
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.

Introduction

Virus-writers are using increasingly complex and sophisticated techniques in their bid to circumvent anti-virus 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 that anti-virus products typically search for. Anti-virus software, though essential, cannot combat such threats alone; an email exploit detection tool is also necessary.

Introduction.....	2
What is an exploit?	2
Difference between anti-virus software and email exploit detection software.....	2
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

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 anti-virus products.

Difference between anti-virus software and email exploit detection software

Anti-virus software is designed to detect KNOWN malicious code. 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 anti-virus package, simply because it uses a totally different way of securing email.

Anti-virus 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 anti-virus engine.

Exploit engine requires less updates

An exploit engine needs to be updated less frequently than an anti-virus engine because it looks for a method rather than a specific virus. Although keeping exploit and anti-virus 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 anti-virus vendor is aware of its emergence, and certainly before the anti-virus 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 anti-virus 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 anti-virus updates were released.

Though both viruses used the same exploit, anti-virus 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.

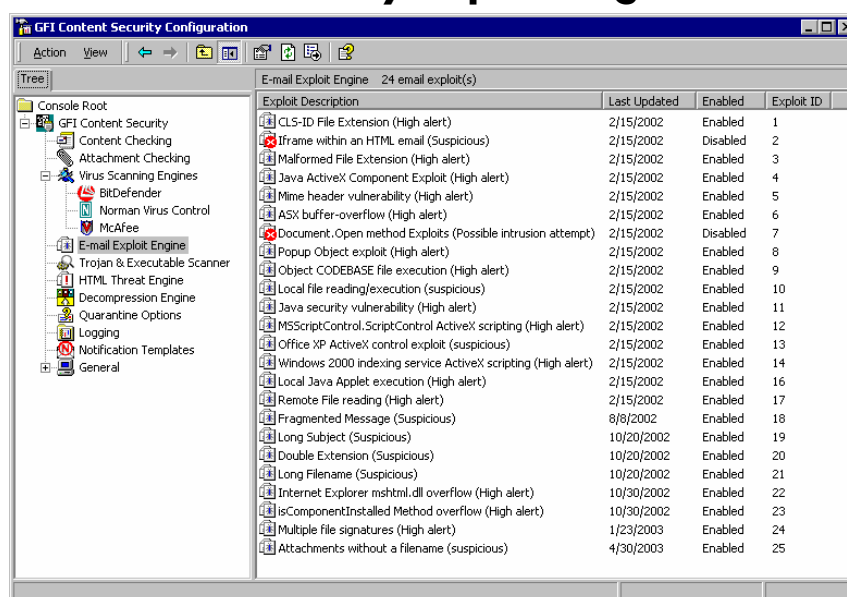
What it does: Allows spammers and phishers (scammers, or people trying to defraud computer users) to fool users to visit a malicious website instead of a legitimate one.

Object data file execution

Viruses: Bagle.Q.

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

The GFI MailSecurity exploit engine



Exploit Description	Last Updated	Enabled	Exploit ID
CLS-ID File Extension (High alert)	2/15/2002	Enabled	1
Iframe within an HTML email (Suspicious)	2/15/2002	Disabled	2
Malformed File Extension (High alert)	2/15/2002	Enabled	3
Java ActiveX Component Exploit (High alert)	2/15/2002	Enabled	4
Mime header vulnerability (High alert)	2/15/2002	Enabled	5
ASX buffer-overflow (High alert)	2/15/2002	Enabled	6
Document.Open method Exploits (Possible intrusion attempt)	2/15/2002	Disabled	7
Popup Object exploit (High alert)	2/15/2002	Enabled	8
Object CODEBASE file execution (High alert)	2/15/2002	Enabled	9
Local file reading/execution (suspicious)	2/15/2002	Enabled	10
Java security vulnerability (High alert)	2/15/2002	Enabled	11
MSScriptControl.ScriptControl ActiveX scripting (High alert)	2/15/2002	Enabled	12
Office XP ActiveX control exploit (suspicious)	2/15/2002	Enabled	13
Windows 2000 indexing service ActiveX scripting (High alert)	2/15/2002	Enabled	14
Local Java Applet execution (High alert)	2/15/2002	Enabled	16
Remote File reading (High alert)	2/15/2002	Enabled	17
Fragmented Message (Suspicious)	8/8/2002	Enabled	18
Long Subject (Suspicious)	10/20/2002	Enabled	19
Double Extension (Suspicious)	10/20/2002	Enabled	20
Long Filename (Suspicious)	10/20/2002	Enabled	21
Internet Explorer mhtml.dll overflow (High alert)	10/30/2002	Enabled	22
IsComponentInstalled Method overflow (High alert)	10/30/2002	Enabled	23
Multiple file signatures (High alert)	1/23/2003	Enabled	24
Attachments without a filename (suspicious)	4/30/2003	Enabled	25

The exploit engine configuration in GFI MailSecurity

The first email security product to protect against email exploits is GFI MailSecurity for

Exchange/SMTP, a package that includes an email exploit detection engine as one of several key components designed to provide comprehensive protection against email threats. Drawing on GFI's leading research on email exploits, this industry-first engine detects signatures of currently known email exploits and blocks any messages containing those signatures. The majority of the hazards identified by GFI MailSecurity's exploit engine are not detected by any other program on the market today. 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 is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 160,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at <http://www.gfi.com>.

© 2007 GFI Software. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

