SOPHOS

Protection for Mac and Linux computers: genuine need or nice to have?

The current risk to computers running non-Windows platforms is small but growing. As Mac and Linux computers become more prevalent within organizations, they are likely to become more of a target for hackers as a way in to the rest of the network and a means of infecting websites. This paper investigates the real threat from non-Windows platforms. It discusses the dangers of them distributing Windows viruses, examines the implications of their growing popularity, and highlights regulatory pressure to protect them.

A Sophos white paper

October 2008

Protection for Mac and Linux computers: genuine need or nice to have?

The current threat

The sheer number of desktops, laptops, and servers running Windows makes them an easy and readily available target for malware writers and spammers. Assessment of an organization's requirements for protection against viruses, spyware, Trojans, and worms has therefore tended to concentrate on the Windows environment. Meanwhile, the network security risk arising from unprotected non-Windows computers has sometimes been downplayed or overlooked altogether.

The need to protect the gateway from malicious code – whatever the operating system – is pretty well accepted. However, acceptance is not clear-cut over endpoint protection, as most malware continues to target Windows platforms, with only a tiny proportion being created specifically for Mac and Linux platforms.

The fact that most malware continues to be written for Windows computers encourages the argument that investment in protection for non-Windows computers at the endpoint is unnecessary. So why, then, is it important for organizations to protect non-Windows computers?

The fact that most malware continues to be written for Windows computers encourages the argument that investment in protection for non-Windows computers at the endpoint is unnecessary.

Essentially there are four reasons:

- Although there are comparatively few non-Windows viruses, the ones that do exist represent real threats.
- Linux servers are a target for hackers who use them as a means of connection to attached Windows computers.
- Non-Windows computers can and do harbor and deploy the much more widespread Windows malware.
- Government and industry regulations increasingly oblige organizations to put anti-malware protection on all computers, whether or not that organization agrees there is a risk.

Non-Windows malware

Vulnerabilities on any platform are liable to exploitation. This is increasingly true as virus writers, spammers, and hackers join forces to steal data and money from unsuspecting businesses through spyware, phishing, and similar attacks. Vendor-issued security patches to eliminate system vulnerabilities are as likely to be published for Mac and UNIX operating systems as they are for Windows. While these might currently be issued less in response to an actual exploitation of vulnerability and more as a proactive measure, the need for patching illustrates the fact that non-Windows operating systems do exhibit vulnerabilities. These can be – and have been – exploited.

So the risk of infection on non-Windows platforms is not to be dismissed out of hand. The relatively low number of viruses, Trojans, worms, and spyware attacks on non-Windows environments does not reflect an inability to create viruses for these operating systems, rather a greater interest in targeting Windows with its vast user base.

However, as the following examples show, there is real interest from some in targeting Mac and Linux platforms:

- **OSX/Leap-A** The first piece of malware for Mac OS X arrived in February 2006 and uses the iChat instant messaging system to spread itself to other users – in a similar way to an email or instant messaging worm on Windows.
- **Linux/Rst-B** This virus was first detected in February 2002, and is the virus that Linux users are most likely to encounter today, as it replicates on up-to-date distributions. It infects hacking tools used to gain access to Linux servers. During a recent three-month period, about 70% of hacking tools downloaded by hackers to one honeypot was found to be infected with Linux/Rst-B.[1]
- **OSX/RSPlug-A** This Trojan, the first piece of financially motivated malware for Mac, changes DNS server settings to gain control of HTTP traffic with the aim of redirecting web traffic to malicious sites. It was first detected in November 2007.
- **OSX/Hovdy-A** Discovered in June 2008, this Trojan can steal passwords, open firewalls to give hackers access, and disable security settings on Mac OS X computers.

The attraction of Linux servers

Hackers target servers as a means to gain control over a network of computers, and it is very common for Windows networks to include a server running UNIX or Linux. Vulnerabilities, such as a weak SSH password, can allow hackers to convert a Linux server into a botnet controller, and install malware that will compromise desktop Windows computers. These botnets of hijacked, zombie computers are then used to steal information, send spam – indeed, 90% of spam comes from botnets – or to launch Denial of Service attacks.

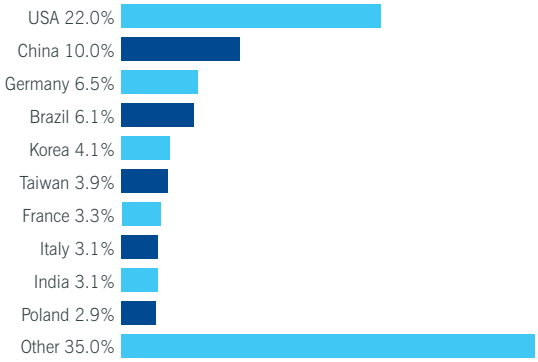

Figure 1: Linux/RST-B infections by country

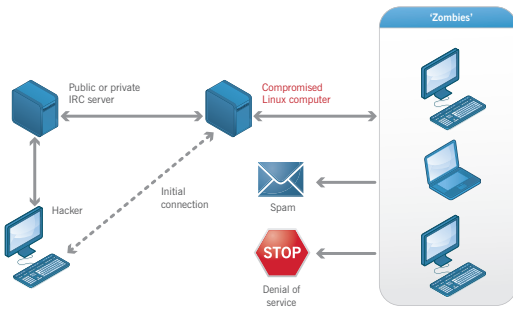

Figure 2: Using a Linux server to create zombies on the network

In addition, a large proportion of Apache web servers are hosted on Linux (or some flavor of UNIX). Increasingly, these servers are being targeted by hackers as a means of placing malicious code on legitimate websites. As shown in Figure 3, almost 60% of infected websites in January to June 2008 were hosted on Apache servers – a significant increase from 49% in 2007.

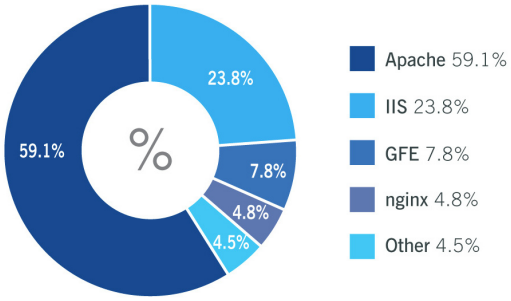

Figure 3: Web server software most commonly used on infected websites, January-June 2008

The hidden threat to Windows computers

It is because most corporate networks – even those which would class themselves as "non-Windows" – include some Windows computers that makes the protection of all computers on the network important. Whatever is on one computer can, by virtue of being connected to another, be transmitted to the other.

Fundamentally, a virus or any other piece of malware is simply a file, just like any other file. It can get onto an organization's desktops and servers in any number of different ways. It can be downloaded from CDs, DVDs, USB drives, email, internet downloads, instant messaging, and so on. The fact that the file can **infect** only those computers running a particular operating system is irrelevant – it can be saved anywhere. Often the user of the computer on which the file is stored is not aware that there is a virus because it is only when it gets to the Windows computer that the virus becomes active.

Even though the design of UNIX and Macs makes them less vulnerable to viruses than earlier versions of Windows, there is still a significant threat to network security because computers harboring the malware can quietly transmit it to Windows computers. For example, UNIX computers can easily transmit the virus to Windows computers via the Samba file-sharing system. In addition, it only takes one network-aware worm to be emailed from a non-Windows to a Windows computer, for the whole Windows network to be infected.

Complacency among UNIX and Mac users can be a danger here – just as it was for "Typhoid Mary", a New York City cook in the early 1900s named Mary Mallon, who was a healthy carrier of typhoid, and refused to believe that she was a danger to her employers, despite infecting many of them with the disease.

Increasing regulatory pressure

Regulatory bodies, uninterested in platform support, approach the issue from a completely different viewpoint and have introduced a raft of legislation. Acts, such as the US's Sarbanes-Oxley (SOX) act and HIPAA (Health Insurance Portability and Accountability Act), and the UK's Data Protection Act, are designed to protect the rights and privacy of individuals – and all place additional requirements on IT administrators to maintain and protect data integrity within their networks.

SOX lays a legal obligation on public traded companies to protect all machines associated with financial records. HIPAA does the same for health data. Many IT managers infer from the acts that all file servers within a network that manage financial or health information – regardless of platform –

therefore require anti-virus protection. The acts stipulate the need for:

- **Information security** Nothing should alter original data, and there must be a clear alert in the event of any attempt to modify or destroy information.
- **Proof of control** There must be proof that compliance efforts are working. Event logs, audit trails, and reporting are critical to meeting these goals.

In addition, recognized industry bodies, such as the Payment Card Industry, also impose requirements for all computers holding personal data to be adequately protected.

> *Government and industry regulations require all computers holding personal data to be adequately protected.*

The recent updated version of the PCI Data Security Standard, version 1.2, expanded the requirement of platform protection by removing the exclusion of UNIX-based operating systems or mainframes. Mac OS X is a UNIX-based system and Linux is UNIX-like, so these operating systems should also be protected by anti-virus software.

In addition, this new version of the Data Security Standard has also expanded its definition of malicious software and now includes the requirement to protect against rootkits – software which enables someone, either legitimately or maliciously, to take control of a Windows or UNIX-based machine undetected.

The future threat

Threats that target the Windows operating environment will remain dominant because it will still be easier to infect huge numbers of Windows computers as there will continue to be huge numbers of Windows computers out there.

However, although Microsoft will continue to dominate the endpoint for many years to come, there are reasons to suggest that non-Windows platforms will become more attractive to virus writers, who will target them more than they have in the past. Improved protection on Windows systems and the changing nature of the threat, with financial gain rather than adolescent bravado the motivating force, makes it likely that less prevalent operating systems will increasingly be exploited.

In addition, it is clear that both Mac and UNIX/Linux are increasing in popularity. Linux servers represented 12.7% of the overall server market ($1.6 billion) in Q1 2007[2]. Mac – already having a high share of the media and education market – saw sales reach an all-time record in Q3 2008[3] when almost 2.5 million computers were shipped, partly due to their increasing prevalence in business environments.

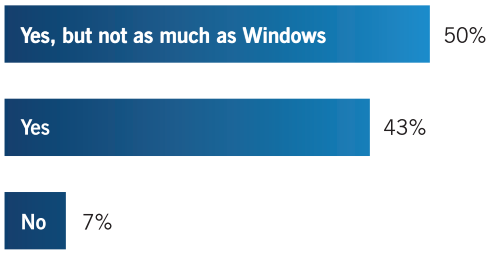

Figure 4: Belief that Macs will be targeted more often in future

It is likely malware authors will want to tap into this growing Mac and Linux user base. Indeed in a Sophos web poll conducted at the beginning of 2008, 93% of respondents (compared to 79% in 2006) said they believed that Macs would be

targeted more in the future.[4] In the same poll, the percentage that thought that Macs would not be targeted as much as Windows computers also dropped from 59% in 2006 to 50%, as shown in Figure 4, on the previous page.

There is also the possible future development of web-based threats to consider. Malware is currently written for specific operating systems with the web being used solely as a delivery mechanism. However, in the future, malware payloads could be delivered entirely within the browser environment, independent of any operating system. In that scenario, Mac, Linux and Windows computers will all be equally at risk of malware infection.

> *Users are always potentially the weak link in the security chain.*

Meeting the security challenge

Users are always potentially the weak link in the security chain, OSX/Leap-A, for example being spread by instant messaging. No matter what the operating system – Mac, Linux, UNIX, NetWare, OpenVMS, Windows – what they have in common is that their users are all just as susceptible to social engineering as each other and can be tricked into downloading malware onto their computers. Meeting the security challenge is a two-pronged solution combining ongoing organization-wide education about best practice and powerful, reliable protection.

By including computers running non-Windows operating systems as part of the general network security, IT departments will ensure that the very real risk of these computers infecting Windows computers is addressed. They will also ensure that the risk of the non-Windows computers themselves being infected is eliminated.

At the same time, running a robust anti-virus solution on all endpoint desktops, laptops, and servers will ensure that organizations comply with increasingly stringent legislative requirements for data protection and alerts about data modification. Through event logs and reporting, they will also satisfy the requirement for proof of control and remove the risk of the ramifications of failing to meet compliance protocols.

Summary

Leaving non-Windows computers unprotected against malware introduces another field of vulnerability in a landscape already abundant with threats. Although the current risk of infection on computers running non-Windows operating systems is small, particularly outside the Mac strongholds of education and media, it is real and will increase as part of the trend towards stealthily targeted attacks by financially motivated virus writers, spammers, and hackers. By protecting computers running Linux, UNIX, Mac and the like, organizations will not just block non-Windows malware and satisfy increasing legal demands for data protection. More importantly, they will prevent Windows malware being stored and distributed across their IT network, significantly reducing the risks to business continuity and integrity.

The Sophos solution

Sophos Endpoint Security and Control protects against viruses, spyware, adware and hackers, and controls removable storage devices and unauthorized software usage, providing cross-platform security and control for desktops, laptops, file servers and mobile devices – including Windows, Mac and Linux. To find out more about Sophos products and evaluation, visit www.sophos.com

SophosLabs encourages Linux users to use its free detection tool to search for Linux/Rst-B infections. Find out more about this free tool at www.sophos.com/rst-detection-tool

Sources

1 The case for AV for Linux: Linux/RST-B, Virus Bulletin, August 2008

2 Linux server market share keeps growing
www.linux-watch.com/news/NS5369154346.html

3 Apple reports record third quarter results
www.apple.com/pr/library/2008/07/21results.html

4 Sophos web poll, January 29 - February 7 2008
www.sophos.com/pressoffice/news/articles/2008/02/mac-poll.html

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM