3 Strategies to Protect Endpoints from Risky Applications

Though most organizations have invested considerable time and effort in improving their endpoint risk management processes, many of them are ill-equipped to handle the myriad of third-party applications that are increasingly introducing the most risk into today's IT environment. That's because as the typical IT organization has worked on reducing the risk profile of PC and server operating systems, cyber criminals have started to look for greener pastures — namely among third-party applications.

August 2010

Introduction

Though most organizations have invested considerable time and effort in improving their endpoint risk management processes, many of them are ill-equipped to handle the myriad of third-party applications that are increasingly introducing the most risk into today's IT environment. That's because as the typical IT organization has worked on reducing the risk profile of PC and server operating systems, cyber criminals have started to look for greener pastures — namely among third-party applications.

And that's why the SANS Institute has named client-side application vulnerabilities one of the top IT security priorities facing organizations today. No longer is it simply OK to focus on Microsoft products — organizations must extend their protection to all of their third-party applications.

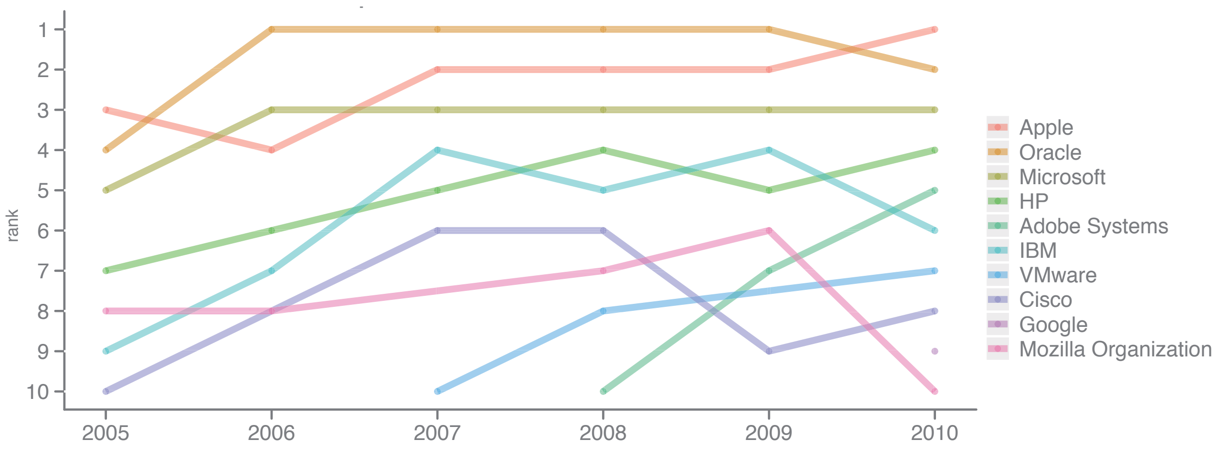
App Attack

If there's one truth that security researchers have uncovered today about the criminal hacking community, it's that the bad guys are engaged in a love affair with the application layer.

Microsoft has made strides in hardening its operating system from attacks and improving its patch release process. More organizations than ever are patching their operating systems in a timely fashion. But in an application-rich business environment, cyber criminals are having a field day attacking un-patched client-side applications.

In fact, researchers say that in recent years 93 percent of vulnerabilities exploited in the wild are client-side application flaws. And in 2009, four of the top five exploited vulnerabilities were in third-party applications.[1]

Rank of Top-10 Vendors with Most Vulnerabilities



Source: Secunia Half Year Report 2010

[1] Symantec Global Internet Threat Security Report

There's no more stark an example of this trend as there is among PDF and document readers, which are fast becoming a favorite target among all applications. In the first quarter of 2010, nearly 50 percent of all detected attacks exploited flaws in Adobe PDF readers.[2] Though Adobe has acknowledged the increasing risks to its product and tasked its developers with creating a patch release schedule similar to Microsoft's Patch Tuesday, the risks are numerous if organizations are not regularly taking advantage of Adobe's patches.

Because not only are the bad guys taking advantage of flaws within commercial applications, they're also targeting a bevy of Web application vulnerabilities. Researchers found that in 2009, 49 percent of vulnerabilities were within Web applications.[3]

> The number of vulnerability disclosures for document readers, editors and multimedia applications rose by 50 percent in 2009.[4]

According to a recent SANS report[5], the problem of un-patched client-side vulnerabilities is one of the two most pressing priorities organizations need to address to mitigate cyber security risks. SANS estimates that most organizations today take at least twice as long to patch third-party application vulnerabilities than they do to patch operating system vulnerabilities.

The reason why attacks on the application layer are exponentially increasing is because the strategy works. Attackers know that even as organizations have improved their operating system protection and OS vendors have plugged many of the security gaps within their platforms, the security community has far more catching up to do with similarly flawed applications. According to one set of research, there are at least 2.7 billion un-patched applications running on machines within the U.S. alone. And 98 percent of Windows machines have at least one un-patched application.[6]

> "Waves of targeted e-mail attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly used programs such as Adobe Reader, QuickTime, Adobe Flash and Microsoft Office. This is currently the primary initial infection vector used to compromise computers that have Internet access. Those same client-side vulnerabilities are exploited by attackers when users visit infected websites. Because the visitors feel safe downloading documents from the trusted sites, they are easily fooled into opening documents and music and video that exploit client-side vulnerabilities. Some exploits do not even require the user to open documents. Simply accessing an infected website is all that is needed to compromise the client software."

SANS's "The Top Cyber Security Risks" report

[2] Kaspersky

[3] IBM X-Force 2009 Trend and Risk Report

[4] IBID

[5] SANS Top Cyber Security Risks

[6] Secunia

Gaps in Free Tools

Oftentimes businesses choose to save money by utilizing free and effective tools such as Windows Server Update Services (WSUS) to handle Windows patches and cross their fingers in hopes that other updaters for their applications are as effective as the Microsoft utility. Unfortunately, trends are showing the Achilles heel in this plan is that this strategy gets harder to implement as more applications need to be patched.

The third-party applications that are so ubiquitous in the modern IT environment simply aren't being managed by the free patching tools that many organizations have opted to put their trust in. Even those applications that offer free automatic updaters, such as Adobe Reader and Java, pose a lot of challenges to IT staff. Many of the individualized updaters offer few or no mechanisms to centrally manage multiple machines and no way to coordinate and deploy patches across a number of different applications.

And then there are those applications that don't even have an automatic updater, particularly those custom applications and Web apps that so many organizations have grown to depend on. Even when vulnerabilities are found in these applications, organizations that rely only upon tools such as WSUS have no easy way to quickly deploy custom patches across the infrastructure. While it is possible to create some custom patches, the process is arduous, manual and error prone.

Asking IT to effectively manage application risks using such a primitive set of tools is like asking someone to put a puzzle together with an incomplete set of pieces and no table on which to assemble them.

Continued »

Defense-in-Depth with Three Application Risk Strategies

The data shows that risks posed by vulnerable applications continue to mount. Organizations that acknowledge that a grab-bag of free patching tools to close the gaps left by these flaws is not failsafe quickly see that there has to be a better way to mitigate third-party application risks.

Ideally, organizations should approach the problem with a three-pronged strategy that layers multiple security technologies to achieve defense-in-depth. The three major strategies at organizations' disposal to better reign in application risks are:

- Antivirus
- Comprehensive Patch and Configuration Management
- Application Whitelisting

Antivirus:

The most fundamental of all security defenses, antivirus is the first line of defense in cleaning up the stream of malware that buffets organizations' third-party application vulnerabilities every day. In today's dynamic threat environment, organizations face an enormous variety of malware, including spyware, Trojans, rootkits, viruses and more, that is growing in volume, scope and sophistication. Much of today's malware is fueled by financially motivated cyber criminals trying to gain access to valuable corporate, consumer and personal data. And a large percentage of it is dedicated to breaching third-party applications, which malware developers know are more prone to attack and more easily compromised without notice.

Organizations need antivirus software that provides fast and accurate identification of the vast amount of known malware. And with malware's increasing sophistication, organizations need antivirus protection that employs multiple detection techniques to identify and block unknown malware that takes advantage of zero-day exploits. This includes the traditional signature-matching techniques that antivirus is well-known for as well as behavioral techniques that can pinpoint suspicious code, applications and exploit activity on an endpoint.

How Malware Spreads

In a recent study, researchers found that some of the most common means of malware propagation are found within the application stack. Organizations that can leverage antivirus to detect propagation behavior and suspicious application activity will get a head start on protecting their endpoints. The following seven methods are the most common chosen by malware coders:

- File-sharing executables: Used in 72% of attacks
- Common Internet File System (CIFS) File Transfer: Used in 42% of attacks
- E-mail Attachment File Transfer: Used in 25% of attacks
- Remotely Exploitable Vulnerability: Used in 24% of attacks
- File sharing, P2P: Used in 5% of attacks
- HTTP, Embedded URI, Instant Messenger: Used in 4% of attacks
- SQL: Used in 2% of attacks[7]

[7] Symantec Global Internet Security Threat Report Symantec Global Internet Security Threat Report

Comprehensive Patch and Configuration Management:

The escalating risks within the application layer merge together to make the choice of comprehensive third-party patch management solutions over free, vendor-supplied patch management tools an obvious one. The small savings an organization collects by going with the latter are typically eaten up in additional operational overhead and potentially costly breaches when inconsistent practices lead to the inevitable.

Implementing a comprehensive patch management tool that can automate the patching process across all applications and all machines within your organization gives you the power to more easily mitigate application layer risks.

Additionally, many of the vulnerabilities that hackers target within third-party applications are part of larger blended attacks that build on additional configuration and system vulnerabilities found within the endpoint. Organizations also need the capability to address those configuration problems and vulnerabilities—particularly those without a patch— to diminish the risk of an attack doing great harm.

Application Patch Lag

A recent study by Securosis brings this trend of application patch lag into crystal-clear focus. When the security research firm queried nearly 100 businesses about their patch management practices, it found that 85 percent of organizations rated themselves as having some level of maturity. But among those same participants, 40 percent or more reported that they have no or only informal patch management processes in place for non-operating-system vulnerabilities. And even those organizations that utilize tools tend to rely on a whole laundry list of updaters to apply all of their application patches.[8]

“Companies tend to utilize multiple-vendor and third-party tools in their patch management process,” the Securosis report says. “Given the variety of assets managed this is not surprising, but it does emphasize the value that a heterogeneous patch management tool could provide to organizations.”

Continued »

[8] Symantec Global Internet Security Threat Report

Application Whitelisting:

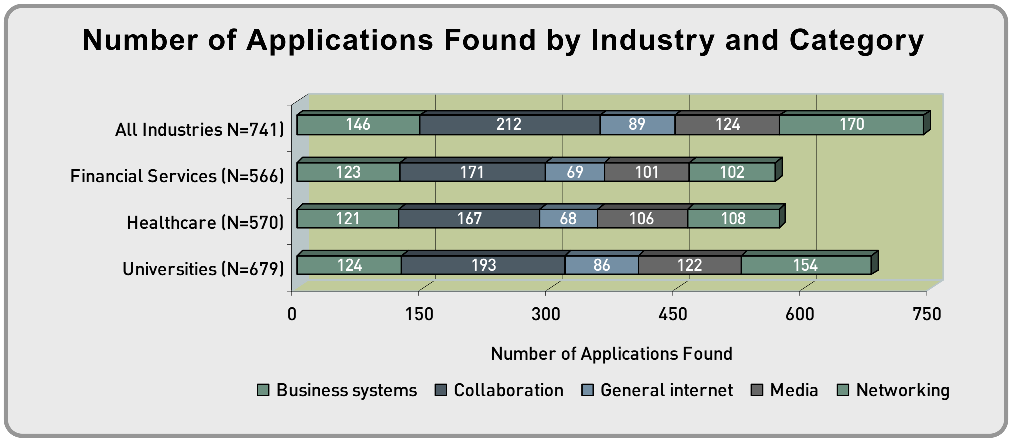
While a great many of an organization's employees really do need the bulk of the applications on their machines, there still exist plenty of risky non-essential applications that end up installed on machines without any kind of application controls.

An application whitelisting solution can help organizations better control the process of application deployment and ensure that only essential third-party applications land on a machine. This can prevent users from installing unknown applications that could be filled with un-patched vulnerabilities or from even installing software that is actually malware masquerading as a benign application. By allowing only known-good and fully patched applications to run within an environment, organizations will proactively eliminate many of the problems associated with third-party applications.

Applications Running Rampant

A recent survey of the most common applications running within 347 large organizations worldwide found nearly 750 applications frequently running on their systems during a six-month period. Increasingly, these applications — such as social networking applications, instant messaging, peer-to-peer applications and Web 2.0 collaboration apps — are enabled to hop from port to port, use port 80 or port 443, and tunnel other applications. Some stats:

- 65% of applications were designed for Web accessibility
- 30% of applications were client-server-based
- 22% of applications were capable of port-hopping
- 23% of applications were capable of tunneling[9]


Number of Applications Found by Industry and Category

Source: Palo Alto – The Application Usage and Risk Report, Spring 2010

[9] Symantec Global Internet Security Threat Report

Conclusion

The next generation of critical threats besetting IT organizations are originating within the application layer. With such organizations as the SANS Institute warning of the inordinate risks posed by third-party applications and major security research outfits coming out with data daily that supports these warnings, it is clear that organizations can no longer afford to ignore where and how employees deploy third-party applications.

To truly address the risks posed by these applications, organizations need to adopt a layered strategy that includes antivirus, patch and configuration management, and application control. Ideally, organizations should seek out solutions that can roll up all three of these strategies into a single seamless platform. Running together, an advanced antivirus tool, smart patch management and configuration management tools, and granular application whitelisting controls achieve a synergy of risk management that could not be attained individually.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension, Lumension Patch and Remediation, Lumension Vulnerability Management Solution, "IT Secured. Success Optimized.", and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.888.725.7828
fax: +1.480.970.6323