RSA CONFERENCE 2006

The Laws of Vulnerabilities

Terry Ramos
Qualys
02/15/06 - HT1-202

Are We Getting Better or Worse ?

What is a vulnerability?

How significant is this vulnerability?

How prevalent is this vulnerability?

How easy is this vulnerability to exploit?

Are any of my systems affected by this vulnerability?

How quickly should I patch this vulnerability?

Security Trend Indicators

- Malicious Code (↑)
- Vulnerabilities (↑)
- Spam and Spyware (↑)
- Phishing and Identity Theft (↑)

….and

- Time to Exploitation (↓)

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

Second Generation Threats

- Active worms
- Leveraging known vulnerabilities
- Low level of sophistication in spreading strategy (i.e. randomly)
- Non Destructive Payloads
- Remedy: Identify and Fix Vulnerabilities

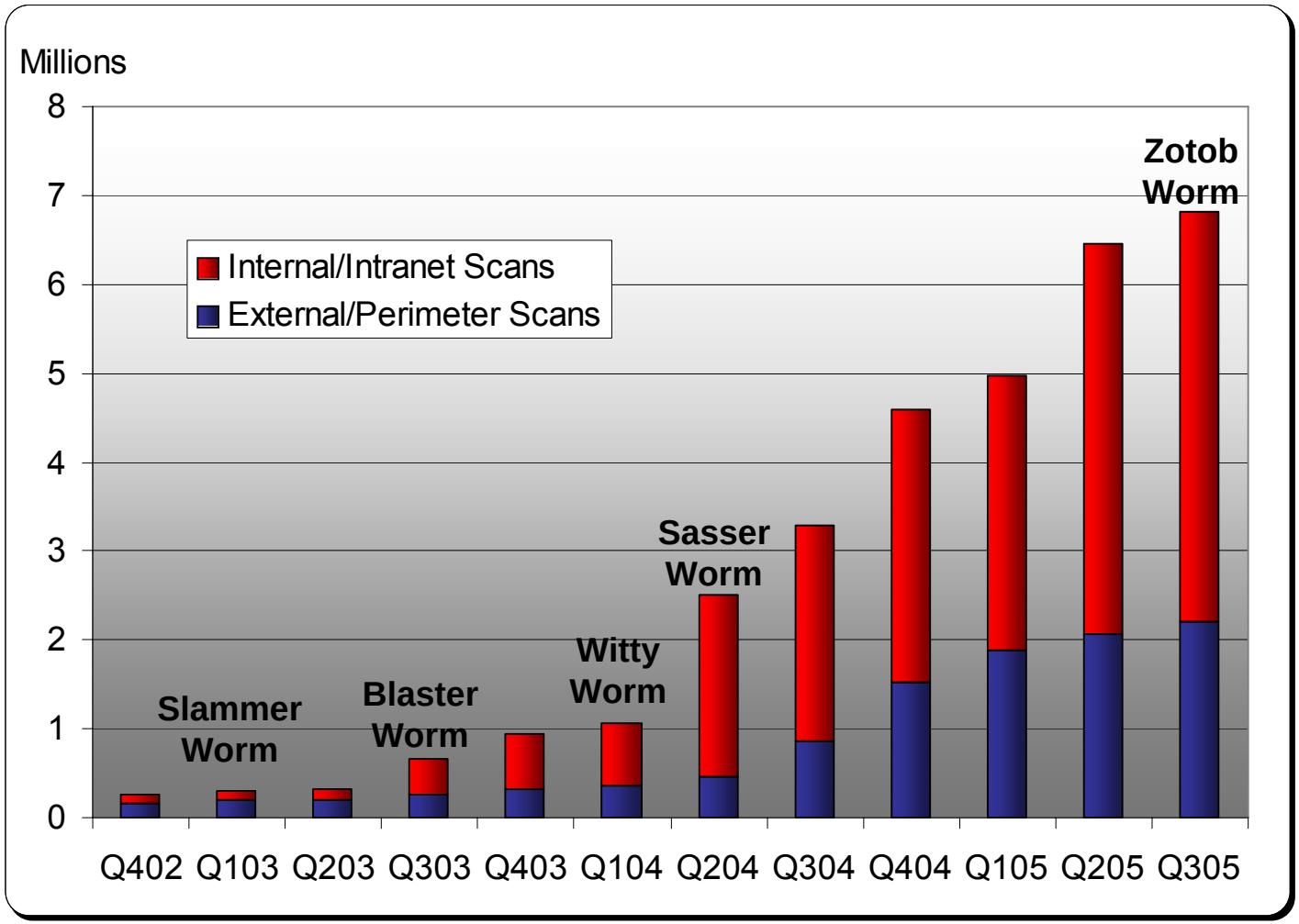
Third Generation Threats

- Automated Attacks Leveraging Known and Unknown Vulnerabilities
- Collaboration of Social Engineering and Automated Attacks
- Multiple Attack Vectors
  - Email, Web, IM, Vulnerabilities,…
- Active Payloads
- Remedy: Security Enforcement / NAC / NAM

The Laws of Vulnerabilities: Studying Vulnerabilities and Patching

- Objective: Understanding prevalence of critical vulnerabilities over time in real world
- Timeframe: 2002 - Ongoing
- Data Source:
  - 70% Global Enterprise networks
  - 30 % Random trials
- Methodology: Automatic Data collection with statistical data only – no possible correlation to individual user or systems
- Scanning: Agentless/Remote

Analyzing 32,000,000 Vulnerability Scans



Raw Results

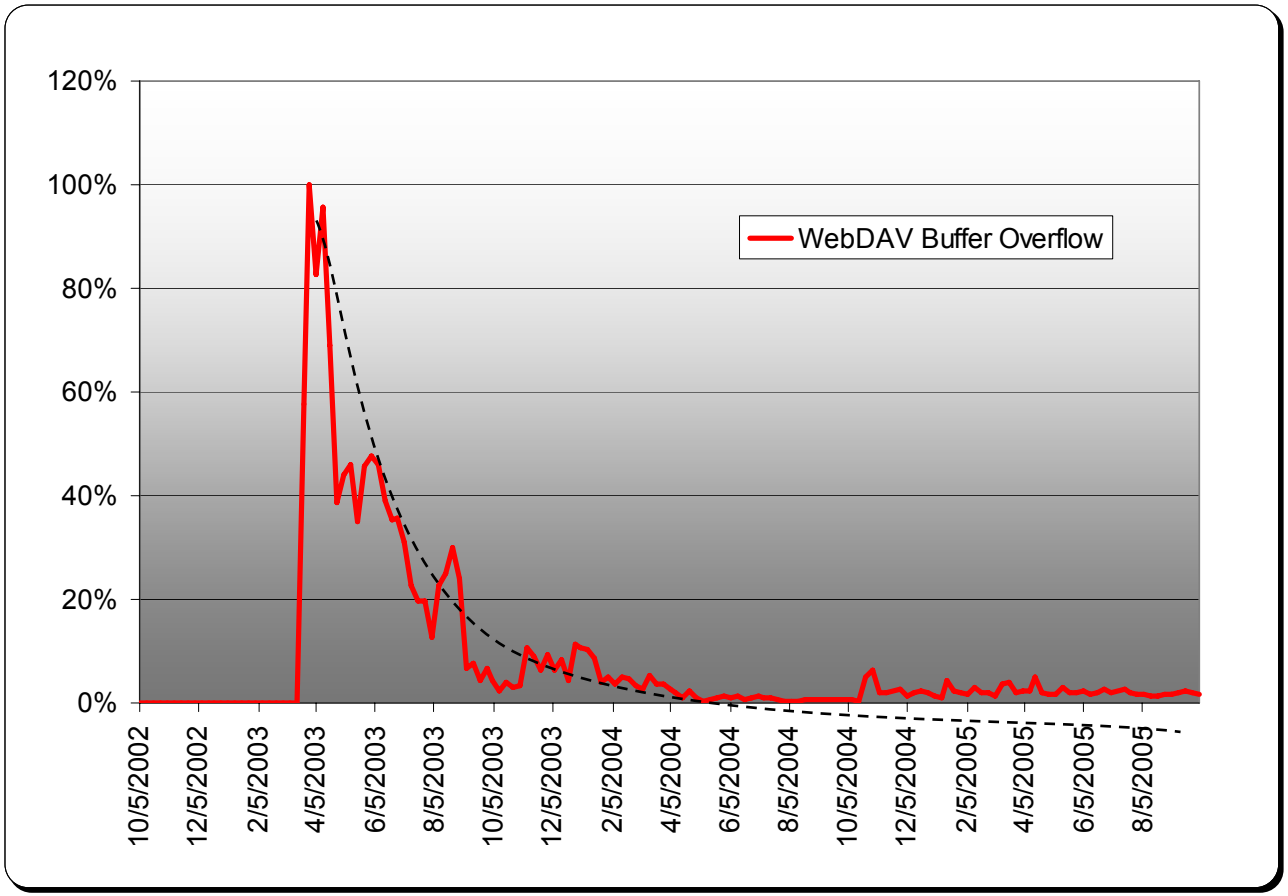
- Largest collection of global real-world vulnerability data:
  - —32,147,000 IP-Scans from Q3/2002 to Q3/2005
  - —21,347,000 critical vulnerabilities identified
- Scope of Vulnerabilities included
  - —1,060 out of 1,556 unique critical* vulnerabilities

* Providing an attacker the ability to gain full control of the system, and/or leakage of highly sensitive information. For example, vulnerabilities may enable full read and/or write access to files, remote execution of commands, and the presence of backdoors.

The Changing Vulnerability Landscape

- From server to client applications
- Before: Vulnerabilities in server applications:
  - Webserver, Mailserver, Operating System services,
- Now: More than 60% of new critical vulnerabilities in client applications:
  - Web Browser, Backup Software, Media Player, Antivirus Software, Flash, …

Microsoft WebDAV Vulnerability

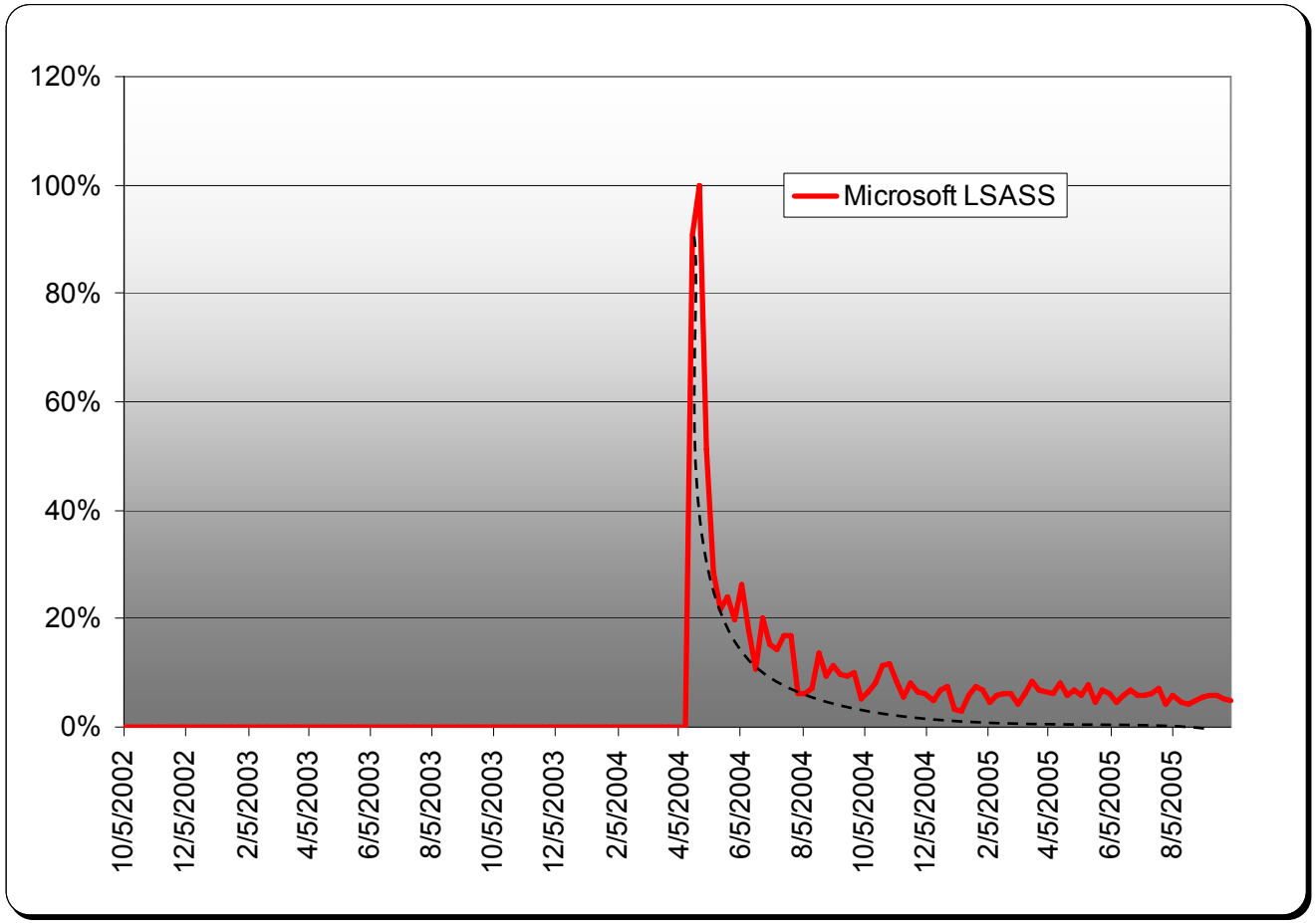


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

Released: March 2003

Buffer Overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

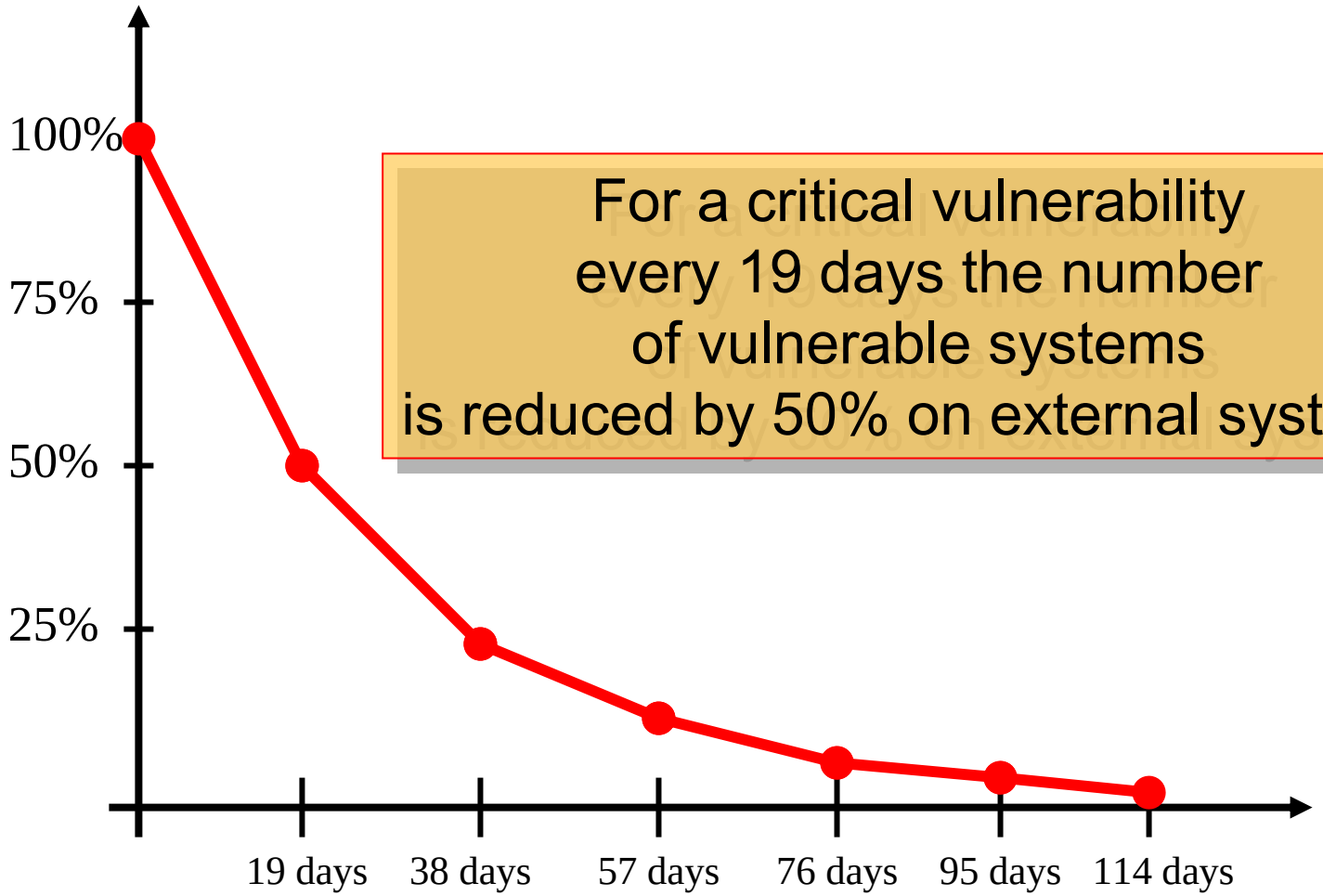


Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

CAN-2003-0533
Qualys ID 90108

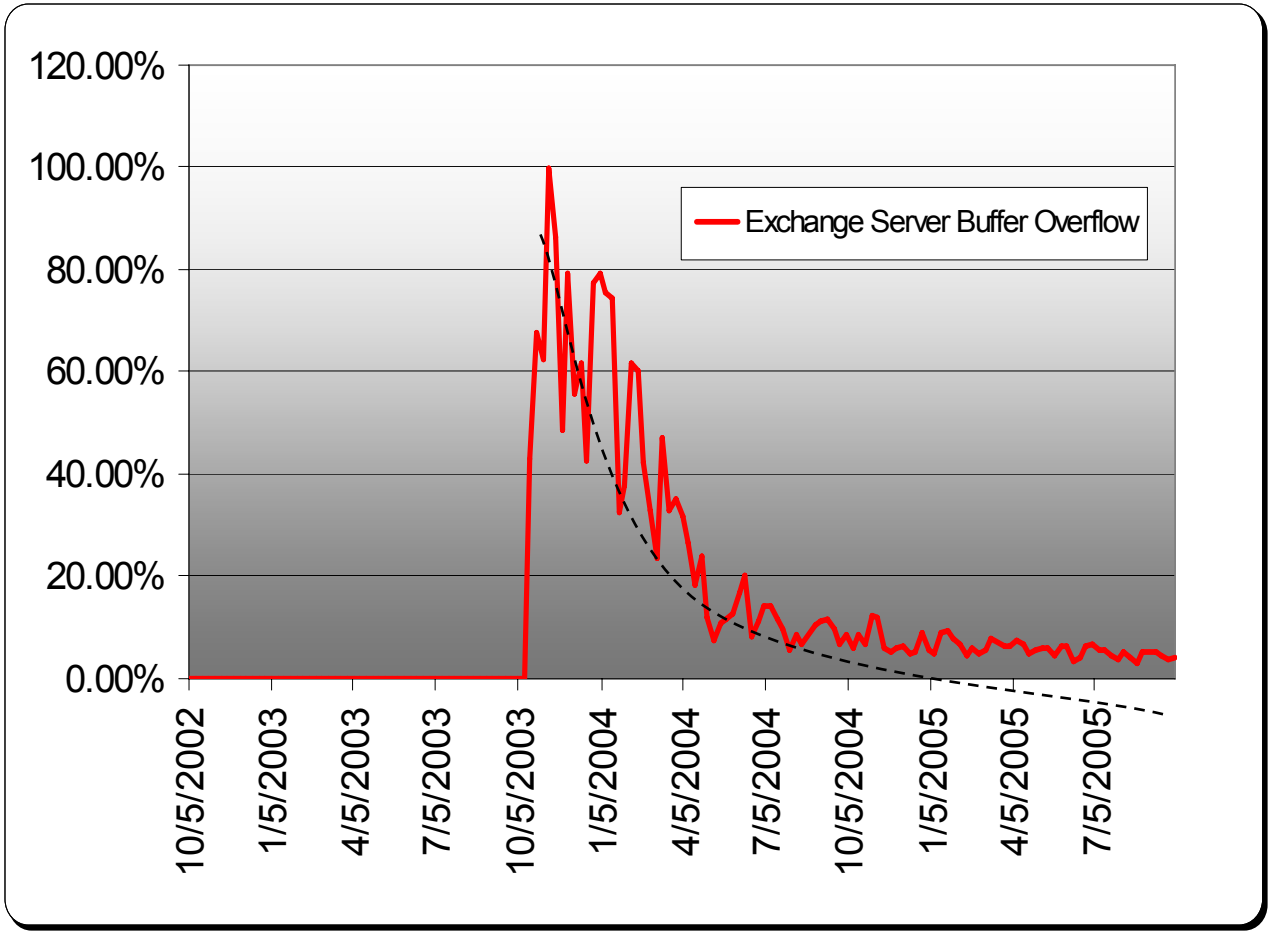
Released: April 2004

Vulnerability Half-Life



For a critical vulnerability
every 19 days the number
of vulnerable systems
is reduced by 50% on external systems

Microsoft Exchange Server Buffer Overflow Vulnerability

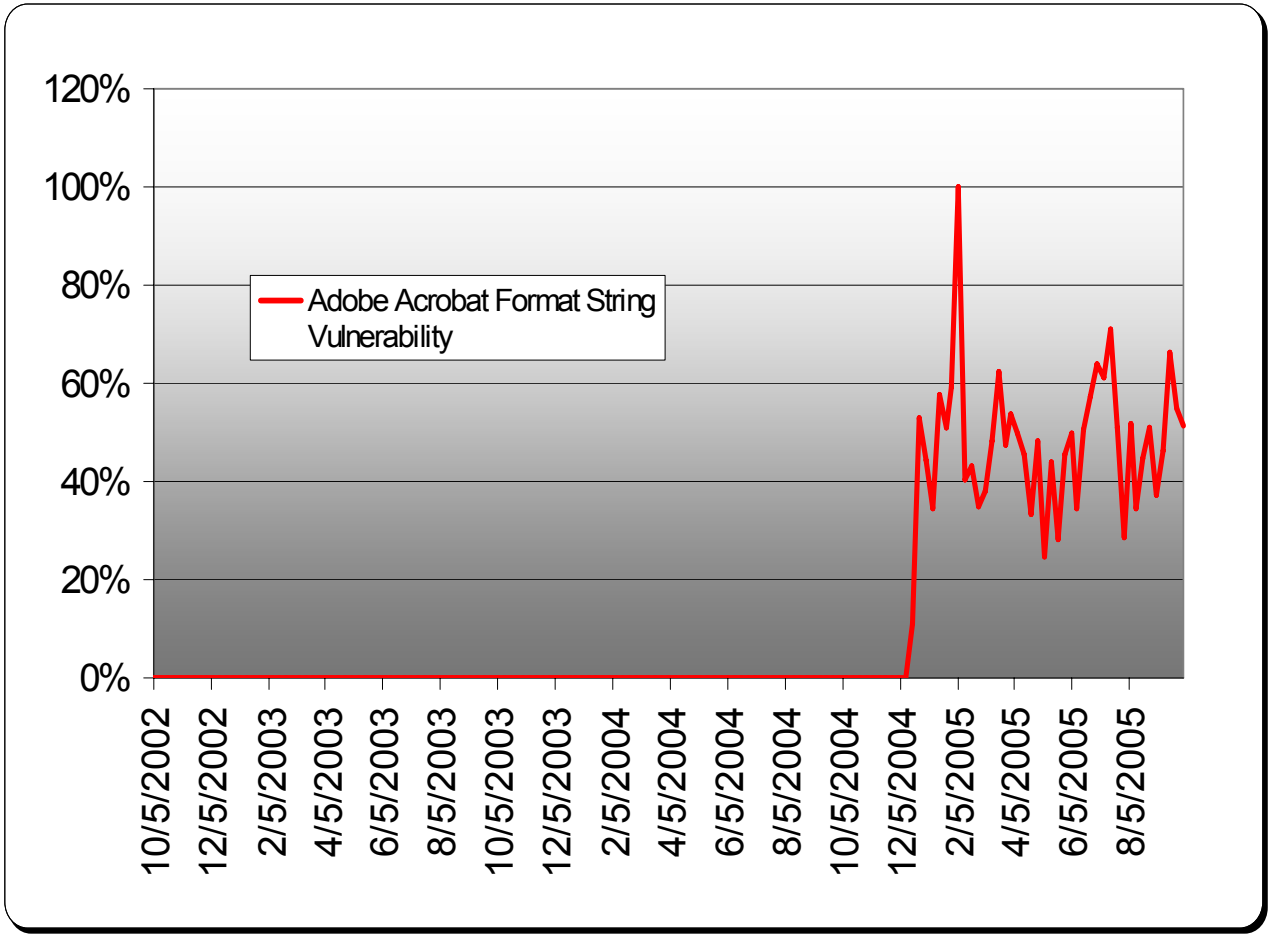


Microsoft Exchange Server Buffer Overflow Vulnerability

CAN-2003-0714
Qualys ID 74143

Released: October 2003

Adobe Acrobat Reader Format String Vulnerability

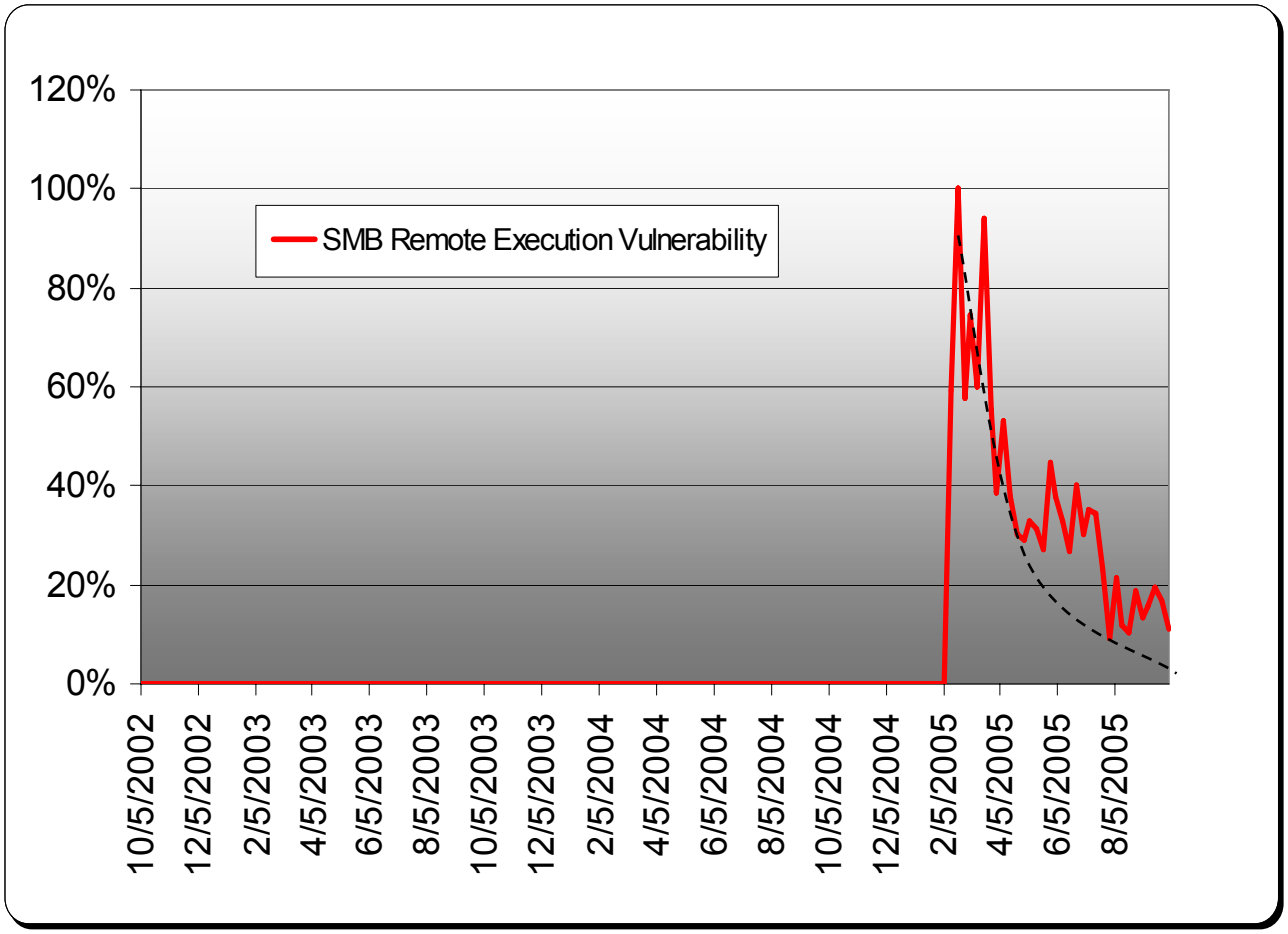


Adobe Acrobat Reader
Format String Vulnerability

CAN-2004-1153
Qualys ID 38385

Released: December 2004

Microsoft Server Message Block Remote Execution (MS05-011)

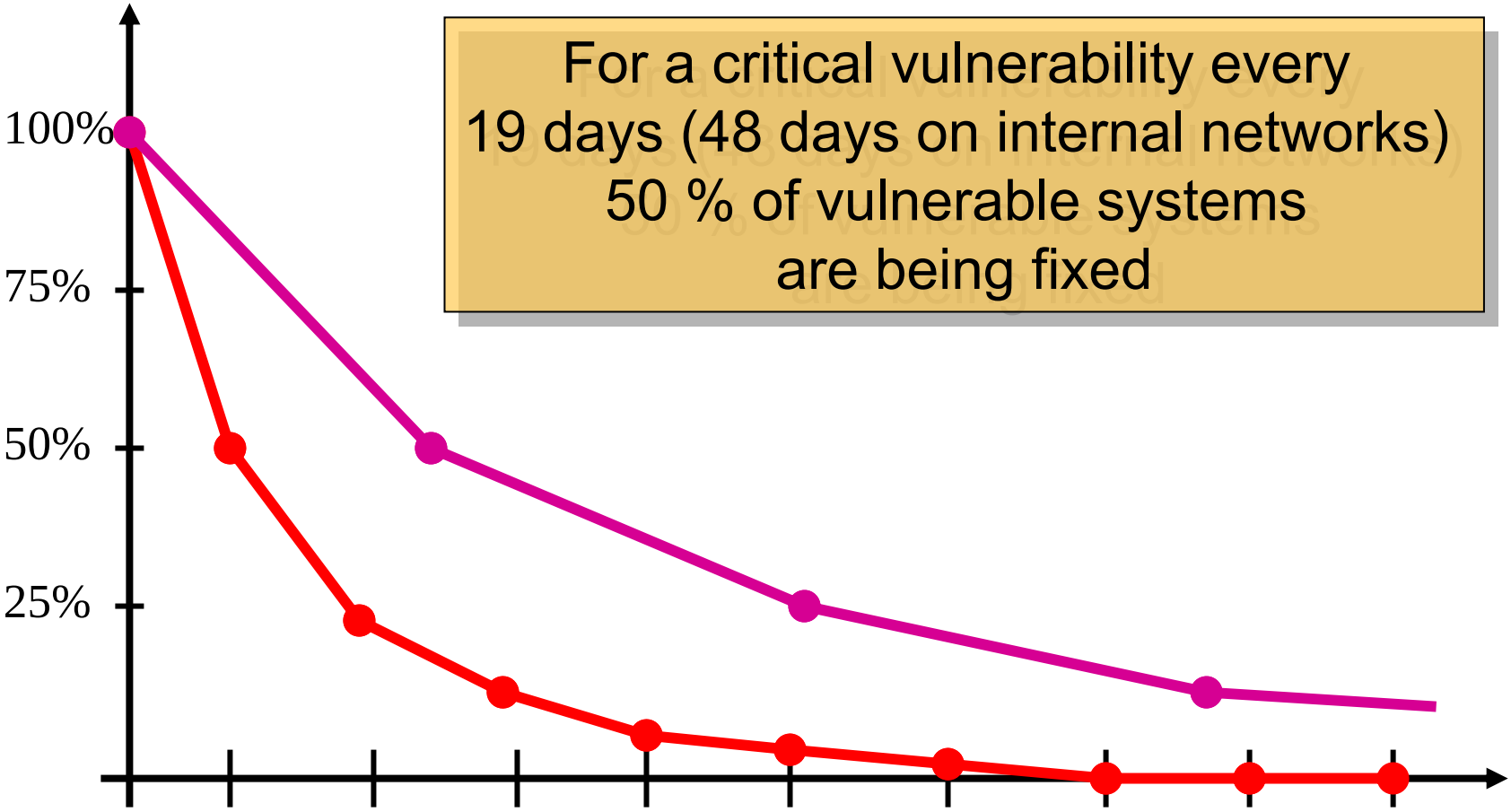


Remote Code Execution Vulnerability in Microsoft Server Message Block (SMB)

CAN-2005-0045
Qualys ID 90230

Released: February 2005

External vs. Internal Half-life

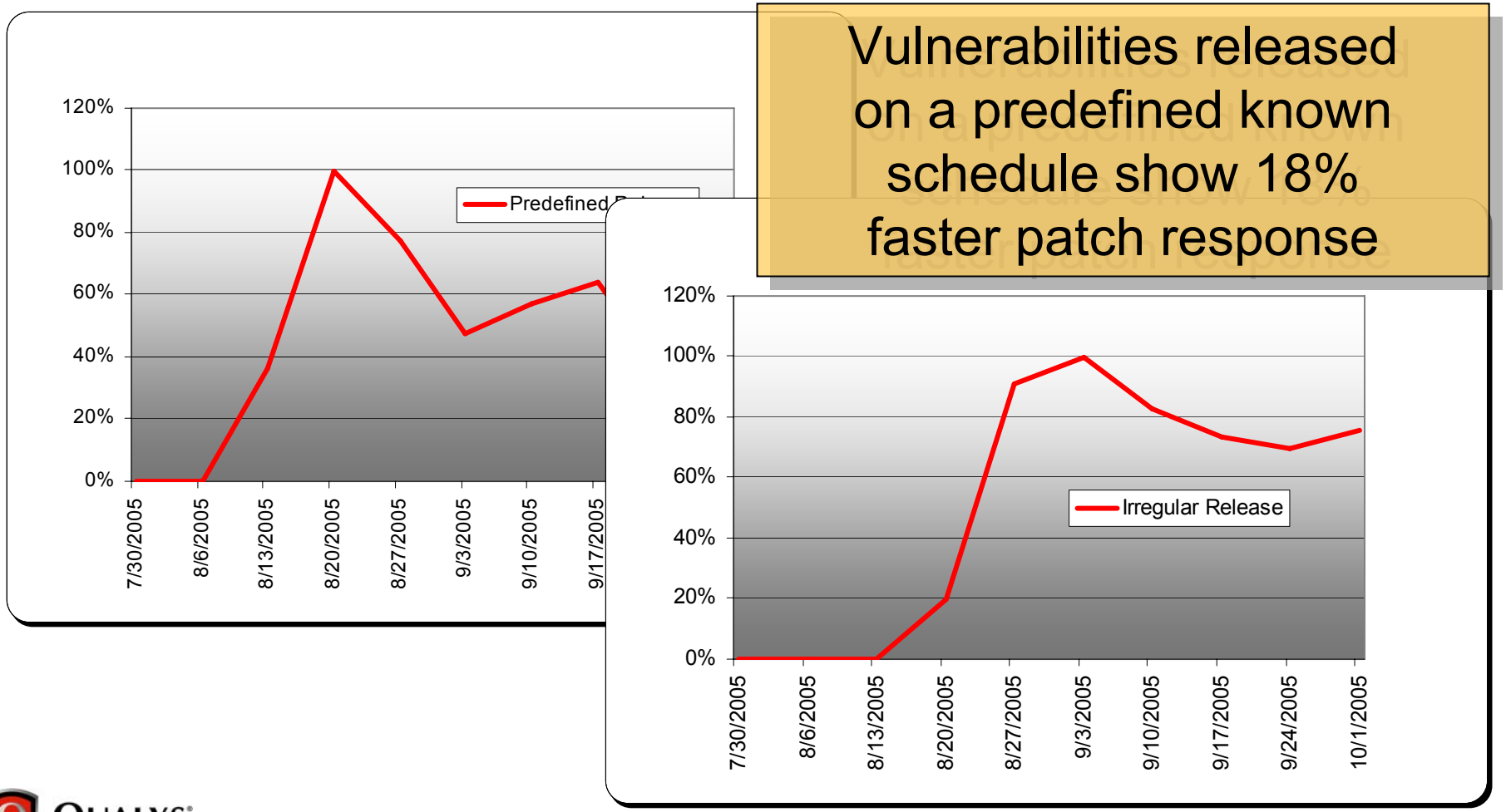


For a critical vulnerability every
19 days (48 days on internal networks)
50 % of vulnerable systems
are being fixed

The Changing Half-life

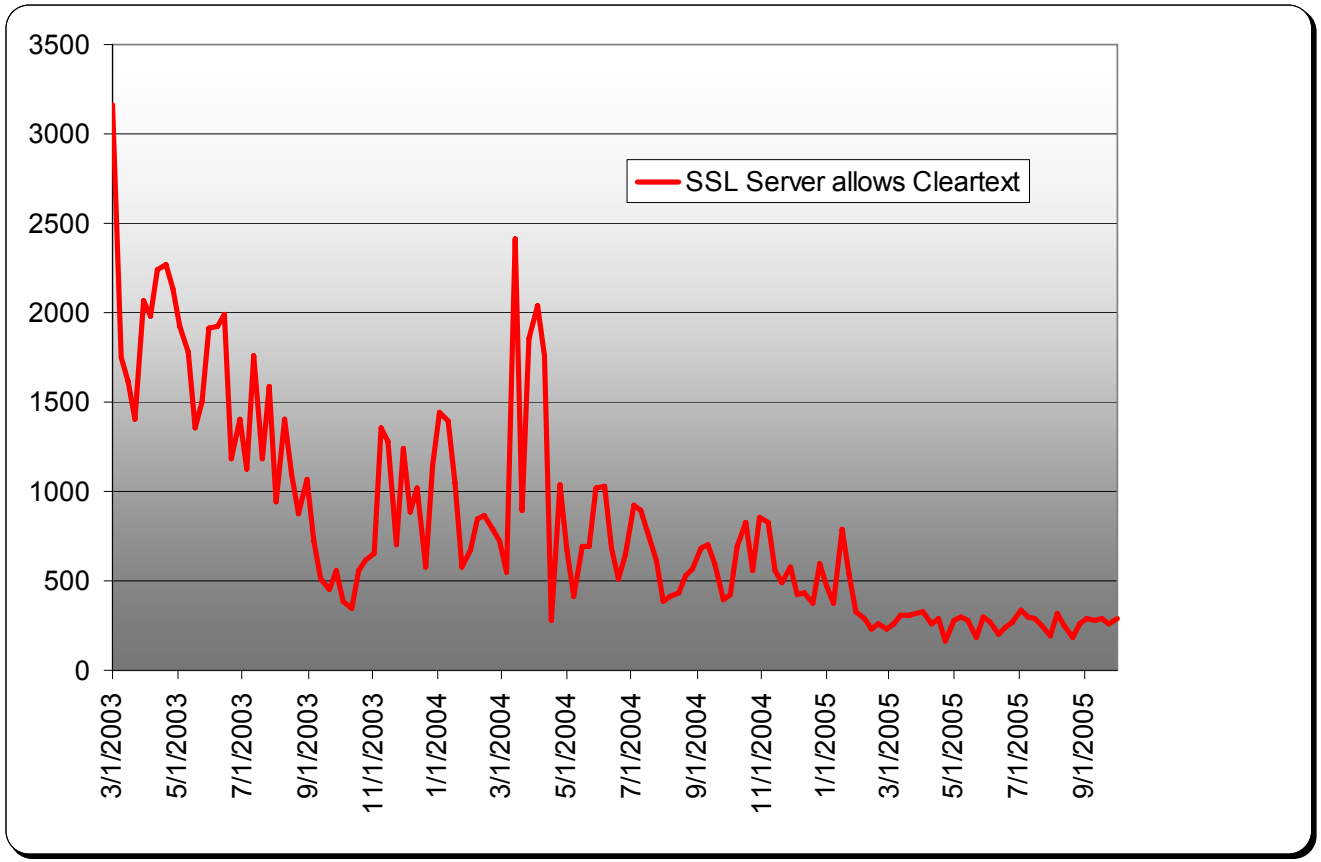
	2003	2004	2005	2006
External Half-life	30 days	21 days	19 days	?
Internal Half-life	-	62 days	48 days	?

Predefined vs. Irregular Vulnerability Releases



Vulnerabilities released on a predefined known schedule show 18% faster patch response

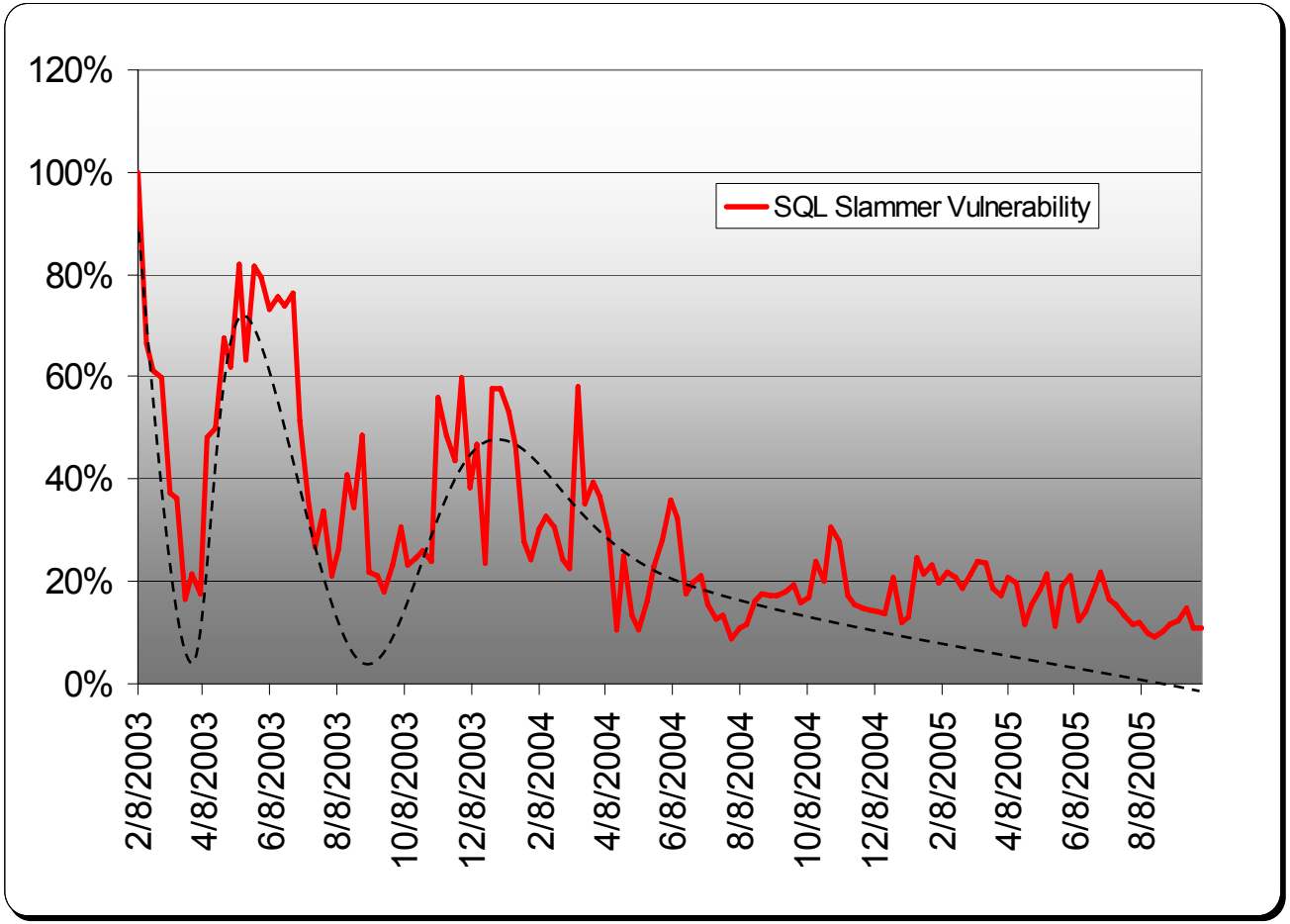
SSL Server Allows Cleartext Communication



SSL Server Allows Cleartext Communication

Qualys ID 38143

SQL Slammer Vulnerability

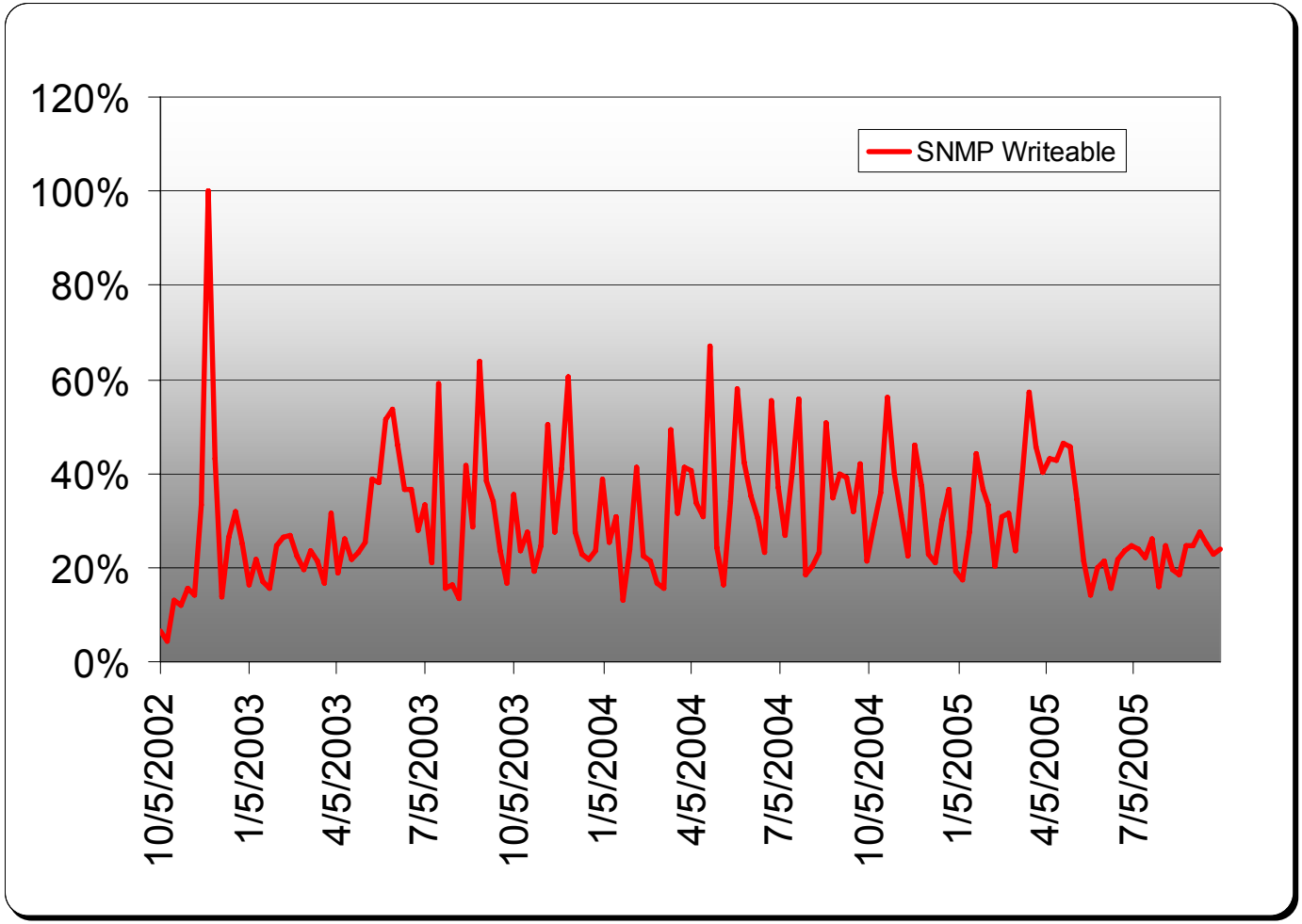


MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability

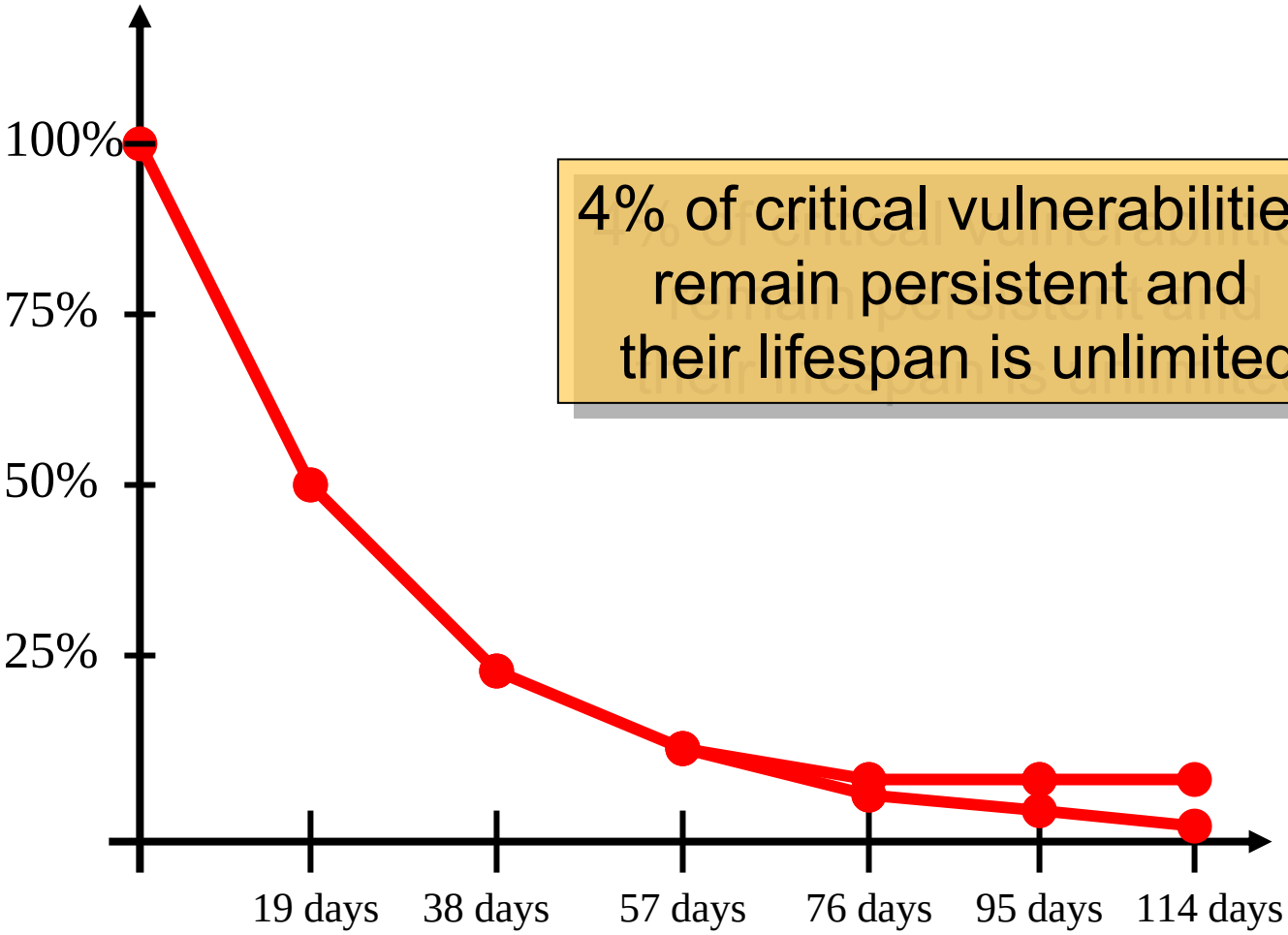
CAN-2002-0649
Qualys ID 19070

Released: July 2002

Lingering Vulnerabilities: SNMP Writable

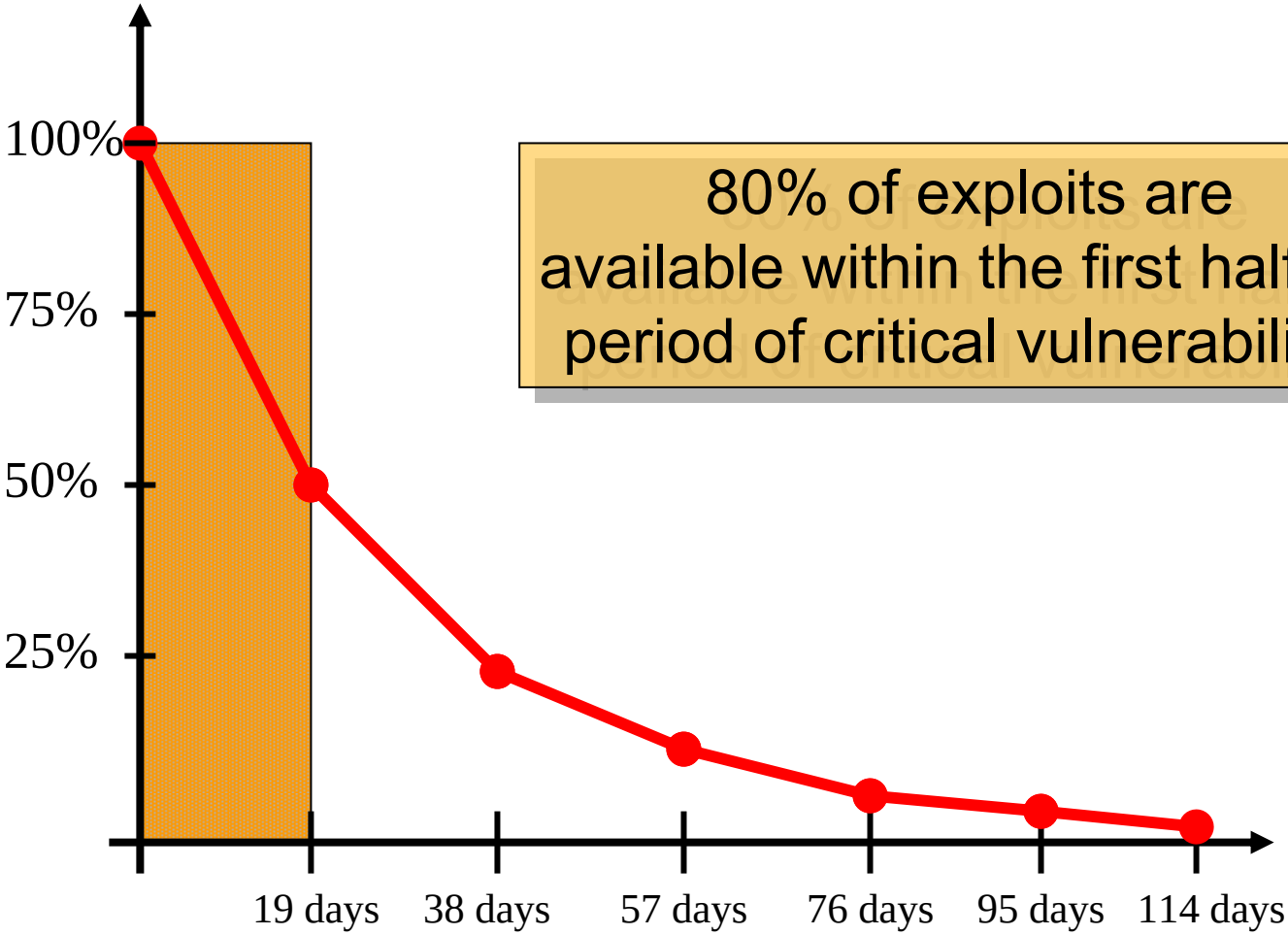


Vulnerability Lifespan



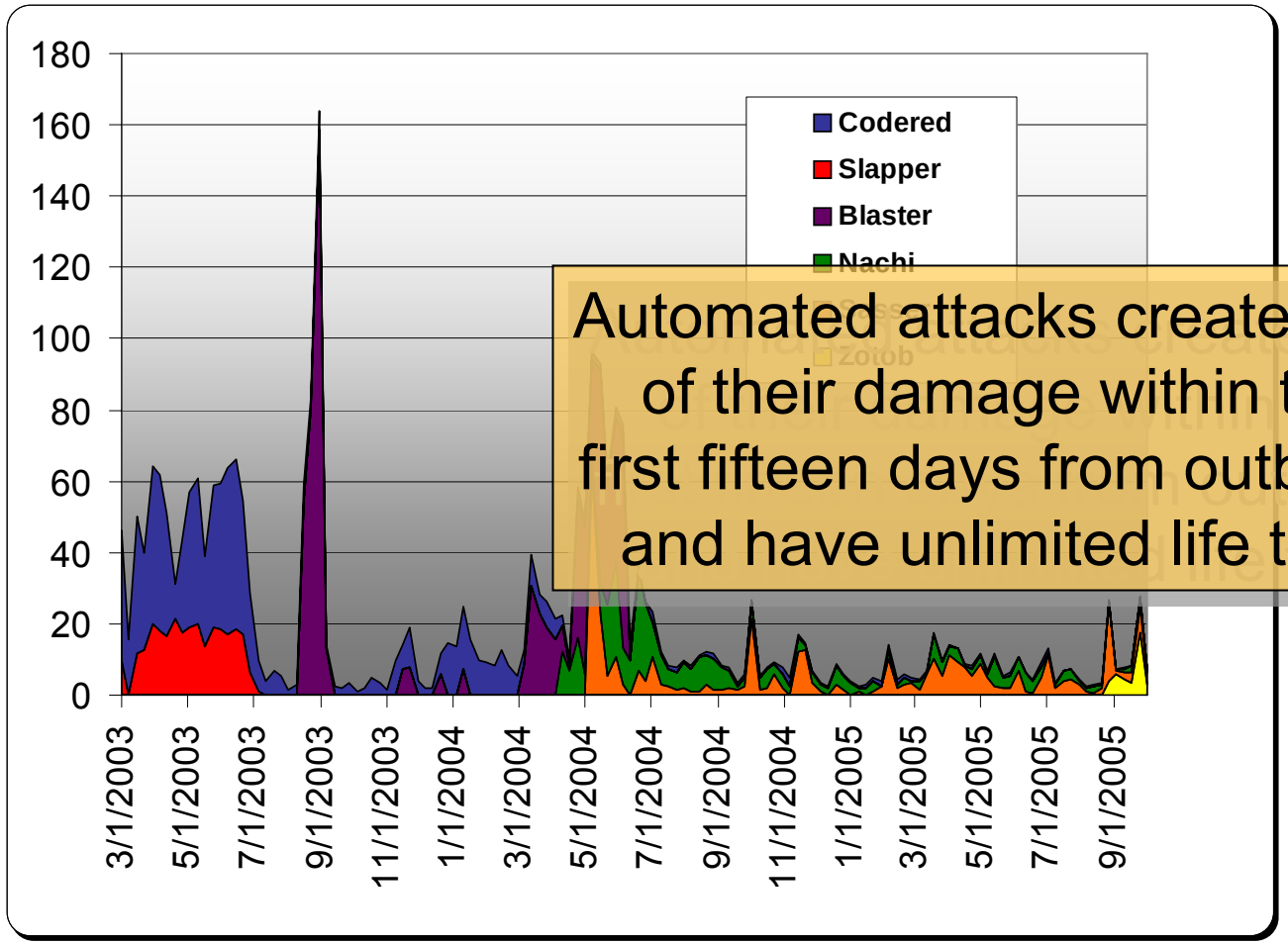
4% of critical vulnerabilities remain persistent and their lifespan is unlimited

Window of Exposure



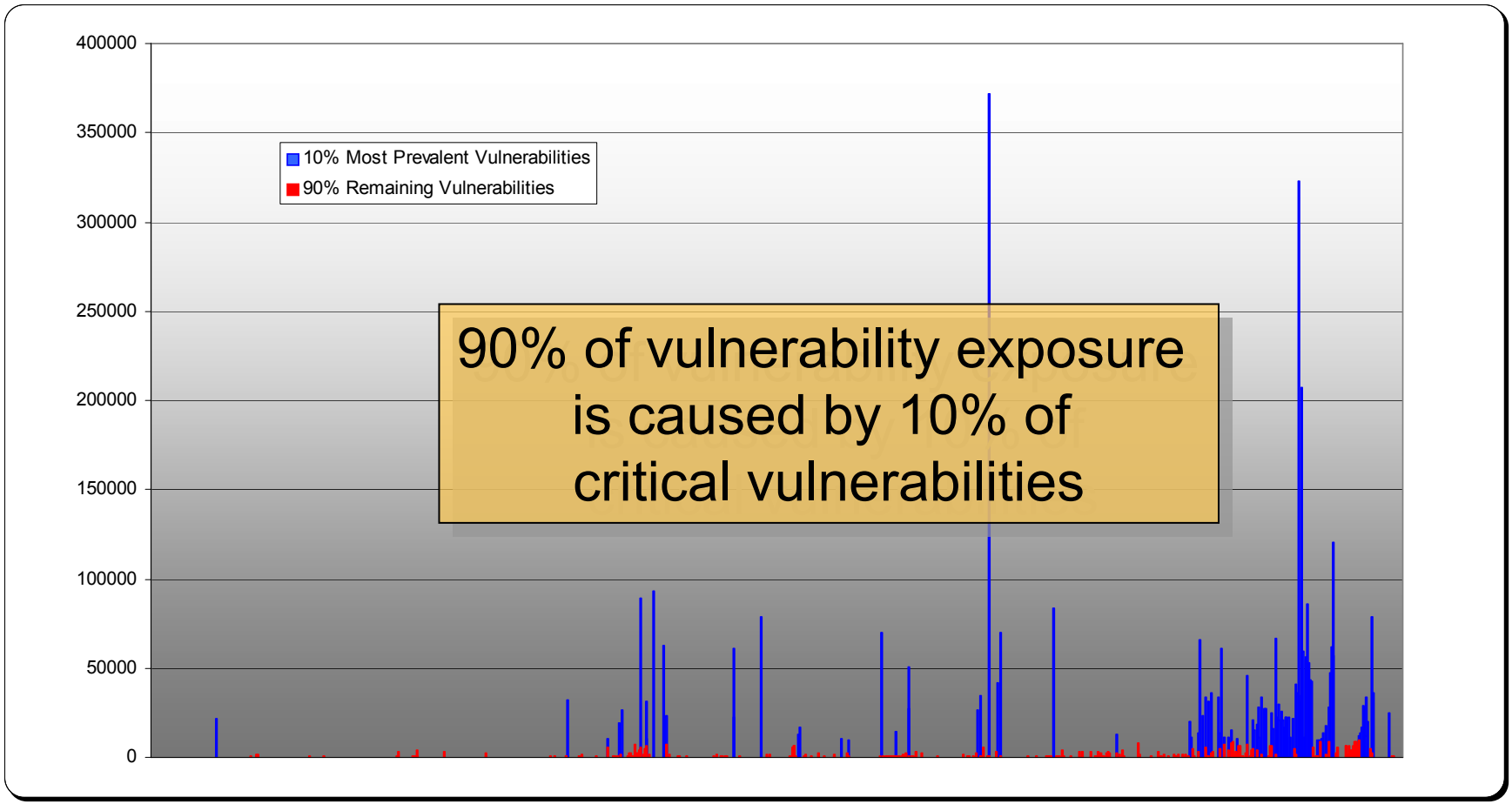
80% of exploits are available within the first half-life period of critical vulnerabilities

A Continuous Cycle of Infection

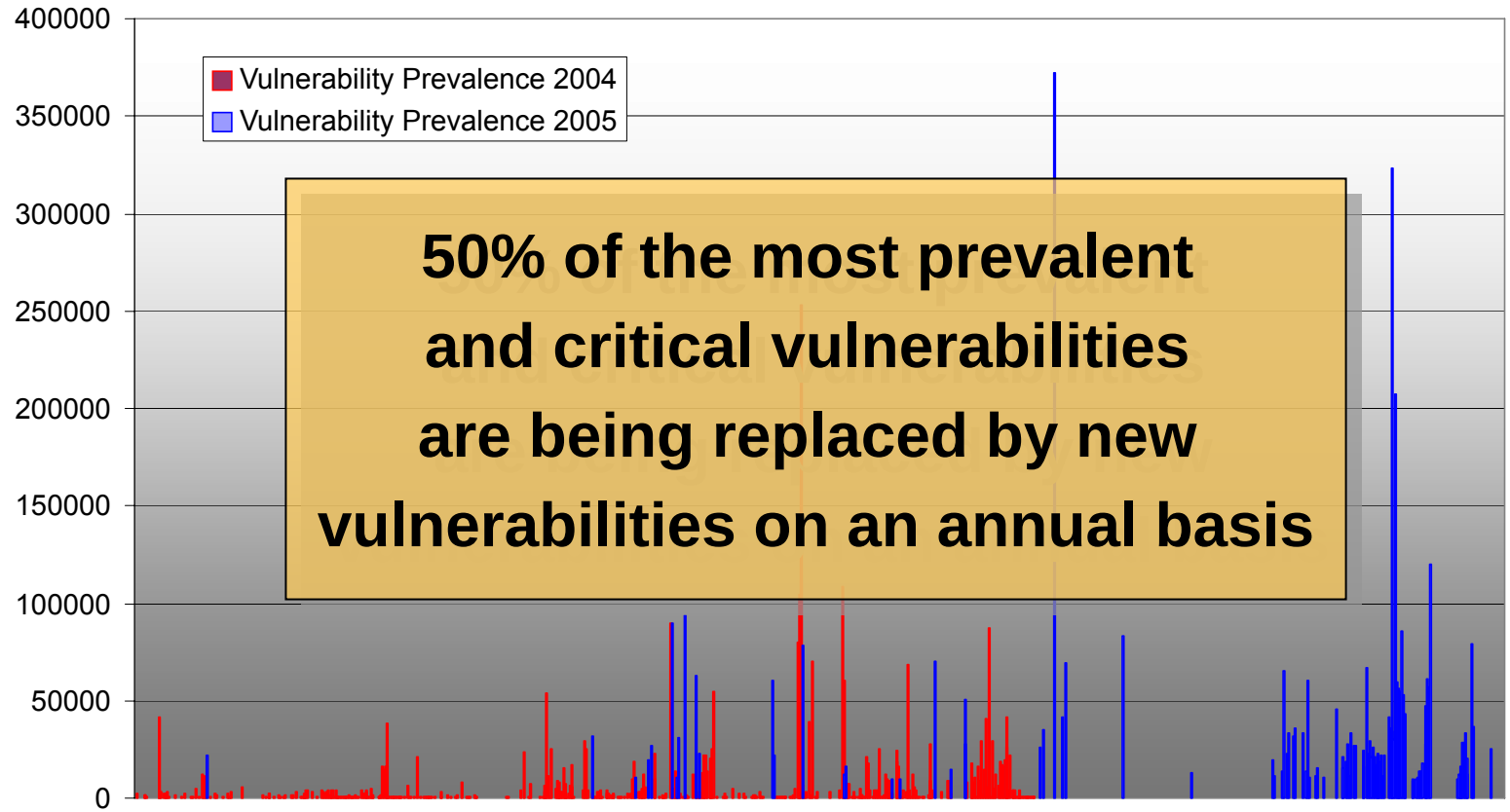


Automated attacks create 85% of their damage within the first fifteen days from outbreak and have unlimited life time

Mapping Vulnerability Prevalence



The Changing Top of the Most Prevalent



Top 10 External (Most Prevalent and Critical Vulnerabilities) as of November 15, 2005

Title	Qualys ID	CVE Reference	External Reference
Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)	90108	CAN-2003-0533	MS04-011
Buffer Management Vulnerability in OpenSSH	38217	CAN-2003-0693	CA-2003-24
Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability	50080	CAN-2003-0694	CA-2003-25
Microsoft Windows RPC Runtime Library Vulnerability	68528	CAN-2003-0813	MS04-012
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	90103	CAN-2003-0818	MS04-007
Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities	90244	CAN-2005-0048	MS05-019
Microsoft SMB Remote Code Execution Vulnerability	90252	CAN-2005-1206	MS05-027
Writeable SNMP Information	78031	N/A	N/A
Unauthenticated Access to FTP Server Allowed	27210	N/A	N/A
SSL Server Allows Cleartext Communication Vulnerability	38143	N/A	N/A

Top 10 Internal (Most Prevalent and Critical Vulnerabilities) as of November 15, 2005

Title	Qualys ID	CVE Reference	External Reference
Microsoft Messenger Service Buffer Overrun Vulnerability	70032	CAN-2003-0717	MS03-043
Microsoft Windows RPC Runtime Library Vulnerability	68528	CAN-2003-0813	MS04-012
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	90103	CAN-2003-0818	MS04-007
Microsoft Word Vulnerability Could Allow Remote Code Execution	110031	CAN-2005-0558	MS05-023
Microsoft SMB Remote Code Execution Vulnerability	90252	CAN-2005-1206	MS05-027
Microsoft Windows Print Spooler Service Remote Code Execution	90270	CAN-2005-1984	MS05-043
Microsoft MSDTC and COM+ Remote Code Execution Vulnerability	90274	CAN-2005-2119	MS05-051
Graphics Rendering Engine Multiple Code Execution Vulnerabilities	90284	CAN-2005-2123	MS05-053
Microsoft Internet Explorer Cumulative Patch Missing	100030	CAN-2005-2127	MS05-052
Adobe Acrobat Reader Remote Buffer Overflow Vulnerability	38461	CAN-2005-2470	N/A

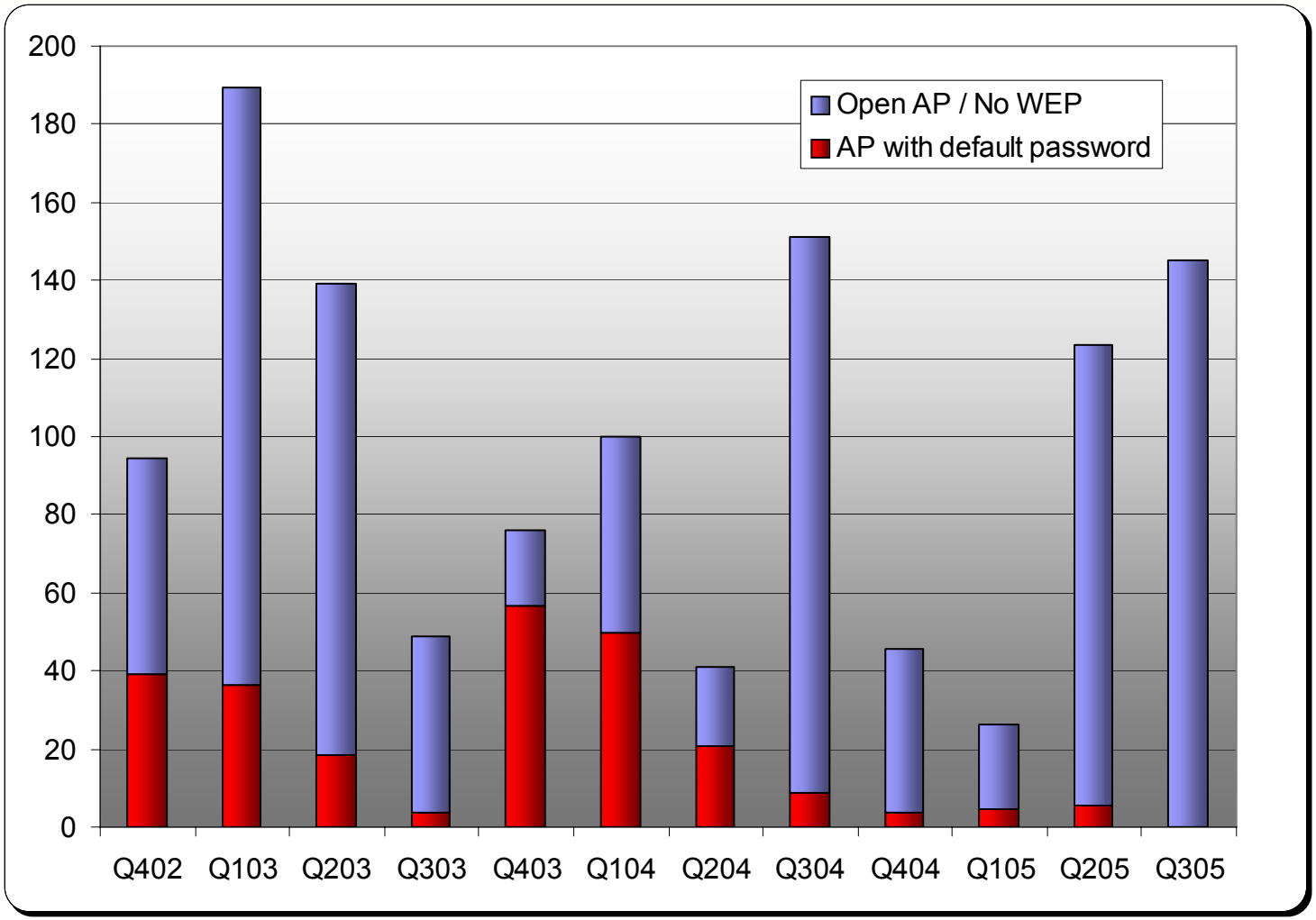
The Record Breakers

- Fastest fixed Vulnerability
  - Windows Plug and Play vulnerability - MS05-039
- Longest lingering critical vulnerability
  - SNMP Writeable
- Most Prevalent critical vulnerability
  - Microsoft Windows DCOM RPC
- Most active Worm:
  - Blaster

Myth About Wireless Security

Emerging technologies, such as wireless networks are a significant security vulnerability in enterprise environments

The Real World: Configuration Issues in Wireless Access Points



Conclusion: Wireless Security Vulnerability

The issue of security vulnerabilities in Wireless devices is significantly overrated – only 1 in nearly 20,000 critical vulnerabilities is caused by a wireless device.

The Laws of Vulnerabilities

#1. Half-Life

The half-life of critical vulnerabilities is 19 days on external systems and 48 days on internal systems, and doubles with lowering degrees of severity

#2. Prevalence

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

#3. Persistence

4% of critical vulnerabilities remain persistent, and their lifespan is unlimited

The Laws of Vulnerabilities

#4. Focus

90% of vulnerability exposure is caused by 10% of critical vulnerabilities

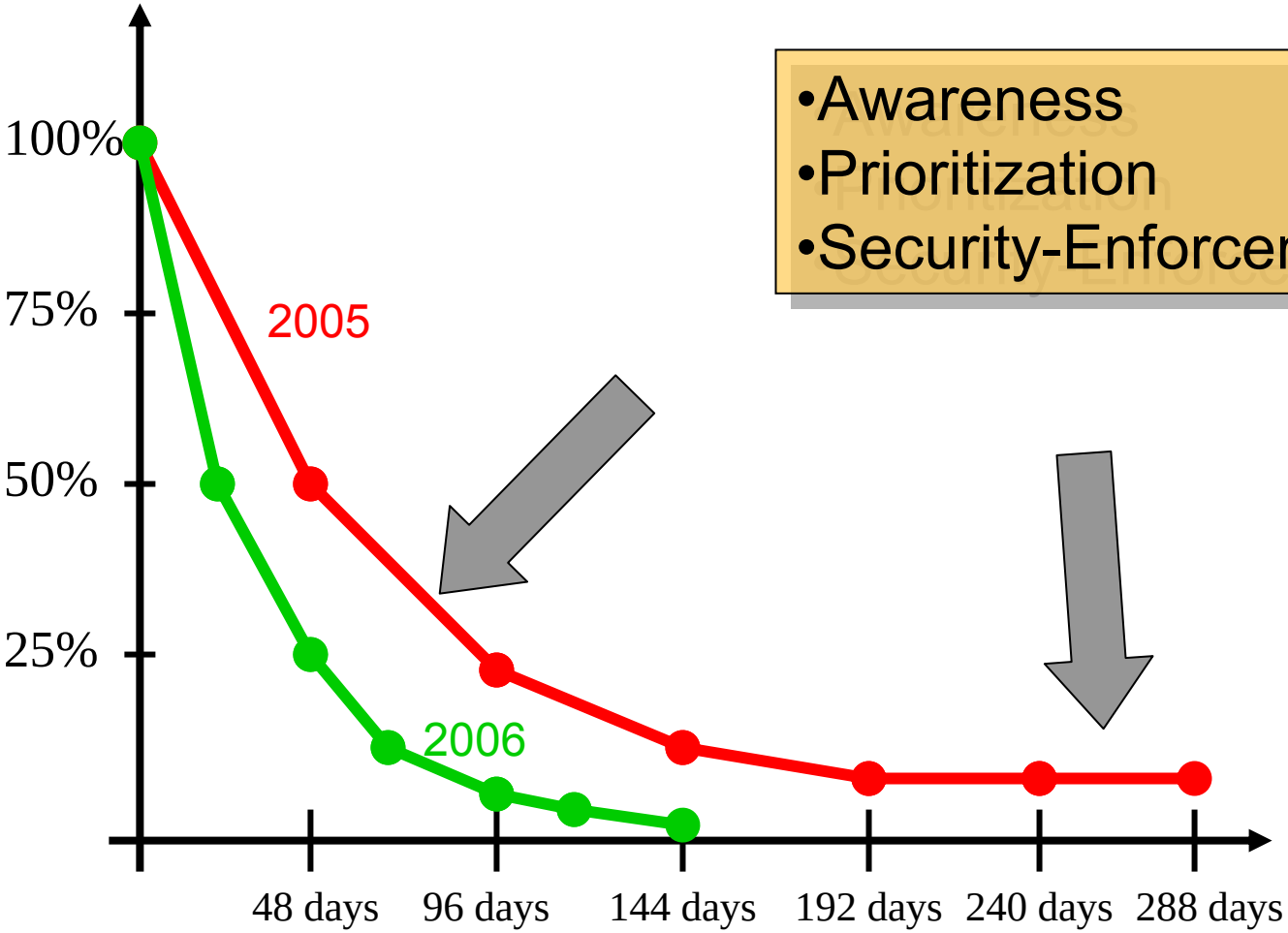
#5. Window of Exposure

The time-to-exploit cycle is shrinking faster than the remediation cycle. 80% of exploits are available within the first half-life period of critical vulnerabilities

#6. Exploitation

Automated attacks create 85% of their damage within the first fifteen days from the outbreak and have unlimited life time

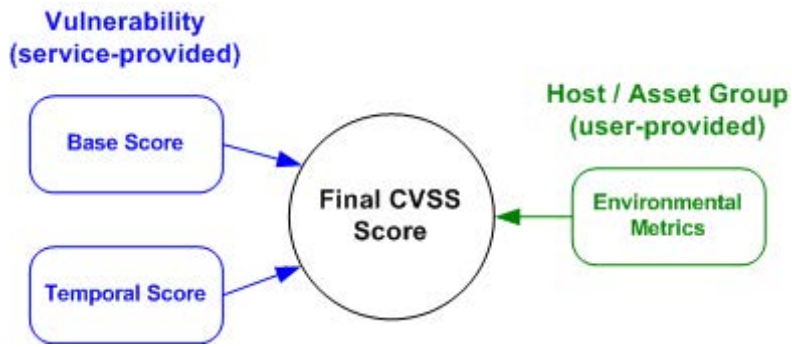
Goal for 2006: Shortening the Half-Life of Critical Vulnerabilities by 20%



- Awareness
- Prioritization
- Security-Enforcement

Common Vulnerability Scoring System (CVSS)

- Industry Standard for common vulnerability scoring supported by CERT, Mitre, Cisco, Symantec, Microsoft, and Qualys
- CVSS provides an industry standard vulnerability scoring that allows corporations to take into consideration their own security metrics
- User customizable scoring based on three criteria
  - Base - Inherent threat of the vulnerability
  - Temporal - Time of vulnerability's existence
  - Environmental - User environment variables
- Customer Benefits
  - Prioritize remediation on critical assets
  - Identify risk on individual hosts



Proposed Solutions

- Establish enterprise vulnerability management program
- Network Admission Control (NAC) is a new trend to stop threats before they affect the enterprise
- Enforce best practices for configuration and policy management
- New standard for prioritization of remediation – CVSS

Summary and Actions We Can Take

- Significant progress on improving the remediation cycle
- Predefined vulnerability release schedules are shortening the patch cycle
- Need to counter the shrinking time-to-exploit cycle
- Goal: Shortening the Half-Life of vulnerabilities by 20% within one year
- Required: Your support to reach this goal

Thank You

- References:
  - http://www.qualys.com/laws This presentation and any future updates
  - http://www.qualys.com/top10 Continuously updated Top Ten Index of most prevalent and critical external and internal vulnerabilities
  - http://www.qualys.com/top10scan Free Top Ten Assessment Tool
  - http://www.first.org/cvss Information about CVSS
- Comments and Suggestions: tramos@qualys.com