

*GFI White Paper*

# *Protecting your network against email threats*

The need for comprehensive server-based email security

This white paper explains why antivirus software alone is not enough to protect your organization against the current and future onslaught of email viruses and threats. Examining the different kinds of email attacks and issues that threaten today's organizations, this paper describes the need for a solid server-based email security solution to safeguard your network.

## Contents

Introduction.....	3
The threat of email viruses and trojans.....	3
The threat of information leaks.....	3
The threat of emails containing malicious or offensive content.....	3
Methods used to attack your email system.....	3
The shocking ease of creating a virus today.....	4
Why antivirus software or a firewall is not enough.....	4
The solution: A proactive approach.....	5
About GFI MailSecurity for Exchange/SMTP.....	5
About GFI® .....	5

## *Introduction*

This white paper explains why antivirus software alone is not enough to protect your organization against the current and future onslaught of computer viruses. Examining the different kinds of email threats and email attack methods, this paper describes the need for a solid server-based content-checking gateway to safeguard your business against email viruses and attacks as well as information leaks.

## *The threat of email viruses and trojans*

The widespread use of email has provided hackers and crackers with an easy way to distribute harmful content to the internal network. Hackers can easily circumvent the protection offered by a firewall by tunneling through the email protocol, since it does not analyze email content.

CNN reported in January 2004 that the MyDoom virus cost companies about US\$250 million in lost productivity and tech support expenses, while NetworkWorld (September 2003) cited studies that placed the cost of fighting Blaster, SoBig.F, Wechia and other email viruses at US\$3.5 billion for US companies alone.

Furthermore, email is also used to install trojans, targeted specifically at your organization to obtain confidential information or gain control of your servers. Described as “instructive viruses” or “spy viruses” by computer security experts, these can be potent tools in industrial espionage. A case in point is the email attack on Microsoft’s network in October 2000, which a Microsoft Corp. spokesman described as “an act of industrial espionage pure and simple”. According to reports, Microsoft’s network was hacked by means of a backdoor trojan virus maliciously emailed to a network user.

## *The threat of information leaks*

Organizations often fail to acknowledge that there is a great risk of crucial data being stolen from within the company. Various studies have shown how employees use email to send out confidential corporate information. Be it because they are disgruntled and revengeful, or because they fail to realize the potentially harmful impact of such a practice, employees use email to share sensitive data that was officially intended to remain in-house.

As the 2003 Hutton enquiry in the UK demonstrated, government officials and BBC executives were found to have used email to make disclosures that were confidential. A March 1999 PC Week article referred to a study where, out of the 800 workers surveyed, 21-31% admitted to emailing confidential information - like financial or product data – to recipients outside the company.

## *The threat of emails containing malicious or offensive content*

Emails sent by staff containing racist, sexist or other offensive material can make your company vulnerable from a legal point of view. In September 2003, UK firm Holden Meehan Independent Financial Advisors had to pay a former employee £10,000 for failing to guard her from email harassment. Chevron notoriously had to pay \$2.2 million to four employees after they had allegedly received sexually harassing email. Under British law, employers are held responsible for emails written by employees in the course of their employment, whether or not the employer consented to the mail. The insurance company Norwich Union was asked to pay \$450,000 in an out-of-court settlement as a result of emailed comments relating to competition.

## *Methods used to attack your email system*

To get to grips with the kind of email threats present today, it is best to take a quick look at the current main methods of email attack. These include:

### **Attachments with malicious content**

Melissa and LoveLetter were among the first viruses to illustrate the problem with email attachments and trust. They made use of the trust that exists between friends or colleagues. Imagine receiving an attachment from a friend who asks you to open it. This is what happened with Melissa, AnnaKournikova, SirCam and other similar email worms. Upon running, such worms usually proceed to send themselves out to email addresses

from the victim's address book, previous emails, webpage caches to the local machine and similar methods. Virus writers place much emphasis on getting the victim to run the attachment. Therefore they make use of different attractive attachment names, such as SexPic.cmd and me.pif.

Many users try to avoid infection from email viruses by only double-clicking on files with certain extensions, such as JPG and MPG. However, some viruses, such as the AnnaKournikova worm, make use of multiple extensions to try trick the user into running the file. The AnnaKournikova virus was transmitted via an email attachment named 'AnnaKournikova.jpg.vbs' which dupes recipients into believing that they are receiving a harmless JPG image of the famous tennis star, rather than a Visual Basic Script containing infectious code.

In addition, the Class ID (CLSID) extension allows hackers to hide the actual extension of the file, thereby concealing the fact that cleanfile.jpg is actually a nasty HTA (HTML application) file.

This method currently also circumvents various email content filtering solutions which make use of simple file checking methods, thus enabling the hacker to reach the target user with greater ease.

### **Emails triggering known exploits**

The Nimda worm took the Internet by surprise, circumventing many email security tools and breaking into servers and corporate networks as well as infecting the home user. The trick in Nimda is that it runs automatically on computers having a vulnerable version of Internet Explorer or Outlook Express. Nimda was one of the first in a line of viruses that exploit one flaw or another in order to disseminate. Variants of the Bagle virus that emerged in March 2004, for instance, exploited an old Outlook flaw in a bid to spread without any user intervention.

### **HTML mail with embedded scripts**

Nowadays, all email clients can send and receive HTML mail. HTML mail can include scripts and Active Content, which can allow programs or code to be executed on the client machine. Outlook and other products use Internet Explorer components to display HTML email, meaning they inherit the security vulnerabilities found in Internet Explorer.

Viruses based on HTML scripts have the added danger of being able to run automatically when the malicious mail is opened. They do not rely on attachments; therefore the attachment filters found in antivirus software are useless in combating unknown HTML script viruses.

The BadTrans.B virus, for example, combines an email exploit with HTML to propagate, using HTML to launch an attachment automatically once the email is received.

### ***The shocking ease of creating a virus today***

Anyone with a little knowledge of Visual Basic can unleash chaos by exploiting well-known vulnerabilities in various commonly used email clients and products. A visit to the SecurityFocus site, for instance, will reveal various exploits that are available for Microsoft Outlook. A malicious script kiddie with the intent of producing a virus can just modify the exploit code - which is publicly available! - to execute his/her code.

For example, an exploit for Internet Explorer and MS Access, which could be easily applied to Outlook and Outlook Express, is described on Guninski.com. A virus writer could easily exploit this to run Visual Basic code as soon as the victim opens the infected email. This would infect all HTML files and send itself to all the contacts on the recipient's email address book. A key feature of this virus, however, is that it would execute simply when the user opens the email containing malicious HTML.

### ***Why antivirus software or a firewall is not enough***

Some organizations lull themselves into a false sense of security upon installing a firewall. This is a wise step to protect their intranet, but it is not enough: firewalls can prevent access to your network by unauthorized users. But they do not check the content of mail being sent and received by those authorized to use the system, for instance. This means that email viruses can still pass through this level of security.

Nor does virus-scanning software protect against ALL email viruses and attacks: antivirus vendors cannot

always update their signatures in time against the deadly viruses that are distributed worldwide via email in a matter of hours (such as the recent MyDoom, NetSky.B and Beagle worms). Companies using a single virus-scanning engine alone are not necessarily safeguarded when a new virus is released. A 2004 study by the UK government found, for example, that although 99% of large British companies use antivirus products, 68% of them were infected by viruses during 2003. Similarly, a 2003 study carried out at Hewlett-Packard's research labs in Bristol, found the signature update approach to virus detection and elimination to be fundamentally flawed, simply because worms can spread faster than antivirus signature updates can be distributed.

### *The solution: A proactive approach*

So how does one protect against these email threats? A proactive approach is needed which involves the content checking of all inbound and outbound email at server level, before distribution to your users. This way, all potentially harmful content is removed from an infected or dubious email, and only then is it forwarded to the user.

By installing a comprehensive email content checking and antivirus gateway on their mail server, companies can protect themselves against the potential damage and lost work time that current and future viruses may cause.

### *About GFI MailSecurity for Exchange/SMTP*

GFI MailSecurity for Exchange/SMTP is an email content checking, exploit detection, threats analysis and antivirus solution that removes all types of email-borne threats before they can affect your email users. GFI MailSecurity's key features include multiple virus engines, to guarantee higher detection rate and faster response to new viruses; email content and attachment checking, to quarantine dangerous attachments and content; an exploit shield, to protect against present and future viruses based on exploits; an HTML Sanitizer, to disable HTML scripts; a Trojan & Executable Scanner, to detect malicious executables; and more. To read more and download a trial version, visit <http://www.gfi.com/mailsecurity>.

### *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 enterprises (SMEs) 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 SMEs, 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**

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

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

[ussales@gfi.com](mailto: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](mailto: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](mailto: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](mailto:sales@gfiap.com)



### 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.