can be automatically installed on your system along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links or attachments in e-mail messages, or via instant messaging clients. Therefore, be informed and selective about what you install on your computer.
- ▶ Don’t just click those “Yes, I accept” buttons on end user licensing agreements (EULAs). Some spyware and adware applications can be installed after, or as a by-product of accepting the EULA. Read them carefully to examine what it means in terms of privacy. The agreement should clearly explain what the product is doing and provide an uninstaller.
- ▶ Beware of programs that flash ads in the user interface. Many spyware programs track how you respond to these ads, and their presence is a red flag. When you see ads in a program’s user interface, you may be looking at a piece of spyware.



Thank you!

Questions?

