Gerhard Eschelbeck
CTO and VP Engineering
Qualys

BlackHat Conference July 2004

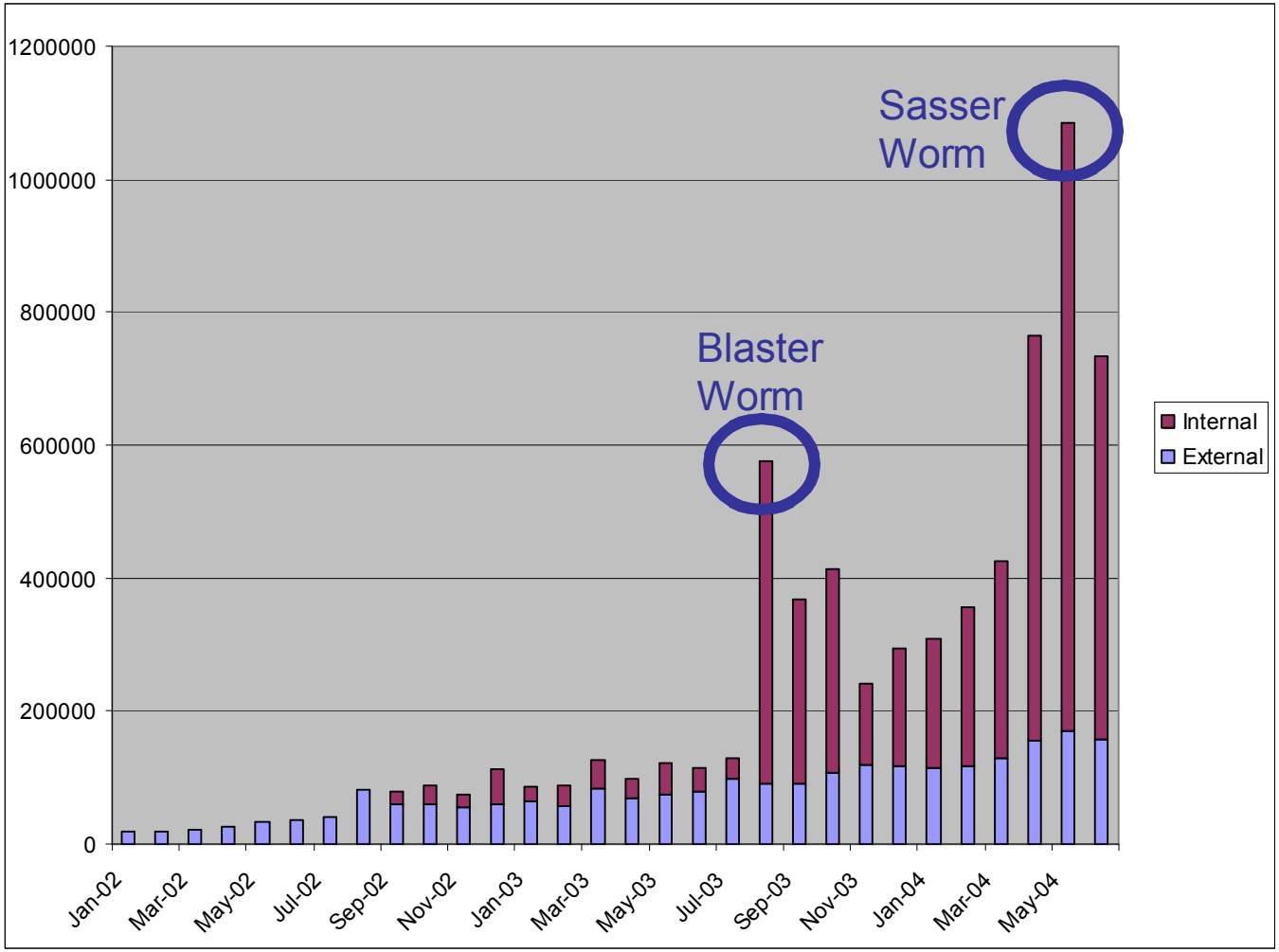
Agenda

- Methodology
- One Year After: Update on the External Data
- The Internal Data
- The Laws of Vulnerabilities
- Summary and Action

Research

- Objective: Understanding prevalence of critical vulnerabilities over time in real world
- Timeframe: January 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

External and Internal Data Sources



Raw Results

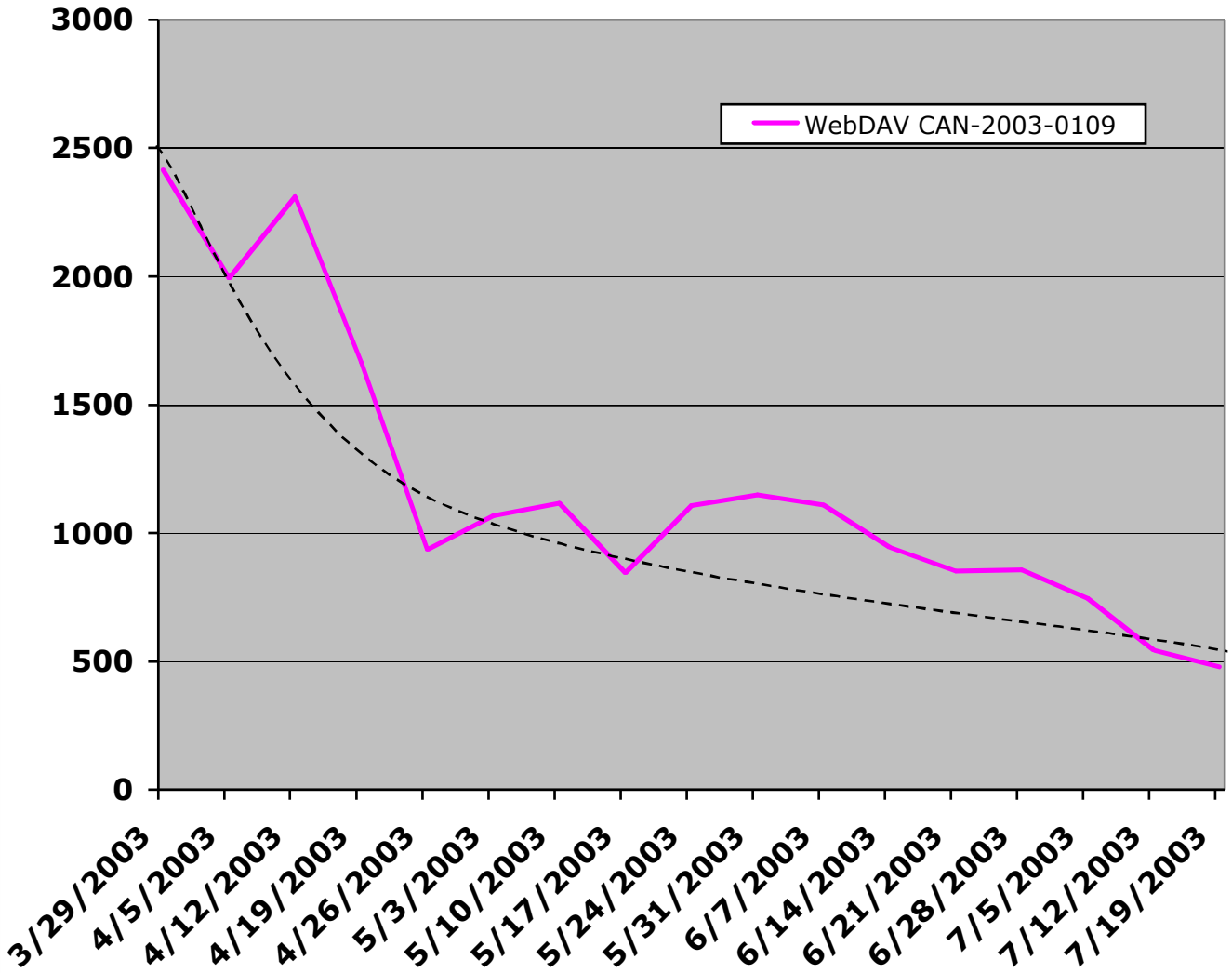
- Largest collection of global real-world vulnerability data:
  - 6,627,000 IP-Scans since begin 2002
  - 2,275 out of 3,374 unique vulnerabilities detected in the real world
  - 3,834,000 total critical* vulnerabilities found
  - 1,031 out of 1,504 unique critical vulnerabilities detected in the real world

* 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.

Analysis Performed

- Identifying Window of Exposure
- Lifespan of Critical Vulnerabilities
- Resolution Response
- Trend over Time
- Vulnerability Prevalence

Microsoft WebDAV Vulnerability

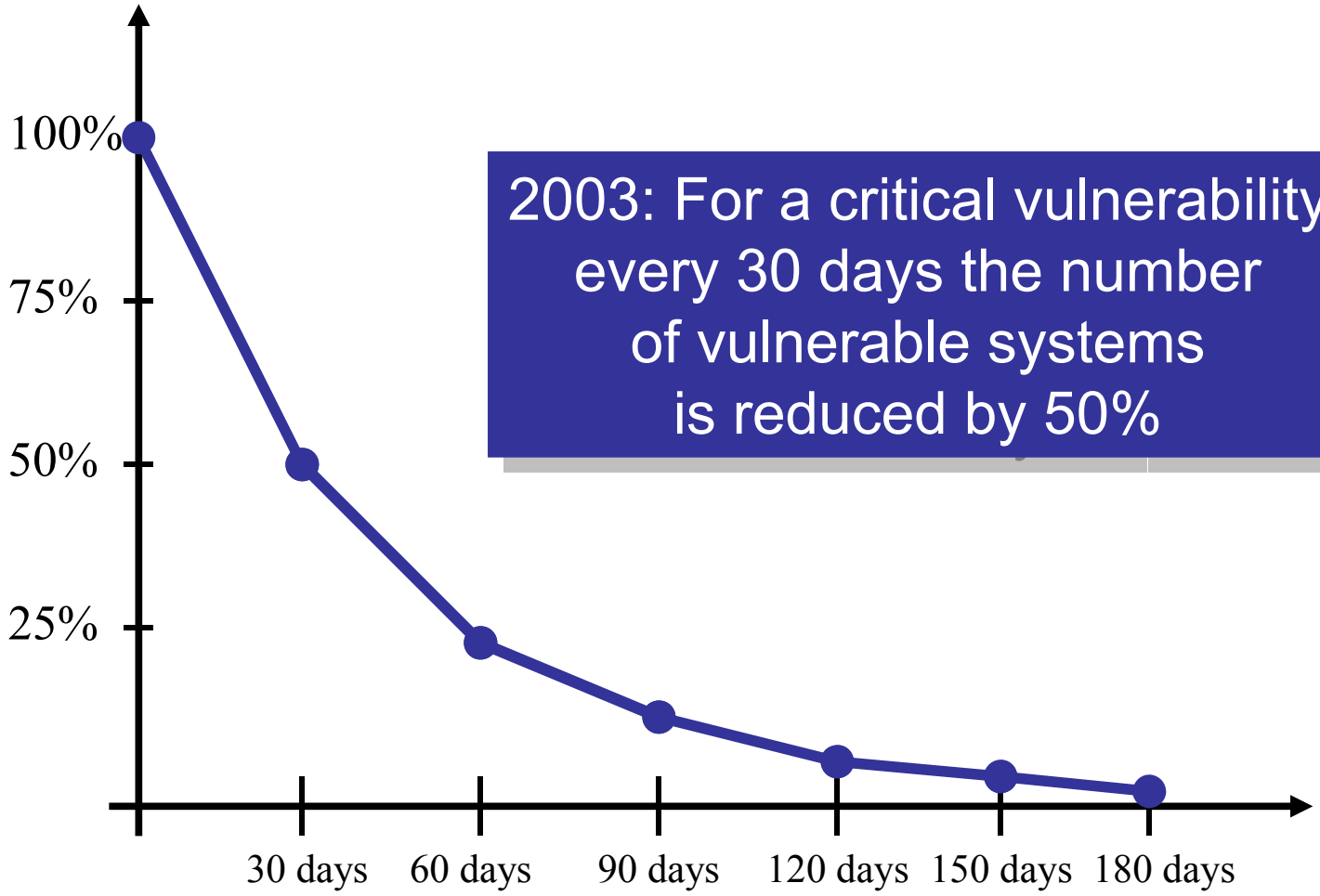


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

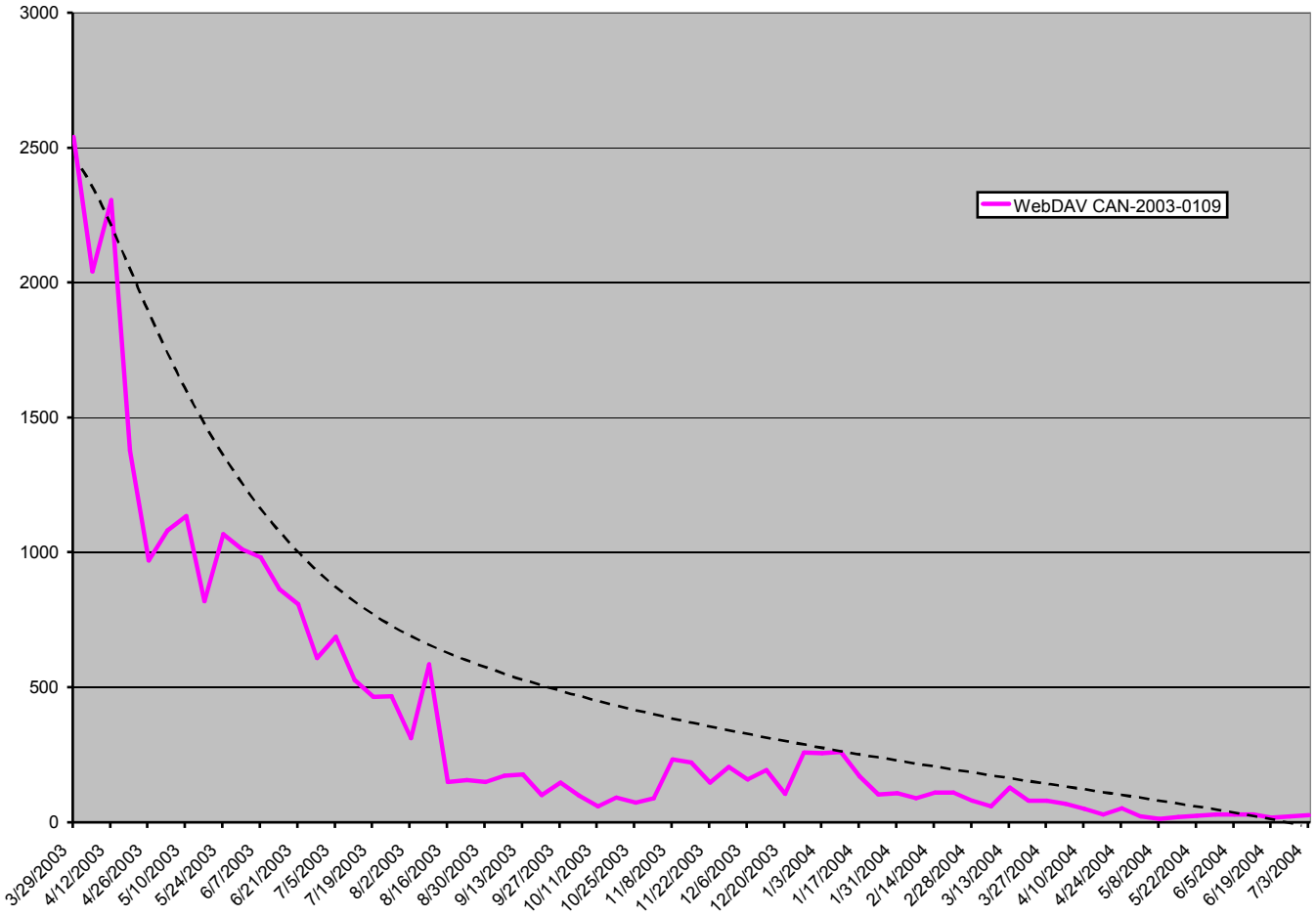
Released: March 2003

Vulnerability Half-Life



2003: For a critical vulnerability every 30 days the number of vulnerable systems is reduced by 50%

Microsoft WebDAV Vulnerability

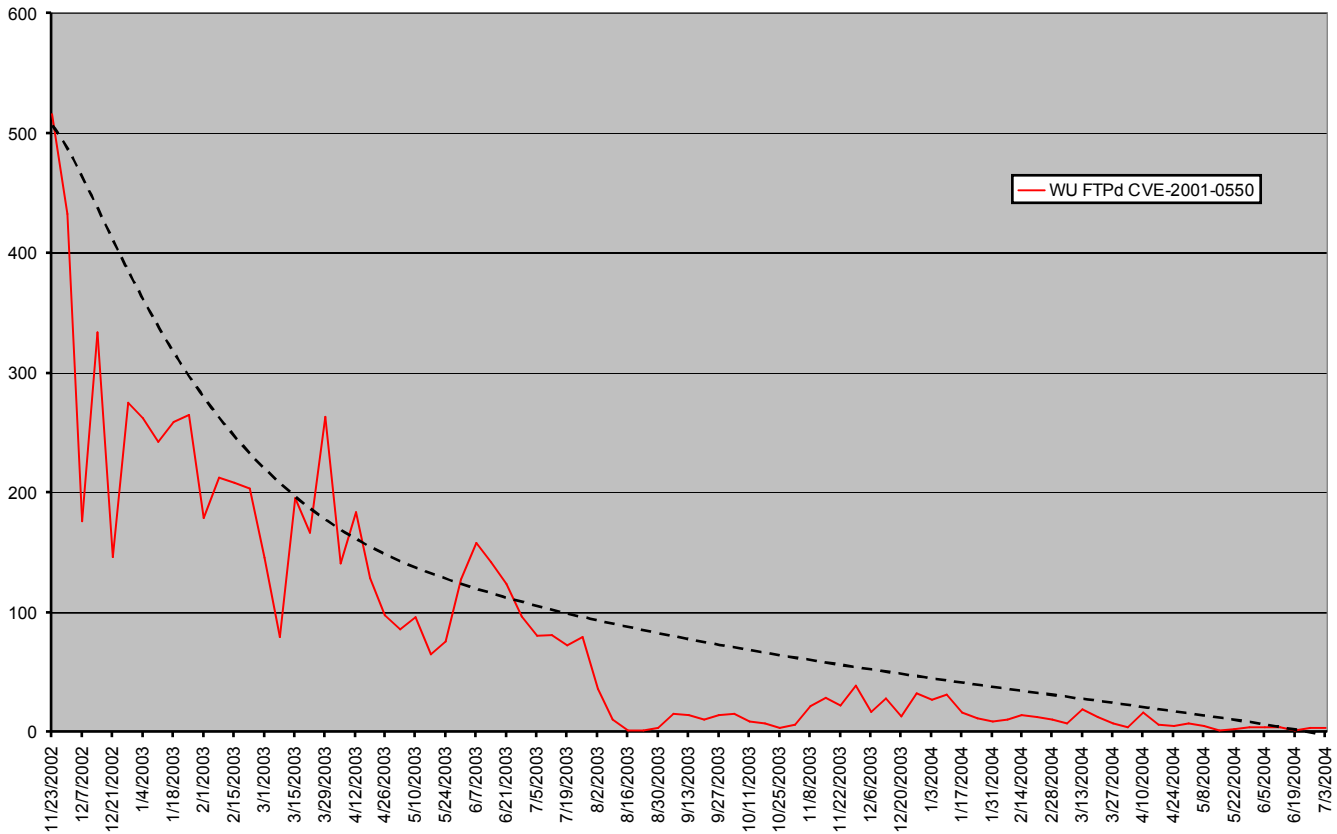


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

Released: March 2003

WU-FTPd File Globbing Heap Corruption Vulnerability

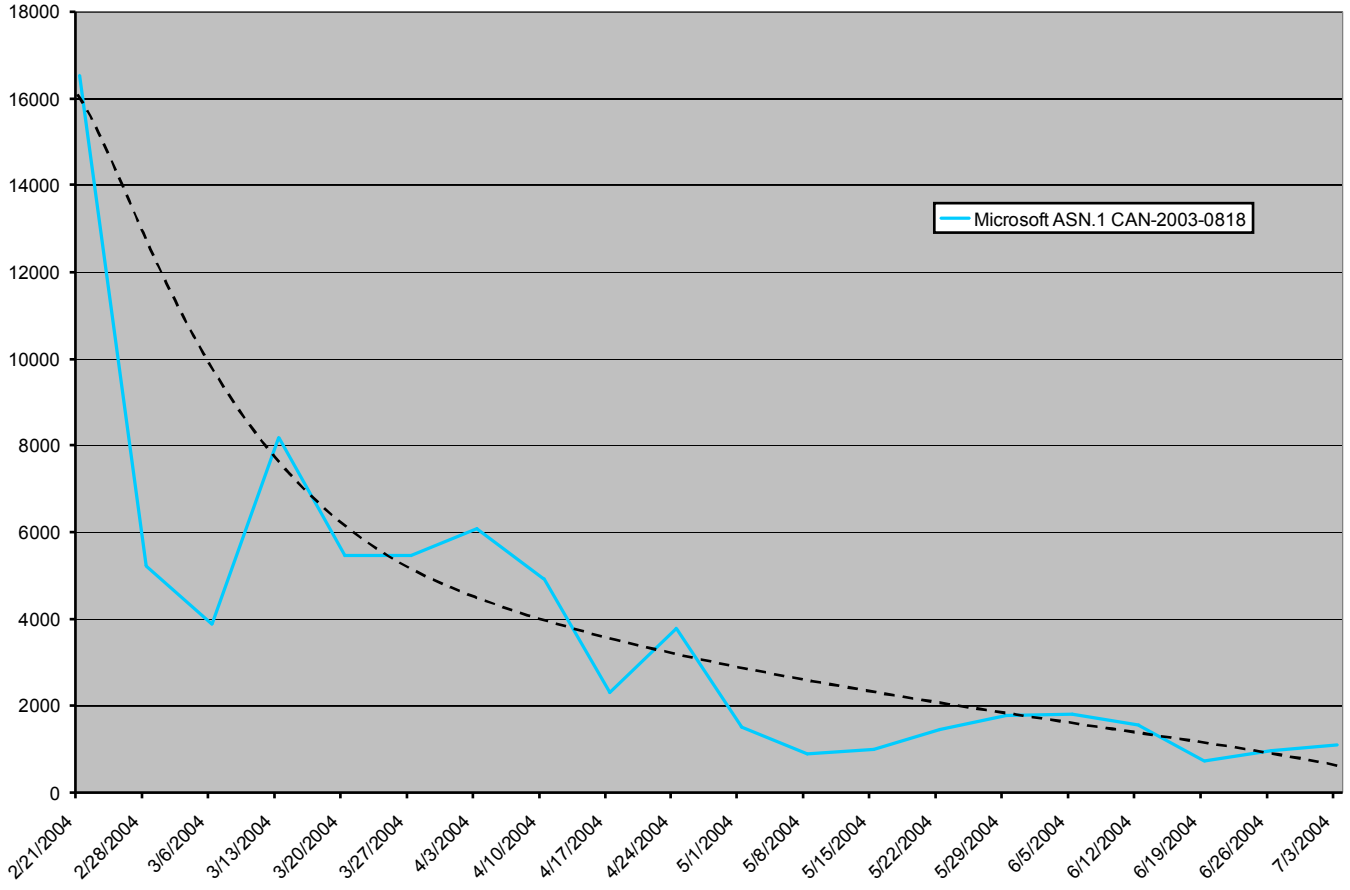


WU-FTPd File Globbing Heap Corruption Vulnerability

CVE-2001-0550
Qualys ID 27126

Released: November 2001

Microsoft Windows ASN.1 Library Integer Handling Vulnerability

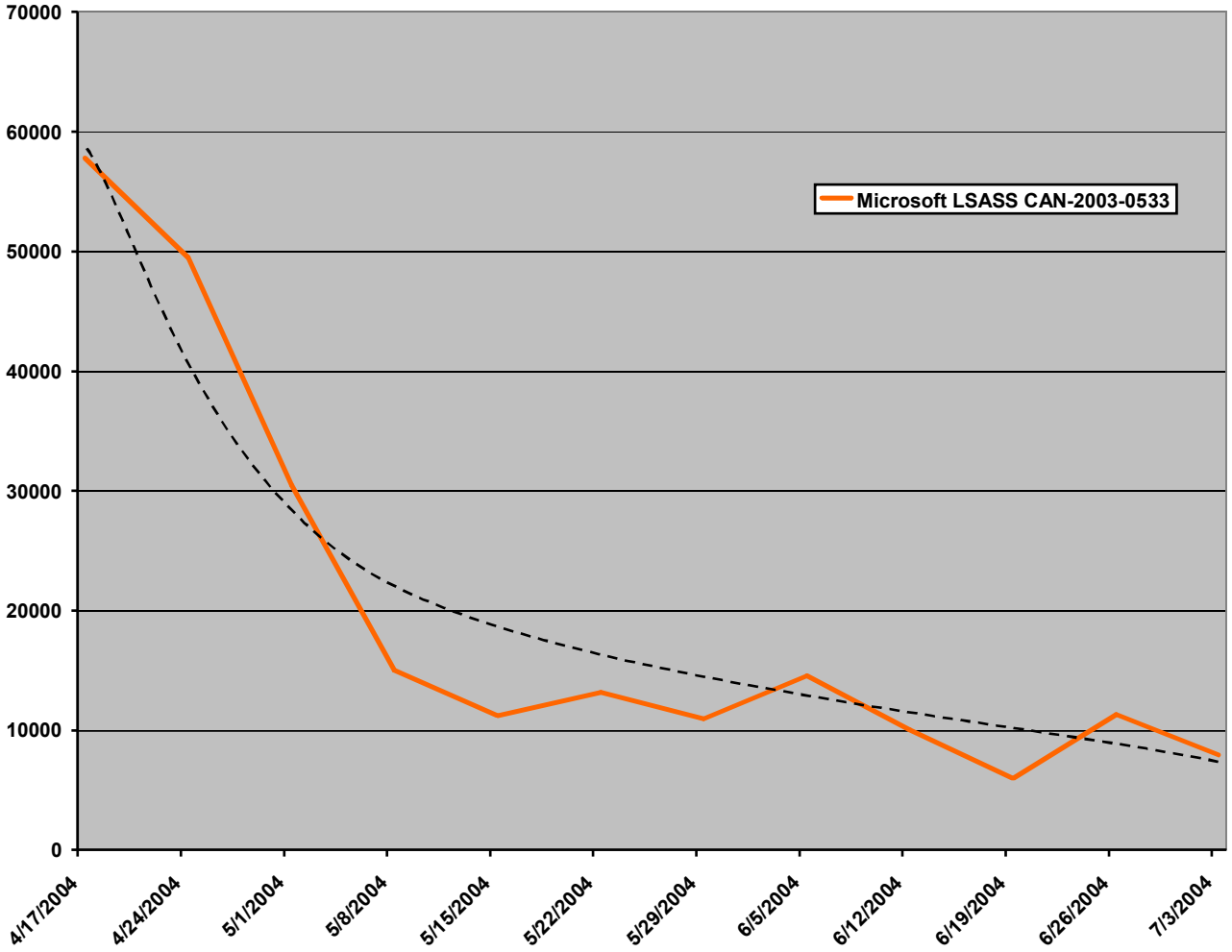


Microsoft Windows ASN.1 Library Integer Handling Vulnerability

CAN-2003-0818
Qualys ID 90103

Released: February 2004

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

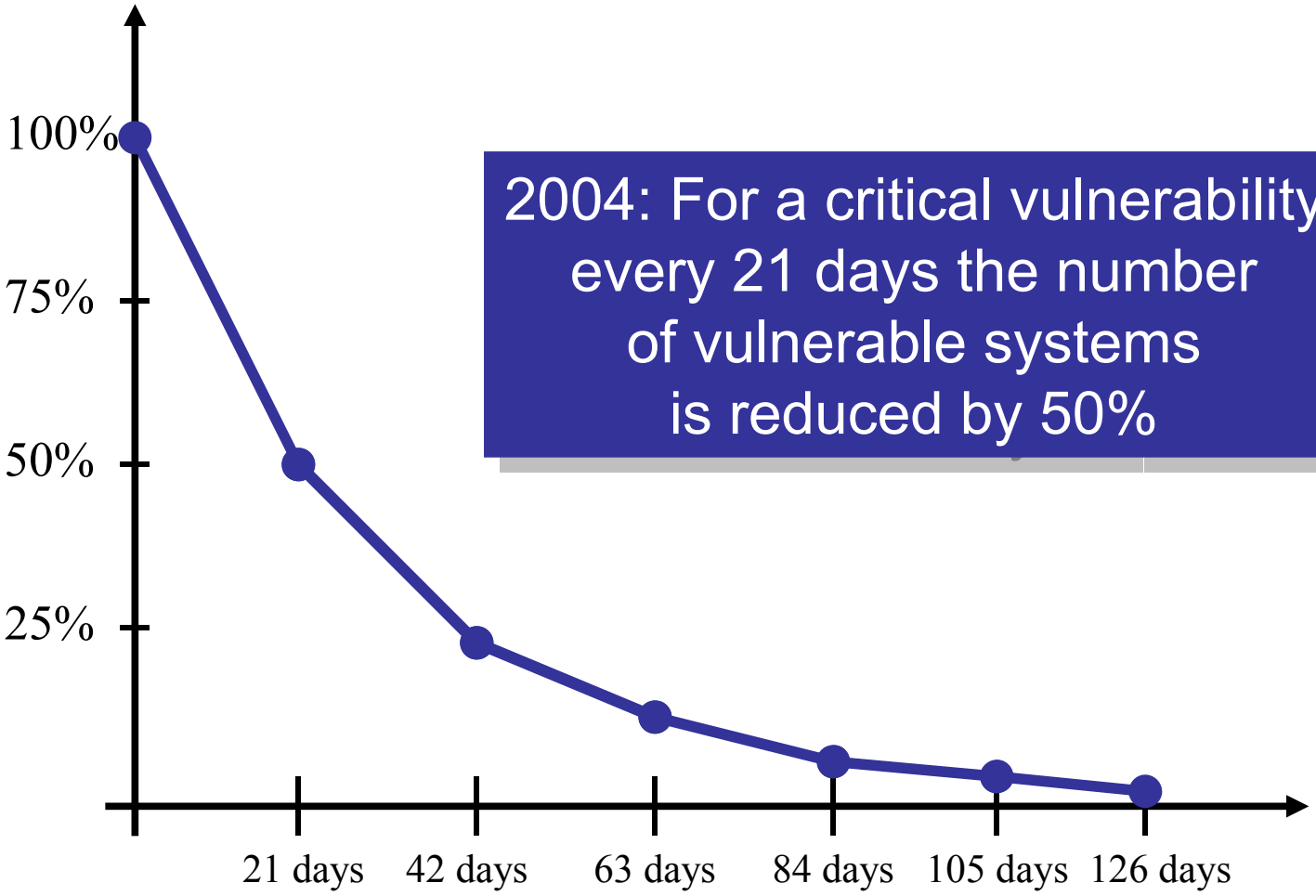


Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

CAN-2003-0533
Qualys ID 90108

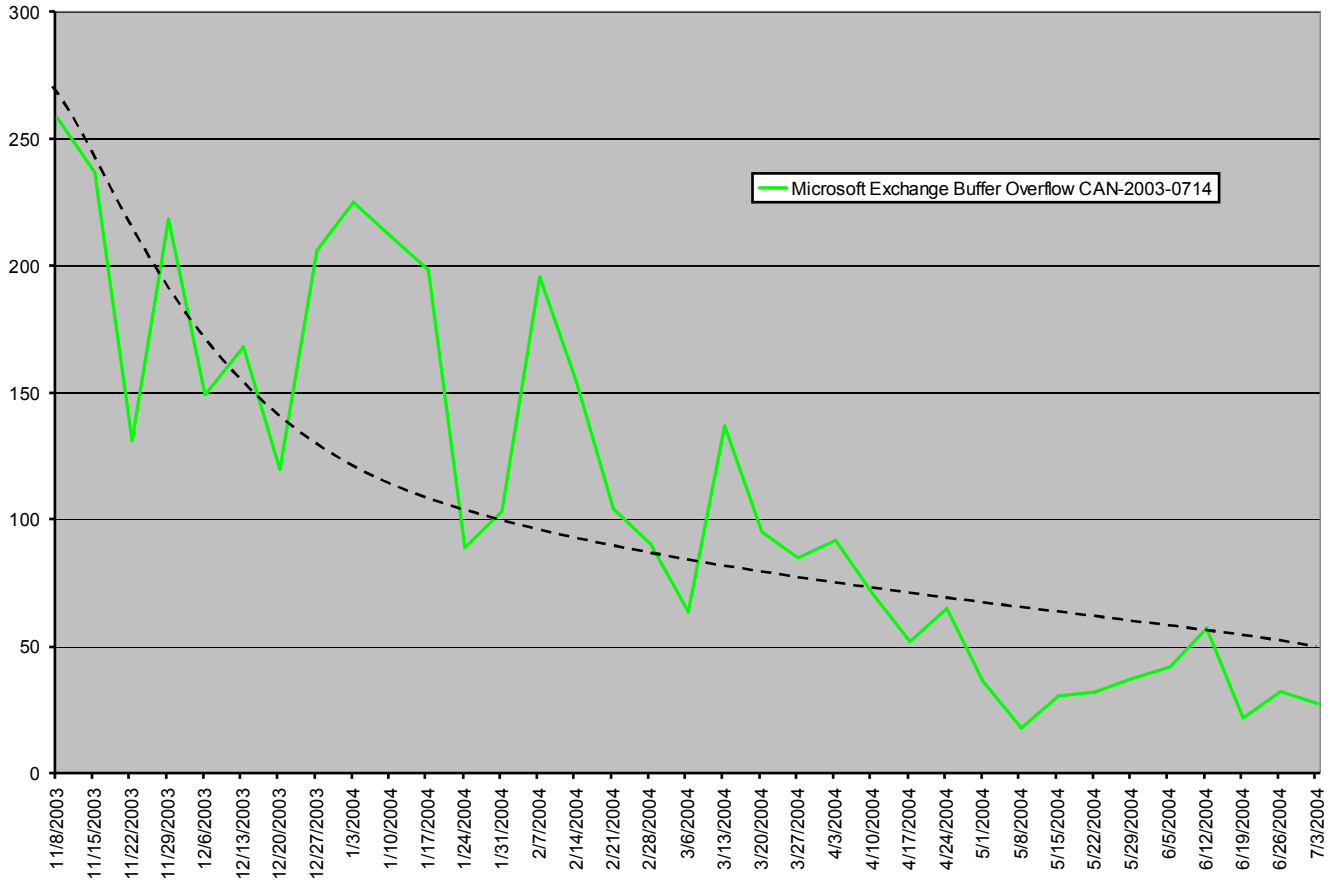
Released: April 2004

Vulnerability Half-Life



2004: For a critical vulnerability every 21 days the number of vulnerable systems is reduced by 50%

Microsoft Exchange Server Buffer Overflow Vulnerability

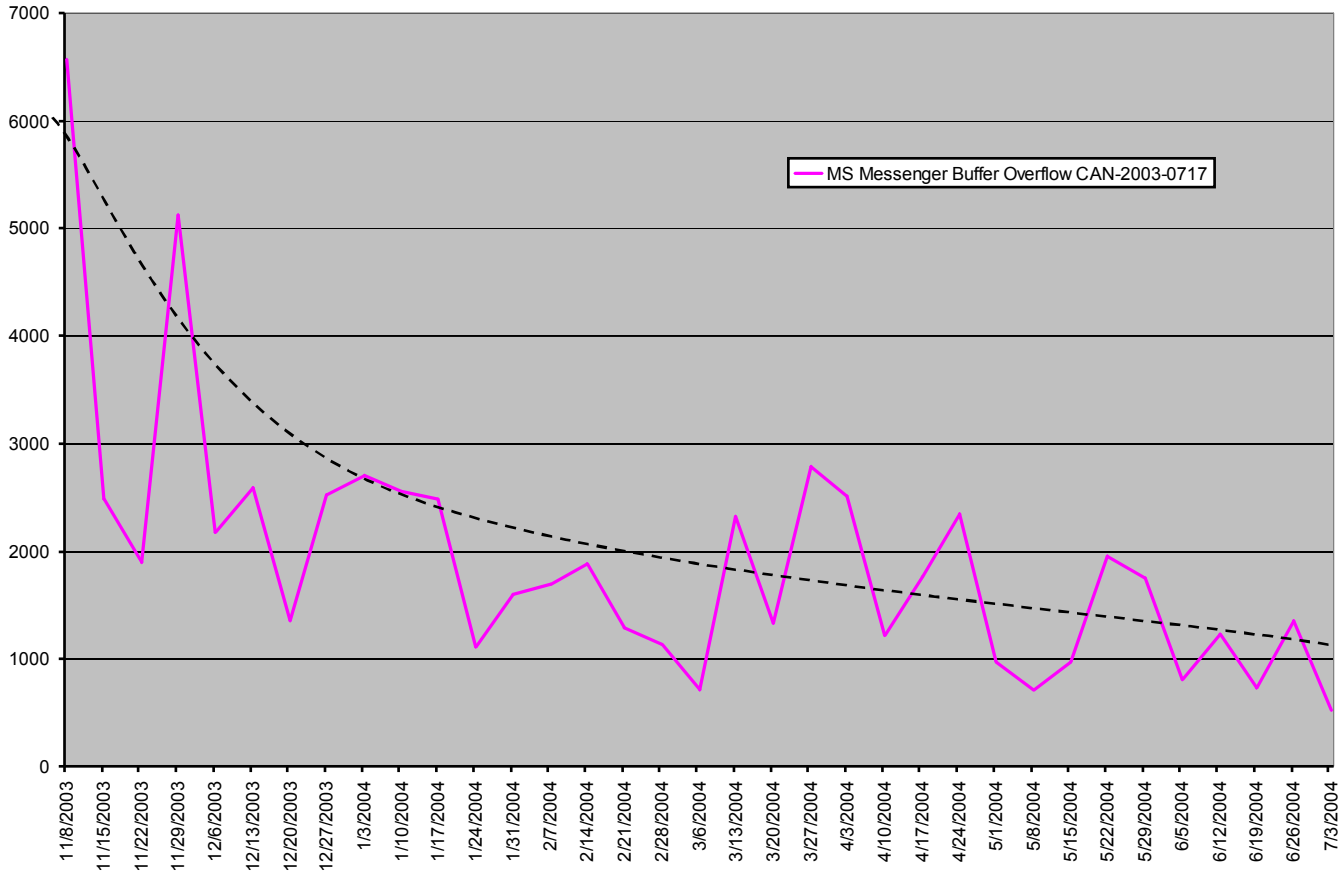


Microsoft Exchange Server Buffer Overflow Vulnerability

CAN-2003-0714
Qualys ID 74143

Released: October 2003

Microsoft Messenger Service Buffer Overflow Vulnerability

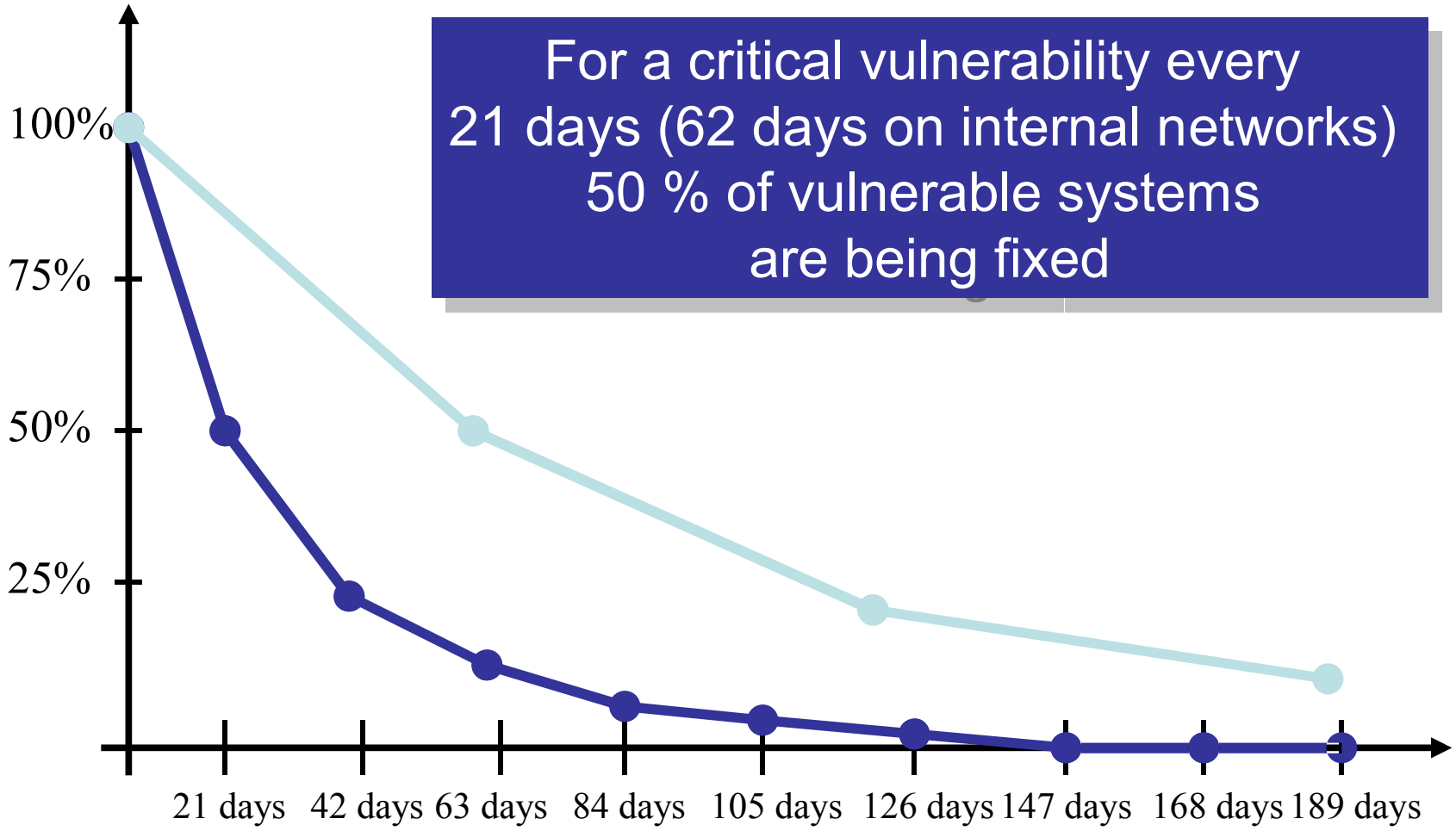


Microsoft Messenger Service Buffer Overflow Vulnerability

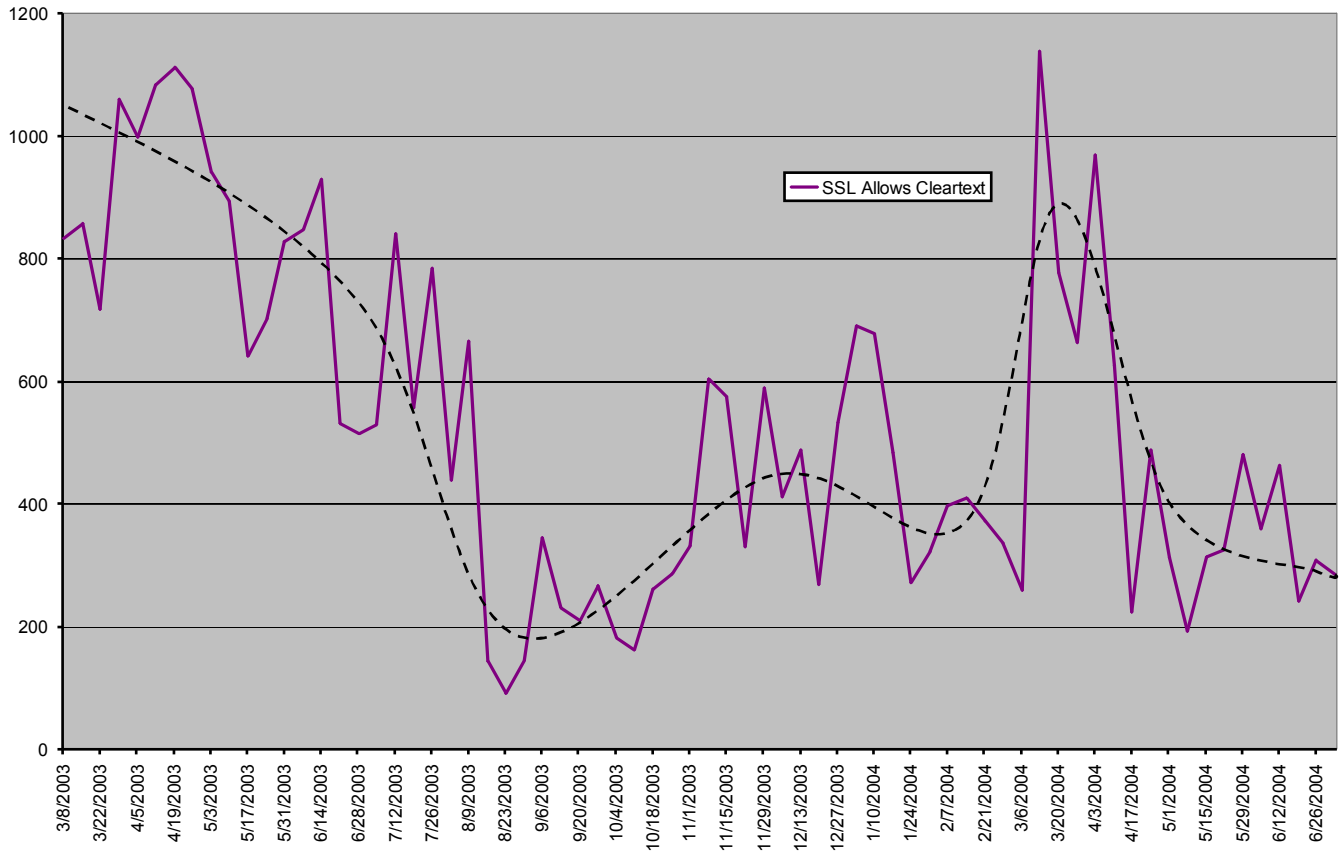
CAN-2003-0717
Qualys ID 70032

Released: October 2003

External vs. Internal Vulnerability Half-Life



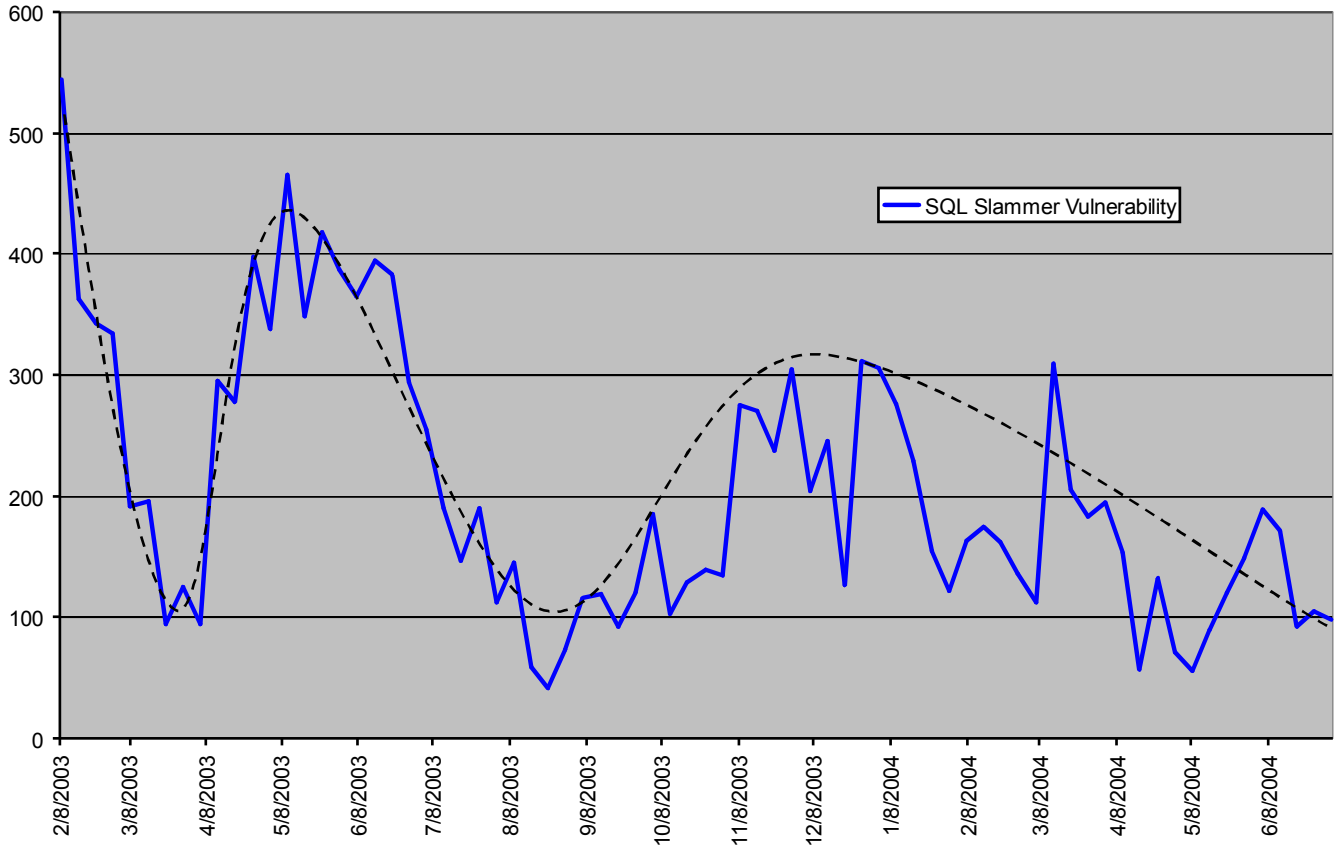
SSL Server Allows Cleartext Communication



SSL Server Allows Cleartext Communication

Qualys ID 38143

SQL Slammer Vulnerability

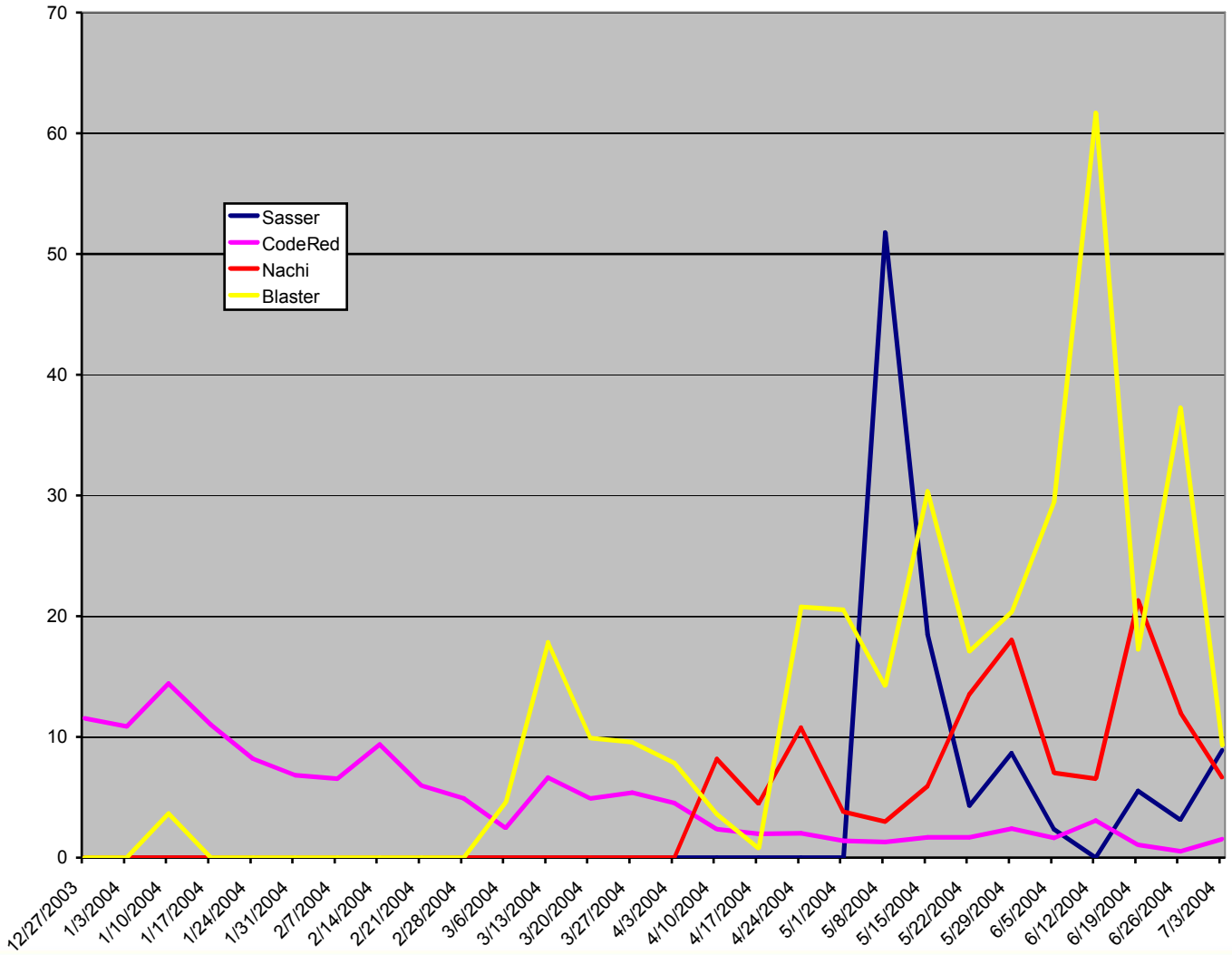


MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability

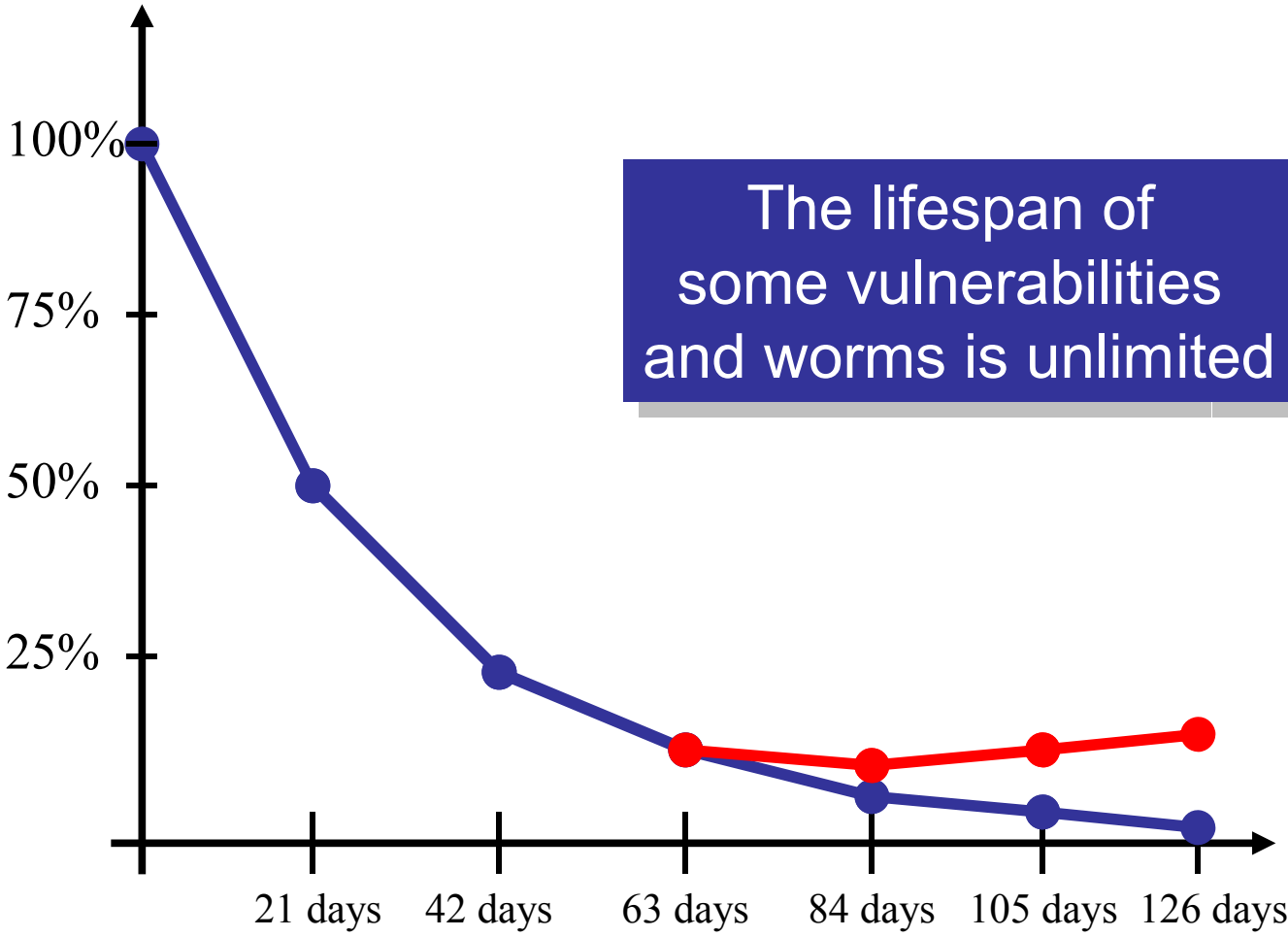
CAN-2002-0649
Qualys ID 19070

Released: July 2002

A Continuous Cycle of Infection

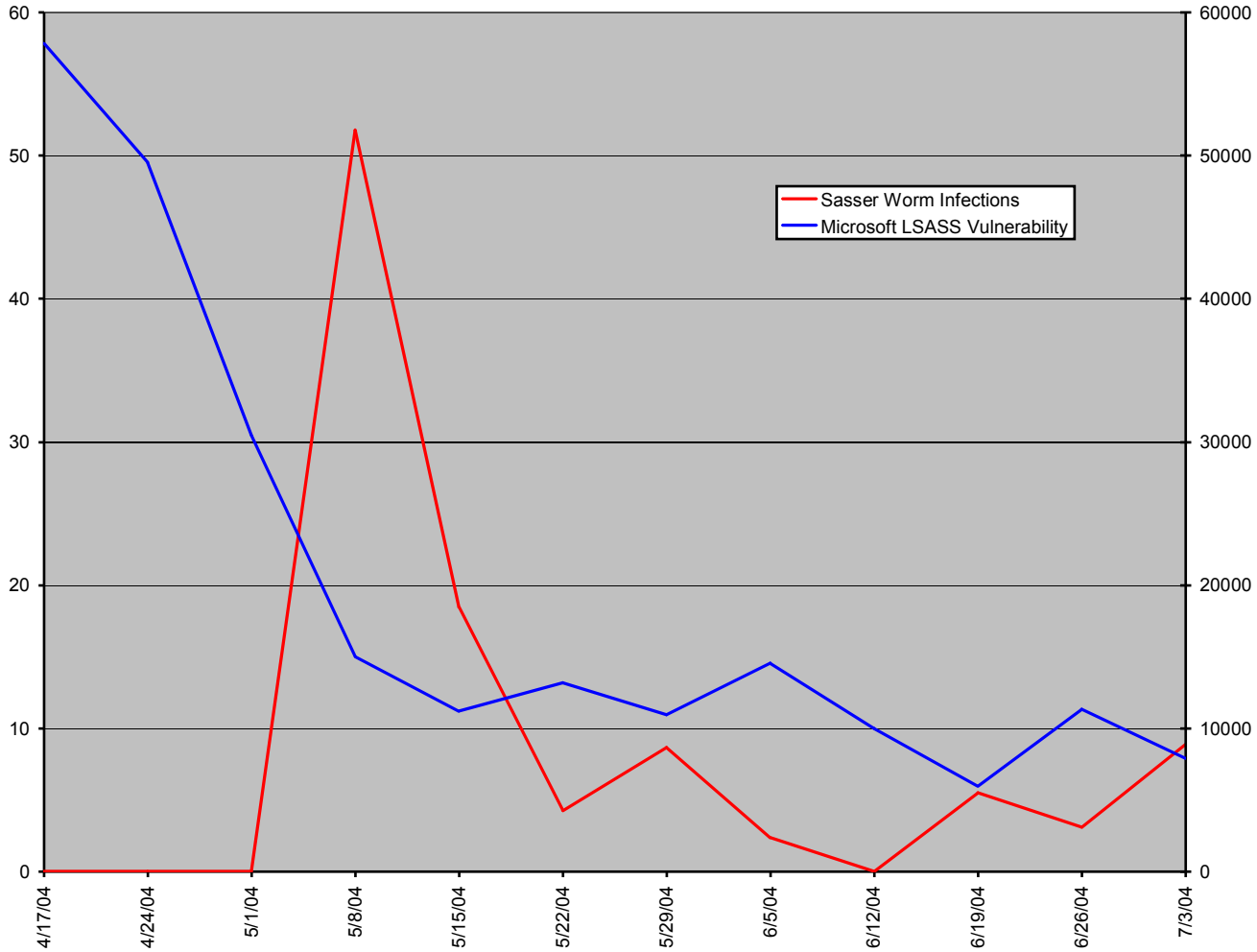


Vulnerability Lifespan



The lifespan of some vulnerabilities and worms is unlimited

The Sasser Worm and its Victims

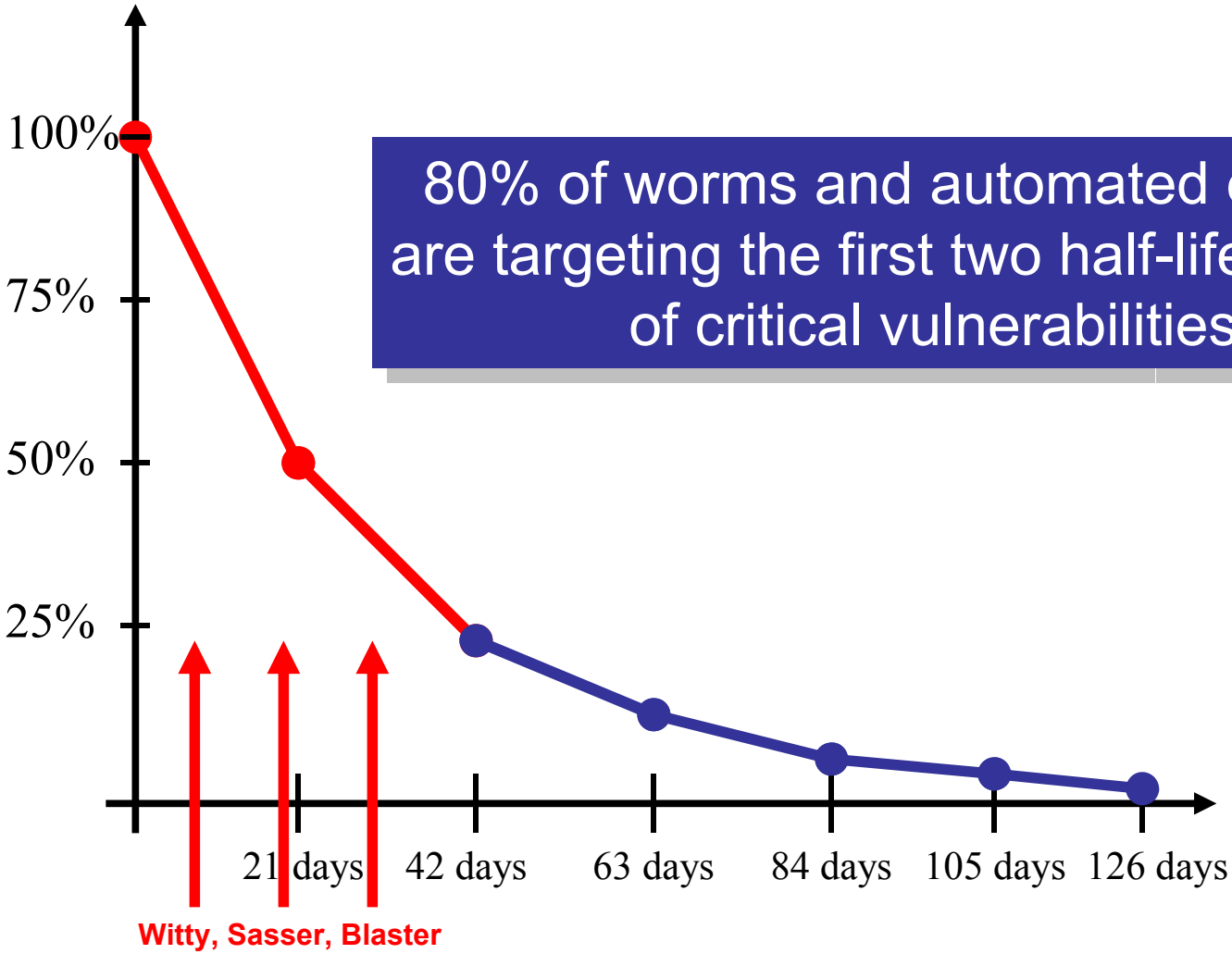


Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

CAN-2003-0533
Qualys ID 90108

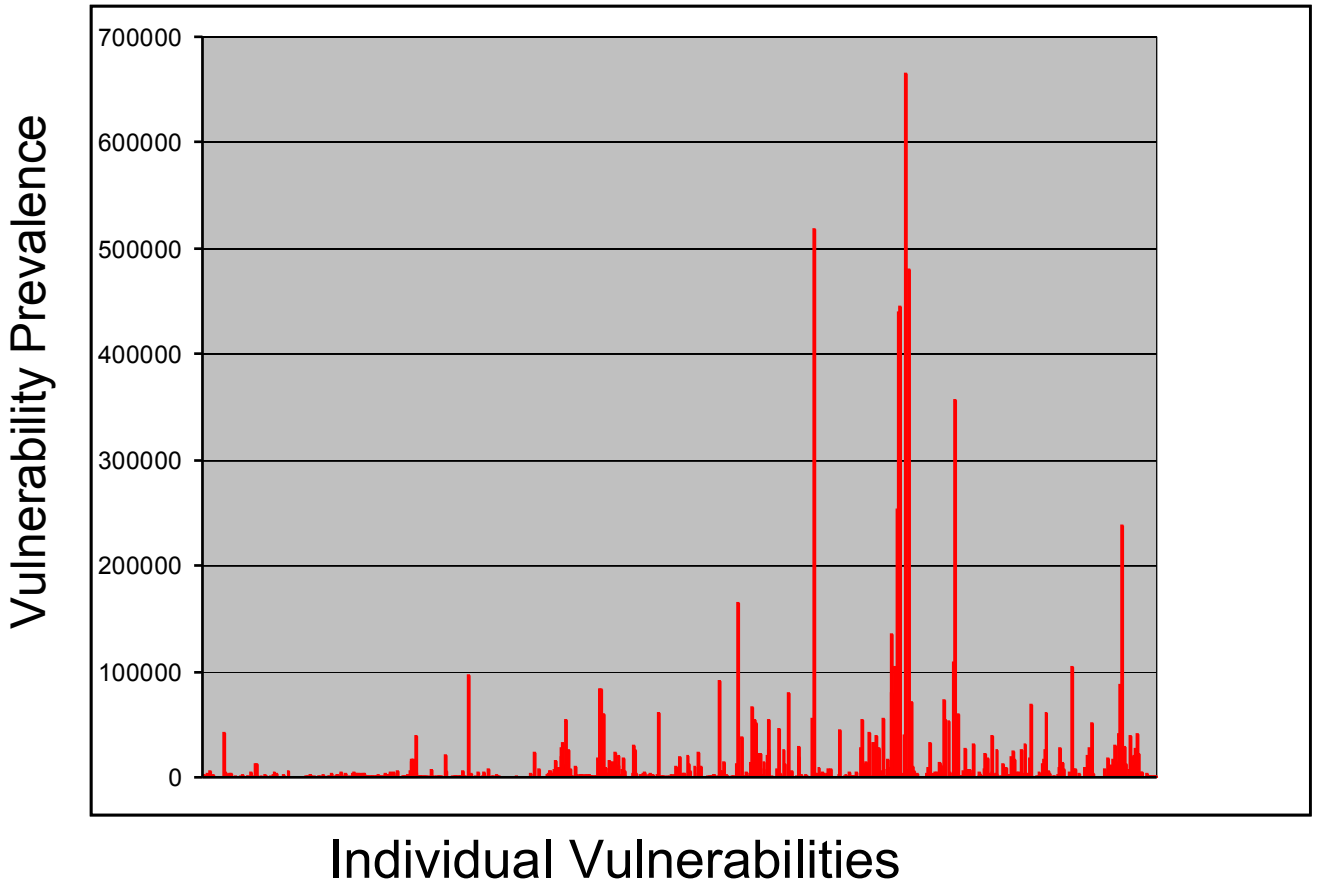
Released: April 2004

The Impact of an Exploit



80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities

Mapping Vulnerability Prevalence



The Changing Top of the Most Prevalent

Vulnerability	CVE	Jul-02	Jan-03	Jul-03	Jan-04	Jul-04
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 FTP Connection Status Request Denial of Service Vulnerability	CVE-2002-0073	x	x			
Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability	CVE-2002-0079	x	x			
Microsoft IIS HTR ISAPI Extension Heap Overflow Vulnerability	CVE-2002-0364	x	x			
Microsoft IIS 4.0/5.0			x	x		
Microsoft IIS CGI Fil			x	x		
Microsoft IIS Malforr			x	x		
Microsoft IIS HTR CI			x	x	x	
Apache Chunked-Er			x	x	x	x
OpenSSH Challenge			x	x	x	x
Multiple Vendor SNM			x	x	x	
ISC BIND SIG Cache			x	x	x	
Microsoft Windows				x	x	x
Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161			x	x	x
Microsoft SMB Request Handler Buffer Overflow Vulnerability	CAN-2003-0345			x	x	
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352			x	x	x
Microsoft DCOM RPCSS Service Vulnerabilities	CAN-2003-0528				x	x
Microsoft Messenger Service Buffer Overrrun Vulnerability	CAN-2003-0717					x
Buffer Overflow in Microsoft Local Security Authority Subsystem Service (LSASS)	CAN-2003-0533					x
Microsoft RPCSS Code Execution Variant	CAN-2003-0813					x
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	CAN-2003-0818					x

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

Top 10 External (Most Prevalent and Critical Vulnerabilities) as of July 28, 2004

Title	Qualys ID	CVE Reference	External Reference
Apache Chunked-Encoding Memory Corruption Vulnerability	86352	CVE-2002-0392	CA-2002-17
Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	86479	CAN-2003-0109	MS03-007
Microsoft Windows DCOM RPCSS Service Vulnerabilities	68522	CAN-2003-0528	MS03-039
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 RPCSS Code Execution Variant	68528	CAN-2003-0813	MS04-012
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	90103	CAN-2003-0818	MS04-007
SSL Server Allows Cleartext Communication Vulnerability	38143	N/A	
Writeable SNMP Information	78031	N/A	

Top 10 Internal (Most Prevalent and Critical Vulnerabilities) as of July 28, 2004

Title	Qualys ID	CVE Reference	External Reference
Microsoft SQL Weak Database Password	19001	CAN-2000-1209	
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	68518	CAN-2003-0352	MS03-026
Microsoft Windows DCOM RPCSS Service Vulnerabilities	68522	CAN-2003-0528	MS03-039
Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)	90108	CAN-2003-0533	MS04-011
Microsoft Messenger Service Buffer Overrun Vulnerability	70032	CAN-2003-0717	MS03-043
Microsoft Windows Wokrstation Service Remote Buffer Overflow Vulnerability	90078	CAN-2003-0812	MS03-049
Microsoft Windows RPCSS Code Execution Variant	68528	CAN-2003-0813	MS04-012
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	90103	CAN-2003-0818	MS04-007
Microsoft Internet Explorer Cumulative Security Update not installed	100004	CAN-2003-1026	MS04-004
Microsoft Outlook Express Cumulative Security Update not installed	90110	CAN-2004-0380	MS04-013

The Laws of Vulnerabilities

1. **Half-Life**

   The half-life of critical vulnerabilities is 21 days on external systems and 62 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

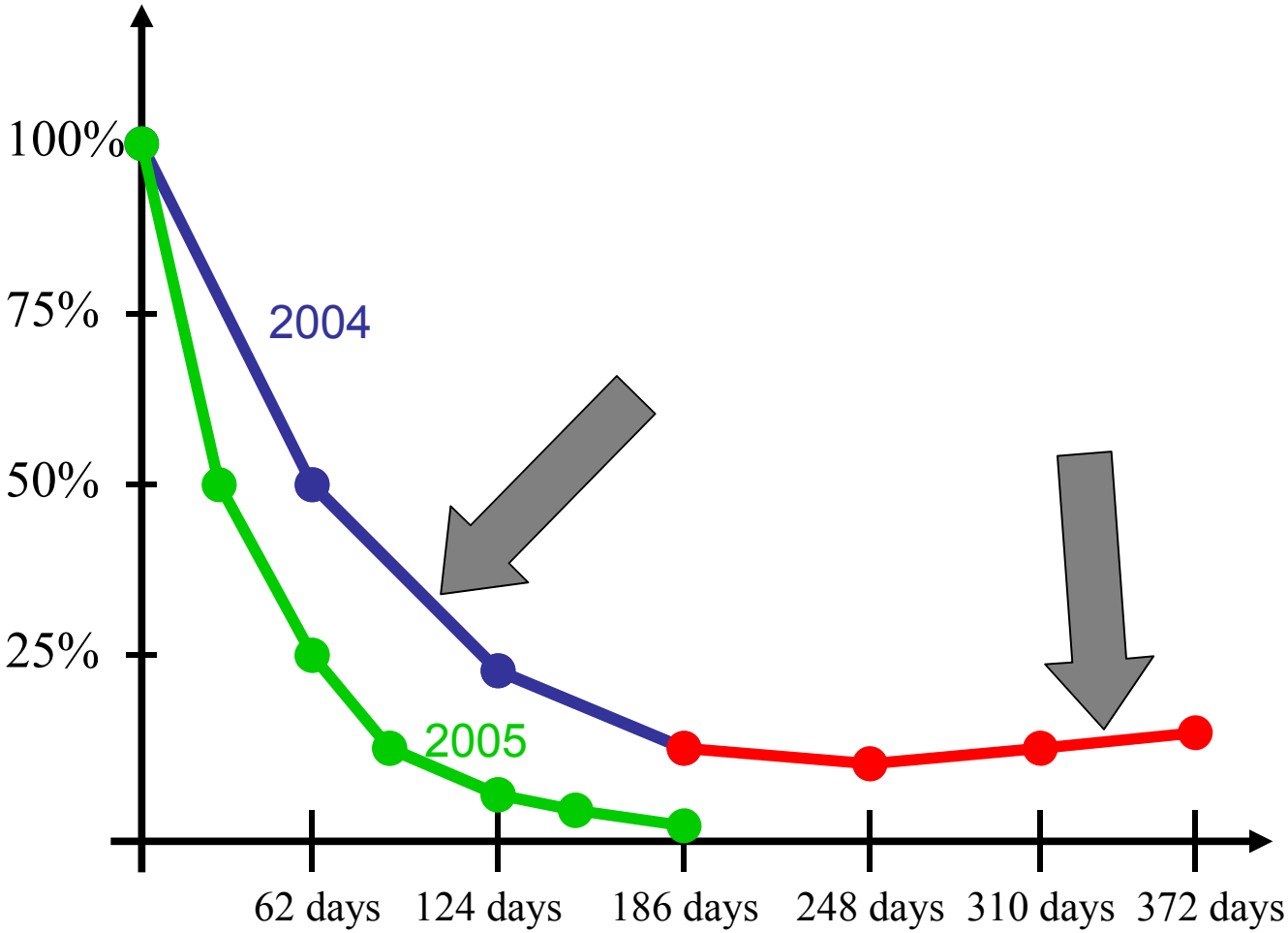
3. **Persistence**

   The lifespan of some vulnerabilities and worms is unlimited

4. **Exploitation**

   The vulnerability-to-exploit cycle is shrinking faster than the remediation cycle. 80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities

Goal: Shortening the Half-Life of Critical Vulnerabilities for Internal systems to 40 days



Summary and Actions we can take:

- Significant progress on the Remediation Cycle (30 to 21 days) for external Vulnerabilities
- Goal: Shortening the Half-Life of internal vulnerabilities from 62 days to 40 days within one year
- Required: Your support to reach this goal
- 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
- Comments and Suggestions: geschelbeck@qualys.com