QUALYS™

CISCO SYSTEMS

Threats of the Future … Be prepared

Patrick HUGUET
Managing Director EMEA, Qualys

June 17, 2004 – EBU

Qualys Mission & Company Overview

- Single focus on Managed Vulnerability Assessment
- 1400+ key customers growing at 100+ per month, includes:
  - Allied Irish Bank, Royal Bank of Scotland, Crédit Agricole, Société Générale, BASF, Mercedes-Benz, Allianz, AXA-IM, Swiss Re, Swisslife, Air France, Migros, LVMH, Cartier, Tag-Heuer, British Telecom, Cable & Wireless, KPN, Portugal Telecom, T-Mobile, Swisscom…
  - Google, Apple, Adobe, Peoplesoft, Hewlett-Packard, Agilent, VeriSign, New-York Trade Board, Chicago Board of Options Exchange, Federal Reserve Bank, First State Bank, Bank of the West, Cincinnati Children's Hospital, Blue Cross/Blue Shield…
- Founded in March 1999
  - 120+ Employees, 60+ in R&D and operations
  - Global offices in US, France, Germany and UK
- Advisors
  - Howard Schmidt, Becky Bace, Phil Zimmerman
- $60M in funding
  - Trident Capital, Deutsche Bank ABS Ventures, Philippe Courtot (CEO) & VeriSign
- Headquartered in Redwood Shores, CA

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

Where are the issues ?

- A Multitude of insecure Protocols and Services
  - telnet, ftp, snmp
- Known default settings
  - Passwords, SNMP community strings
- System Design Errors
  - Setup and Access control errors
- Software Implementation Flaws
  - Input validation, lack of sanity checks
- User Triggered Issues
  - Email and Browser related

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
- 40 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

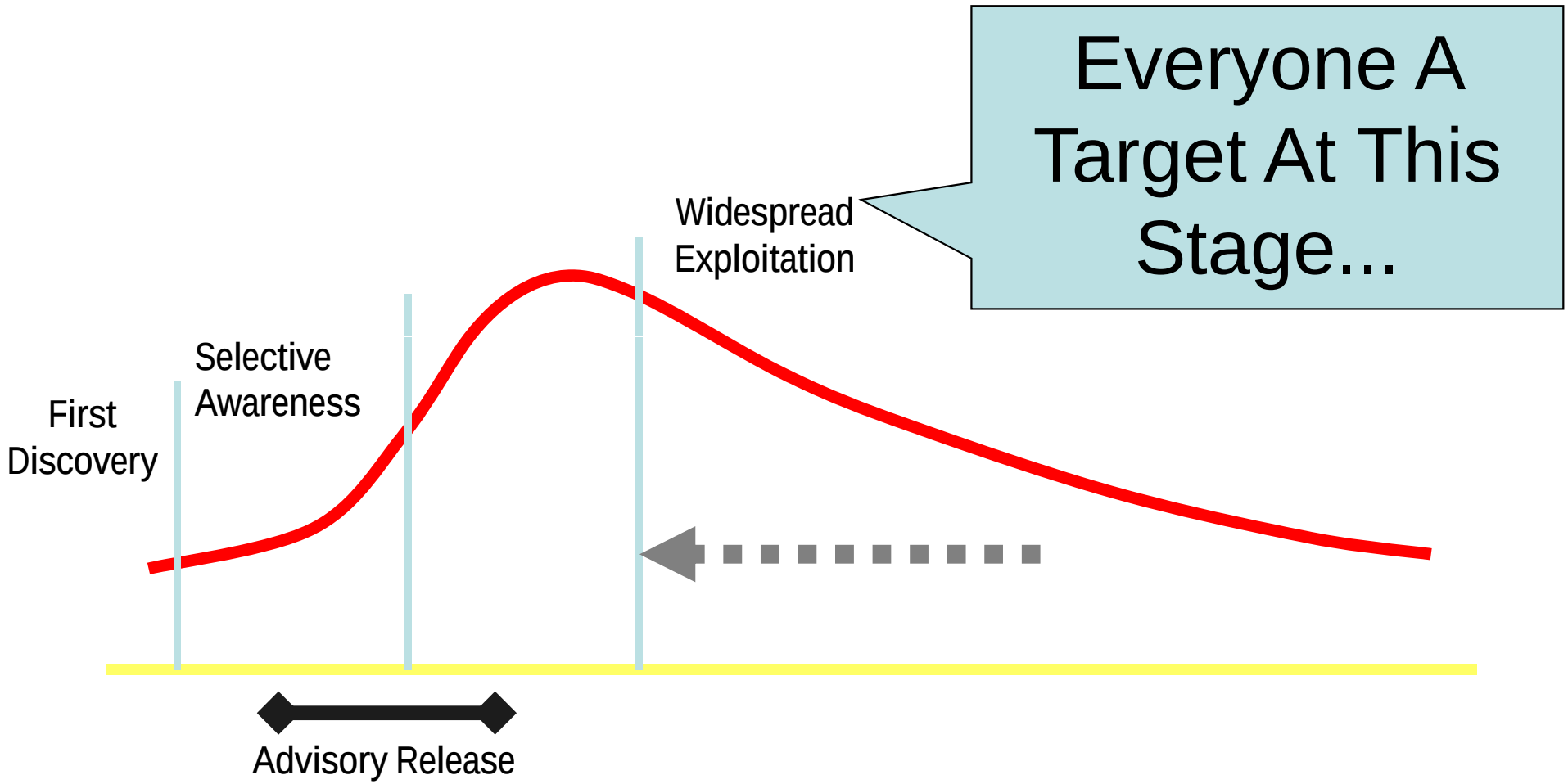
Second Generation Threats

- 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

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



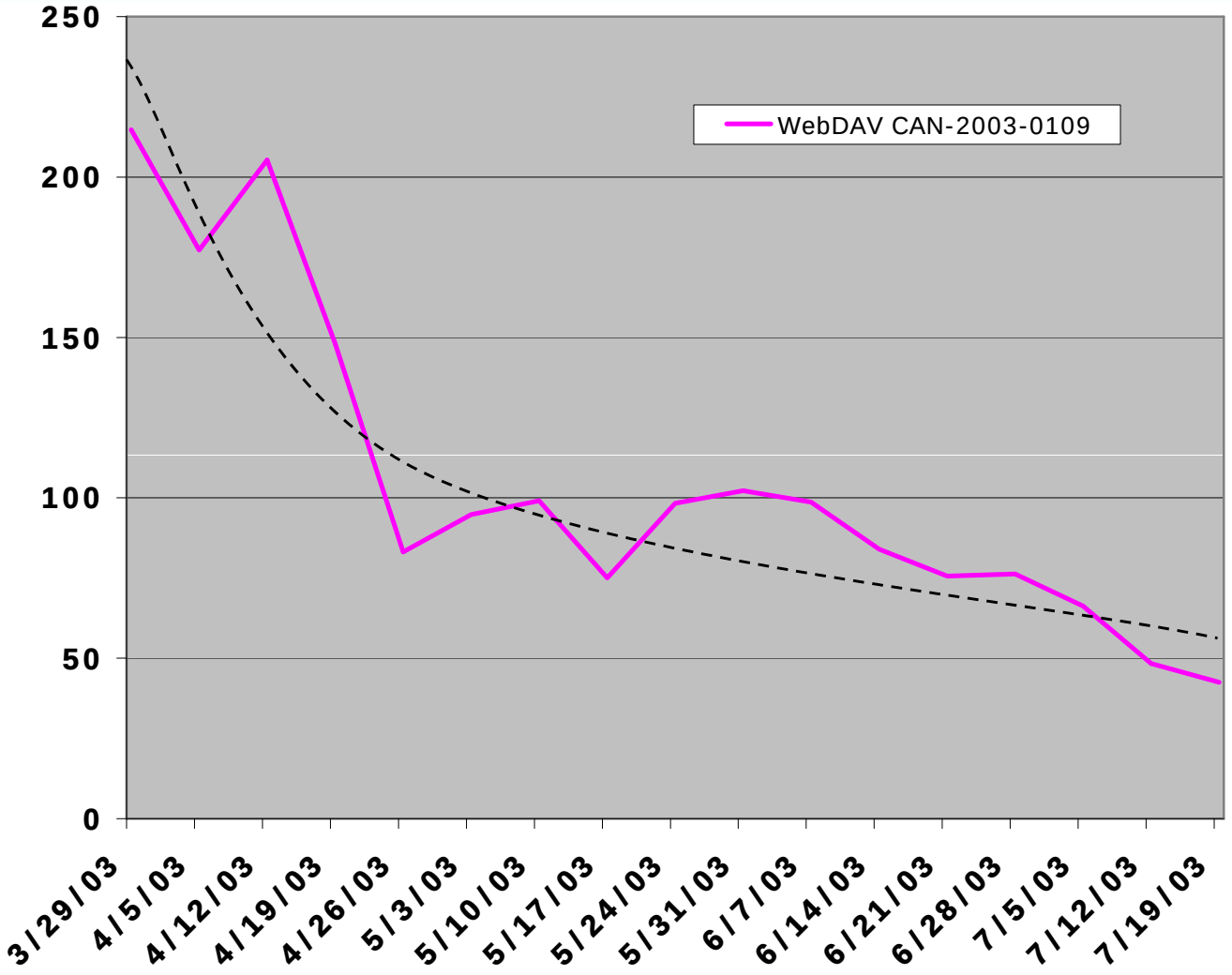
Third Generation (Future) Threats

- 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, Wireless Networks, Voice over IP,...)

Qualys 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:
  - **3,011,000 IP-Scans**
  - **1,905,000 total critical vulnerabilities**
  - **2,054 unique vulnerabilities**
  - **1,175 unique critical vulnerabilities**

Microsoft WebDAV Vulnerability

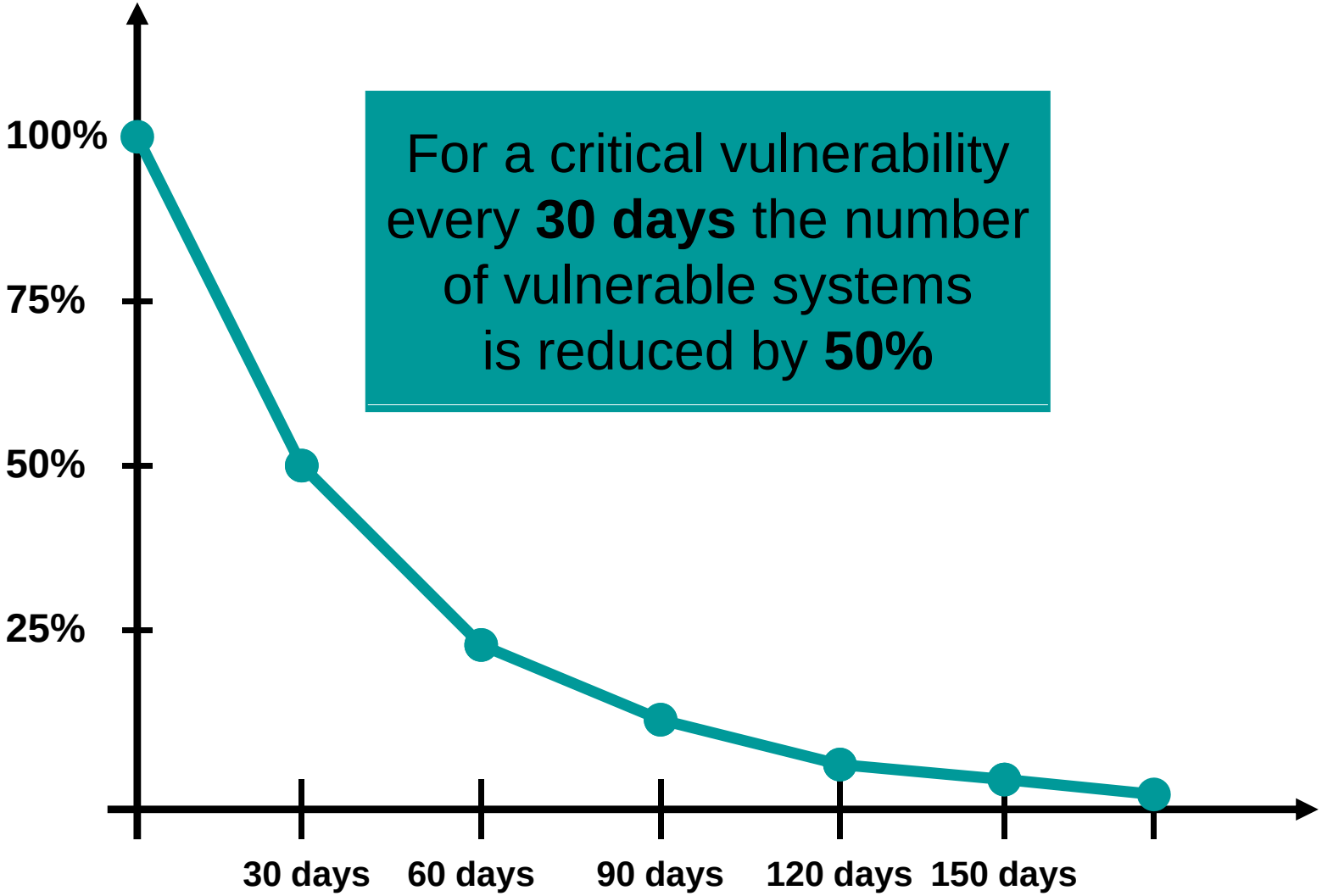


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

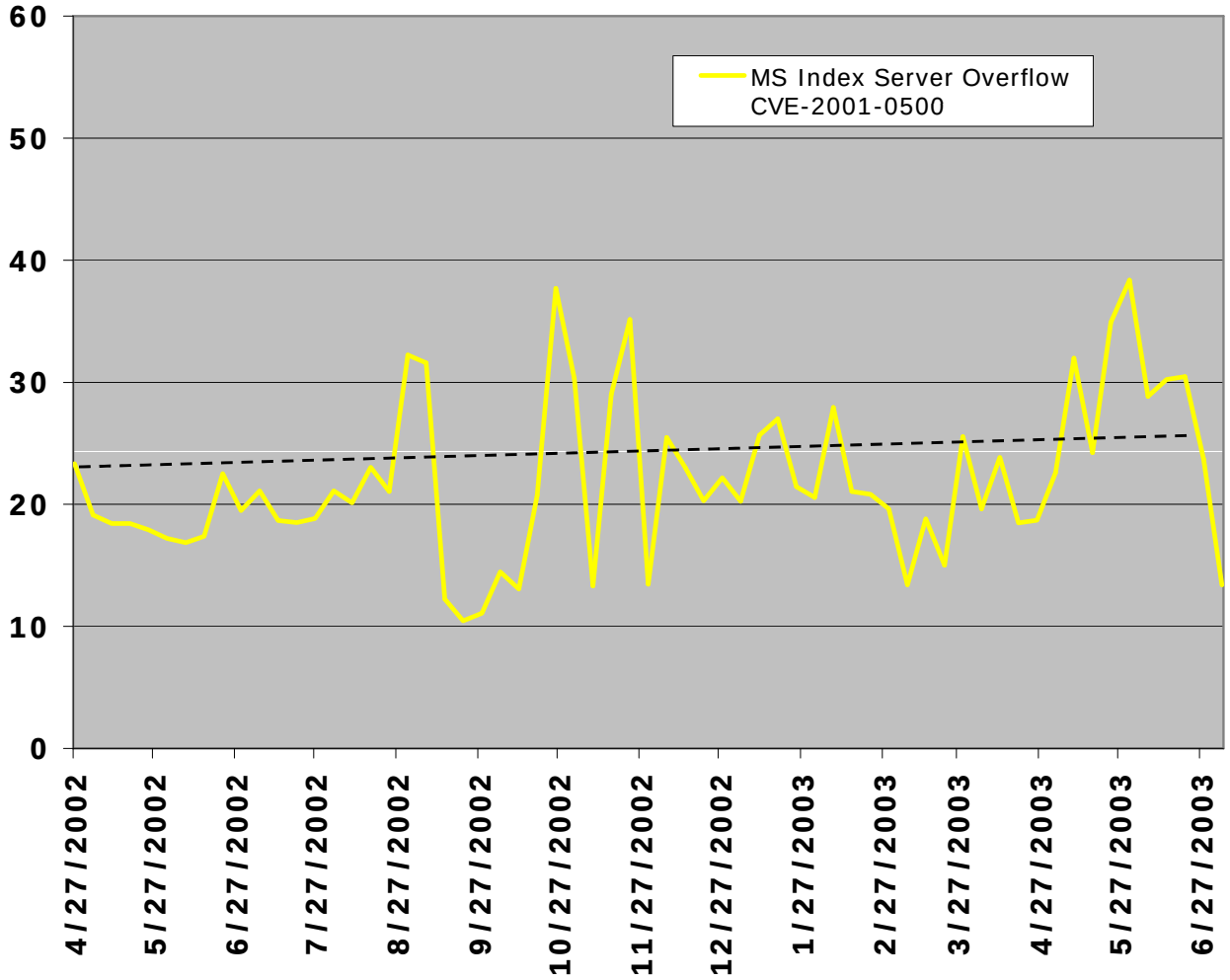
Released: March 2003

Vulnerability Half-Life



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

MS Index Server Overflow (CodeRed)

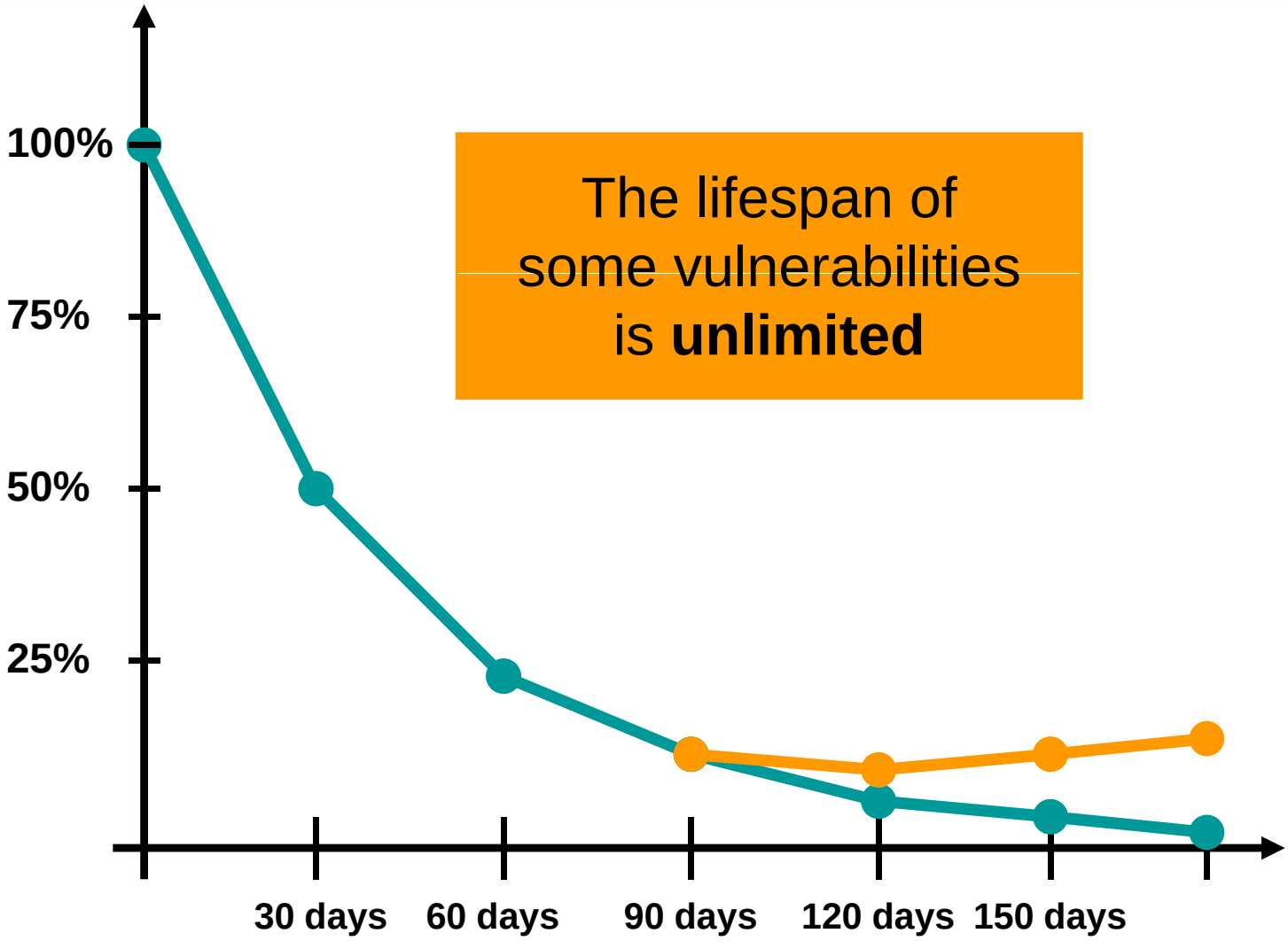


Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability

CVE-2001-0500
Qualys ID 86170

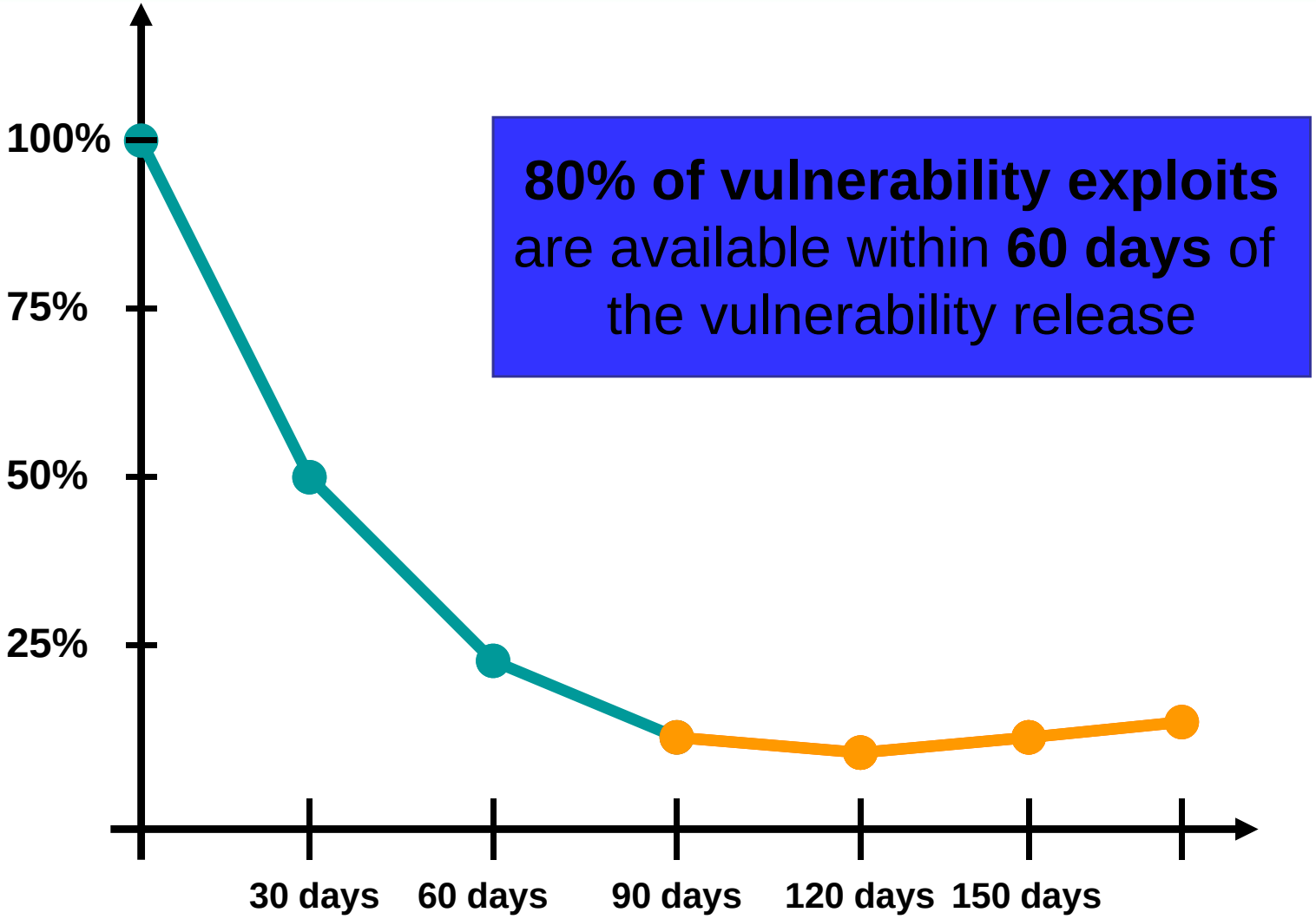
Released: June 2001

Vulnerability Lifespan



The lifespan of some vulnerabilities is **unlimited**

The Impact of an Exploit



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

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			x	
Microsoft IIS FTP Connec			x	
Microsoft IIS Chunked En			x	
Microsoft IIS HTR ISAPI E			x	
Microsoft IIS 4.0/5.0 Exter			x	x
Microsoft IIS CGI Filenam			x	x
Microsoft IIS Malformed H			x	x
Microsoft IIS HTR Chunke			x	x
Apache Chunked-Encoding Memory Corruption Vulnerability	CVE-2002-0392	x	x	x
OpenSSH Challenge-Response Authentication Integer Overflow Vulnerability	CVE-2002-0639	x	x	x
Multiple Vendor SNMP Request And Trap Handling Vulnerabilities	CAN-2002-0012		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

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

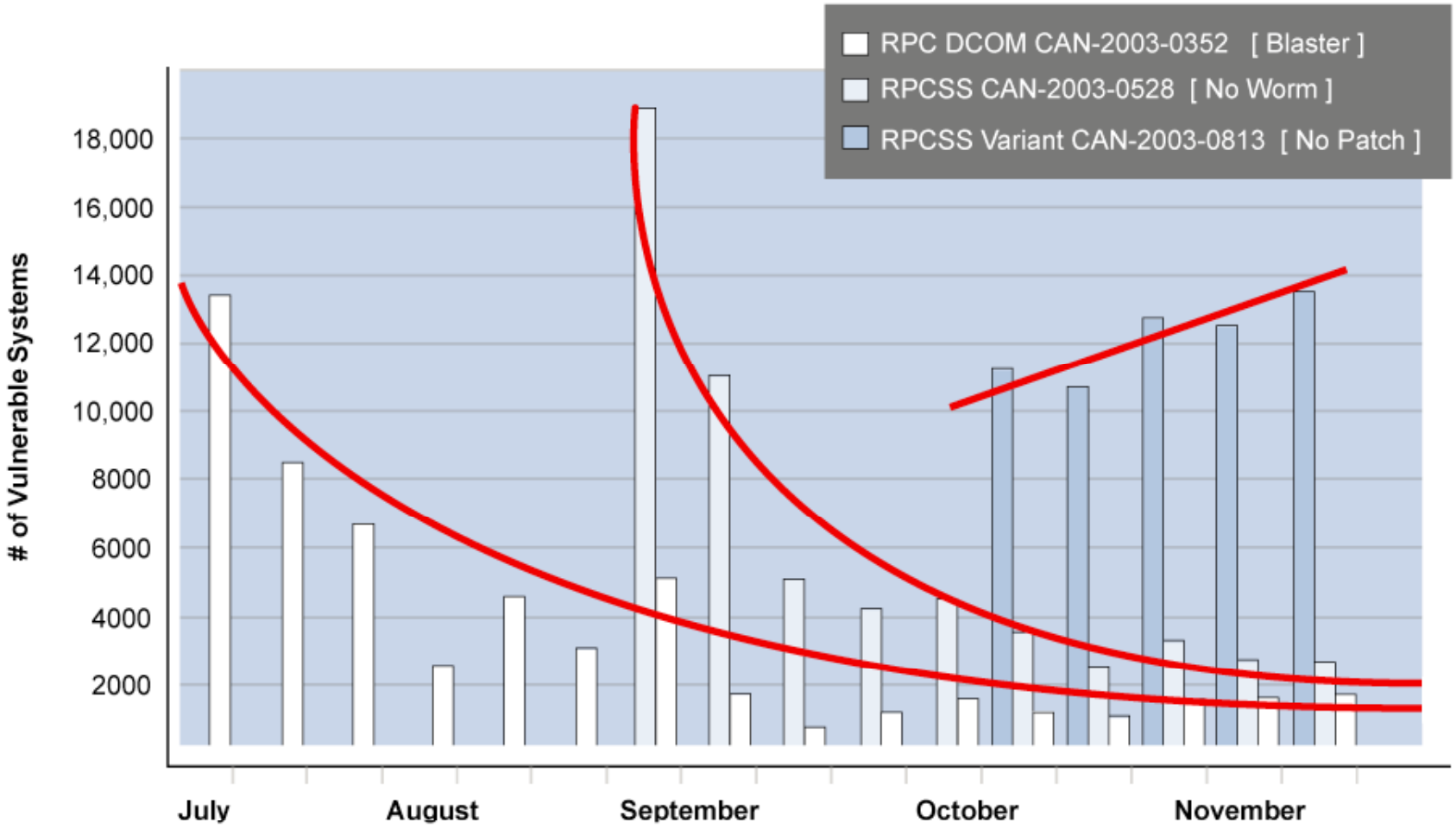
RV10 Index of Most Prevalent Vulnerabilities

April 27, 2004

Microsoft IIS Malformed HTR Request Buffer Overflow Vulnerability	**CVE-2002-0071**
Apache Chunked-Encoding Memory Corruption Vulnerability	**CVE-2002-0392**
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**
Microsoft Windows DCOM RPCSS Service Vulnerabilities	**CAN-2003-0528**
Microsoft Messenger Service Buffer Overrun Vulnerability	**CAN-2003-0717**
Microsoft Windows RPCSS Code Execution Variant Vulnerability	**CAN-2003-0813**
Microsoft Windows ASN.1 Library Integer Handling Vulnerability	**CAN-2003-0818**
Writeable SNMP Information	**No CVE assigned**

To Watch in 2004:

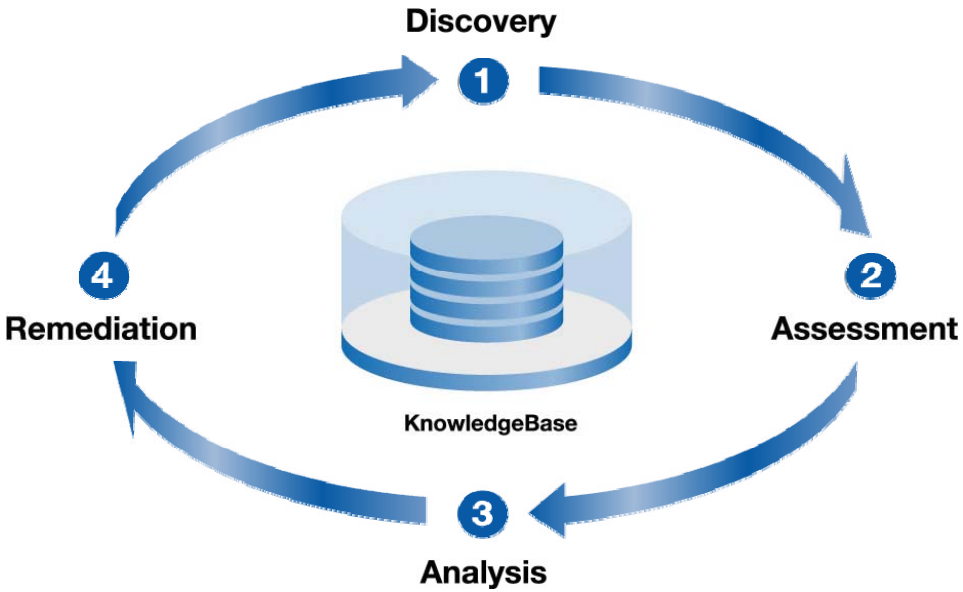
Remote Procedure Call Vulnerabilities

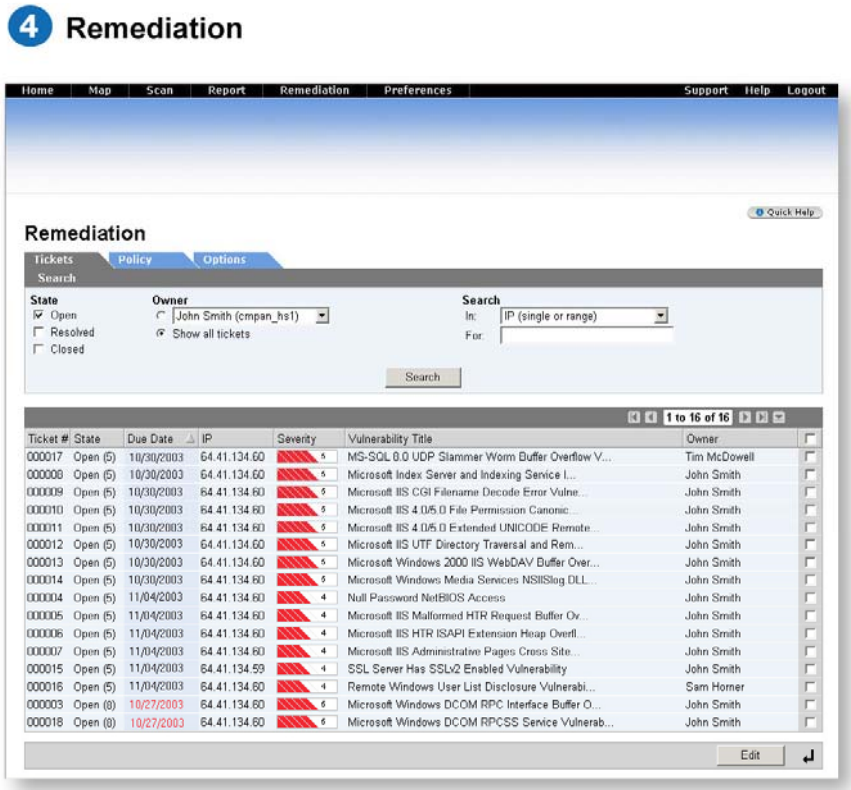


Proactive Approach: Vulnerability Management

1) Identify network topology and points of entry
2) Identify services, operating systems and applications
3) Identify and prioritize critical vulnerabilities
4) Remedy vulnerabilities and verify fixes

Vulnerability Management Defined





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
for your attention

phuguet@qualys.com

www.qualys.com