

*GFI White Paper*

# *Why you need an email exploit detection engine*

The danger of email exploits

This white paper explains what email exploits are, provides examples of common email exploits, and discusses why a non signature-based approach (i.e., not a virus engine) is needed to protect against email exploits.

## Contents

Introduction.....	3
What is an exploit?.....	3
Difference between antivirus software and email exploit detection software..	3
Exploit engine requires less updates.....	3
The Lessons of Nimda, BadTrans.B, Yaha and Bugbear.....	3
Other examples of exploits.....	4
The GFI MailSecurity exploit engine.....	4
About GFI®.....	5

## *Introduction*

Virus-writers are using increasingly complex and sophisticated techniques in their bid to circumvent antivirus software and disseminate their viruses. A case in point was the notorious Nimda virus that used multiple methods to spread itself and was based on an exploit rather than on the virus/trojan behavior for which antivirus products typically search. Antivirus software, though essential, cannot combat such threats alone; an email exploit detection tool is also necessary.

## *What is an exploit?*

An exploit uses known vulnerabilities in applications or operating systems to execute a program or code. It 'exploits' a feature of a program or the operating system for its own use, such as executing arbitrary machine code, read/write files on the hard disk, or gain illicit access.

## *What is an email exploit?*

An email exploit is an exploit launched via email. An email exploit is essentially an exploit that can be embedded in an email, and executed on the recipient's machine once the user either opens or receives the email. This allows the hacker to bypass most firewalls and antivirus products.

## *Difference between antivirus software and email exploit detection software*

Antivirus software is designed to detect known malicious codes. An email exploit engine takes a different approach: it analyses the code for exploits that could be malicious. This means it can protect against new viruses, but most importantly against unknown viruses/malicious code. This is crucial as an unknown virus could be a one-off piece of code, developed specifically to break into your network.

Email exploit detection software analyzes emails for exploits – i.e., it scans for methods used to exploit the OS, email client or Internet Explorer – that can permit execution of code or a program on the user's system. It does not check whether the program is malicious or not. It simply assumes there is a security risk if an email is using an exploit in order to run a program or piece of code.

In this manner, an email exploit engine works like an intrusion detection system (IDS) for email. The email exploit engine might cause more false positives, but it adds a new layer of security that is not available in a normal antivirus package, simply because it uses a totally different way of securing email.

Antivirus engines do protect against some exploits but they do not check for all exploits or attacks. An exploit detection engine checks for all known exploits. Because the email exploit engine is optimized for finding exploits in email, it can therefore be more effective at this job than a general purpose antivirus engine.

## *Exploit engine requires less updates*

An exploit engine needs to be updated less frequently than an antivirus engine because it looks for a method rather than a specific virus. Although keeping exploit and antivirus engines up-to-date involve very similar operations, the results are different. Once an exploit is identified and incorporated in an exploit engine, that engine can protect against any new virus that is based on a known exploit. That means the exploit engine will catch the virus even before the antivirus vendor is aware of its emergence, and certainly before the antivirus definition files have been updated to counter the attack. This is a critical advantage, as shown by the following examples that occurred in 2001.

## *The Lessons of Nimda, BadTrans.B, Yaha and Bugbear*

Nimda and BadTrans.B are two viruses that became highly known worldwide in 2001 because they infected a colossal number of Windows computers with Internet access. Nimda alone is estimated to have affected about 8.3 million computer networks around the world, according to US research firm Computer Economics (November 2001).

Nimda is a worm that uses multiple methods to automatically infect other computers. It can replicate through email using an exploit that was made public months before Nimda hit, the MIME Header exploit. BadTrans.B is a mass-mailing worm that distributes itself using the MIME Header exploit. BadTrans.B first appeared after the Nimda outbreak.

With their highly rapid infection rate, both Nimda and BadTrans.B took antivirus vendors by surprise. Though the vendors tried to issue definition file updates as soon as they learned about each virus, the virus had already succeeded in infecting a large number of PCs by the time the antivirus updates were released.

Though both viruses used the same exploit, antivirus vendors had to issue a separate definition file update for each. In contrast, an email exploit detection engine would have recognized the exploit used and identified the attempt to automatically launch an executable file using the MIME header exploit. As a result, it would have blocked both worms automatically, preventing infection.

## Other examples of exploits

### Double extension vulnerability

Viruses: Klez, Netsky and Lovegate.

What it does: Malicious files are given a double extension such as filename.txt.exe to trick the user into running the executable.

### URL spoofing exploit

Viruses: No virus/worm has been found to be using this method. However it has been used to inject backdoors on Windows computers.

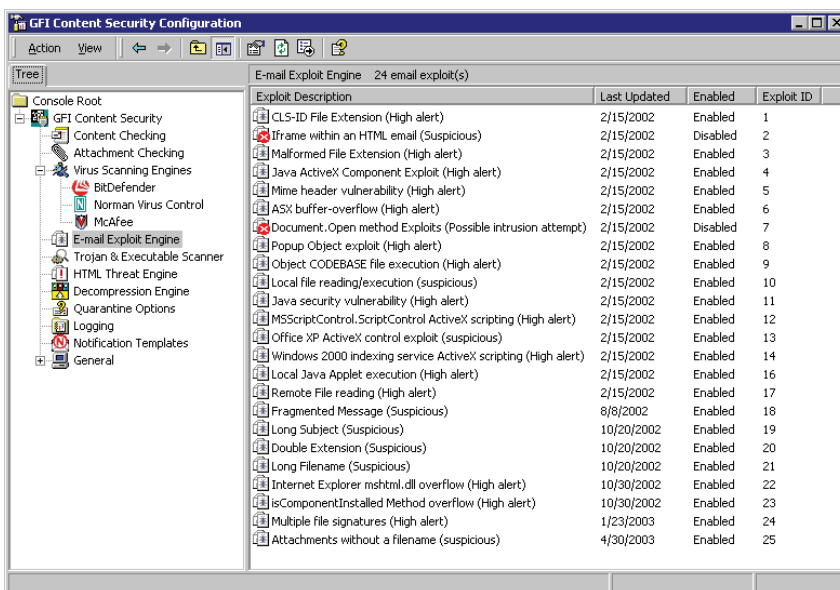
What it does: Allows spammers and phishers (scammers, or people trying to defraud computer users) to fool users to visit a malicious website instead of a legitimate one.

### Object data file execution

Viruses: Bagle.Q.

What it does: Allows attackers to automatically infect unpatched versions of Internet Explorer/Outlook (Express) by downloading and executing code from an HTTP site.

## The GFI MailSecurity exploit engine



The exploit engine configuration in GFI MailSecurity

**GFI MailSecurity™ for Exchange/SMTP** includes an email exploit detection engine as one of several key components designed to provide comprehensive protection against email threats. Drawing on GFI's research on email exploits, this engine detects signatures of currently known email exploits and blocks any messages containing those signatures. GFI MailSecurity contains checks for all important email exploits and can also automatically download new exploit checks as they become available.

Other GFI MailSecurity 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 HTML threats engine, to disable HTML scripts; a Trojan & Executable Scanner, to detect malicious executables; and more. For further information and to download a full trial, please visit <http://www.gfi.com/mailsecurity>.

## **About GFI**

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SME) 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.