
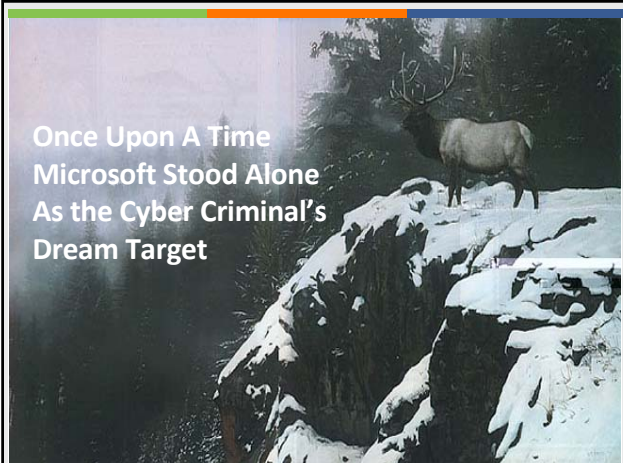


<h2>Preventing Client Side Attacks</h2> <p>Yesterday's Trusted Web Site is Today's Malicious Server</p>	
	<p>Kim L. Berndt Director</p> <p>February 17, 2011</p>

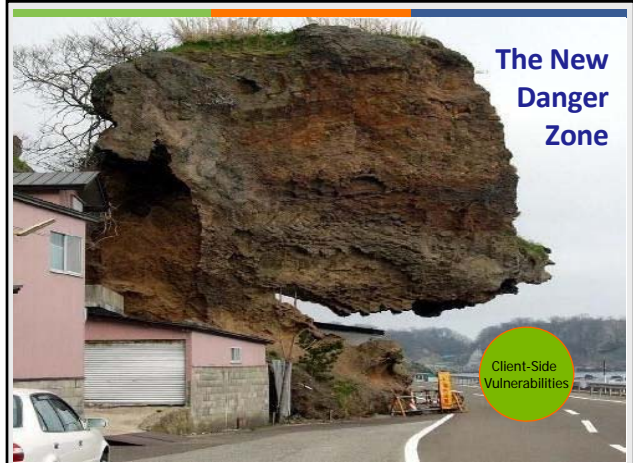


Agenda:


- Attacks are no longer centered on the Microsoft operating system or confined to the data center.
- Patching 3rd party applications is not the same as patching the operating system.
- Best Practice: Controls for IT Audit, Security, and Operations.
- TFTF: Tales From The Field



Once Upon A Time
Microsoft Stood Alone
As the Cyber Criminal's
Dream Target



The New
Danger
Zone



Client-Side
Vulnerabilities

shavlik

Targets in the New Danger Zone

The image displays six logos arranged in two rows. The top row contains Adobe Reader (red and white), Internet Explorer (blue 'e' with a yellow ring), and Firefox (orange and blue globe). The bottom row contains Adobe Flash (red circle with white 'f'), Apple QuickTime (blue circle with white 'Q'), and Microsoft Office (four colored squares above the word 'Office').

shavlik

Over the Past Few Years Application Vulnerabilities Have Surpassed OS

- Adobe Reader - 45 bugs, averaging about one per week
- Microsoft's Internet Explorer had 30 bugs
- Mozilla Firefox - 102 bugs
- Rounding out the list
 - Adobe Flash and Shockwave
 - Apple QuickTime, iTunes, Safari, and more
 - Microsoft Office
 - Sun JRE

<http://www.forbes.com/2009/12/10/adobe-hackers-microsoft-technology-cio-network-software.html>

shavlik

Hackers leverage zero-day weakness in IE 6 for targeted attack against Google and more than 30 other companies.

The image shows a man in a dark jacket and pants walking from right to left in front of a large white sign with the Google logo. The sign also features the Chinese characters '谷歌' (Google) below the logo. In the background, there are windows of a building.

I don't use those apps in my datacenter
My datacenter is safe and an attack on workstations or laptops would be minimal.

shavlik

Hackers don't have to find you, end users are leading them to your door

- Client-Side Vulnerabilities are Now the Primary Infection Vector
- Targeted email attacks are exploiting client-side vulnerabilities in Adobe Reader, Apple QuickTime, Adobe Flash and Microsoft Office
- Those same client-side vulnerabilities are exploited by attackers when users visit infected web sites

<http://www.sans.org/top-cyber-security-risks/>

Hackers don't have to find you, end users are leading them to your door

"The top Web-based attack for the quarter was related to malicious PDF activity, which accounted for 36 percent of the total.

Last quarter, malicious PDF activity accounted for 57 percent of the total Web-based attacks."

Internet Security Threat Report

April – June 2010, the latest series of the Symantec Intelligence Quarterly

<http://www.symantec.com/business/theme.jsp?themeid=threatreport/>

Hackers don't have to find you, end users are leading them to your door

"Symantec believes that the relative simplicity and effectiveness of using attack toolkits has contributed to the upward trends observed in cybercrime and that these kits are being used in a majority of malicious attacks carried out over the Internet. For example, one major kit, ZeuS, alone accounted for more than 90,000 unique malicious code variants as of August 2009...responsible for infecting millions of computers."

Symantec Report on Attack Kits and Malicious Web Sites – January 2011

Hackers don't have to find you, end users are leading them to your door

"Many different attack kits are available with a range of exploits and a wide array of attack vectors.

Increasingly, attack toolkits include exploits for vulnerabilities that affect multiple applications and technologies. This increases the likelihood that an attack will succeed because there is a greater chance that the victim will be using one of the vulnerable applications and that **one of the applications is unpatched.**"

Symantec Report on Attack Kits and Malicious Web Sites – January 2011

Define Enterprise:

- Is it based on employees?
- Is it based on systems?
- Is it based on the complexity of the network?
- Is it based on an Audit requirement?
- Is it based on Public vs. Private ownership?
- Why is a 10,000 employee business different than a 100 employee business?

Security, Operations, Audit



Q. How does IT Security ensure systems and applications are being patched?

A. IT Security must first know exactly what the organization owns.

- You simply can not secure what you don't know you have!

Inventory Assessment



Step 1: Asset Inventory

- Systems: Domain, Non-Domain, Virtual Systems- On + Offline.
- Applications: (Office, 3rd Party, Browsers, In-House)
- Users: (Administrative Users, Standard Users,)
- Virtual Hosts: VMware ESXi, Microsoft Hyper-V, other.

Risk Assessment



Step 2: Prioritization

- Which systems are the highest value to the organization?
- Who has access to these systems today and why?
- Who ultimately owns these systems- Audit, Operations, Security, Business Unit, Executives?

Baseline Reporting



- Understand which machines are the highest asset value
 - According to severity that you've assigned
- Create reports on
 - status of patches missing per machine
 - User Accounts (Who is Admin)
 - Security Policy (Local, GPO)
- Track who performed each patch deployment and when patches were installed
- Important for Compliance/Regulatory reporting

Scheduled Release vs. Out of Band



- Microsoft Patch Tuesday- Second Tuesday of the Month recommends Critical Patches should be installed within 24 hours.
- Microsoft Out of Band Patches- MS10-002, MS08-067: how long before these were applied, are they still missing?
- How does your patch process change when Microsoft or another vendor goes out of band?
- Adobe releases “quarterly” and has issued out of band security patches in Feb/June/Aug/Oct/Nov of 2010

Don't USE IE! Don't USE ADOBE! -France, -Germany, SANS



- How do I replace ubiquitous apps in an enterprise setting?
- How do I roll out PDFXchange Viewer or Foxit Reader?
- Is Firefox really any better than IE?
- Google Chrome installs at the user level, not an enterprise application.

Organizations Should Still Say No to Standardizing on One Browser



- A standard of at least two different browsers from different vendors can provide more security than a single browser from a single vendor.

Publication Date: 26 February 2010/ID Number: G00174224

Complexity Keeps Growing!



- How do I reduce my attack surface?
- Am I more or less vulnerable with two browsers?
- What about the plug-ins for both sets of browsers – Flash.

shavlik

Patching 3rd Party Apps is Exponentially More Difficult

Microsoft has mature patch process

SLIDE 22

shavlik

Microsoft Patch Process Sets the Bar

Structured Guidance: Advance Notification, Patch Tuesday Release Cycle,

Research: MSRC, Technet, Security Research + Defense Blog, MAPP, Exploitability Index

Tools: WU, MBSA, WSUS, SCCM

Workarounds: Gpolicy, Fix it Tools

Support: Free Email and Support Calls

Zero Day Process: Will go Out-of-Band if needed



shavlik

WSUS

A recent Gartner report titled *The Patch Management Market: Collision or Coexistence?* dated March 3, 2008, states that "Organizations accepting WSUS as 'good enough' have significantly higher labor costs for content analysis, testing and deployment."

"Microsoft's WSUS comes as part of our University Select Agreement, but WSUS is limited and does not provide the application coverage we need. Different software tools are used by different departments to resolve and manage the patching process, such as custom-built scripts, in order to handle applications not supported by WSUS - which add to IT cost and resources."

--Pritpal S. Rehal, Senior IT Systems Administrator for University of York

shavlik

Adobe

Structured Guidance: Advance Notification, Quarterly Updates

Research: Adobe PSIRT Blog

Tools: Adobe Updater, Adobe Download Manager- Be Sure to Reboot!! (C:\Programfiles\NOS)

Workarounds: Adobe Javascript Blacklist Framework- "Some Registry Work Required"

Support: Online Forum, Email, Phone

Zero Day Process: Will address in the next quarterly patch- **Out-of-Band Feb 15, 2010/June 29/Aug 19/Oct 5/Nov 16**

TFTF: Adobe Reader



Home User vs. Enterprise User

Automatic Updates: Doesn't work for the Enterprise! Windows update became WSUS – Adobe could learn from this.

Adobe MSP format does not conform to SCCM (**now fixed**).
<http://forums.adobe.com/thread/537967>

Want to push the latest of Adobe and end up pushing Google and Yahoo Tool bars and Open Office (got the consumer version not the enterprise version). End users self-updating.

Legacy versions: (Reader 5,6 vs. 7,8,9)

Adobe Cont'd...



Q: How do I know that Adobe Flash Player is installed correctly?

A: Adobe Flash Player requires users to restart their browser after installation. To validate that Adobe Flash Player is installed correctly, visit www.adobe.com/software/flash/about/.

http://kb2.adobe.com/cps/520/cpsid_52001.html#noteone

TFTF: Adobe Flash



Want to patch Flash

- What version(s) do I have?
- IE or Firefox?
- Is Firefox open?
- IE, no problem. But you need to know what you are running and what versions!

Oracle\Sun Java



Structured Guidance: Notification, Patch Release cycle?

Research <http://blogs.sun.com/security/category/alerts>

Tools: Java Update,

Workarounds: NA,

JQS: Java Quick Launch Support- service that you need to stop for Java to update.

Support: Paid Support- Premium.

Zero Day Process: NA

TFTF: Oracle\Sun JAVA



- When you upgrade or patch JAVA, please leave the previous “Vulnerable” version installed.
 - Some applications won’t work without those older versions.
 - Push the patch but left the older versions on – and their vulnerabilities on system. (Note- latest versions Java 6 update14 and newer will uninstall previous versions. Some versions of Java won’t install on 64-bit operating systems!
- What is my risk?
 - How do I know which version of JAVA is registered with the OS?

Apple



Structured Guidance: “ For the protection of our customers, Apple does not disclose, discuss or confirm security issues until a full investigation has occurred and any necessary patches or releases are available. To learn more about Apple Product Security, see the [Apple Product Security website](#).”

Research: See Above

Tools: Apple Software Update, Apple Download Site, Bonjour,

Support: Phone or Email- “Make sure to have your hardware serial number available”!
And well let’s just say they might hang up on you....seriously.

Zero Day Process: See Above

Apple iTunes



When will you accept that a consumer application (iTunes) is running in the enterprise

- Does anyone not have an executive using an iPhone?
- When I go to patch iTunes it is really: iTunes, Safari, QuickTime
- Apple’s “New Painful Patching Methodology”

TFTF: Apple iTunes



Apple’s “New Painful Patching Methodology”

- What does a browser have to do with patching iTunes? Apparently everything.
- Patch iTunes, also get
 - Safari
 - QuickTime
 - MobileMe
 - Bonjour
- Home User “Double Click” vs. Enterprise “Silent Install”
- Apple Application Support
- How do you feel about apps going outbound?

Custom Built Applications



- How many of you have custom applications that you either built internally or purchased from an ISV?
- How many were notified by your software vendor or development teams to tell you their code was not vulnerable to (MS09-035) "Vulnerabilities in Microsoft Active Template Library (ATL) which Could Allow Remote Code Execution"?

This was an out of band patch!

- How many checked Visual Studio for this patch?

Best Practice Recommendations



1. Operating System "Security" patches and Service Packs
2. Browsers: IE, Firefox, Safari do each individually.
3. Plug- Ins: Flash, Silverlight, Java, iTunes, Skype
4. Office Versions, Office Converters, Install Media
(more)

Best Practice Recommendations



5. .Net, MSXML
6. Media Players: Quicktime, Real Player, Windows Media
7. Adobe Reader, PDF Reader
8. Custom Built or 3rd Party Applications
(more)

Best Practice Recommendations



9. Database Systems
10. Citrix Presentation (Install and Execute Modes)
11. Virtual Hyper Visor, Templates, Offline VM's.

Shavlik Data Team Lives this Daily



Special recognition to Shavlik Patch Patrol for their contributions.

Resources

- <http://securitycenterblog.shavlik.com/>
- <http://www.shavlik.com/webinars.aspx>
- <http://www.adobe.com/support/security/>
- <http://support.apple.com/kb/HT1222>
- <http://blogs.sun.com/security/category/alerts>
- <http://www.microsoft.com/technet/security/current.aspx>
- <http://www.microsoft.com/technet/security/bulletin/Ms09-035.msp>