The Laws of Vulnerabilities: Patching Progress and how to Expedite It

By: Jason Falciola, GCIH, GAWN
Technical Account Manager, Northeast

IT Roadmap
Boston, MA

May 25, 2010

Qualys, Inc.
www.qualys.com
Introduction

• Qualys Perspective
• Patch Management
• Patch Progress Data
• Common Steps
• Case Studies
• Lessons Learned
• Summary
• References
• Q&A
Patch Management

• Patches are an intrinsic part of a defense-in-depth program:
  – fix root causes - vulnerabilities
  – stay with the machine – which become increasingly mobile
    – Laptops
    – Servers with virtualization
• After user education patching is the most efficient weapon against malware as it deals with the “drive-by-download” infection vector
• Must consider the concept of “threats” at the same time
Patch Progress - Laws of Vulnerabilities

- Worldwide coverage – 2009
- 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 Area and Application Type
  - 5 major industries
  - Operating System and Applications
Laws of Vulnerabilities 2.0 – 2009 data

- **Half-life** - the time interval for reducing occurrence of a vulnerability by half.

- **Prevalence** – measures the turnover rate of vulnerabilities in the ‘Top 10’ list during a year.

- **Persistence** – total life span of vulnerabilities.

- **Exploitation** – time interval between an exploit announcement and the first attack.
Overall Critical Vulnerabilities – 72M data points

Half-Life = 29.5 days
Laws 2.0 – Half-Life by Industry

Finance Sector

Half-Life: 23 days

Service Sector

Half-Life: 21 days

Wholesale/Retail Sector

Half-Life: 24 days

Manufacturing Sector

Half-Life: 51 days
Laws 2.0 – Prevalence

60% turnover as compared to 50% in 2004

Top 10 Critical Vulnerabilities - predominantly Windows

- Adobe Flash Player Multiple Vulnerabilities (APSB07-12)
- Adobe Flash Player Update to Address Security Vulnerabilities (APSB09-01)
- Adobe Acrobat and Adobe Reader Multiple Vulnerabilities (APSB08-15)
- Adobe Reader JavaScript Memory Corruption Vulnerability (APSA09-02/APS09-06)
- Sun Java Multiple Vulnerabilities (244988 and others)
- Microsoft Office PowerPoint Could Allow Remote Code Execution (MS09-017)
- Microsoft Excel Remote Code Execution Vulnerability (MS09-009)
- Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)
- WordPad/Office Text Converters Remote Code Execution Vulnerability (MS09-010)
- Vulnerabilities in Microsoft DirectShow Allow Remote Code Execution (MS09-028)
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
  – 2 Out-of-band releases by Microsoft in 2010
  – Others: Adobe Acrobat Reader, Firefox 3.5

• Automatic exploit generation has been demonstrated

• Exploit availability is now measured in single-digit days
  – MS08-001 – 14 days, MS08-073 – 12 days, MS09-001 – 7 days
  – Microsoft Exploitability index validity = 30 days
Patch Progress Data

- Patch Progress uneven
  - Industries
  - Applications

Source: Project Quant - Securosis
Patch Management – Common Steps

• Intelligence – Monitoring
  – NVD, Secunia, Symantec, US CERT, Verisign
  – Vendors: Adobe, Apple, Microsoft, Oracle, RedHat

• Testing
  – Internal Lab
  – First and Second Adopters Group

• Deployment
  – Automation
  – Agent based: BigFix, Lumension, WSUS
  – Remote: Shavlik

• Verification
Case Study 1 – Large Media org in NA

- 10,000+ IPs under Management
- Windows and Macintosh Workstations
  - 10 days for critical OS and Application patches
- Backend Infrastructure
  - 30 days (database, applications)
- Quality Assurance
  - Phase 1 – “volunteers” < 1 % - day 2
  - Phase 2 – 10 % day 3 and 4
  - Phase 3 – 100 % starts day 5
Case Study 2 – Global Financial

- **50,000+ IPs under Management**
- **Windows Workstations**
  - 5 days for critical OS and Office patches
- **Backend Infrastructure**
  - 30 days (database, applications)
- **Quality Assurance**
  - Phase 1 – 1% - day 1
  - Phase 2 – 10% day 2 and 3
  - Phase 3 – 100% starts day 4
Case Study 3 – Global Manufacturer

- 300,000+ IPs under Management
- Windows Workstations
  - 8 days for critical OS and Office patches
- Backend Infrastructure
  - 30 days (database, applications)
- Quality Assurance
  - Phase 1 – 1 % - day 1
  - Phase 2 – 10 % day 2 and 3
  - Phase 3 – 100 % starts day 4
Common Characteristics

Divide and Conquer

◆ Vertical Partitioning
  • Workstations = streamlined testing, fast patching
  • Servers = longer test cycles, normal patching
  • Slow patching on request -> additional security techniques
    – Stringent Firewalling
    – Bastion Hosts
    – IPS systems
Common Characteristics

◆ **Horizontal Partitioning**
  - Internet Explorer = streamlined testing, fast patching
  - Adobe Reader = streamlined testing, fast patching
  - Office Applications = streamlined testing, fast patching
  - Servers = longer test cycles, normal patching
  - Slow patching on request -> additional security techniques
    - Stringent Firewalling
    - Bastion Hosts
    - IPS systems

◆ **Patch prioritization tools**
Patch Priority:

1. Apply Microsoft Windows XP Service Pack 3
   which will fix MS06-025, MS05-039, MS07-056, MS07-034, MS07-011, MS08-022 and 35 other vulnerabilities.

2. Apply MS09-037 - Fix for: Microsoft Active Template Library (ATL) Remote which will fix MS07-056, MS06-076, MS06-016, MS06-005, MS06-024, MS06-043, MS07-047

3. Apply MS09-028 - Fix for: Microsoft DirectShow Remote Code Execution Vulnerability which will fix MS08-033, MS09-011, MS07-064

4. Apply MS09-034 - Fix for: Microsoft Internet Explorer Cumulative Security Update which will fix MS09-019, MS09-014

5. Apply Microsoft Office 2003 Service Pack 3
   which will fix MS07-042, MS06-061
Sample Patch Prioritization Tools

1. Apply Microsoft Windows XP Service Pack 3 which will fix MS06-025, MS05-039, MS07-056, MS07-034, MS07-011, MS08-022 and 35 other vulnerabilities.

2. Apply MS09-037 - Fix for: Microsoft Active Template Library (ATL) Remote which will fix MS07-056, MS06-076, MS06-016, MS06-005, MS06-024, MS06-043, MS07-047

3. Apply MS09-028 - Fix for: Microsoft DirectShow Remote Code Execution Vulnerability which will fix MS08-033, MS09-011, MS07-064

4. Apply MS09-034 - Fix for: Microsoft Internet Explorer Cumulative Security Update which will fix MS09-019, MS09-014

5. Apply Microsoft Office 2003 Service Pack 3 which will fix MS07-042, MS06-061
Lessons learned

• Accurate Inventory crucial

• Need more than one Automated Patch System to cover all platforms

• Verification necessary to
  – Assure Coverage
  – Detect Patch failures

• Mobile systems benefit from Patch availability in the DMZ

• Standard builds/reduced privilege can help

• You’re only as strong as your weakest link
Up and Coming

• Virtualization
  – Additional vulnerabilities
  – Dormant VM patching

• Autonomous Applications
  – Firefox autonomous patching
  – Chrome with silent patching
  – Adobe Reader, automatic patching

• Smartphones

• Enduser owned systems
Summary

- Diversity and Mobility of IT devices increasing
- Vulnerability/Exploit cycle accelerating
- Standard defenses (FW, AV, etc) stressed
- Patching, a fundamental protection
- Fast patching a challenge to many companies

- Accurate Inventory, an automated Patch system and a trustworthy verification system are key to a successful patching program
References

• Exploit Speed
  http://isc.sans.org/diary.html?storyid=8437

• Project Quant
  http://www.securosis.com/research/project-quant

• Patch Management Community
  http://www.patchmanagement.org

• Qualys Laws of Vulnerabilities 2.0
  http://laws.qualys.com

• Secunia – Security Exposure of Software Portfolios
Questions?

Thank You!

jfalcioia “AT” qualys.com