The Laws of Vulnerabilities

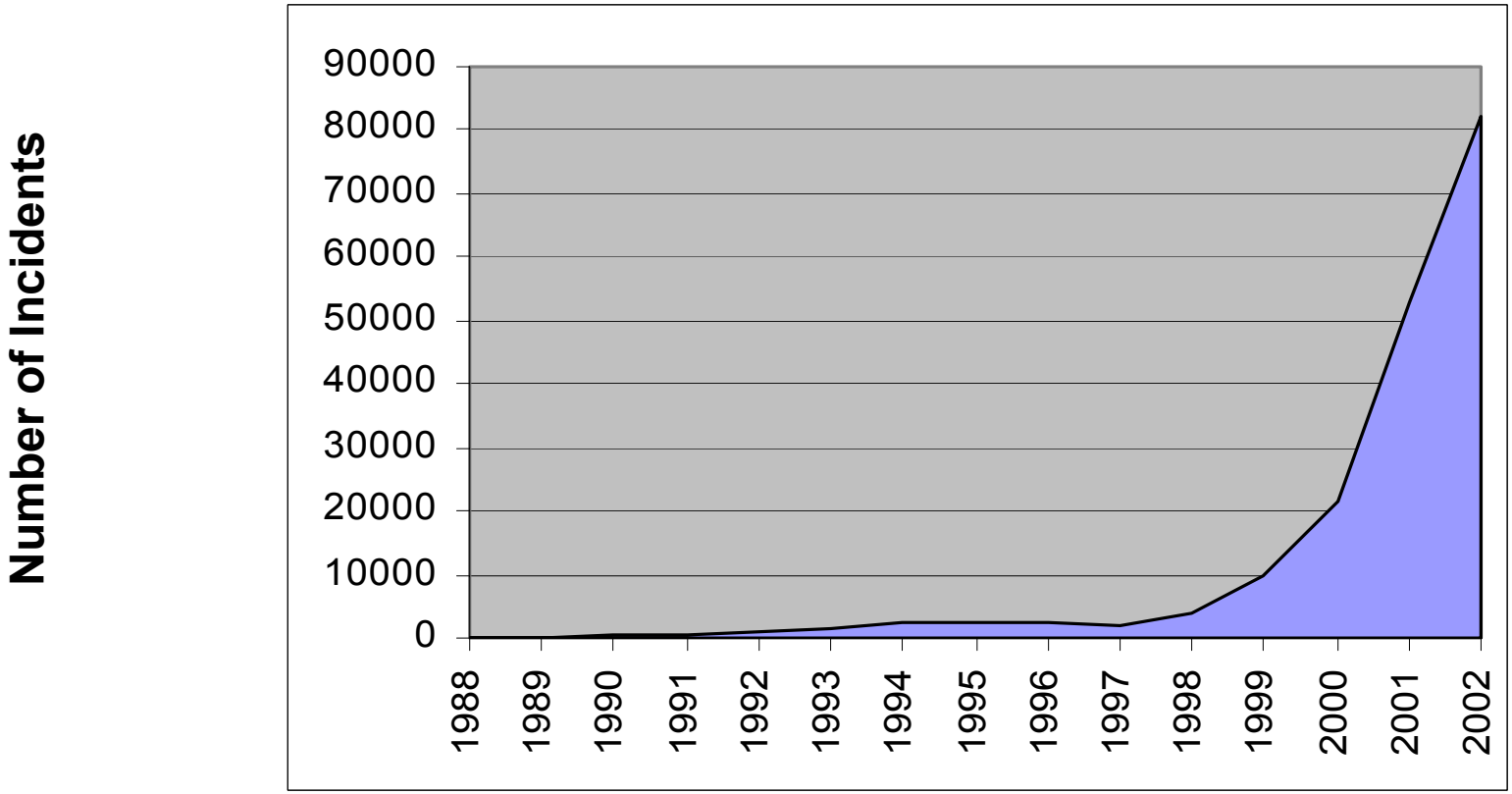
Gerhard Eschelbeck
CTO & VP Engineering, Qualys

September 24, 2003

The worm.sdsc.edu Project

- Experiment: Attaching and monitoring a “default installed” system on the Internet
- Within 8 hours first probe for rpc vulnerabilities was detected
- Within a few days over 20 exploit attempts
- Within a few weeks the system was completely compromised and a network sniffer was installed by an attacker

Security Incidents Trend



Source: CERT, Carnegie Mellon University

Exploiting Systems is Getting Easier

- **Weakening Perimeters**
  - Multiple entry points
  - Wireless and VPN connectivity points
- **Increasing complexity of networks and applications**
  - Thousands of exploitable vulnerabilities
  - Shortage of qualified security staff
- **Increasing sophistication of attacks**
  - Simple and automated attack tools
  - Designed for large scale attacks
  - Attack sources hard to trace

First Generation Threats

- Spreading mostly via email, file-sharing
- Human Action Required
- Virus-type spreading / No vulnerabilities
- Examples: Melissa Macro Virus, LoveLetter VBScript Worm
- Replicates to other recipients
- Discovery/Removal: Antivirus

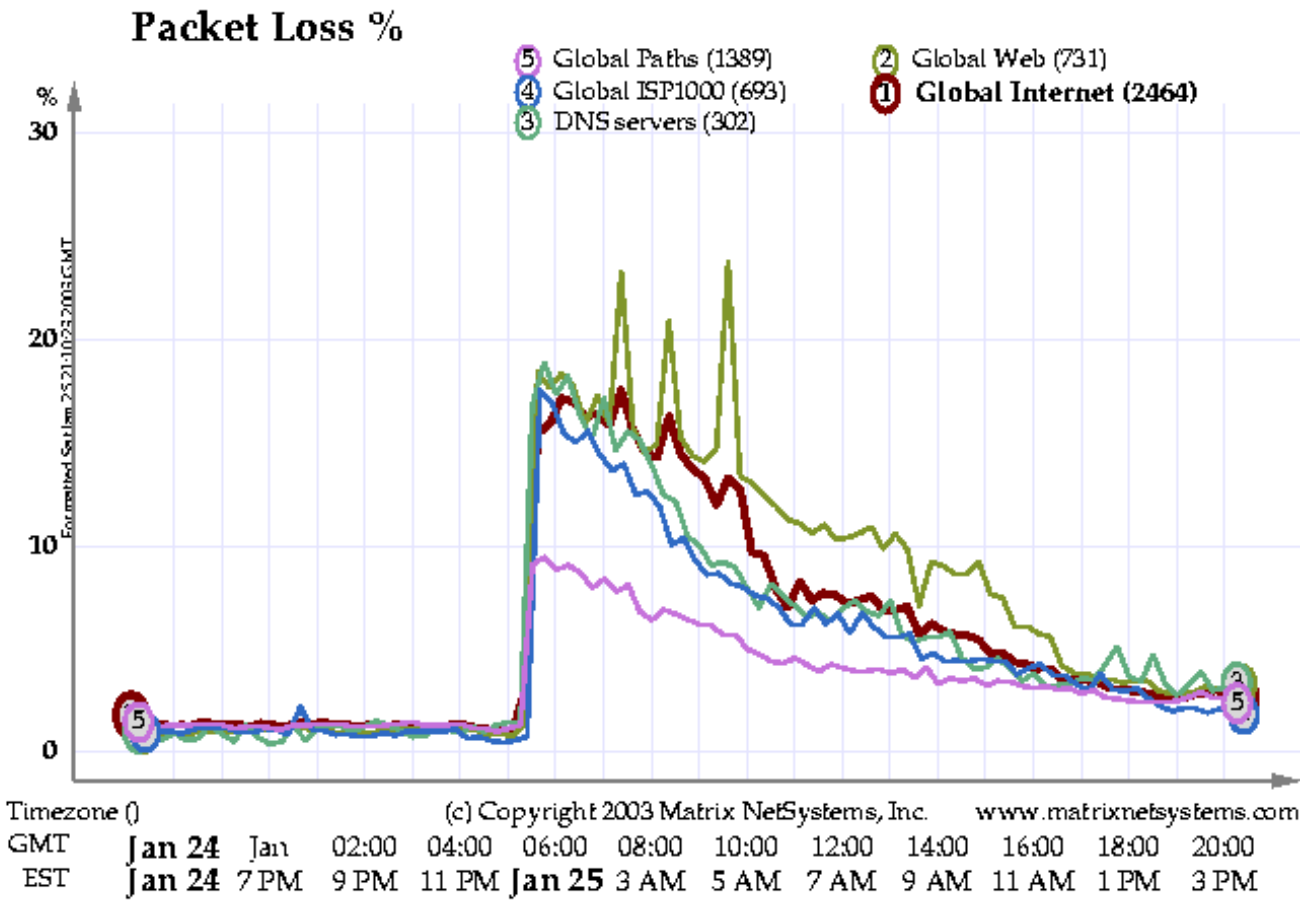
What happened since then ?

- Security flaws in all relevant software packages
- 25 new vulnerabilities per week
- Internet Explorer: ~100 vulnerabilities
- 802.11 wireless security broken
- Successful attacks against the Internet root DNS servers
- Popularity of the “Port 80 Loophole”
- Major worm outbreaks

Second Generation Threats

- Active worms
- Leveraging known vulnerabilities
- Low level of sophistication in spreading strategy (i.e. randomly)
- Non Destructive Payloads
- Blended threats (consists of virus, trojan, exploits vulnerabilities, automation)
- System and Application level attacks
- Remedy: Identify and Fix Vulnerabilities

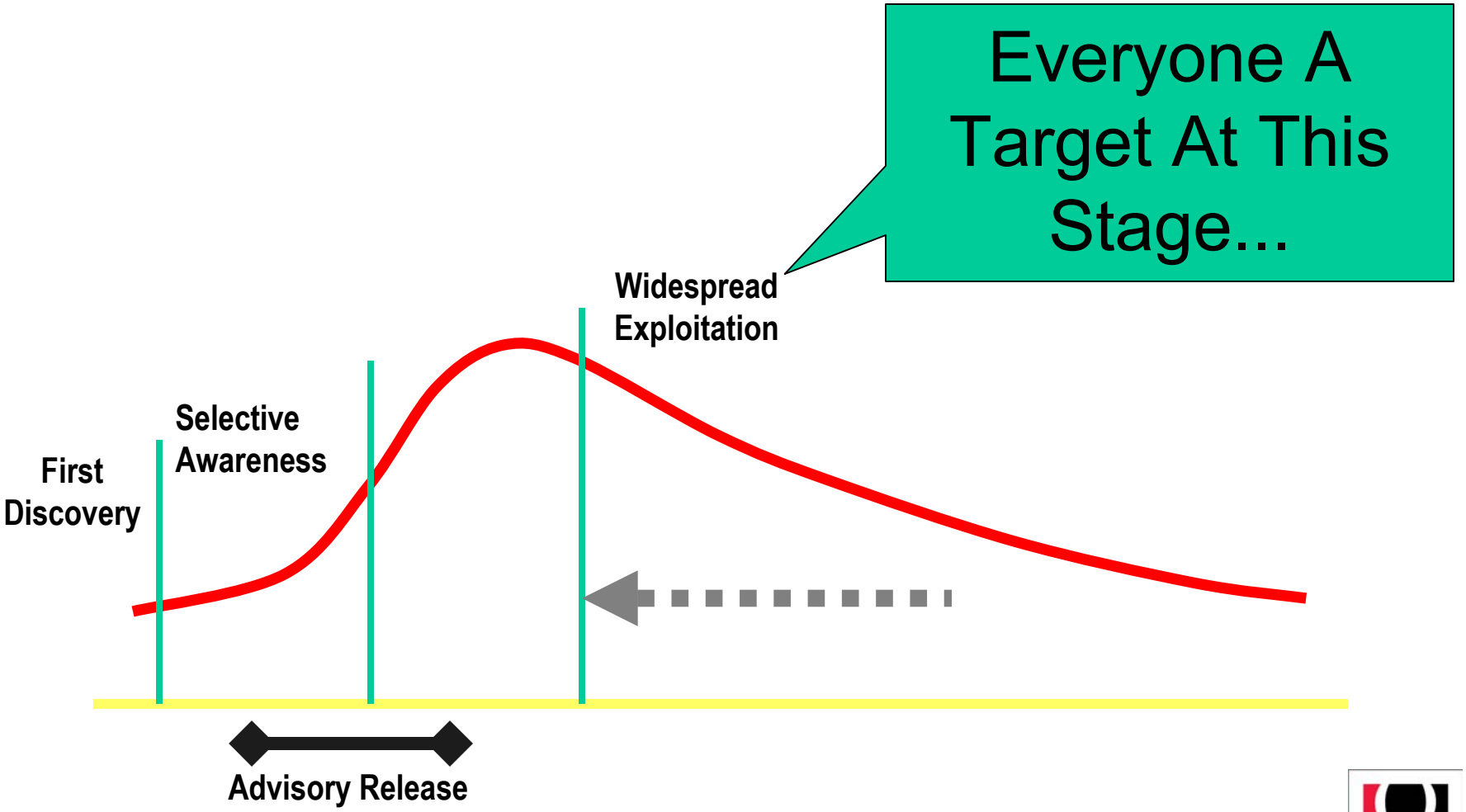
Windows Vulnerabilities in Action:
The Outbreak of the SQL Slammer Worm



What's Next ?

- Improved speed and strategy to identify new vulnerable targets
- Popularity of the exploited system/application/platform
- Affecting New Technologies/Applications
- Shortening Vulnerability/Exploit Life-Cycle

Vulnerability and Exploit Lifecycle



Third Generation (Future) Threats

- Leveraging known and unknown vulnerabilities
- Precompiled list of initial victims to provide aggressive growth
- Active Payloads
- Leveraging polymorphic techniques and encryption to prevent discovery
- Multiple attack vectors
- Impact on new Technologies (Instant Messaging, Web Services, Wireless Networks,..)

Accessing a User's Clipboard

Qualys Browser Checkup - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://browsercheck.qualys.com/vuln/index.php?vulnid=1

My 'Clipboard Reading' Hack

Let's try it now...

What is a Clipboard Reading Hack?

Test Instructions:

Click Read Clipboard to start the clipboard reading test. Make sure your clipboard is not empty. To do so, select some text and hit "CTRL-C" to copy the text to your clipboard.

Read Clipboard

My Browser Hacks:

- Cookie Disclosure
- Clipboard Reading
- Program Execution
- File Execution
- Web Page Spoofing
- Security Zone Spoofing
- Hard Drive Access

Back | Next

Send to a friend | Securing Your Network

Results - Microsoft I...

qualys

CAUTION

mySecretPassword

Read Here:

If text appears in the text box above, then you are vulnerable. If an empty text box appears, make sure your clipboard is not empty. To do so, select some text and hit "CTRL-C" to copy the text to your clipboard and then retry the test.

TRICK INFO

HOW TO FIX IT

CLOSE WINDOW

Internet

Firewalls and IDS are not protecting

- **Enforcement (Firewalls)**
  - Structuring at the network level – building security zones
  - limited visibility at application level
  - Mostly static in decision making
- **Secure Transport (VPN)**
  - Expanding corporate networks into the Internet
- **Monitoring (IDS)**
  - Limited scope of data for decision making
  - Massive amounts of log/report information
  - Mostly reactive

What is Missing?

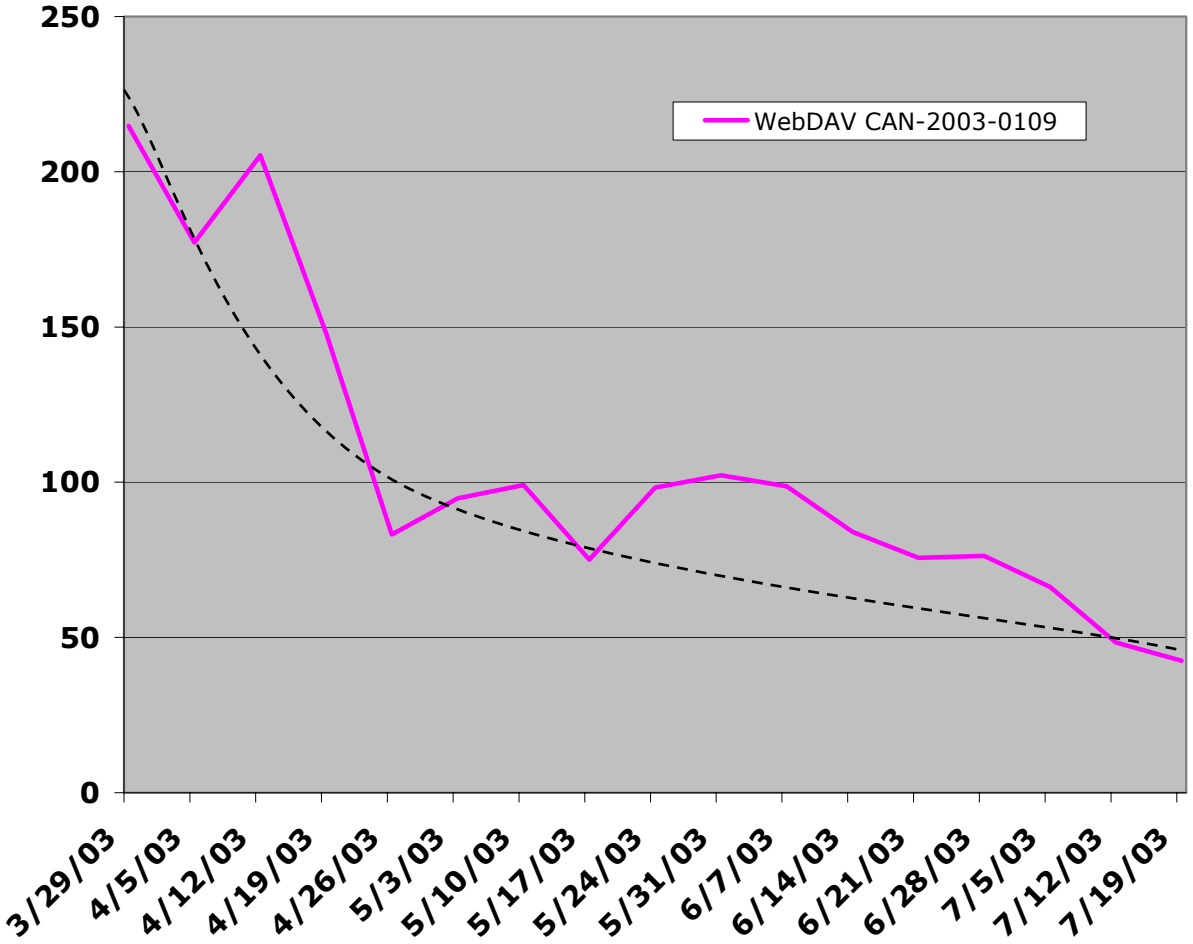
"99% of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available"

Source: CERT, Carnegie Mellon University

Research

- **Understanding prevalence, window of exposure and lifespan of vulnerabilities in real world**
- **Timeframe: January 2002 - Ongoing**
- **Methodology: Automatic Data collection with statistical data only – no possible correlation to user or systems**
- **Largest collection of real-world vulnerability data:**
  - 1,504,000 IP-Scans
  - 1,240,000 total critical vulnerabilities
  - 2,041 unique vulnerabilities
  - 1,175 unique critical vulnerabilities

Microsoft WebDAV Vulnerability

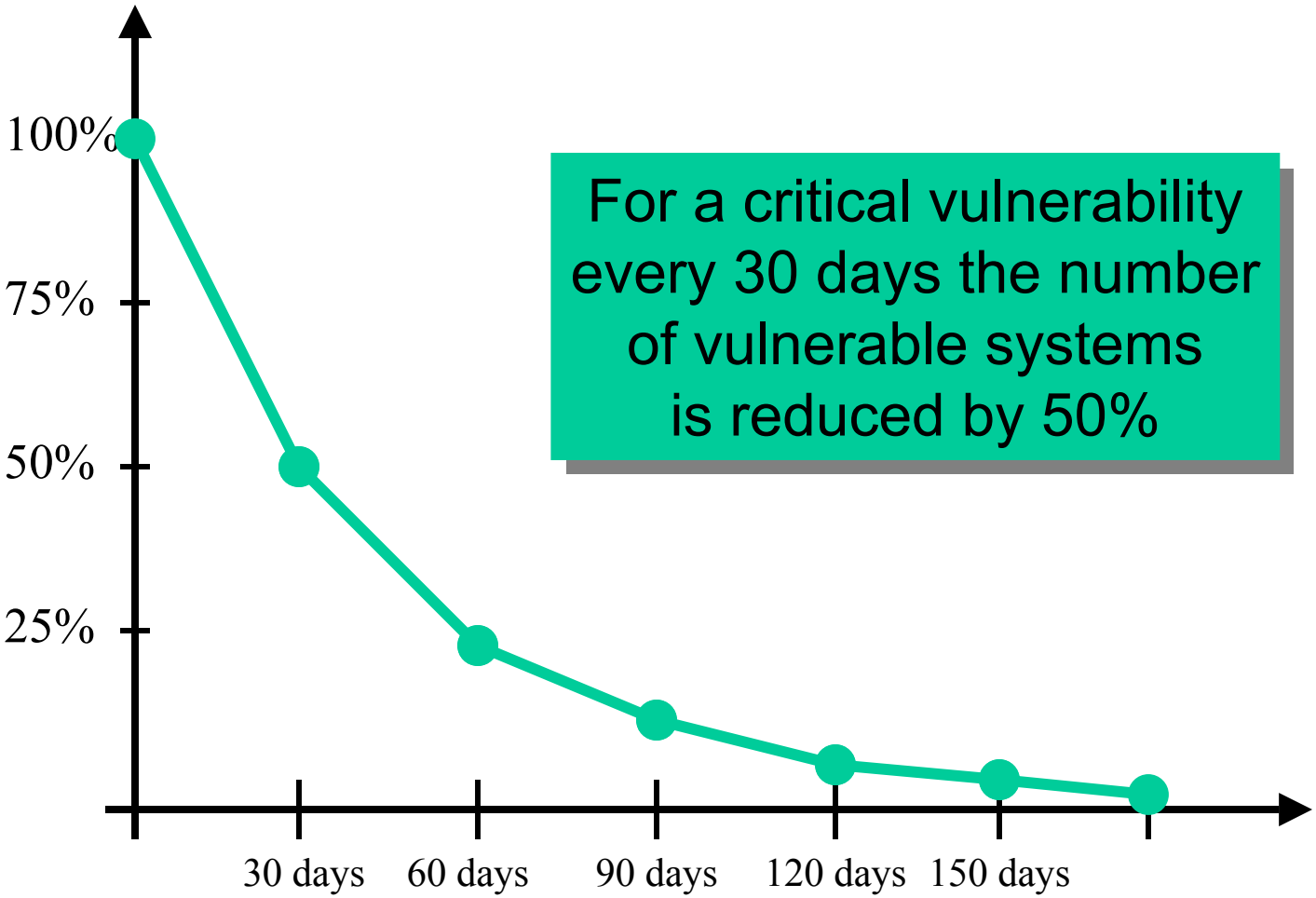


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

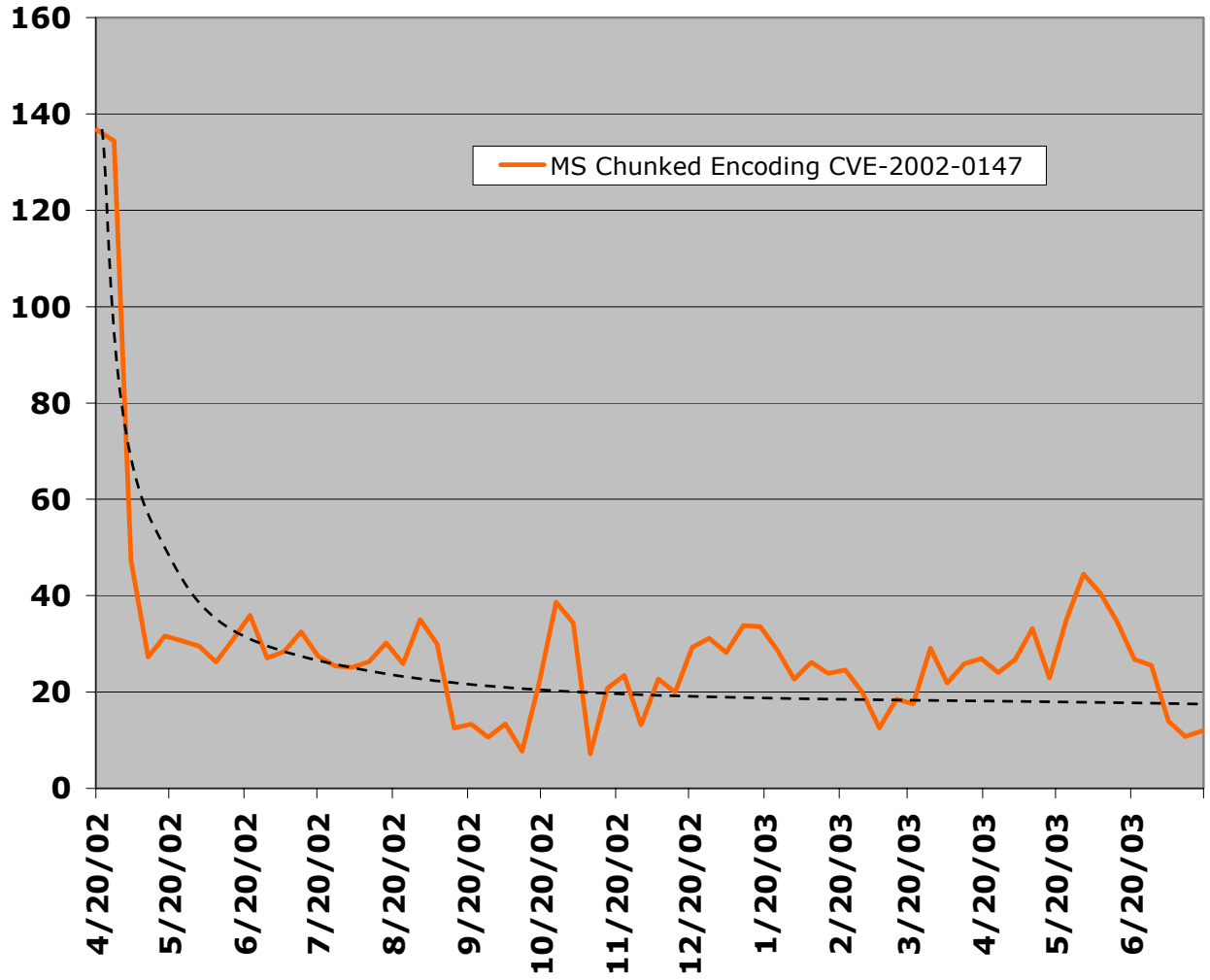
Released: March 2003

Vulnerability Half-Life



For a critical vulnerability every 30 days the number of vulnerable systems is reduced by 50%

MS Chunked Encoding Overflow

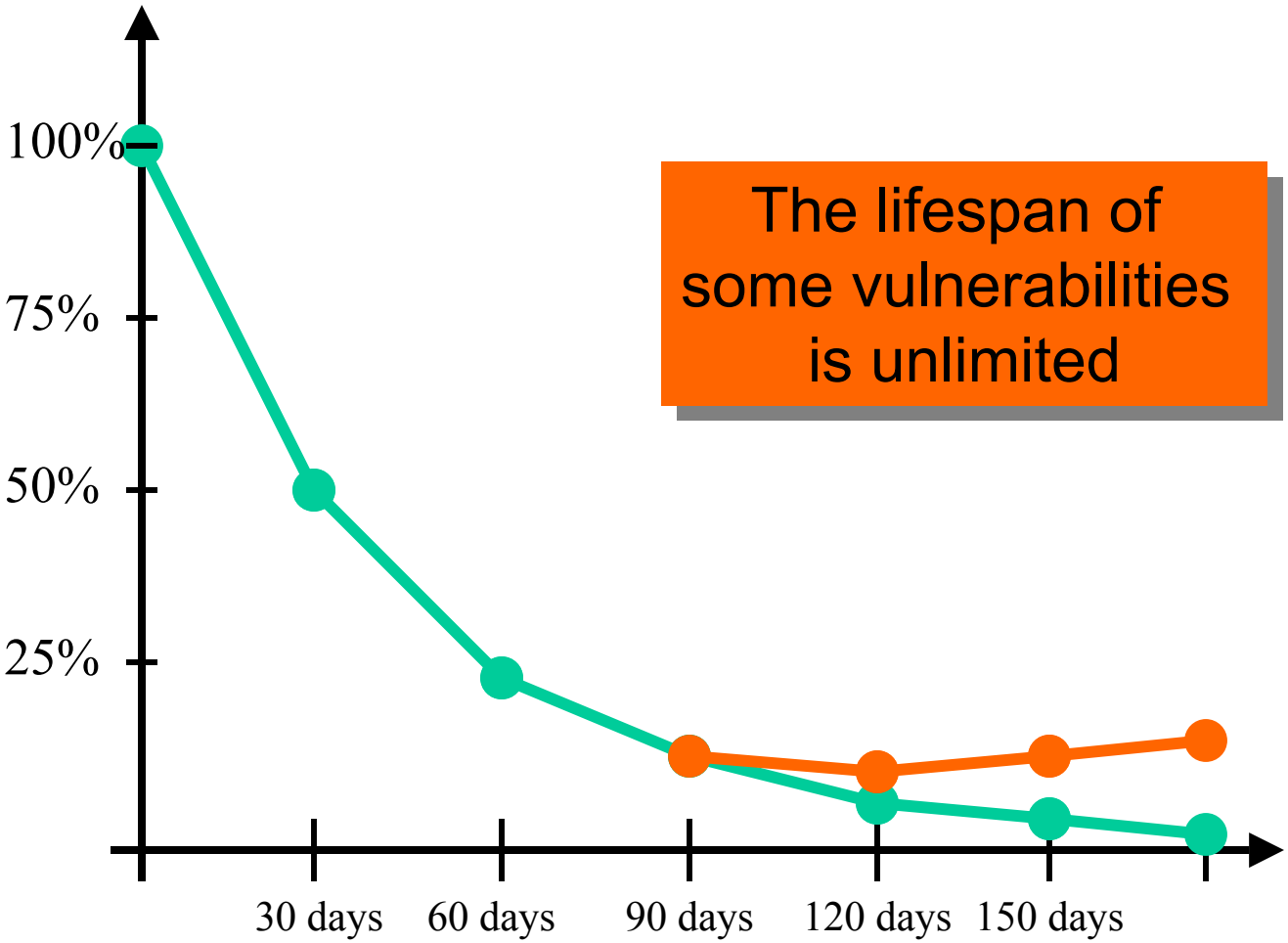


Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability

CVE-2002-0147
Qualys ID 10571

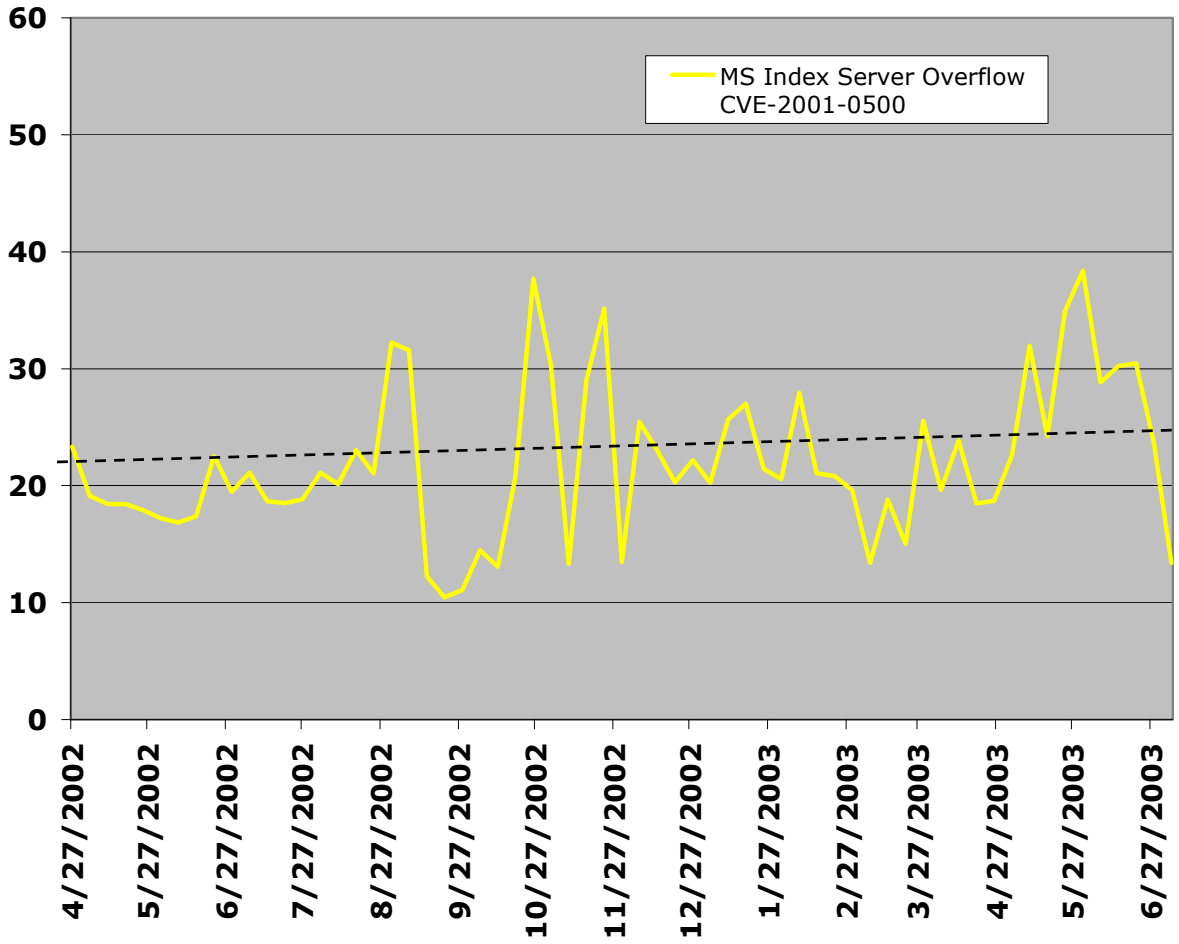
Released: April 2002

Vulnerability Lifespan



The lifespan of some vulnerabilities is unlimited

MS Index Server Overflow (CodeRed)

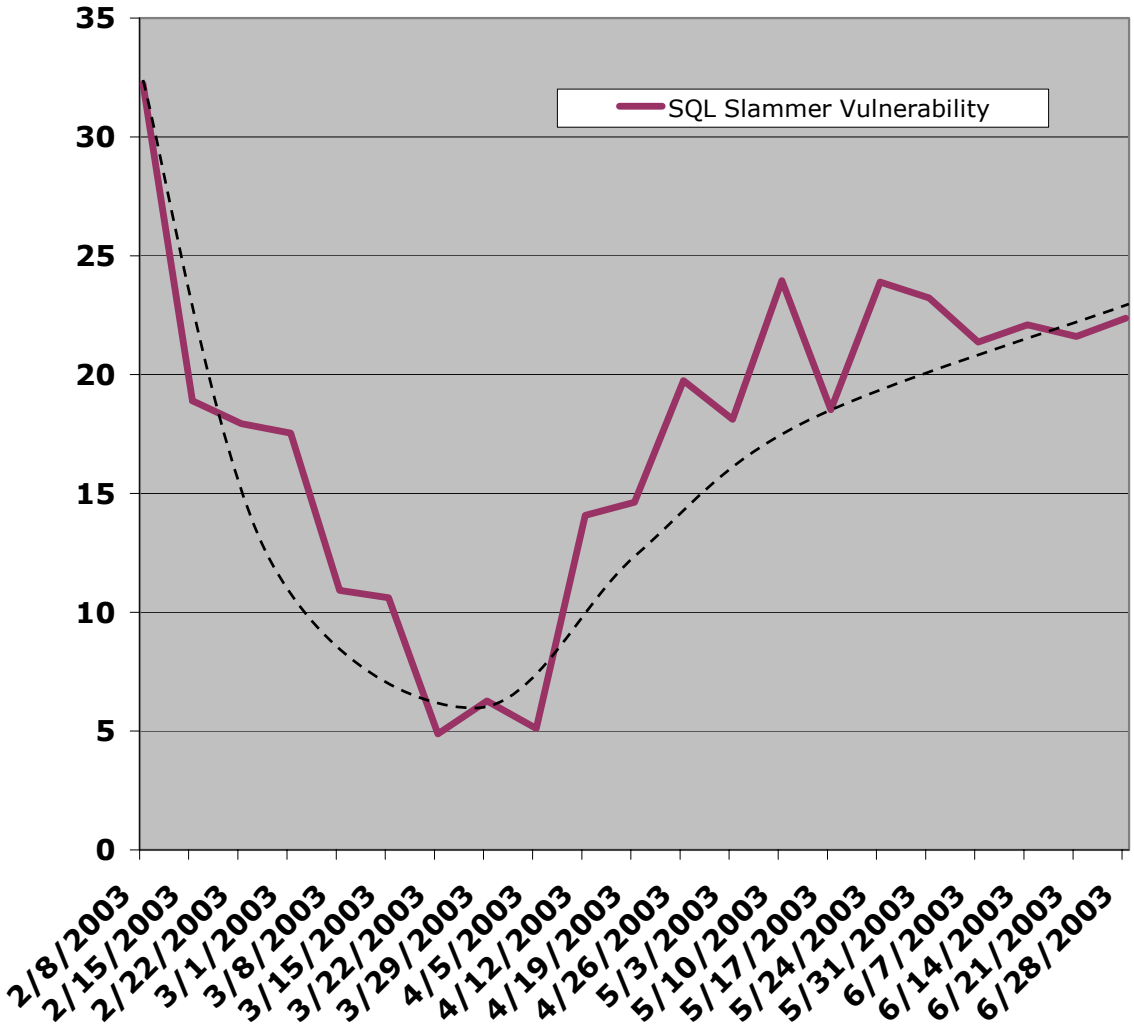


Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability

CVE-2001-0500
Qualys ID 86170

Released: June 2001

SQL Slammer Vulnerability



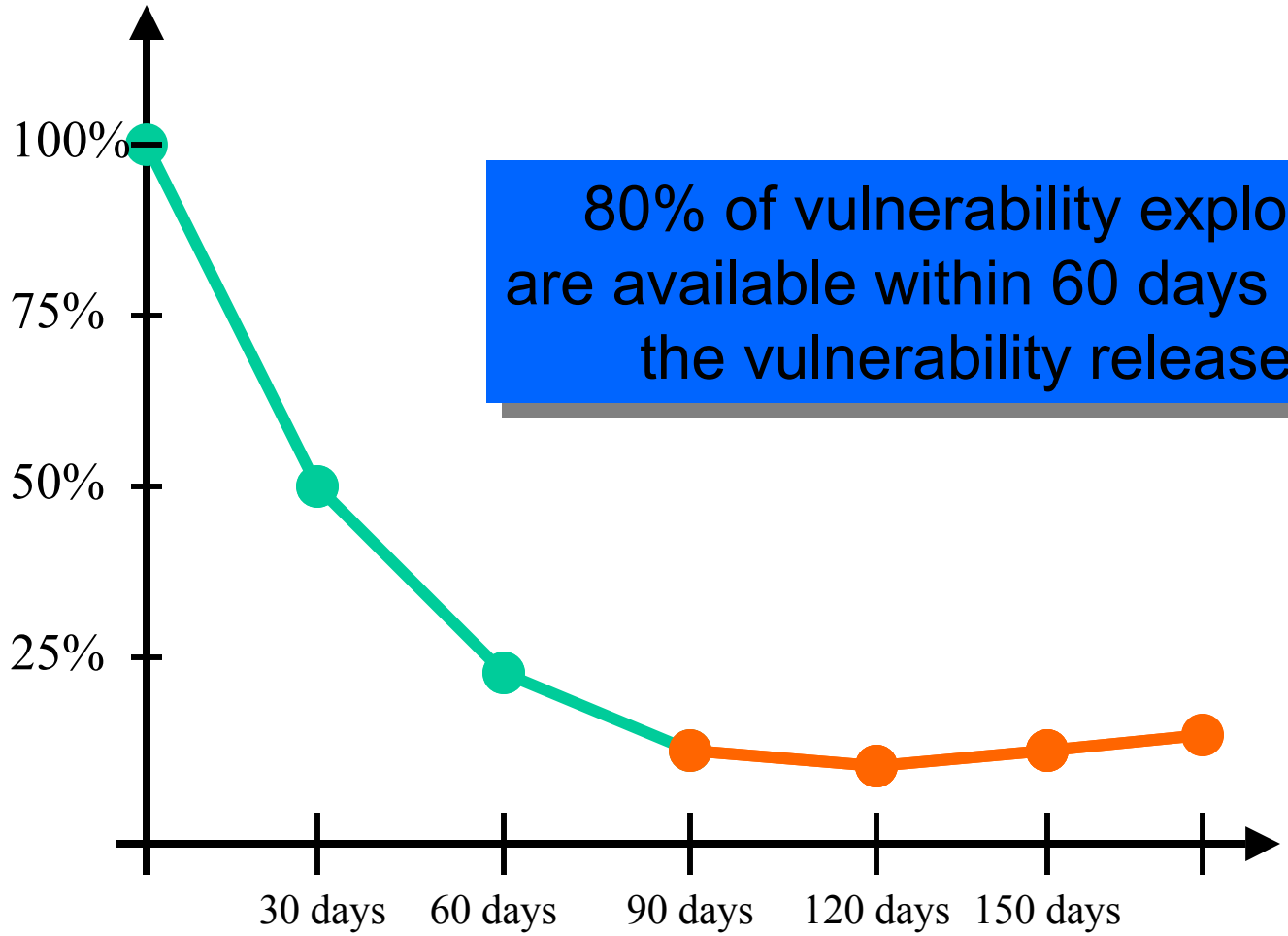
MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability

CAN-2002-0649
Qualys ID 19070

Released: July 2002

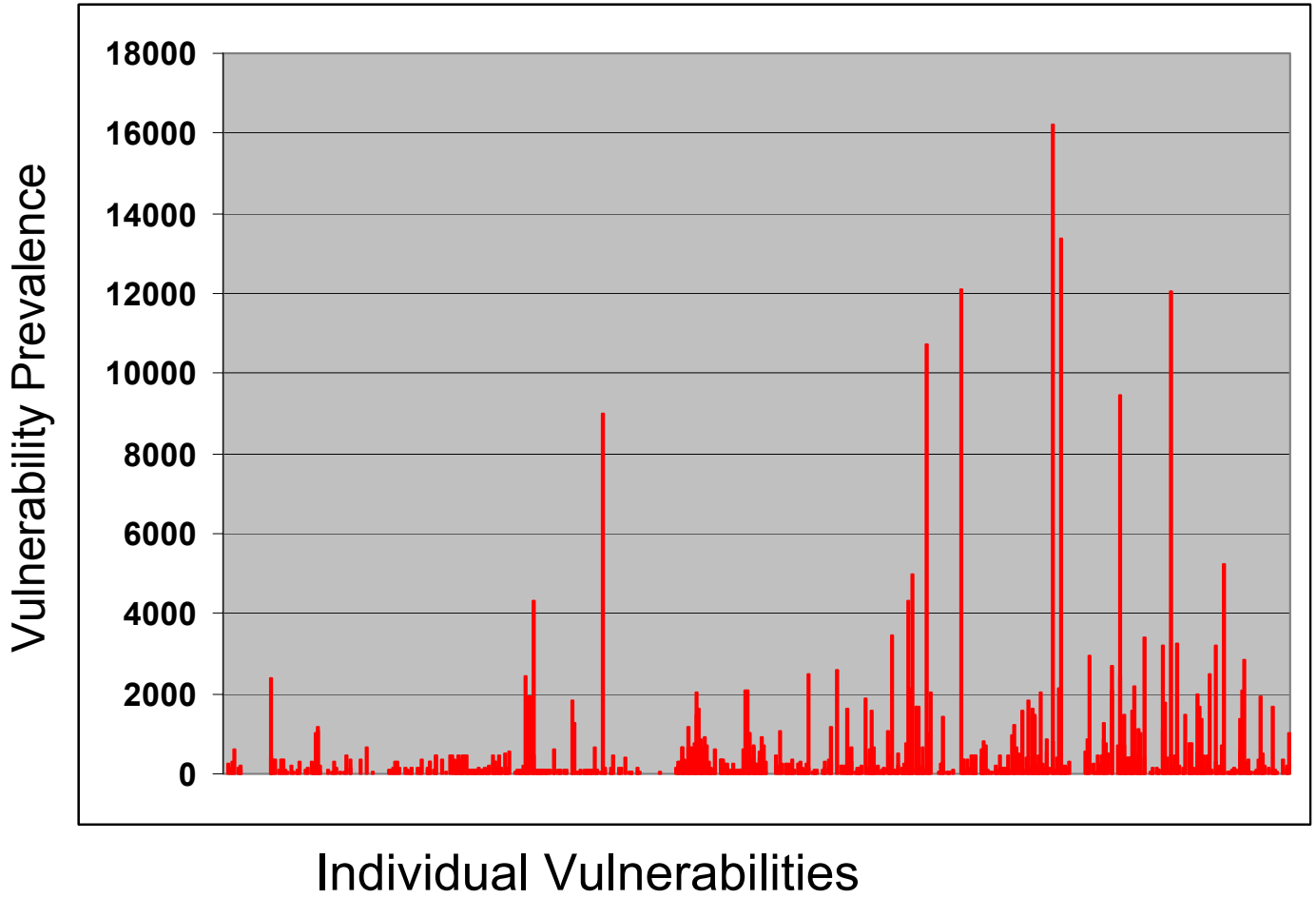
qualys

The Impact of an Exploit



80% of vulnerability exploits are available within 60 days after the vulnerability release

Mapping Vulnerability Prevalence



The Changing Top of the Most Prevalent

Vulnerability	CVE	Jul-02	Jan-03	Jul-03
Apache Mod_SSL Buffer Overflow Vulnerability	CVE-2002-0082	x		
Microsoft Exchange 2000 Malformed Mail Attribute DoS Vulnerability	CVE-2002-0368	x		
Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500	x	x	
Microsoft IIS	[illegible]		x	
Microsoft IIS			x	
Microsoft IIS			x	
Microsoft IIS			x	x
Microsoft IIS			x	x
Microsoft IIS			x	x
Microsoft IIS			x	x
Apache Chur			x	x
OpenSSH Ch			x	x
Multiple Vendor SNMP Request And Trap Handling Vulnerabilities	[illegible]		x	x
ISC BIND SIG Cached Resource Record Buffer Overflow (sigrec bug) Vulnerability	CAN-2002-1219		x	x
Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	CAN-2003-0109			x
Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161			x
Microsoft SMB Request Handler Buffer Overflow Vulnerability	CAN-2003-0345			x
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352			x

50% of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities on an annual basis

qualys

Two Recent Examples

- **Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (CAN-2003-0352)**
  - Released July 16
  - Within two days in the top 10 most prevalent vulnerabilities
  - Since July 20 ranking in the top 10
  - Working exploit code released
  - Worms started circulating August 11
- **Cisco IOS Malformed IPV4 Packet Denial Of Service Vulnerability (CAN-2003-0567)**
  - Released July 16
  - Exploit code released on July 18
  - Currently ranking on position 29 on the top 10 most prevalent vulnerabilities

The Laws of Vulnerabilities

1. Half-Life

The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity

2. Prevalence

50% of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities on an annual basis

3. Persistence

The lifespan of some vulnerabilities is unlimited

4. Exploitation

80% of vulnerability exploits are available within 60 days of the vulnerability release

10 Most Prevalent Vulnerabilities (as of September 24, 2003)

Microsoft IIS CGI Filename Decode Error Vulnerability	CVE-2001-0333
Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500
Microsoft IIS Malformed HTR Request Buffer Overflow Vulnerability	CVE-2002-0071
Apache Chunked-Encoding Memory Corruption Vulnerability	CVE-2002-0392
Microsoft Windows DCOM RPCSS Service Vulnerabilities	CAN-2003-0528
Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	CAN-2003-0109
Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352
SSL Server Has SSLv2 Enabled Vulnerability	No CVE assigned
Writeable SNMP Information	No CVE assigned

Summary

- Automated Attacks against widely deployed systems and applications are increasing in number and sophistication
- Next Generation Worms will be spreading faster than any possible human response
- Timely and complete detection and remediation of security vulnerabilities is the most effective preventive measure

Thank You

ge@qualys.com

http://www.qualys.com