



## X-Force Research & Development Newsletter

July 2006

## Mac OSX vs. Microsoft XP

Not less than two years ago, Microsoft found itself fully engaged in combating accusations that Windows was less secure than Linux. After several detailed analytical studies relating to vulnerabilities, out-of-the-box configurations, default services and security patch responses, the end verdict for most observers was a confused draw. The security and integrity of both operating systems (OS) were tied directly to the skills and awareness of the end-user and the myriad applications he may install or use on a daily basis.

So, having ridden the wave at least once this decade, Microsoft Windows now finds itself facing a new antagonist — Apple and its Mac OSX.

You may have seen the new TV and magazine advertising campaign that describes how much better Macs are than Microsoft Windows (visit <http://www.apple.com/getamac/ads/> to see the TV ads). A couple of these advertisements address system security, in particular out-of-the-box configuration and the proliferation of Windows viruses (referencing 114,000 viruses in 2005). Simultaneously, several independent security vendors have published their own analyses and have advised users that they may be more secure using Apple computers running OSX.

For the most part, this advice has been based upon the worldwide proliferation of viruses. Indeed, there are literally hundreds of thousands of viruses and malware that target Microsoft Windows systems and, until February this year, there were no viruses specifically targeting Apple's Mac OSX.

This fact is highly surprising to many security professionals. In the late 1980s, the situation was completely reversed; Apple Macintoshes were commonly associated with viruses, while viruses were not a problem for PCs. Although there have been a couple of hundred macro viruses that affect Microsoft Office on both OSX and Windows, OSX.Leap.A was the first virus that only affected OSX.



OSX.Leap.A, was an instant messaging worm that propagated via iChat by sending a compressed file labeled as "latestpics.tgz" (which contained a hidden payload disguised as a JPEG image file) to the infected user's buddy list. Since February there have been many more viruses targeting OSX.

With this in mind, it is important that users be reminded that not having had a virus is definitely NOT the same as being immune to viruses. From an X-Force perspective, advice from some signature antivirus vendors to switch to OS X echoes the immortal words of Homer Simpson (in the episode "Oh Brother, Where Art Thou?"), "You know that little ball you put on your antenna so you can find your car in a parking lot? That should be on every car!"

### Why is Mac OSX so secure?

A question commonly asked of X-Force is, "Why is Mac OSX more secure than Windows?" The simple fact of the matter is, it is not. OSX has a long development history and has incorporated ideas for service design from several \*NIX variants (such as OPENSTEP, NetBSD, FreeBSD, etc.). This history, coupled with the strong emphasis on graphical user experience, means that OSX suffers from many common \*NIX application frailties in addition to less rigorous access controls.

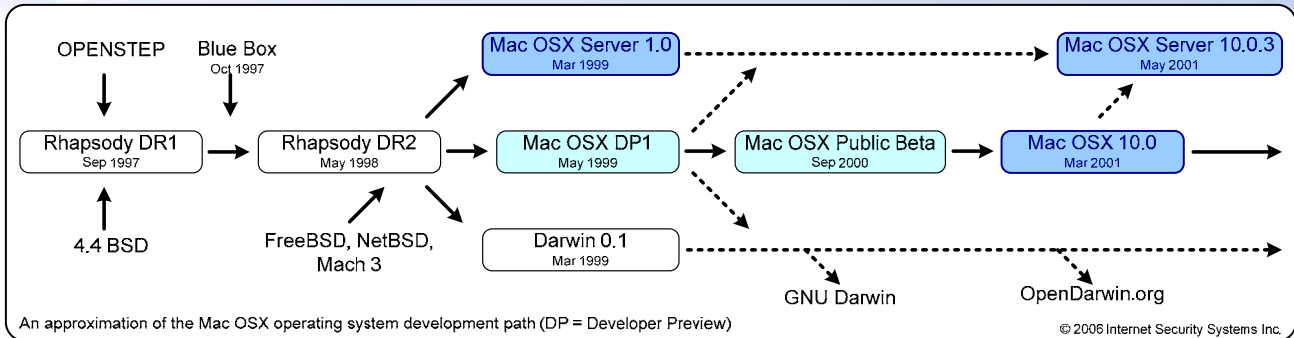
Since its first public appearance as a server operating system in 1999, OSX has suffered from vulnerabilities common to its \*NIX heritage plus those associated with Apple's custom software additions that ship with the operating system. As is typical with \*NIX-based operating systems, it is difficult to precisely track the number of security vulnerabilities that have affected OSX since its first public release. Many analysts have, and continue to, argue over whether the OSX vulnerability count is better or worse than any other popular \*NIX operating system.

The question for many organizations that could contemplate a migration to OSX is, "How does it compare to Microsoft Windows?"

X-Force security analysts have investigated every disclosed vulnerability within both operating systems and have found Apple's Mac OSX to have more vulnerabilities on a like-for-like basis than Microsoft Windows.

To create a level playing field, X-Force compared the desktop variant of Mac OSX 10.x with Microsoft's XP desktop operating system. This analysis included vulnerabilities associated with the base operating system and software installed by default as part of a standard installation. In addition, X-Force security analysts focused upon vulnerabilities from the beginning of 2004 onwards — a period in which both operating systems can be said to have matured into "stable" products and having already had any low-hanging fruit vulnerabilities discovered and consequently fixed.

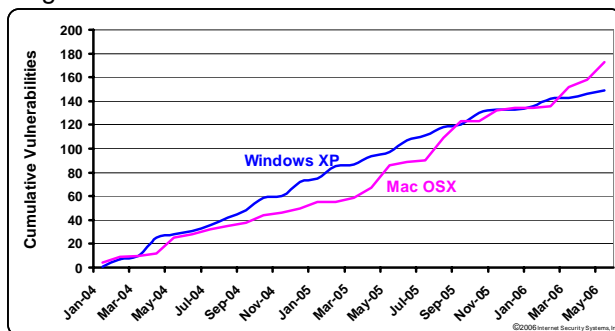
Our analysis revealed that the total number of vulnerabilities associated with the two desktop operating systems were very similar, with OSX actually suffering 13 percent more vulnerabilities



than Windows XP. For much of the last 2½ years, the rate at which vulnerabilities were discovered for both operating systems was very similar even though there was little correlation between the individual vulnerabilities discovered on a monthly basis. It is only since February of this year that the total number of OSX vulnerabilities has overtaken those discovered in Windows XP.

The question that then begs an answer is, “If OSX has more vulnerabilities than Windows XP, and is generally less secure, why are there so few viruses or people attacking it?” In answer, it is important to understand that while OSX is certainly one of the most popular \*NIX desktop operating systems, Apple’s share of the worldwide PC market is tiny — verging on insignificant (2.2% in 2005 [1]).

When it comes to system security, there are typically two key drivers for people wanting to create viruses or malware — commercial gain and kudos. From the commercial gain perspective, it does not really matter what the operating system is; it will still take roughly the same amount of development effort (and legal risk) to create a virus or malware, and the return on investment for targeting OSX installations is simply too little when compared to a popular operating system such as Microsoft Windows. However, this may change over the next few years as OSX proliferation is expected to increase with the adoption of Intel processors within Apple’s product range.



From a kudos perspective, the emphasis is largely upon infecting the most number of machines in the shortest period of time. Building up a massive Botnet network (and retaining control of it) achieves a lot of underground kudos (as well as revenue opportunities). Again, the effort to develop

technologies focused on OSX just does not provide an economical return — at the moment. The only real exceptions are kudos associated with doing something first (e.g., writing the first OSX worm) or the possibility of achieving a lot of media attention.

This latter point about media attention is likely to be a key influencer motivating attackers to target OSX throughout the remainder of this year. The comparison between Oracle’s “Unbreakable” marketing strategy from a couple years ago, and the new Apple advertising campaign harping on viruses and out-of-the-box configuration, can be seen as a call to arms for those who wish to establish a reputation for having proven Apple wrong.

So, for those organizations considering a move to a “more secure” OSX environment, would you like to buy a little ball for your car antenna?

– Gunter Ollmann, Director of X-Force

[1] “Low market share is badge of honor, as far as Mac faithful are concerned,” Mike Langberg, [http://www.siliconvalley.com/mld/siliconvalley/business/columnists/mike\\_langberg/14191452.htm](http://www.siliconvalley.com/mld/siliconvalley/business/columnists/mike_langberg/14191452.htm)

## Understanding Threats

### SCADA Basics

The word “SCADA” sounds like a protocol standard like HTTP or TCP/IP, but it is not. Instead, the acronym refers to the idea of remotely monitoring and controlling things. Any time you see a temperature gauge, emergency warning light or knobs, you have something that could fit under the general term of “Supervisory Control and Data Acquisition” system. Your car’s dashboard is, essentially, a SCADA system. In the TV series *The Simpsons*, Homer Simpson sits at a SCADA console to monitor the Springfield Nuclear Power Plant.

The term gained popularity after September 11 when the press published stories about cyberterrorism. They were afraid that hackers or terrorists could cause a nationwide blackout.

The key issue with SCADA is that all these systems have become computerized. You rarely have dashboards anymore — you have computer programs that simulate dashboards. The data that feeds these virtual dashboards is collected by remote computers that send the data across a normal network. The computers are standard systems based on operating systems like Microsoft Windows or Linux. The networks are standard TCP/IP networks — and these networks are often interconnected with the Internet.

For example, a power plant might hook up a Windows computer to some sensors and switches. The computer would collect and send all the data across a TCP/IP network to a central computer. It would also accept commands from the central computers to change switches and valves. It might also run some software locally to respond to conditions. For example, if the pressure on one sensor got too high, the Windows computer might turn off a valve without waiting for a command from the central system.

The central systems themselves are built from standard tools. Some companies like Windows build their systems using Microsoft components like VisualBasic. Others prefer the UNIX platform and build X Windows applications. In most cases, rather than trying to hack into the remote systems, it is easier for a hacker to get to these central systems. For example, the hacker could just click with the mouse on a virtual button that would send commands to thousands of systems to turn off the power.

One of the most important aspects of SCADA is historical data. These systems are designed not just so humans can watch what is going on, but also so things can be automated. For example, an oil company might gather long-term historical data from all its oil pumps, process that with a supercomputer, then send commands back to the pumps to optimize the flow of oil from the well. It is this sort of data that causes the biggest headaches for SCADA companies. They believe that there is no interconnection between their office networks (which are on the Internet) and their SCADA networks. The operators sitting at the consoles cannot



simultaneously surf the Internet. However, they have a backdoor through which that historical data is shipped to the office network for processing. ISS penetration testers will usually approach from the Internet, penetrate the office network and then follow that historical data back to the SCADA control network.

There is no easy solution to SCADA security. The systems are controlled by outside forces. Companies using SCADA systems must computerize everything because it dramatically lowers costs and increases functionality. Yet, they cannot patch those computers nor give them a good password, which

means they are open to attack by hackers or worms. They therefore try to separate them from the Internet, but find they have to interconnect things more than they wish. There are solutions out there that can help, such as ISS Virtual Patch™ technology, but mostly the SCADA industry is waiting for a major incident to hit somewhere before it starts adopting preemptive solutions.

— Robert Graham, Chief Scientist

## A Month in Review

In this section of the newsletter, X-Force briefly covers some of the security content developed or processed in the month of June.

### Vulnerabilities:

Last month was the biggest ever for new vulnerabilities, with 696 being disclosed, processed and analyzed by X-Force. This represents a 69 percent increase over June last year.

Overall, thus far in 2006, X-Force has covered 42 percent more vulnerabilities than for the same period in 2005.

	Reported					YTD
	Crit.	High	Med.	Low	Total	
June	3	70	539	84	696	3523

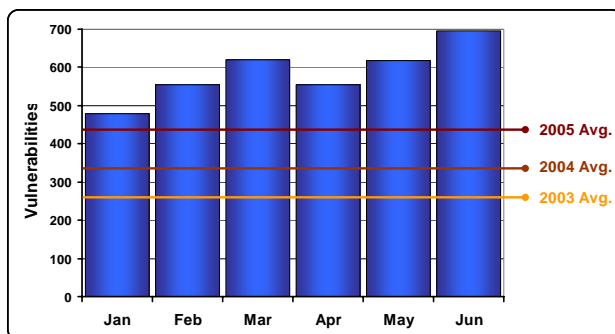
Of these vulnerabilities, 663 were remotely exploitable, 46 could only be exploited locally and 13

could potentially be exploited both remotely or locally.

Vulnerability Breakdown	
<b>Bypass Security</b>	<b>35</b>
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
<b>Data Manipulation</b>	<b>127</b>
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
<b>Denial of Service</b>	<b>47</b>
An attacker can crash or hang a service or system, or take down a network.	
<b>File Manipulation</b>	<b>4</b>
An attacker can create, delete, read, modify or overwrite files.	
<b>Gain Access</b>	<b>405</b>
An attacker can obtain local and remote access. This also includes vulnerabilities in which an attacker can execute code or execute commands, because this usually allows the attacker to gain access to the system.	
<b>Gain Privilege</b>	<b>13</b>
An attacker can gain privileges on the local system only.	
<b>Obtain Information</b>	<b>57</b>
An attacker can obtain information such as file and path names, source code, passwords or server configuration details.	

\* Right-hand column represents unique vulnerability count

### Vulnerabilities per Month vs. Annual Average



Top 5 Vulnerable Vendors	
Microsoft	<b>27</b>
Mozilla	<b>13</b>
Cisco	<b>10</b>
Partical Soft	<b>9</b>
MailEnable, MyBB, Ultimate PHP	<b>7</b>

\* Right-hand column represents unique vulnerability count

### Whiro:

The Whiro 0-day Web crawler project was kept busy last month identifying and classifying hundreds of new Web sites that utilize exploits to compromise vulnerable Web browsers and install malware or other malicious material.

For the month of June, Whiro repeatedly identified exploits embedded within Web sites that targeted 12 vulnerabilities affecting Microsoft Internet Explorer. The following table lists these exploit attempts by prevalence:

Most Prevalent Web Exploits	
MS-ITS CHM file code execution ( <i>MS04-013</i> )	*****
IE createTextRange() ( <i>MS06-013</i> )	****
IE createControlRange() ( <i>MS05-014</i> )	***
DHTML Objects ( <i>MS05-020</i> )	***
IE javaprxy.dll COM object ( <i>MS05-037</i> )	***
IE window() ( <i>MS05-054</i> )	***
RDS.Dataspace ActiveX ( <i>MS06-014</i> )	***
IE COM Objects ( <i>MS05-038</i> )	**
IE COM Objects ( <i>MS05-052</i> )	**
RealPlayer .SMIL (CVE-2005-0455)	*
Media Player BMP Handling ( <i>MS06-005</i> )	*
IE Media Player Plugin ( <i>MS06-006</i> )	*

### Malcode:

In June, the X-Force alpha-testing platform for the Virus Prevention System (VPS) - codename Catfish - identified 7 unique 0-day malcode attacks — before any other antivirus vendor. These 0-day threats comprised variants of four malcode families:

- Two variants of a new worm were first discovered and subsequently named by ISS as W32.Worm.Zade. The worm is commonly referred to as the "World Cup worm" because the e-mails it sends out have a World Cup soccer theme.
- Four new variants of the W32.Backdoor.Breplibot.AS, an IRCBot connecting to a predefined list of IRC servers via port 8080. Some of the W32.Backdoor.Breplibot variants are reported to have been spammed with the subject: "Osama Found Hanged." Thus, they are often referred to as the Osama Virus.
- Finally, toward the end of the month, X-Force uncovered a new downloader Trojan, W32.Downloader.Agent.AJN, which attempted to download and execute a variant of W32.PWS.Goldun, a password stealer with rootkit capabilities. ISS protection engines were able to detect both the downloader and the downloaded password stealer.

### Sample Harvesting:

It is worth noting that as part of the X-Force continued strengthening of ISS antivirus, anti-spyware and anti-malware protection, we investigated and added another 47,626 new samples to our malware zoo this month.

### X-Force Security Content:

#### Level-0 XPU's:

In June, the X-Force team responded to one level-0 vulnerability and its public exploits, and we remained *Ahead of the threat*.

#### New and Extended Protocol Support:

During June, X-Force engineers added one new protocol parser and extended 4 existing PAM protocol parsers. This work included the following protocols:

- Symantec RTVscan
- Microsoft Messenger
- Yahoo Messenger
- HTTP
- HTML

#### New Vulnerability Protection Algorithms:

X-Force added the following security coverage to our products, with 23 new events to address new vulnerabilities:

- Symantec\_Management\_Overflow
- HTTP\_Snort\_Uricontent\_Bypass
- IMAP\_Literal\_Overf
- Image\_EMF\_Long\_Description
- HTML\_Image\_Source\_DoubleExec
- HTTP\_MaxDB\_Percent\_BO
- HTTP\_MaxDB\_LockToken\_BO
- HTTP\_Novell\_iMonitor\_BO
- HTTP\_OpenView\_NNM\_CmdExec
- MSRPC\_MSRTC\_Message\_GUID\_BO
- Email\_Mime\_Header\_Overf
- IP\_Option\_Linux\_DoS
- HTML\_Lotus\_Webaccess\_JS\_XSS
- IMAP\_Mdaemon\_Foldername\_DoS
- CHM\_File\_Detected
- MSRPC\_MaliciousEncryption
- MSRPC\_SuspiciousEncryption

- HTML\_UTF8\_Overf
- HTTP\_IE\_ActiveX\_ControlMemoryCorruption
- HTTP\_Media\_Player\_PNG\_Chunksize\_BO
- MSRPC\_RRaS\_BO
- Image\_WMF\_Polygon\_Overf
- Microsoft\_ICMP\_SourceRoute\_BO

#### New Vulnerability Detection Algorithms:

- SymantecAntivirusClientBo
- WinMs06kb917344Update
- MdropperHTrojan
- FreesshdKeyExchangeBo
- WinMs06kb917734Update
- WinMs06kb916281Update
- WinMs06kb911280Update
- WinMs06kb916768Update
- WinMs06kb918439Update
- WinMs06kb917336Update
- WinMs06kb917953Update
- WinMs06kb914389Update
- WinMs06kb912442Update
- WinMs06kb917736Update
- MsdtcMessageDos

#### New Default Blocking Algorithms:

X-Force added the following default blocking to our products:

- Symantec\_Management\_Overflow
- HTTP\_Snort\_Uricontent\_Bypass
- TCP\_Data\_Changed
- HTTP\_MaxDB\_Percent\_BO
- HTTP\_MaxDB\_LockToken\_BO
- HTTP\_Novell\_iMonitor\_BO
- HTTP\_OpenView\_NNM\_CmdExec
- HTML\_Object\_Styles\_Overflow
- HTML\_UTF8\_Overflow
- HTTP\_IE\_ActiveX\_ControlMemoryCorrupt
- HTTP\_Media\_Player\_PNG\_Chunksize\_BO
- Image\_WMF\_Polygon\_Overflow

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, the Proventia logo, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.