

# Virus protection isn't just a Windows issue

A Sophos white paper

February 2006

There is a common and flawed belief that computers running on non-Windows platforms do not need anti-virus protection. With Macintosh® and UNIX/Linux viruses representing less than 0.2% of the total malware detected by Sophos, this paper looks at the argument for protecting non-Windows computers. It investigates the real threats on these platforms, discusses the dangers of them concealing and distributing Windows viruses, and examines the implications of the growing popularity of non-Windows platforms. The effect of compliance legislation on protection requirements is also highlighted.

---

## The current threat

The sheer numbers of endpoint 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, at face value, the figures for the amount of malware affecting non-Windows and Windows computers encourage the argument that investment in protection for non-Windows computers at the endpoint is unnecessary.

Even high-profile operating systems like Linux and Mac have a tiny number of viruses written for them. SophosLabs™ – a global network of threat analysis centers – currently identifies over 120,000 viruses; of these only about 50 viruses specifically target Macs and just over 100 target UNIX. In addition, macro viruses that target MS Office applications are often written in

such a way that they will activate on Windows but will fail to work properly as soon as they attempt to run on Macs.

So why, then, is it important for organizations to protect non-Windows computers? Essentially there are three reasons:

- 1 Although there are comparatively few non-Windows viruses, the ones that do exist represent real threats.
- 2 Far more significantly, however, non-Windows computers can and do harbor and deploy the much more widespread Windows malware.
- 3 There are regulations that 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 general lack of interest from virus writers. But as the following examples show, there is real interest from some in the hacking community:

---

### **Percentage of total threat**

*Mac malware 0.04%*

*UNIX malware 0.09%*

*Source: SophosLabs*

---

- **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.
- **OSX/Inqtana-A** Arriving less than a week after Leap-A, this worm exploits a Bluetooth vulnerability to spread itself to other unpatched vulnerable Mac OS X computers.
- **Troj/Lindoor-B** Appearing in October 2005, this backdoor Trojan for the Linux operating system allows a malicious user remote shell access to the compromised system and listens for incoming connections.
- **Linux/Mare-A** This worm arrived in December 2005 and spreads via an exploitable PHP script.

## The hidden threat to Windows computers

It is very common to find a UNIX server connected to a large network of Windows computers. Furthermore, most corporate networks – even those which would class themselves as “non-Windows” – include some Windows computers. It is the fact of this connection, whether real or virtual, 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, such as W32/Nyxem-D, to be emailed from a non-Windows to a Windows computer, for the whole Windows network to be infected.

## 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 UK’s Data Protection Act and the US’s Sarbanes-Oxley (SOX) act and HIPAA (Health Insurance Portability and Accountability 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.

## 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. Apple boosted growth in total Macintosh shipments by 48% in Q3 2005<sup>1</sup>, while industry analyst, Gartner, predicts that Linux will have the strongest relative growth of any server operating system during the next five years<sup>2</sup>.

A Sophos web poll conducted in the wake of the discovery of OSX/Leap-A revealed that 79% believe Macs will be targeted more in the future<sup>3</sup>. However, over half said they did not believe the problem would be as great as for Windows, as shown in Figure 1.

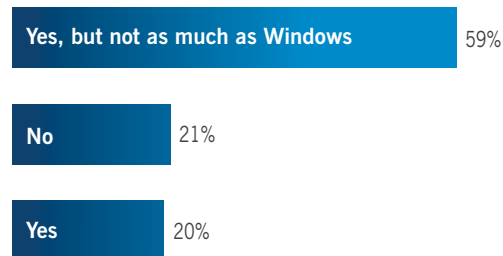


Figure 1: Belief that Macs will be targeted more often in future

## Meeting the security challenge

Just as there has been a belief that non-Windows computers do not constitute a real threat, so popular opinion has tended to be that users of UNIX computers are generally more technically savvy and are better informed about computing best practices than users of other platforms. Even if this were true – and some would argue otherwise – it is less likely to be so as the platform gains in popularity.

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.

---

*“It is true that Mac OS X and Linux are less vulnerable to viruses than DOS is – but so is Windows XP. What they all have in common is that their users can be tricked into downloading viruses and other malware.”*

*Richard Jacobs, Chief Technology Officer,  
Sophos*

---

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.

## About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

---

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2006. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

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, 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.

*Sophos endpoint protection against malware supports more than 25 platforms. To find out how Sophos can protect your business, visit [www.sophos.com](http://www.sophos.com).*

## Sources

- 1 IDC: PC Market Growth Tops 17% As Low-Cost and Portable PCs Continue To Fuel Domestic And International Markets. (<http://www.idc.com/getdoc.jsp?containerId=prUS00259505>), October 2005
- 2 Gartner Group: Linux Making Strong Inroads in Server Market, Jeffrey Hewitt, April 2005
- 3 Sophos web poll, 617 respondents. 16-17 February 2006

**SOPHOS**  
WWW.SOPHOS.COM