

GFI White Paper

Hackers don't discriminate: Viruses attack all platform users

Historically, few viruses have been written to attack Mac-based operating systems. But as the popularity of these devices has increased, so has the popularity of Mac-targeted malware. Regardless of whether your organization uses Windows-based PCs or Macs or a mix of both, you need a solution that provides protection for all operating systems.

Contents

Introduction.....	3
Why Apple is a target.....	3
Mac-based attacks on the rise.....	3
How to protect all operating systems.....	3
Conclusion.....	4
About GFI VIPRE® Antivirus Business.....	4
About GFI.....	4

This white paper explains why Apple has become a popular target for malware writers, outlines recent Mac malware attacks and offers specific strategies to secure both PCs and Macs.

Why Apple is a target

The successful launches of the iPod, iPhone and iPad have catapulted Apple to the forefront of the technology industry. Consumers are now using these Mac OS-based devices to conduct work, and businesses are increasingly allowing their use on corporate networks, if not outright adopting them for company use.

With this rise in popularity, hackers and cybercriminals have now turned their attention to this traditionally ignored audience. However, PC users are far from in the clear. IT security researchers, say hundreds, if not thousands, of new malware codes are discovered every month. New threats are targeting Macs as well as PCs, so it's important to protect your organization's devices and network against both.

Mac-based attacks on the rise

Many Mac users think their machines are impervious to malware, according to Alex Stamos, a security analyst with iSEC Partners. At the 2011 Black Hat conference, he reported that while most users think PCs are susceptible to virus attacks, only 20 percent believe Macs are vulnerable. This perception is a dangerous one, as Mac users may be less suspicious or prepared for malware on their browsers or in their inboxes.

Cybercriminals are clever in their use of social engineering techniques to lure users into unwittingly downloading viruses or other malware. For example, the recent Mac Defender Trojan – also known as the Mac Security Trojan, Mac Protector Trojan, Mac Guard Trojan and Mac Shield Trojan e has caught many Mac users, and even IT professionals, by surprise. This Trojan creates an authentic-looking popup in Mac browsers, warning users that a virus has been detected and suggesting an antivirus program be downloaded. If the user complies, he or she is prompted to pay a license fee for the “protective” software and his or her credit card and personal information are collected.

Other malware, originally written for PC operating systems, has now been retargeted towards Macs. Take the social networking worm Koobface. First detected in 2008, it posts messages with malicious links on Facebook, Myspace and Twitter users' feeds. These links prompt followers to download fake updates and programs, such as an Adobe Flash update, that launch the Koobface worm on the downloaders' machines. A new version of Koobface that targets Mac OS X users, sometimes referred to as Boonana, was detected two years later, in November 2010.

How to protect all operating systems

For both Windows- and Mac-based operating systems, there are certain security measures you must take to protect your employees and your corporate data. First, it's critical to raise employee awareness of the general dangers of malware, as well as the latest known threats. Prepare employees for the types of malware they may come across by showing them examples. You might hold a seminar and share screenshots of the Mac Defender Trojan or the Koobface worm or create a monthly newsletter that outlines new threats and how to protect against them. By demonstrating just how real and convincing these attacks can be, you'll show employees how easy it is to fall victim to them.

While employee education is a powerful approach, antivirus protection is also essential to your business security. Not all business AV solutions are equal, and the one you choose should include:

- » **Powerful scanning technology.** High-quality AV solutions will analyze and detect potential viruses and malware before they infect user machines
- » **Active monitoring and protection.** Most SMBs don't have the time or resources to constantly monitor their networks for security threats. Invest in a solution that protects your network and user machines in real time, automatically.
- » **Malicious web filtering.** Block bad URLs before they hit your network with a solution that uses the latest behavioral analysis and malware URL detection technology.

Conclusion

Today's corporate IT environments are often a mixed bag, supporting not only a variety of devices – smartphones, tablets, laptops and desktops – but also a combination of Windows and Mac operating systems.

Companies must take a practical approach in protecting against malware threats that attack both PCs and Macs. By combining employee education with powerful AV security technology, your organization can mitigate the risks of threats targeting all types of devices and platforms.

About GFI VIPRE® Antivirus Business

VIPRE Antivirus Business combines the latest antivirus and anti-spyware detection and removal technologies to protect against next-generation malware threats in a comprehensive and highly efficient manner. Built by IT administrators for IT administrators, VIPRE is easy to install, easy to deploy and easy to manage with minimal network and system performance impact. The solution delivers superior endpoint protection against viruses, worms, spyware, Trojans, bots and rootkits via a single, powerful anti-malware engine and wide range of detection methods, including Cobra™ heuristics for first-level heuristic analysis and Active Protection™ for real-time malware detection inside the Windows kernel.

For more information, visit <http://www.gfi.com/business-antivirus-software>.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

33 North Garden Ave, Suite 1200, Clearwater, FL USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

ussales@gfi.com

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit <http://www.gfi.com/contactus>



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.