

THE LAWS OF VULNERABILITIES 2.0

COMPARING VULNERABILITY
DYNAMICS BY INDUSTRY

by Wolfgang Kandek, CTO, Qualys, Inc.
Black Hat Briefings, Las Vegas, NV



Panel

- Richard Bejtlich – GE
- Ed Bellis - Orbitz
- Paul Griffiths – Goldman Sachs
- Kris Herrin – Heartland Payment Systems
- Mark Weatherford – State of California



Laws of Vulnerabilities 2004

Research project initiated by former Qualys CTO
Gerhard Eschelbeck

- 3M IPs scanned, 2M vulnerabilities
- 4 findings
 - Half-life – 30 days
 - Prevalence – 50 % renewal annually
 - Persistence – unlimited for some
 - Exploitation – 80 % available with 60 days
- Half-life is the primary indicator for patch speed



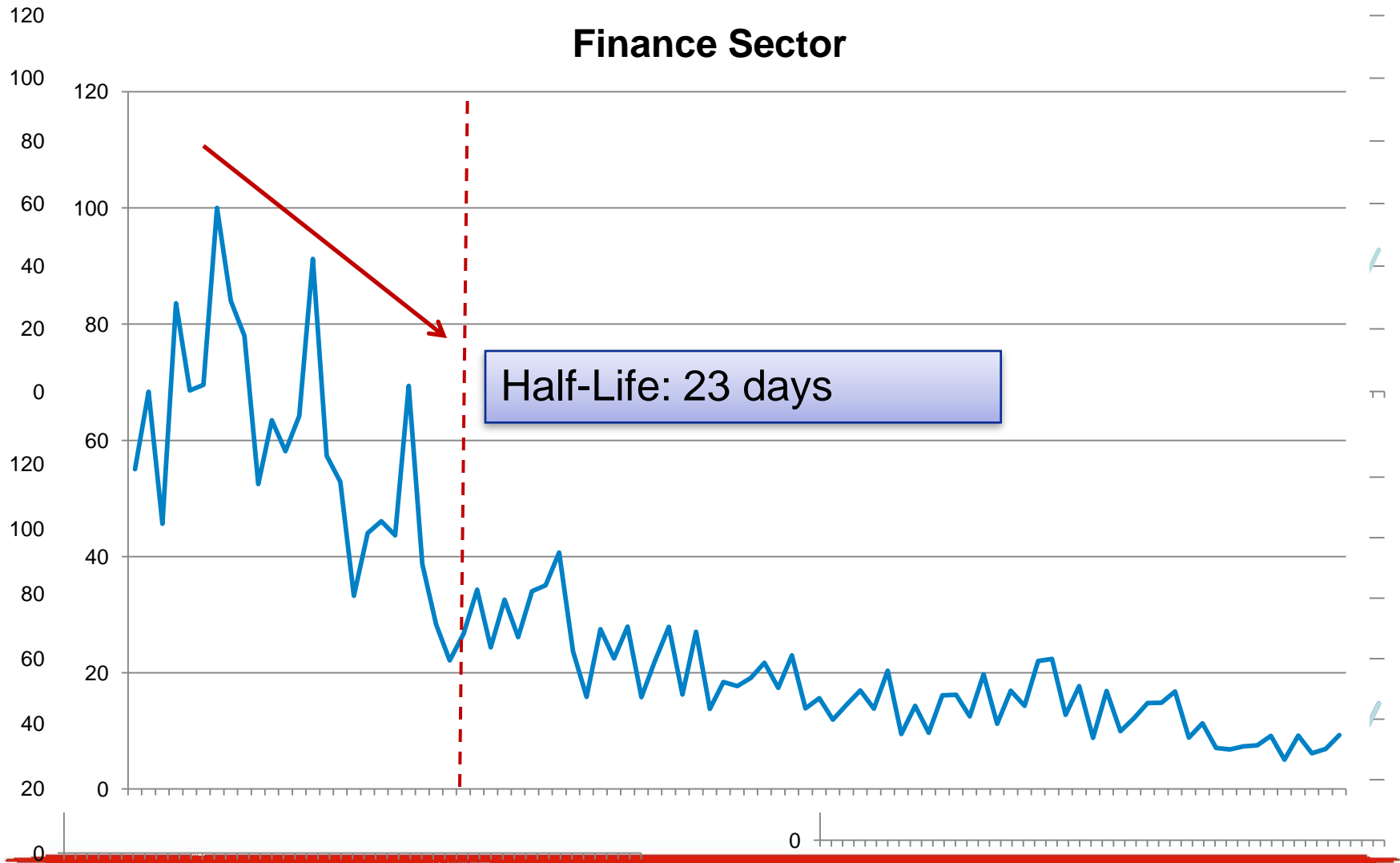
Laws of Vulnerabilities 2.0

Worldwide coverage – 2008

- 80M IPs scanned, 680M vulnerabilities
- 72M+ vulnerabilities of critical severity
- External (Internet) and Internal (Intranet)
 - 200 external scanners and 5000+ internal scanners
- Data is anonymous and non traceable
 - Simple counters are kept during scanning
 - Summarized and logged daily
- Trends by industry
 - 5 major groups

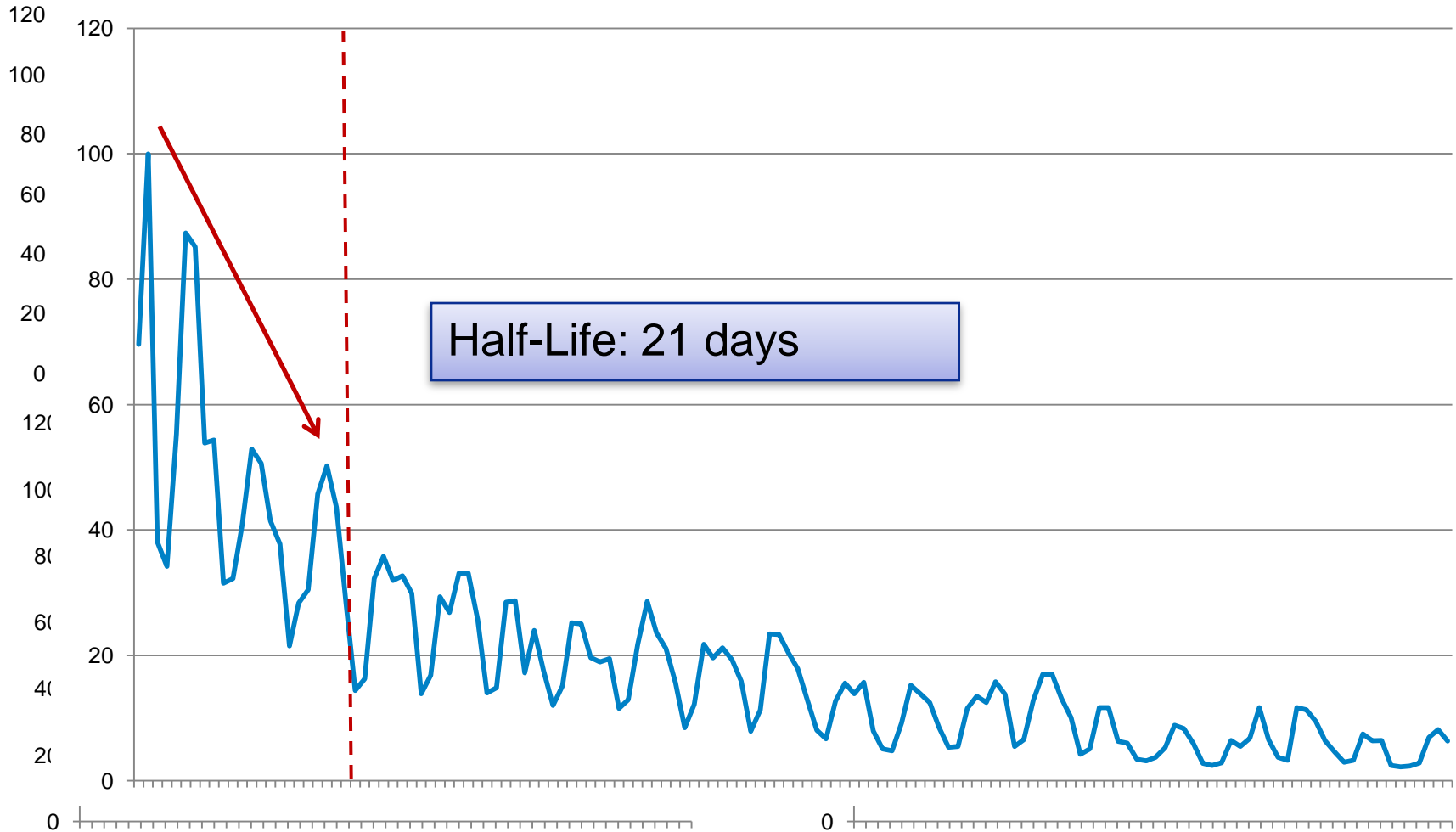


Half-Life by Industry



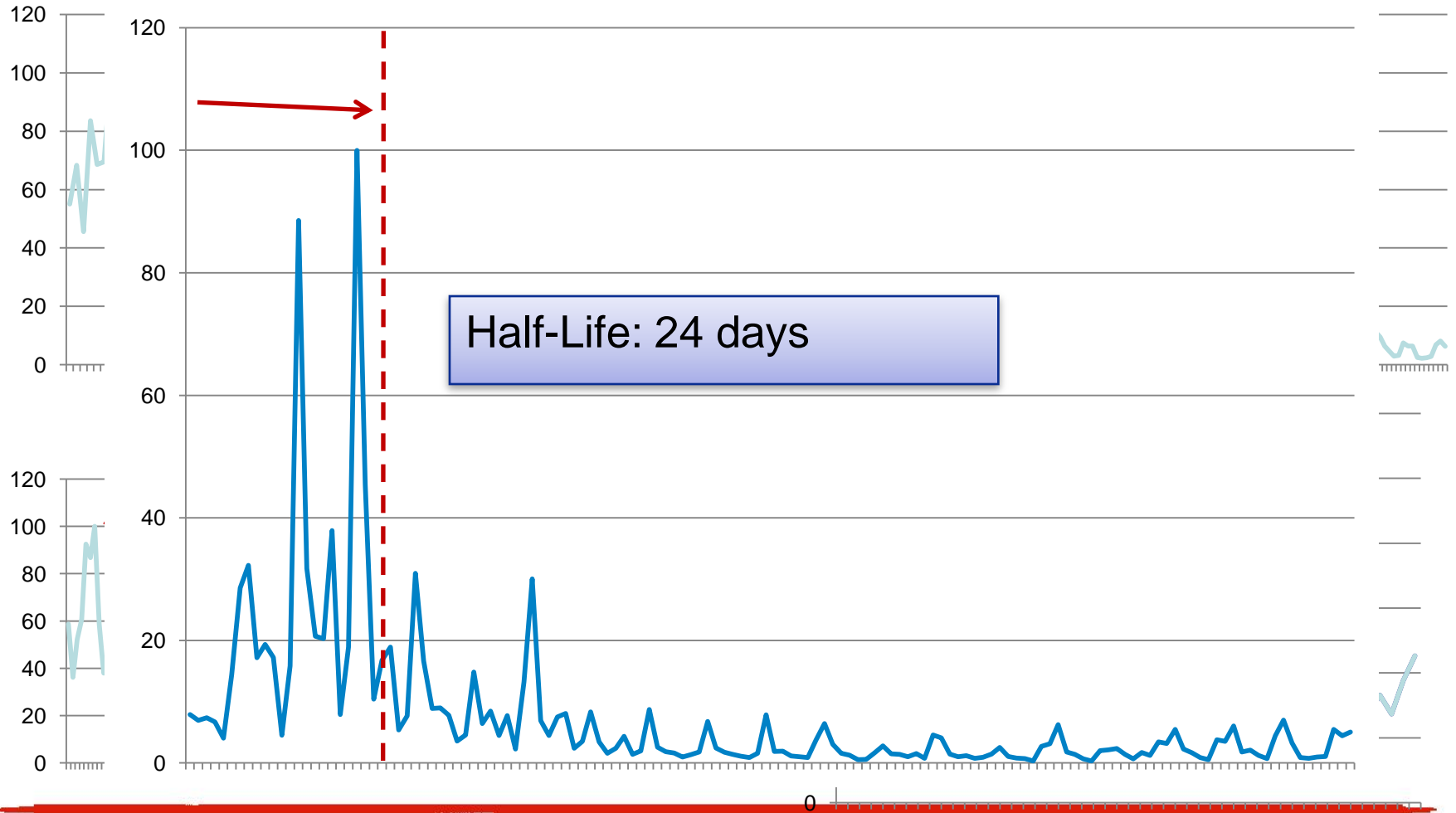
Laws 2.0 – Half-Life by Industry

Service Sector



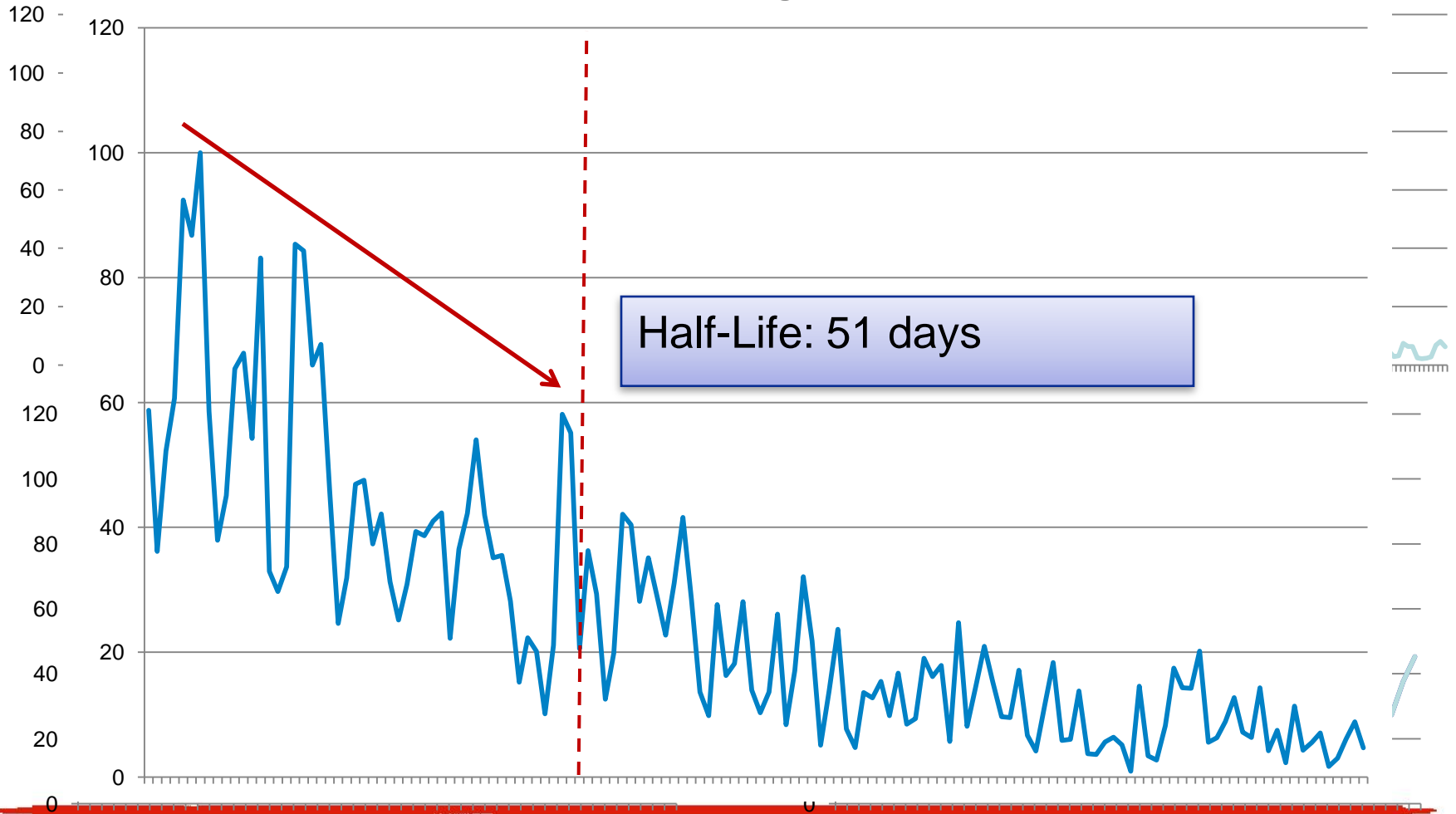
Laws 2.0 – Half-Life by Industry

Wholesale/Retail Sector



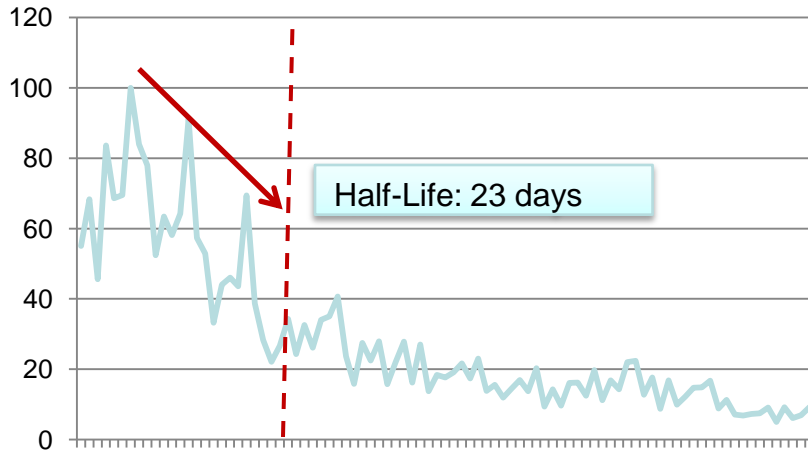
Laws 2.0 – Half-Life by Industry

Manufacturing Sector

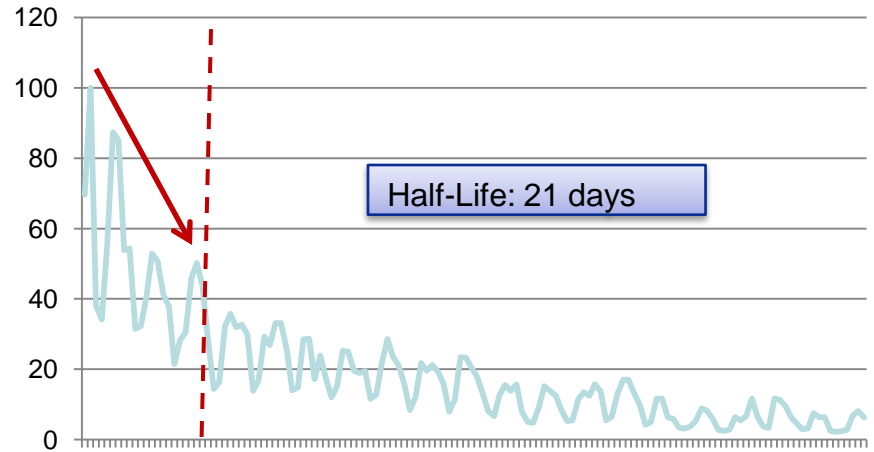


Laws 2.0 – Half-Life by Industry

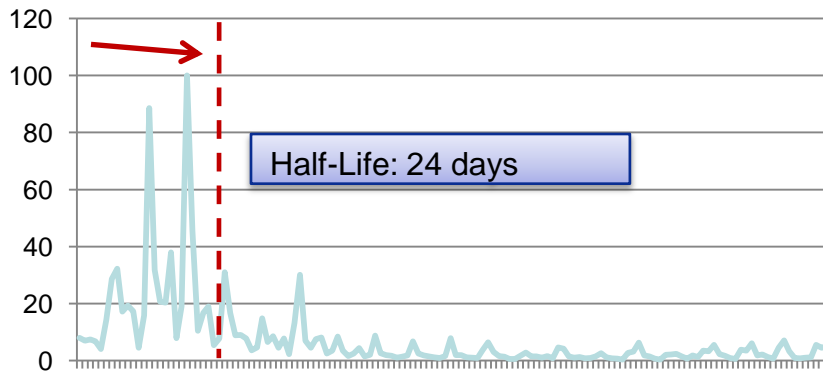
Finance Sector



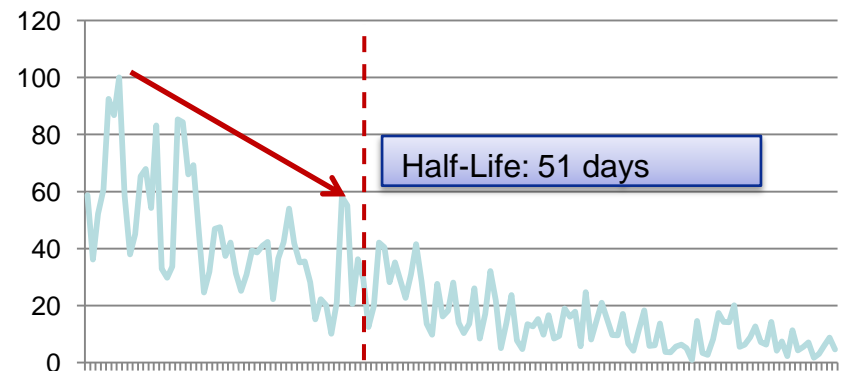
Service Sector



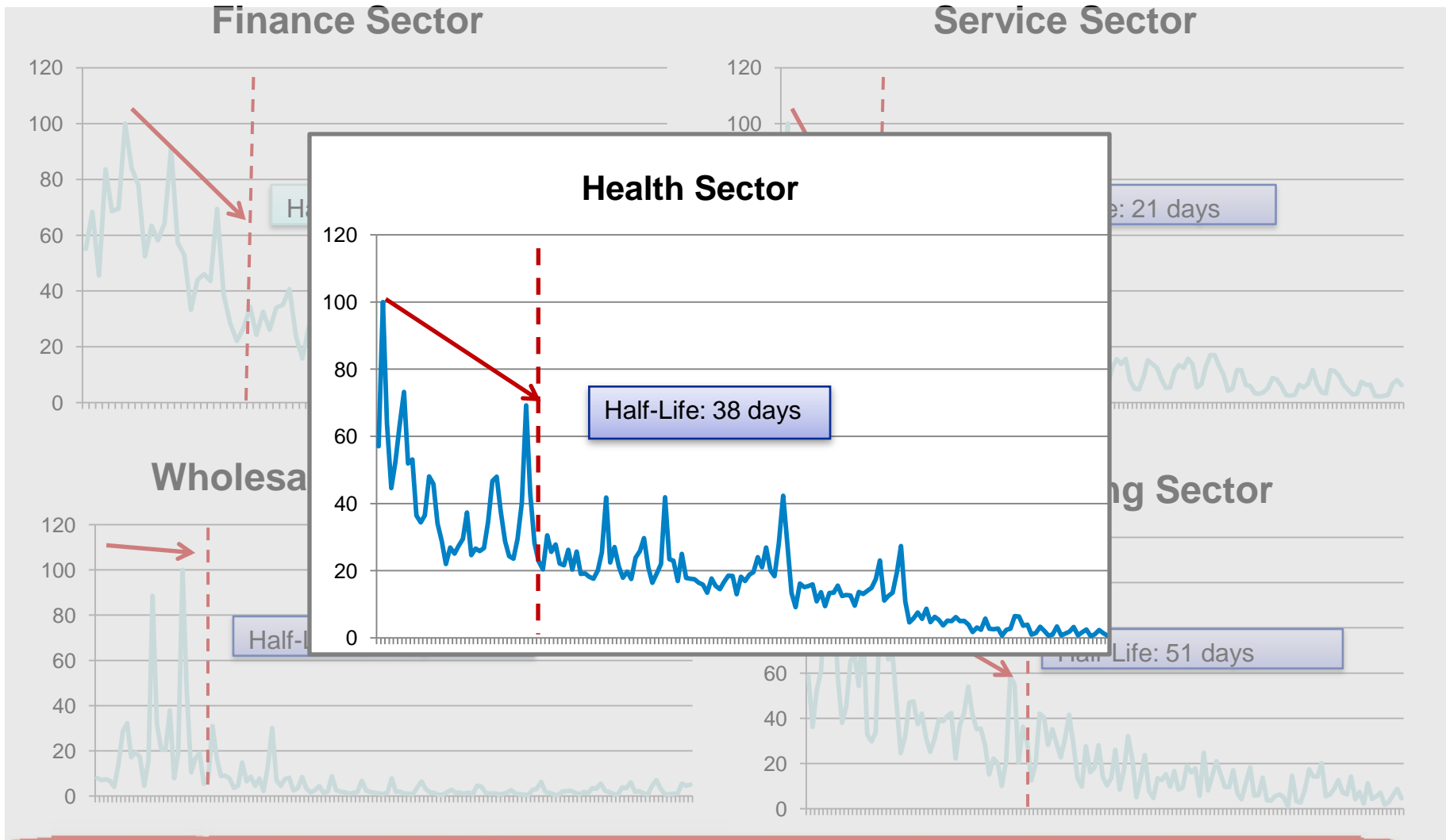
Wholesale/Retail Sector



Manufacturing Sector

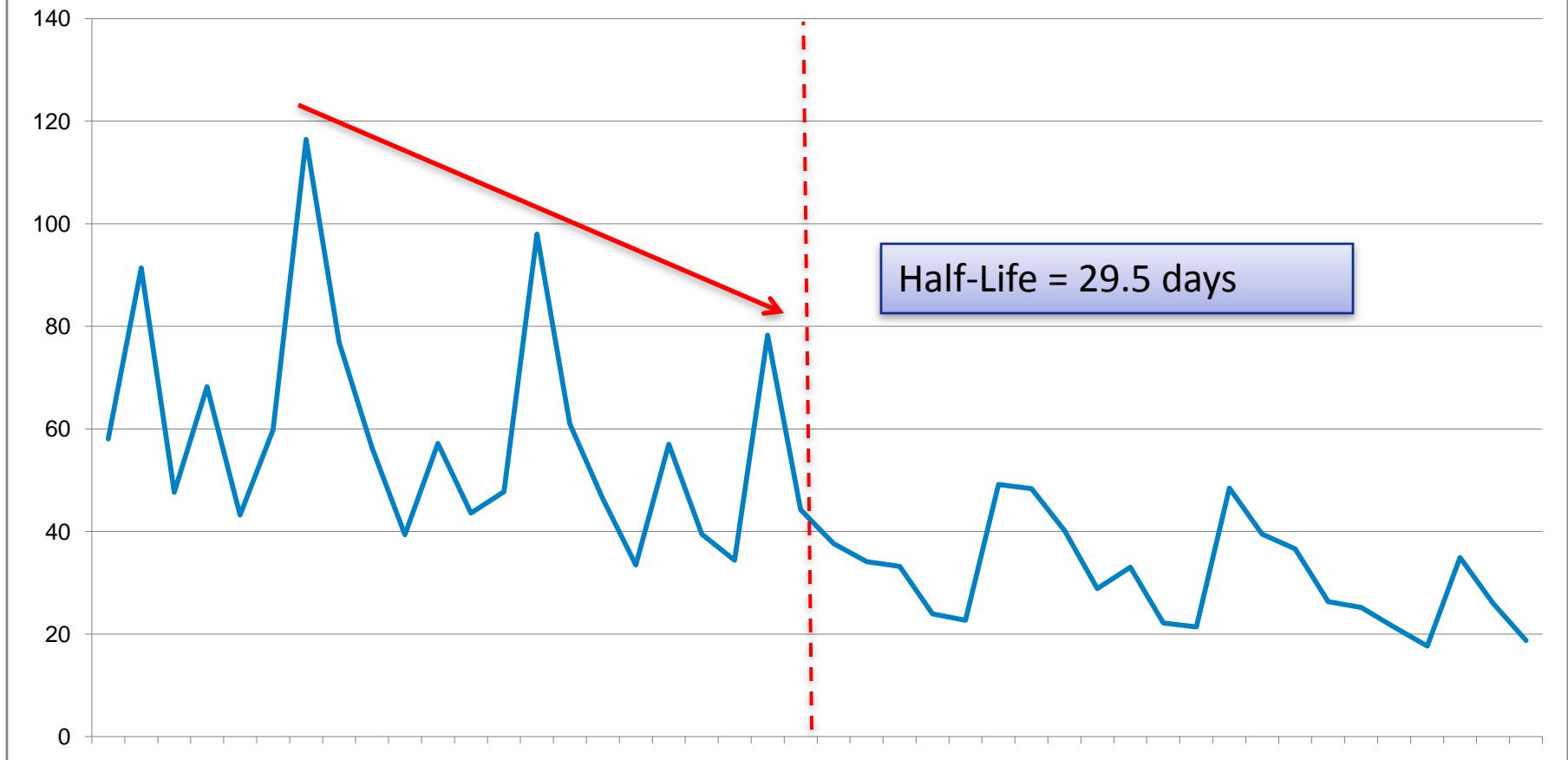


Laws 2.0 – Half-Life by Industry



Laws of Vulnerabilities 2.0 – Half-Life

Overall Critical Vulnerabilities – 72M data points



Laws 2.0 – Prevalence

Top 20 Critical Vulnerabilities - predominantly Windows

- MS08-001 - TCP/IP Vulnerabilities in Windows
- MS08-007 - WebDav Redirector
- MS08-052 - GDI+ Remote Code Execution
- MS08-067 - Windows Server Service
- MS08-010/054 - Internet Explorer
- MS08-007 - Word Remote Code Execution
- MS08-013 - Office Remote Code Execution
- MS08-014 - Excel Header Parsing
- 321644 - Adobe Reader Remote Buffer Overflow
- APSB08-015 - Adobe Reader Multiple Vulnerabilities
- HT1738 - Quicktime
- KB290211 - SQL Server 2000 SP4 not installed

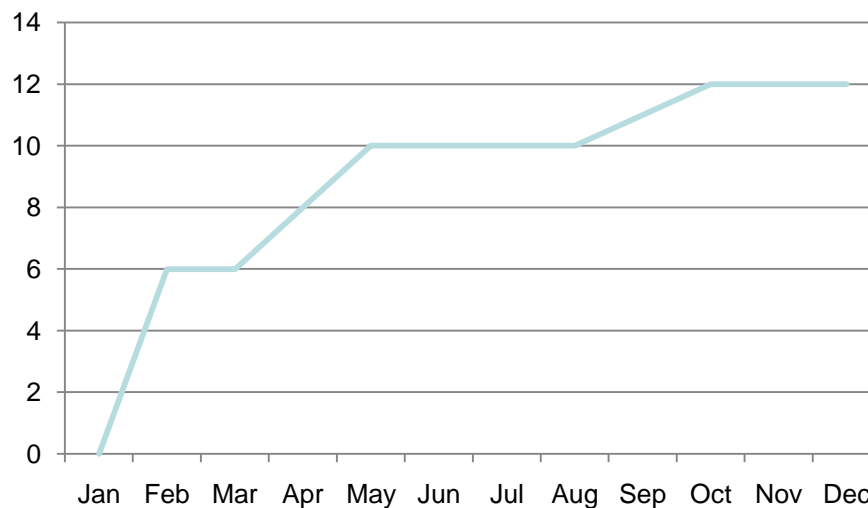


Laws 2.0 – Prevalence

Top 20 Critical Vulnerabilities

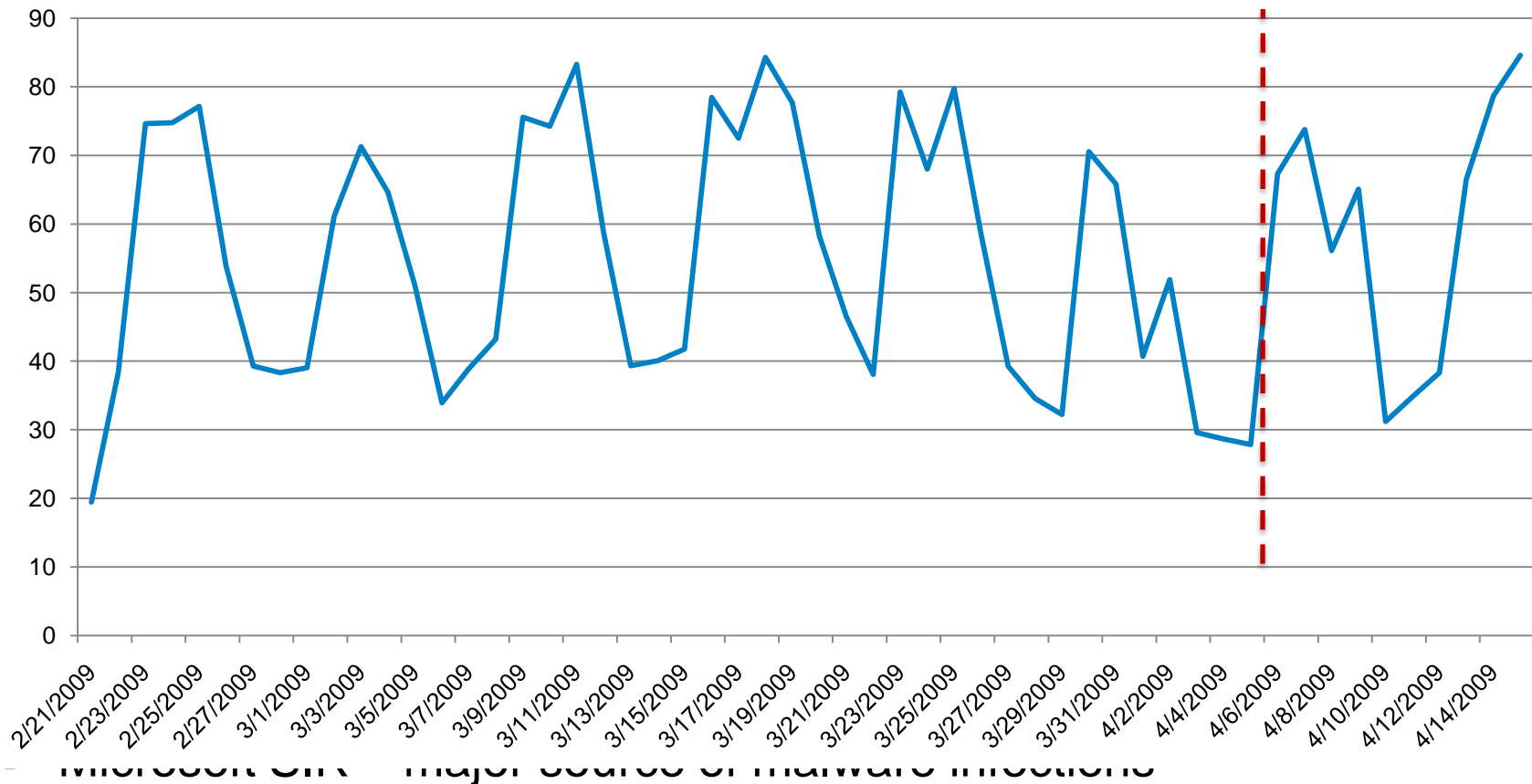
- Tracking change - 60 % change in 2008
 - 50 % in 2004
- Top Stragglers
 - MSFT Office
 - Windows 2003 SP2
 - Sun Java Plugin
 - Adobe Acrobat

Top 20 - changes in 2008



Laws 2.0 – Prevalence

Adobe APSA09-01



Laws 2.0 – Prevalence

Top 20 Critical Vulnerabilities

- Tracking change - 60 % change in 2008

- 50 % in 2004

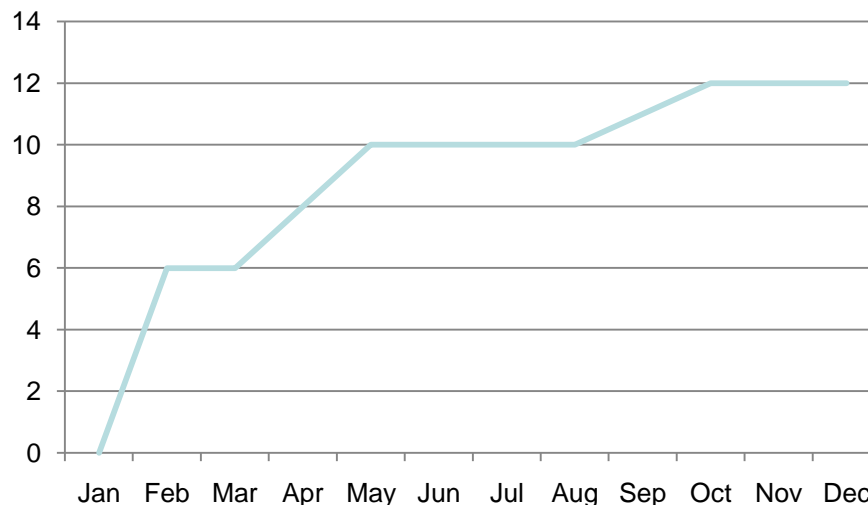
- Top Stragglers

- MSFT Office
- Windows 2003 SP2
- Sun Java Plugin
- Adobe Acrobat

- File format vulnerabilities

- Microsoft SIR – major source of malware infections

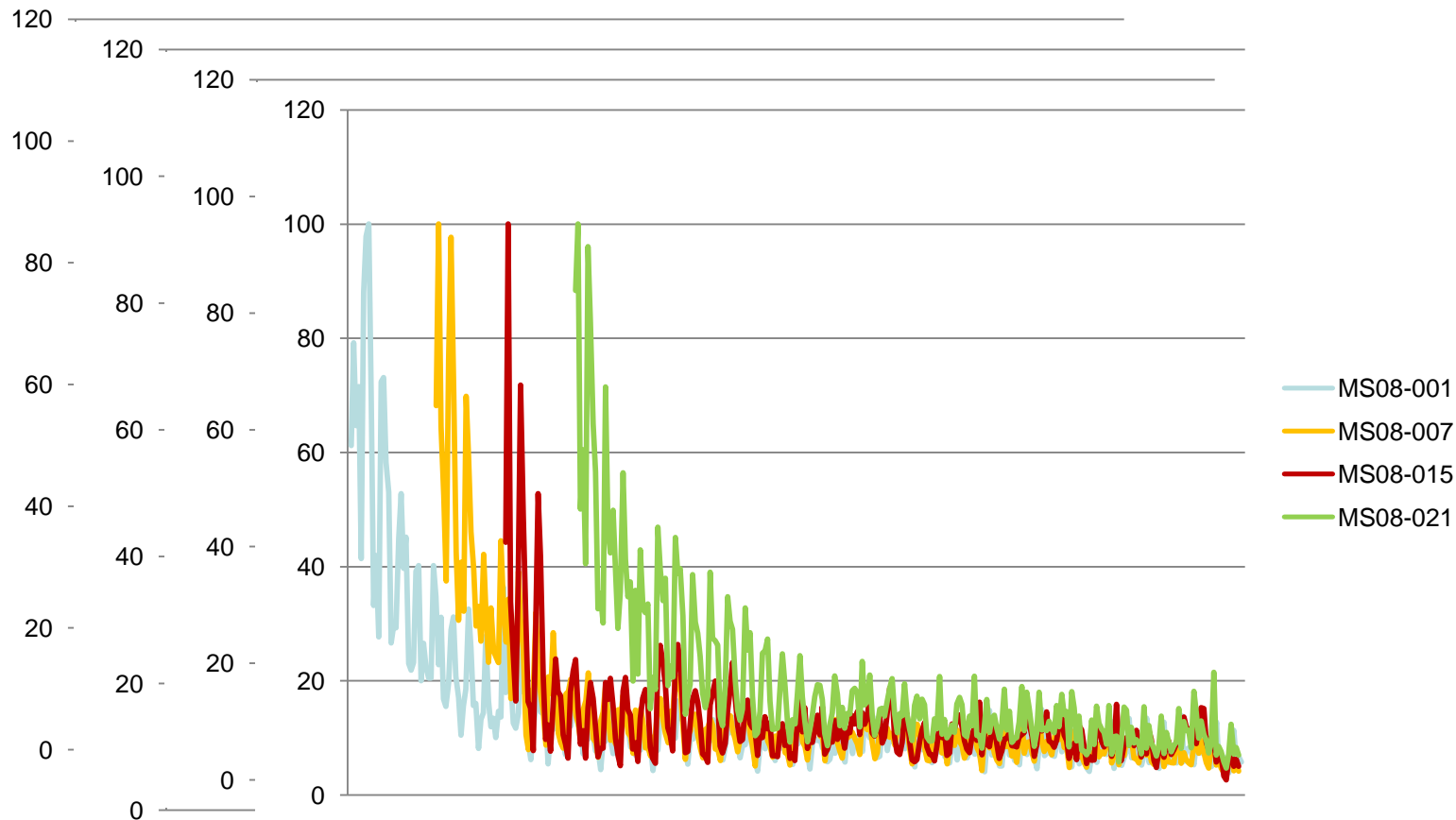
Top 20 - changes in 2008



Laws 2.0 – Persistence

most, if not all

“The lifespan of ~~some~~ vulnerabilities is unlimited”



Laws 2.0 – Exploitation

- Window for the availability of an exploit is constantly shrinking
- Attackers are professional and driven
 - Automatic exploit generation has been demonstrated
- 0-day exploits – 56 in Qualys knowledgebase
 - 2008: 2 Out-of-band releases by MSFT
 - 2009: Excel (968272), PowerPoint (969136), IE (MS09-034)
 - 2009: MSFT April Release – 10 out of 21 had exploits (47 %)
 - 2009: Adobe Acrobat APSA09-01, APSA09-02 and APSA09-03
 - 2009: Firefox 3.5 MFSA 2009-41
- Exploit availability is now measured in single-digit days
 - MS08-001 – 14 days, MS08-073 – 12 days MS09-001 – 7 days



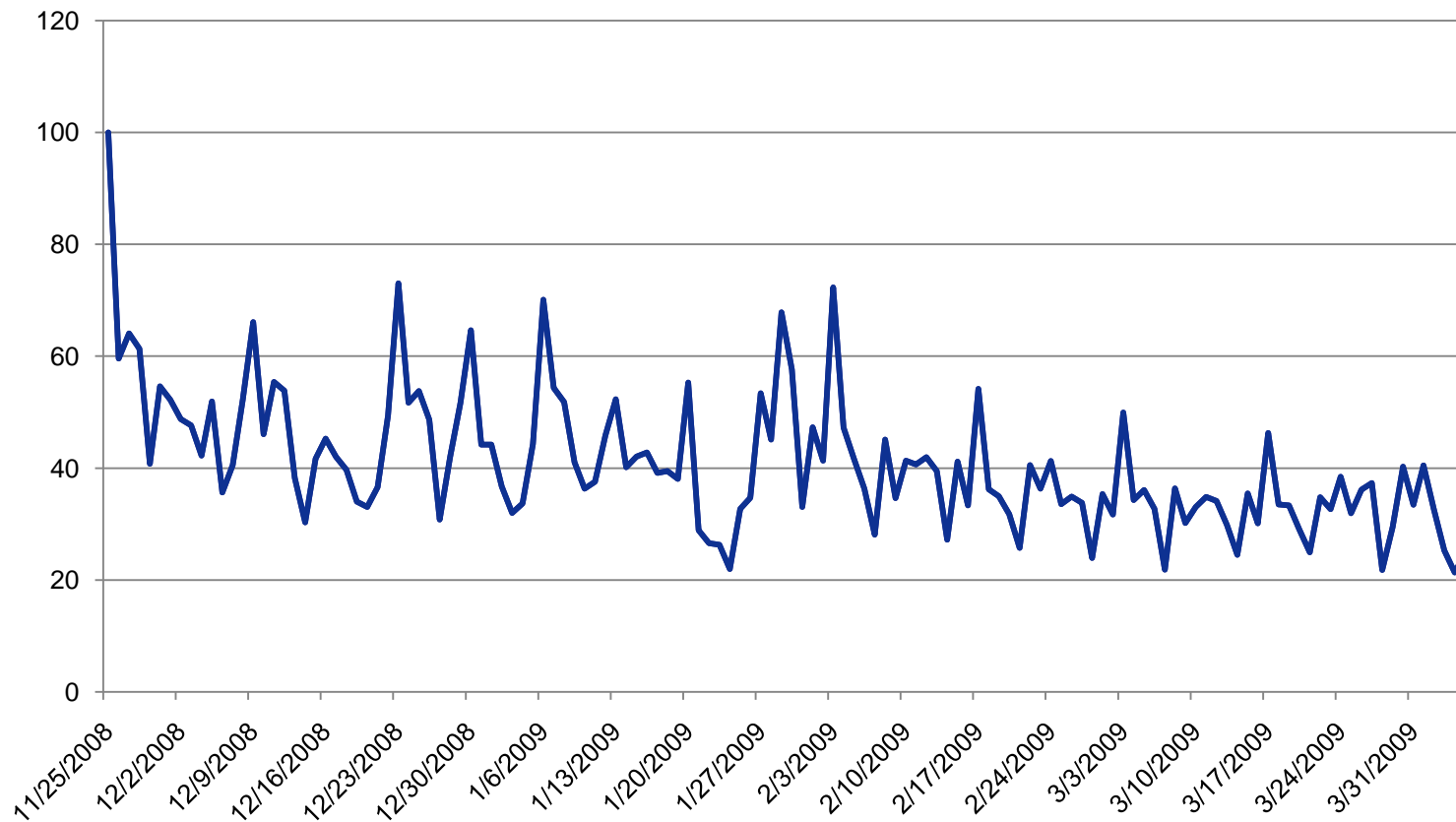
Laws 2.0 – Exploitation - Conficker

High Impact Worm for Windows based OS

- Sep 2008 - first samples of code for vulnerability available
- Oct 2008 – patch out-of-band for critical vulnerability (MS08-067)
- Nov 2008 – Conficker worm appears – 2M -10M infected machines
 - A, B, C, C++,D,E, versions -> release cycle every 6 weeks
 - Each version gets better at infecting and evading detection
 - Attackers are professional experienced coders and driven
- Patch speed – normal, even though highly critical

Laws 2.0 – Exploitation - Conficker

MS08-067



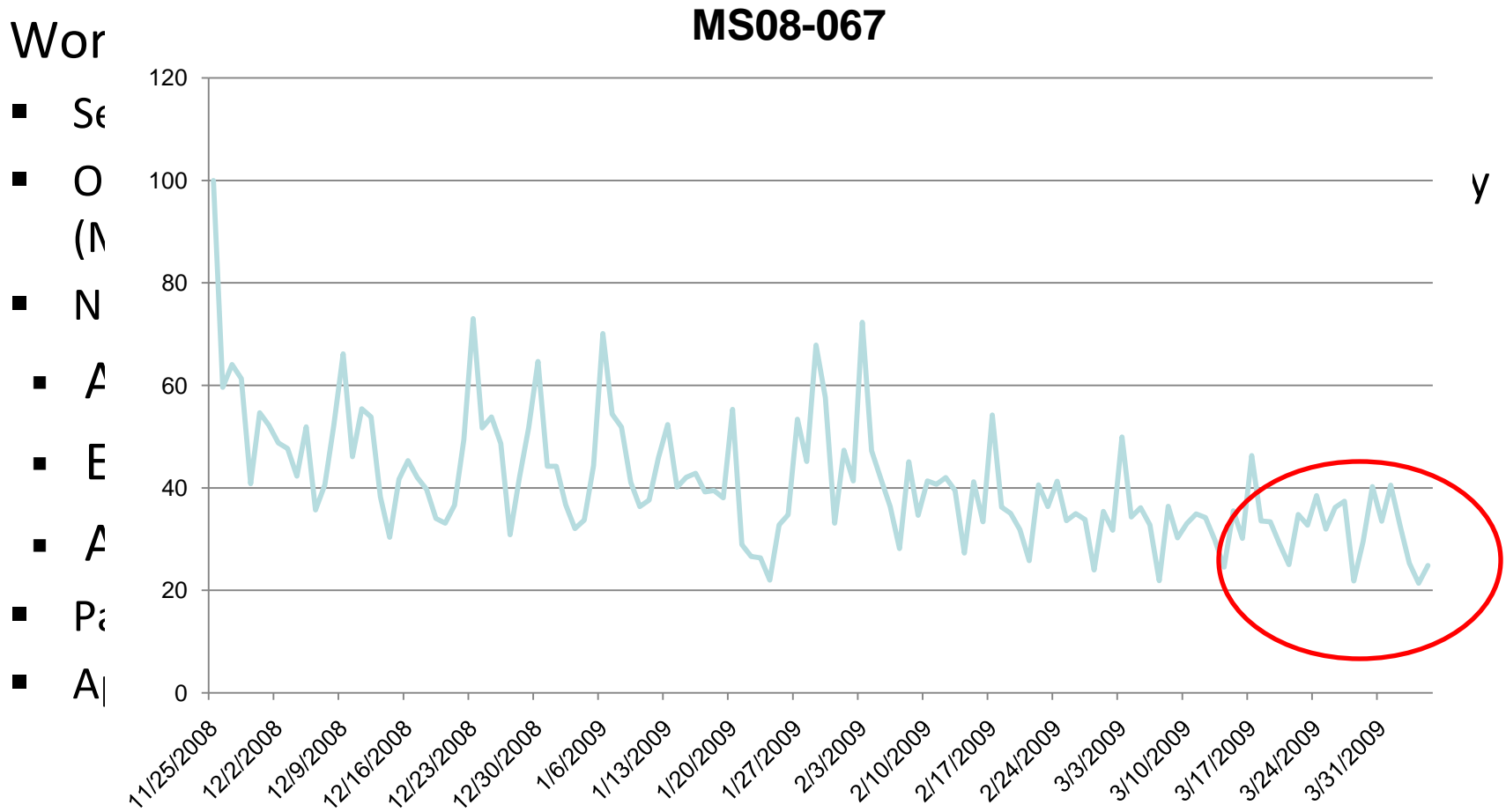
Laws 2.0 – Exploitation - Conficker

High Impact Worm for Windows based OS

- Sep 2008 - first samples of code for vulnerability available
- Oct 2008 – patch out-of-band for critical vulnerability (MS08-067)
- Nov 2008 – Conficker worm appears – 2M -10M infected machines
 - A, B, C, C++,D,E, versions -> release cycle every 6 weeks
 - Each version gets better at infecting and evading detection
 - Attackers are professional experienced coders and driven
- Patch speed – normal, even though highly critical
- April 1st impact



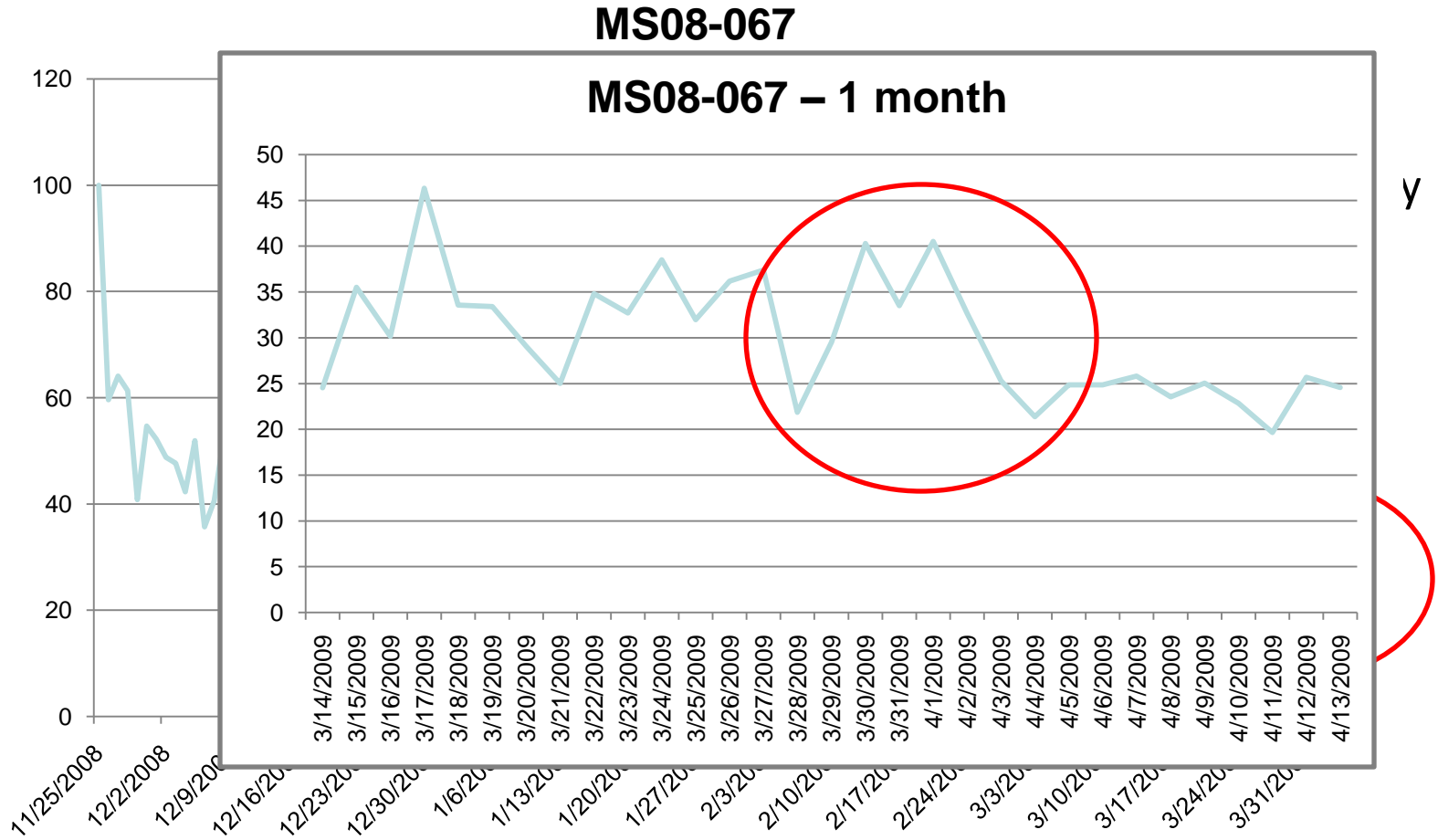
Laws 2.0 – Exploitation - Conficker



Laws 2.0 – Exploitation - Conficker

Wor

- Se
- O
- (M
- N
- A
- E
- A
- Pa
- A



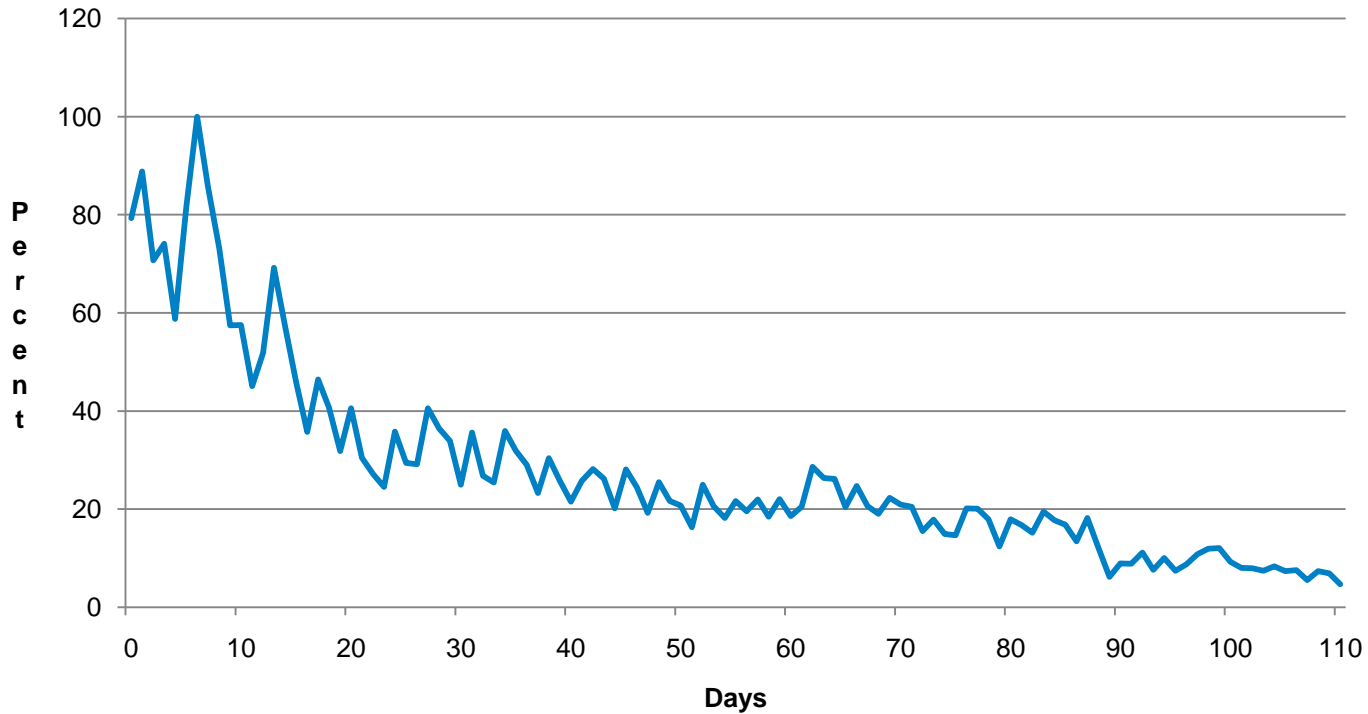
Laws 2.0 – Exploitation - Conficker

High Impact Worm for Windows based OS

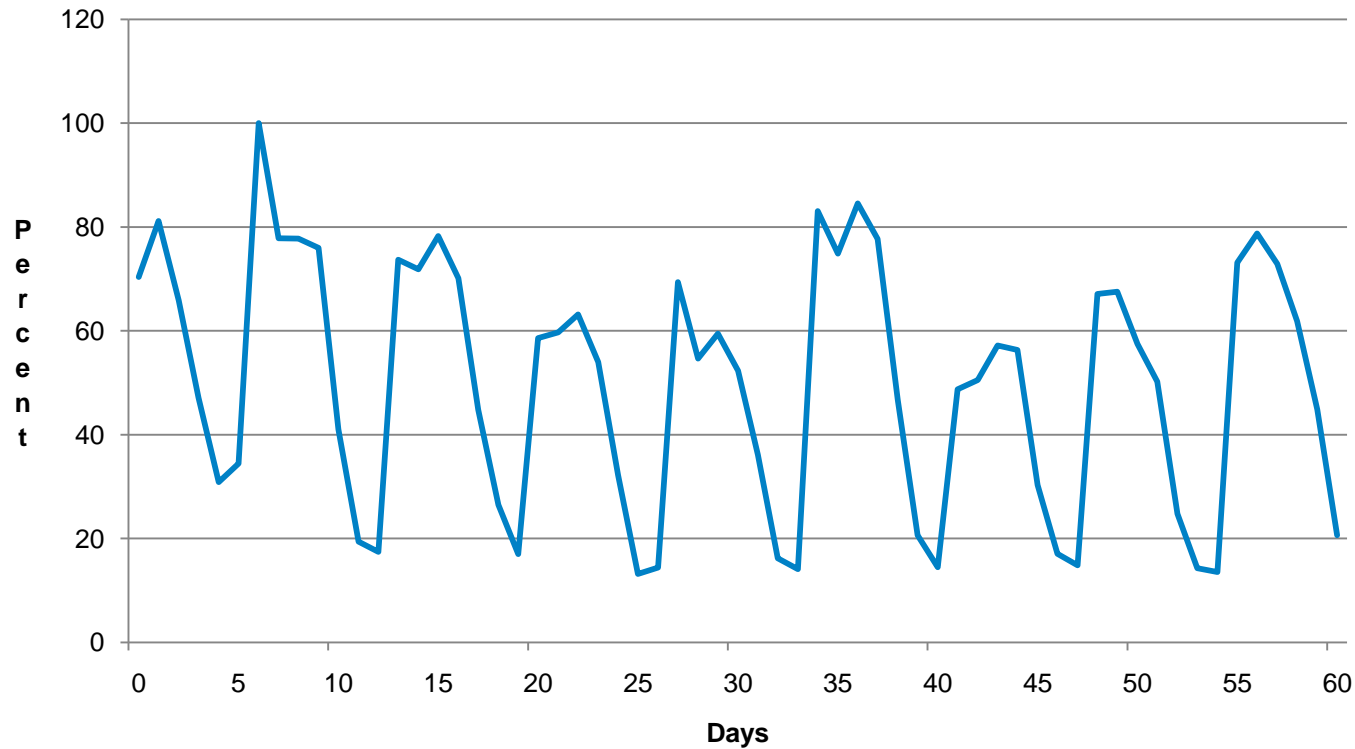
- Sep 2008 - first samples of code for vulnerability available
- Oct 2008 – patch out-of-band for critical vulnerability (MS08-067)
- Nov 2008 – Conficker worm appears – 2M -10M infected machines
 - A, B, C, C++,D,E, versions -> release cycle every 6 weeks
 - Each version gets better at infecting and evading detection
 - Attackers are professional experienced coders and driven
- Patch speed – normal, even though highly critical
- April 1st impact
- Infections occurred all over the world – cost unknown
 - City of Manchester – US\$ 1.4 M plus US\$ 1.0 M for new infrastructure



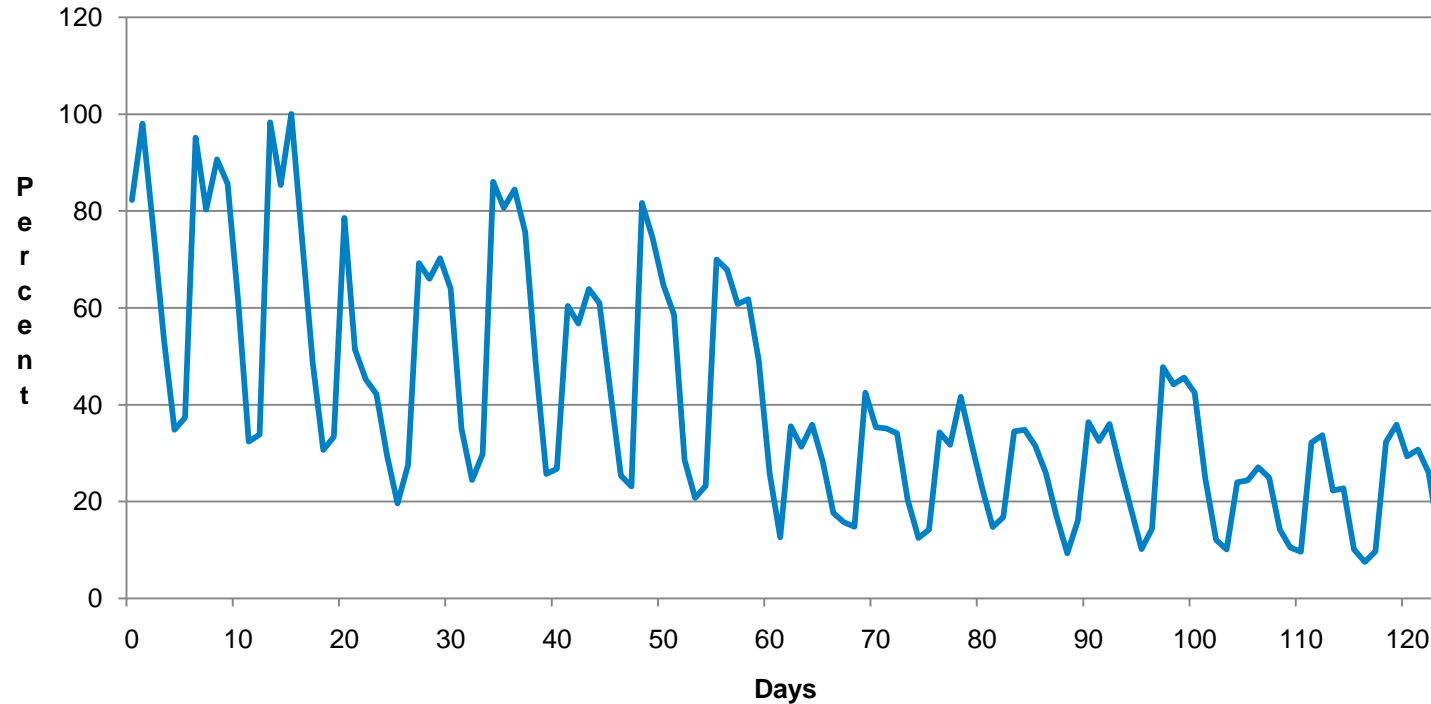
Laws 2.0 – More Half-Life - H1 2009



Laws 2.0 – More Half-Life - H1 2009

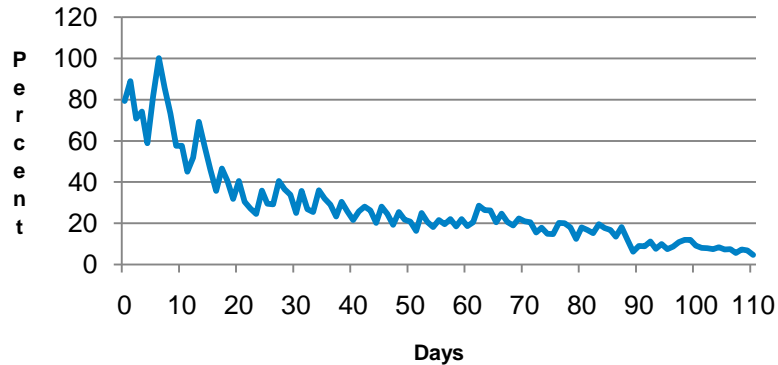


Laws 2.0 – More Half-Life - H1 2009

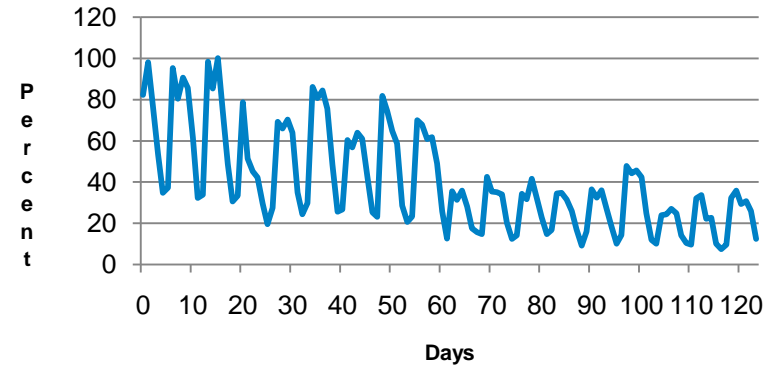


Laws 2.0 – Adding Half-Life - H1 2009

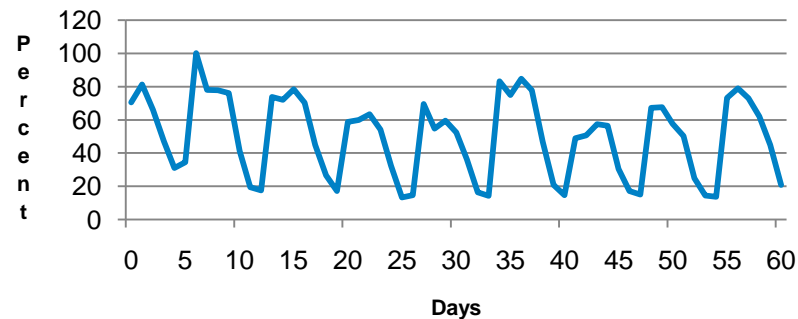
Microsoft OS vulnerabilities



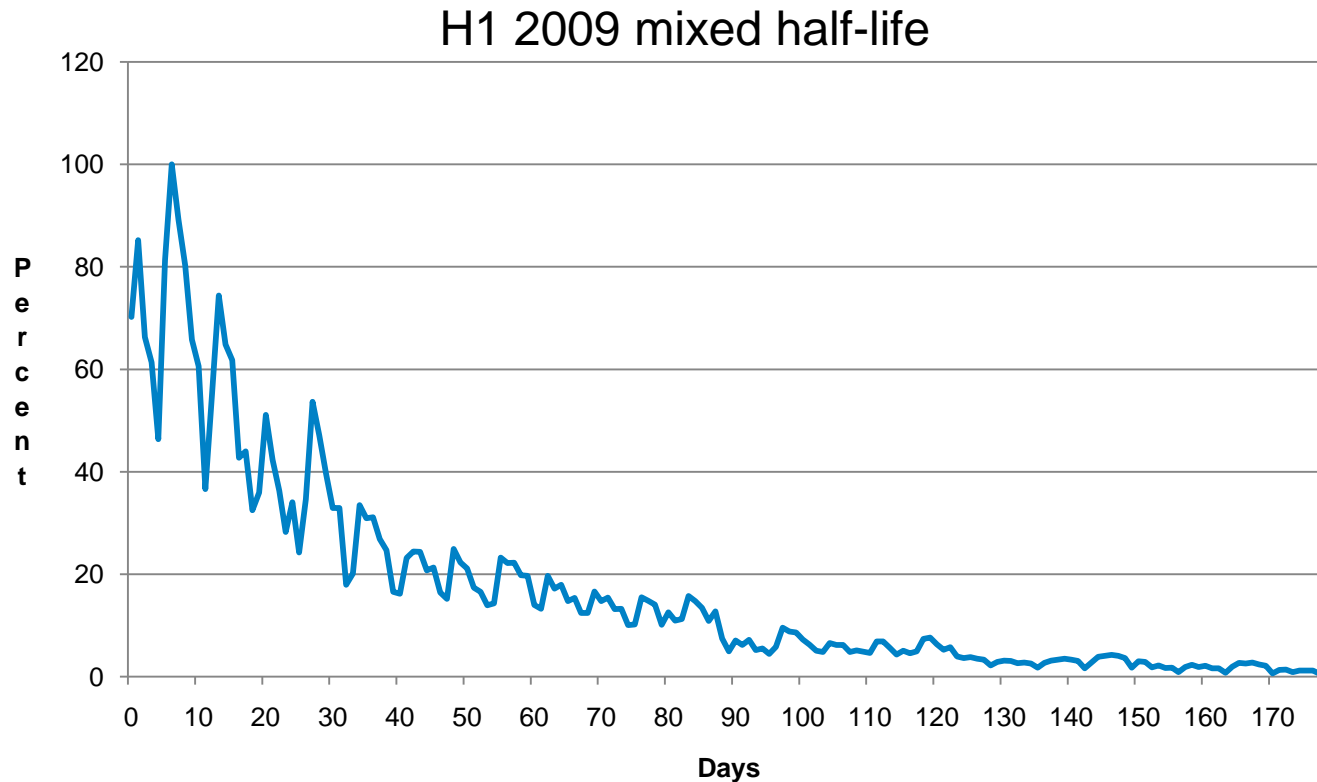
Adobe Acrobat APSA09-1 & APSA09-02



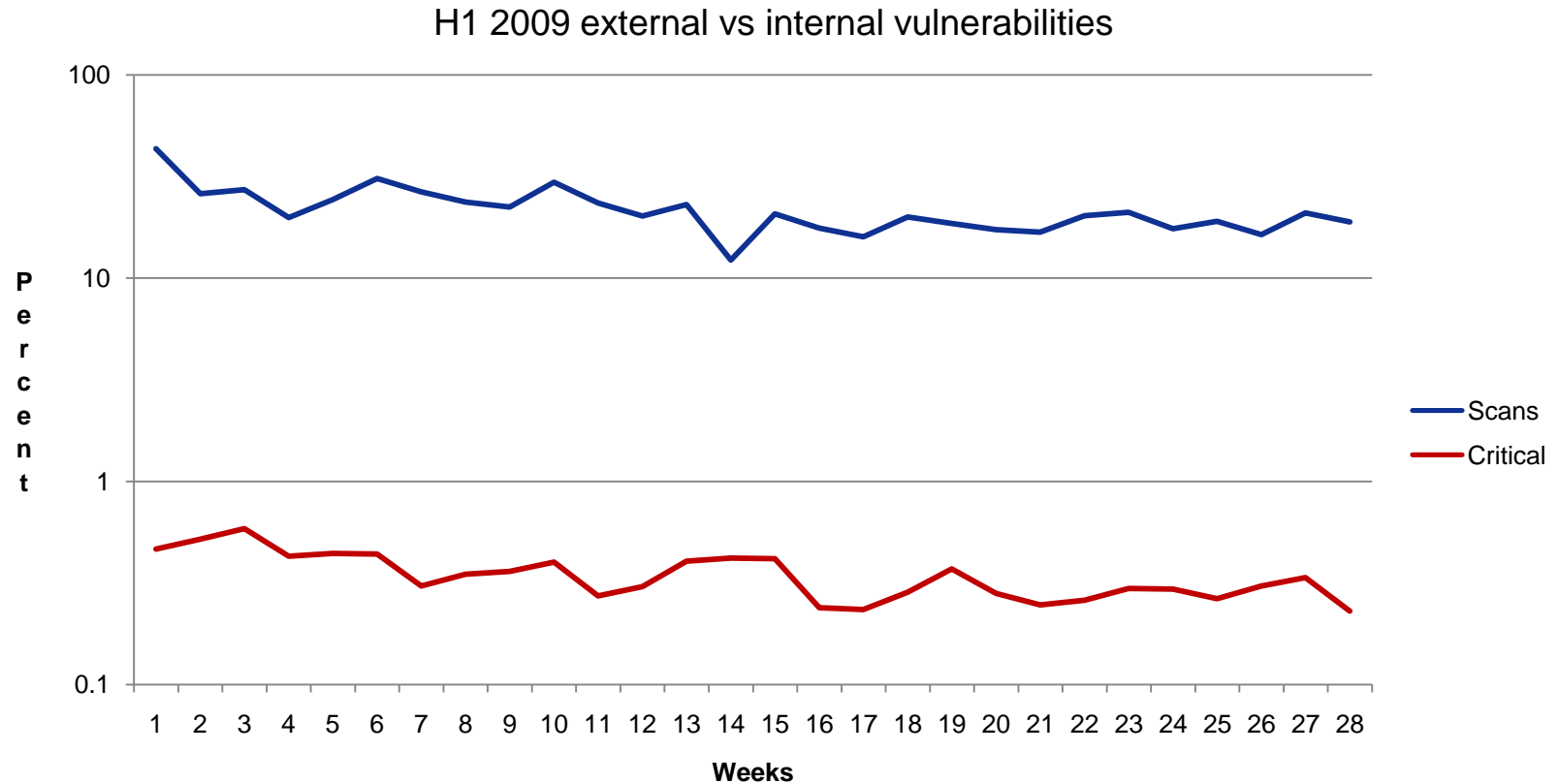
MS09-017 - Powerpoint - 5/12/2009



Laws 2.0 – Adding Half-Life - H1 2009



Laws 2.0 – H1 2009 – Half-Life



Laws 2.0 – Recommendations

- Secure all levels - Map your Infrastructure
 - Perimeter and internal servers
 - Internal Servers
 - Desktops and laptops
 - Machines that move in and out of the network
 - Laptops
 - Internal Servers to the cloud
- Speed up the patch cycle
 - Vertical partition: fast, medium and slow target sets
 - Horizontal partition: robust and sensitive application
 - Lower half-life by focusing on application patching



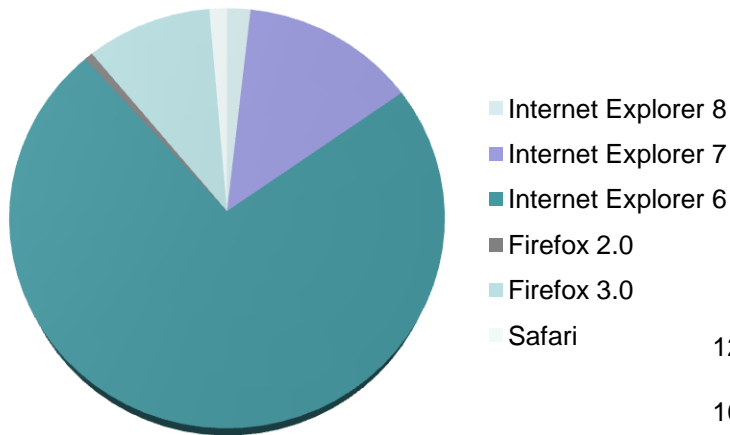
Panel

- Richard Bejtlich – GE
- Ed Bellis - Orbitz
- Paul Griffiths – Goldman Sachs
- Kris Herrin – Heartland Payment Systems
- Mark Weatherford – State of California

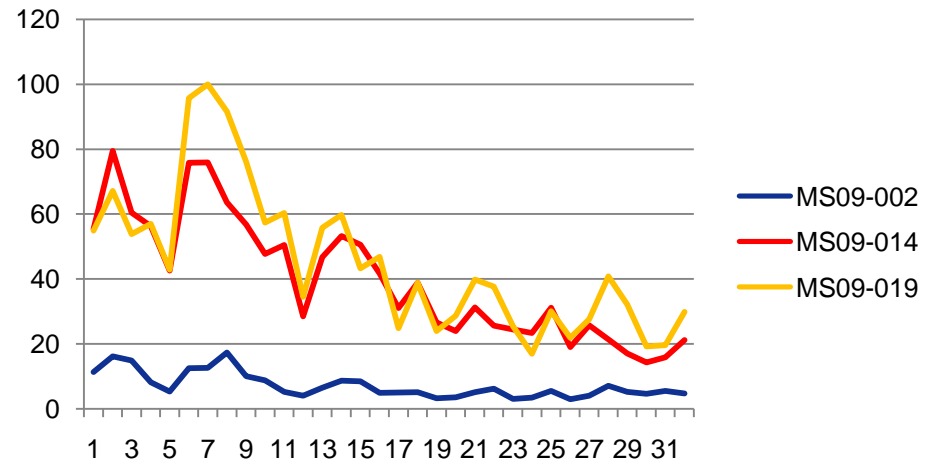


Panel – Browser Usage

Browser Usage on QualysGuard



2009 - Internet Explorer Half-Life



Thank You

Wolfgang Kandek
CTO - Qualys, Inc.
wkandek@qualys.com

blog: <http://laws.qualys.com>
updates on this research project

