



GFI White Paper

Cybercriminals and security attacks: What your business must know

Malware attacks have become increasingly prevalent with more than one million unique malware samples uncovered each month.¹ And with threats on the rise, businesses are starting to question the capabilities of their security infrastructure.

Contents

Introduction.....	3
What the headlines don't tell you.....	3
The malware (r)evolution.....	3
Spear phishing scams.....	3
Poisoned searches.....	3
Keylogging.....	3
Flash drives and USB sticks.....	4
Protect your business with layered security.....	4
About GFI VIPRE® Antivirus Business.....	4
About GFI.....	4

This white paper explores today's top security risks for small and medium-sized businesses (SMBs) and the tools necessary to protect against next-generation malware and cybercrime.

What the headlines don't tell you

Citigroup Inc., Sony Corp., Nintendo, PBS and CIA hacks have all made front-page news recently. Despite widespread coverage of these security breaches, many cybercrimes go unreported in an effort to maintain customer confidence and, in the case of publicly traded companies, protect shareholder value.

Although most headline-making hacks involve large corporations, cybercrime is a very real and steadily growing threat to SMBs. Cybercriminals target SMBs for several reasons, including monetary gain, to access sensitive data or files, to exploit security weaknesses or just for fun.

Cyber attacks are more sophisticated and more targeted than ever. So are the hackers and malware writers getting smarter? Or are anti-malware and endpoint security solutions falling short? It's a little bit of both.

The malware (r)evolution

Traditional viruses represent only a fraction of the current threat landscape. Today, the top security risks for SMBs are:

Spear phishing scams

Targeted email attacks where cybercriminals send fake emails that appear surprisingly authentic. These emails often mimic the look and/or style of communications sent by banks or credit card companies and "phish" for personal information. Oftentimes, spear phishing emails link to malicious websites, where login credentials are stolen, or include malicious attachments, that install malware on end-user machines.

Between July and December 2010, the Anti-Phishing Working Group (APWG) identified 67,677 phishing attacks. Based on this, the analysis of cybercriminal activities – including the development of unique malicious websites – and the financial benefits afforded spear phishing scams, the APWG reports these types of threats will continue to grow exponentially.

As the number of malicious email scams increase, network security measures must also. Traditional AV spam and virus filters are often ineffective in catching spear phishing attempts. With today's threat landscape, it's imperative to choose an antivirus solution that accurately identifies and strips malicious attachments from emails, blocks dangerous URLs and protects users from visiting phishing sites. Employee education is also critical.

Poisoned searches

An estimated 300+ million people conduct Google searches each day. So it's no surprise that malware writers have begun to capitalize on search engine results, using current, popular searches to propagate malware.

These poisoned searches push bogus URLs to the top of SEO rankings, sending users to sites that host malicious code. SEO poisoning is a popular attack vector that capitalizes on high-searched phrases, such as "free porn," and high-profile events, such as the "Royal Wedding." According to the 2010 Websense Threat Report, 22.4 percent of the top 100 Google searches resulted in poisoned URLs, up from 13.7 percent in Q2 of 2009.²

Since poisoned searches have the potential to infect machines or even take down a network, user education is key. Reminding employees to only rely on trusted news sources, type URLs directly into web browsers and to be leery of download prompts may save future headaches.

Keylogging

Commercial keylogging programs serve valid purposes, such as tracking kids' computer-related activities or assessing employees' site visits and online traffic. However, malicious keyloggers do not – operating in stealth mode to grab screenshots, log user activities and gain passwords, financial data and other personal information from machines.

¹ AV-TEST Institute, www.av-test.org/en/statistics/malware

² Websense 2010 Threat Report, www.websense.com/content/threat-report-2010-introduction.aspx

The legality of keylogging and other PC monitoring tools is a hotly debated topic. Regardless, IT administrators must be aware of the existence of keyloggers and monitoring apps on their network, authorized or not. If an employee installs these tools without IT's knowledge, they are exposing the organization to unnecessary risk.

Flash drives and USB sticks

Flash drives and USB sticks allow employees to transfer documents, data and files to work from home or another offsite location. And while doing so may increase employee productivity, it also puts network security at risk. In a July 2011 report from the Ponemon Institute³ 70 percent of companies traced the loss of confidential data to USB sticks. Of that, 55 percent were related to malware attacks. The 2010 Stuxnet worm outbreak is another example of the dangers of USB sticks. This spyware worm spread undetected via infected memory sticks to thousands of machines in the U.S., India, Indonesia and other countries.

So how can the convenience of working remotely be achieved while still keeping the network secure? The answer is simple: choose an antivirus solution that scans self-running media, such as USB drives, for malware when a removable device is inserted.

Protect your business with layered security

Whether your organization has 10 employees, 500 or 50,000, security threats don't discriminate. To ensure that the latest malware doesn't wreak havoc on your business, drain user productivity, or take a major hit on IT resources, you must be prepared with the best security solutions available.

When it comes to AV software, you need a reliable product that automatically scans for the latest viruses and malware. IT should be able to easily monitor the solution, without worries of false positives or strains on network performance. The right AV product will offer protection against zero-day threats, and will scan emails and URLs for malicious code and attachments. New malware is developed rapidly, and your antivirus solution should update frequently and protect against all threats – from the infection vector to the payload execution.

Unfortunately, even the best AV solution cannot always overcome human behavior. Cybercriminals, realizing this, use social engineering techniques to prey on the good, trusting nature of individuals, getting them to click on poisonous URLs and unwittingly open dangerous attachments. Because of this, every business must educate its employees on today's security threats.

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.

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>.

³ "Second Annual Cost of Cyber Crime Study," July 2011, Ponemon Institute

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.