

---

## Waarom u een email exploit engine nodig heeft

---

### Het gevaar van email exploits

Dit white paper legt uit wat email exploits zijn, geeft voorbeelden van veelvoorkomende email exploits, en bespreekt waarom een benadering die niet gebaseerd is op handtekeningen (i.e. geen virusengine) nodig is voor adequate bescherming tegen email exploits.

---

## Inleiding

Virusschrijvers gebruiken steeds geavanceerdere technieken in hun pogingen om antivirussoftware te omzeilen en virussen te verspreiden. Een berucht voorbeeld is het Nimdavirus dat van verschillende methoden gebruik maakte om zich te verspreiden en gebaseerd was op een exploit in plaats van schadelijke programmeercodes waarnaar antivirusproducten zoeken. Antivirussoftware kan dergelijke dreigingen niet alleen bestrijden; u heeft tevens een tool voor email exploit detectie nodig.

Inleiding .....	2
Wat is een exploit? .....	2
Verschillen tussen antivirussoftware en software voor detectie van email exploits .....	2
Exploit engines hebben minder updates nodig .....	3
Nimda, BadTrans.B, Yaha, Bugbear en hun gevolgen .....	3
Andere voorbeelden van exploits .....	4
De GFI MailSecurity exploit engine .....	5
Over GFI .....	6

---

## Wat is een exploit?

Een exploit gebruikt bekende kwetsbaarheden in applicaties of besturingssystemen om een programma of code uit te voeren. Exploits buiten een bepaald kenmerk van een programma of besturingssysteem uit voor hun eigen doeleinden, zoals het uitvoeren van willekeurige code, het lezen of schrijven van bestanden op de harde schijf of het verkrijgen van ongeautoriseerde toegang.

### Wat is een email exploit?

Een email exploit is een exploit die wordt gelanceerd via e-mail. Het gaat om een exploit die in een e-mail is ingebed en kan worden uitgevoerd op de computer van de ontvanger zodra deze het bericht ontvangt of opent. Zo kan de hacker de meeste firewalls en antivirusproducten omzeilen.

---

## Verschillen tussen antivirussoftware en software voor detectie van email exploits

Antivirussoftware is ontworpen om BEKENDE kwaadaardige codes te detecteren. Email exploit engines gaan anders te werk: ze analyseren de code voor exploits die kwaadaardig ZOUDEN KUNNEN ZIJN. Ze kunnen dus bescherming bieden tegen nieuwe virussen en tevens tegen ONBEKENDE virussen/kwaadaardige code. Dit is cruciaal aangezien een onbekend virus speciaal kan zijn ontwikkeld om op uw netwerk in te breken.

Software voor detectie van email exploits analyseert e-mails op exploits die ervoor kunnen zorgen dat er codes of programma's worden uitgevoerd op het systeem van de gebruiker. Het controleert niet of het programma kwaadaardig is. Het gaat er eenvoudigweg vanuit dat er een veiligheidsrisico bestaat als een e-mail een exploit gebruikt om een programma of code uit te voeren.

Een email exploit engine werkt dus als een inbraakdetectiesysteem (IDS – Intrusion Detection System) voor e-mail. De email exploit engine kan voor meer valse meldingen zorgen maar biedt meer beveiliging dan gewone antiviruspakketten doordat het op een totaal andere manier werkt.

Antivirusengines bieden bescherming tegen sommige exploits maar niet tegen alle. Een engine voor exploitdetectie zoekt naar alle bekende exploits. Doordat de email exploit engine is geoptimaliseerd voor het vinden van exploits in e-mail, is hij effectiever dan gewone antivirusengines.

---

## **Exploit engines hebben minder updates nodig**

Exploit engines hoeven minder vaak bijgewerkt te worden dan antivirusengines omdat ze zoeken naar een methode in plaats van naar een specifiek virus. Hoewel het bijwerken van exploit engines en het bijwerken van antivirusengines op een vergelijkbare manier gebeurt, zijn de resultaten verschillend. Als een exploit eenmaal is geïdentificeerd en opgenomen in de database van een exploit engine, kan deze engine beschermen tegen ieder nieuw virus dat op een bekende exploit is gebaseerd. Dit betekent dat de exploit engine het virus kan onderscheppen voordat de fabrikant van antivirussoftware van het virus op de hoogte is en voordat de definitiebestanden zijn bijgewerkt. Dit is een belangrijk voordeel, wat wel blijkt uit onderstaande voorbeelden uit 2001.

---

## **Nimda, BadTrans.B, Yaha, Bugbear en hun gevolgen**

Nimda en BadTrans.B zijn twee virussen die in 2001 wereldwijd bekend werden doordat ze een gigantisch aantal Windowscomputers met internettoegang infecteerden. Volgens het Amerikaanse onderzoeksbureau Computer Economics heeft Nimda alleen al ongeveer 8,3 miljoen computernetwerken over de hele wereld geïnfecteerd (november 2001).

Nimda is een worm die verschillende methodes gebruikt om automatisch andere computers te infecteren. Nimda kan zich via e-mail verspreiden met behulp van een exploit die maanden voordat Nimda toesloeg openbaar was gemaakt: de MIME Header exploit. BadTrans.B is een mass-mailing worm die zich verspreidt door middel van de MIME Header exploit. BadTrans.B dook voor het eerst op na de uitbraak van Nimda.

Fabrikanten van antivirussoftware waren niet voorbereid op de enorme snelheid waarmee Nimda en BadTrans.B computers infecteerden. Hoewel de fabrikanten hun best deden om voor

elk virus zo snel mogelijk definitie-updates uit te brengen, was een groot aantal PC's al geïnfecteerd voordat de updates verkrijgbaar waren.

Hoewel beide virussen gebruik maakten van dezelfde exploit, moesten fabrikanten van antivirussoftware voor elk virus een aparte definitie-update uitbrengen. Een email exploit detection engine daarentegen zou de gebruikte exploit hebben herkend en zou in de gaten hebben gehad dat er geprobeerd werd om een uitvoerbaar bestand te runnen. Beide wormen zouden dus automatisch zijn geblokkeerd.

---

## **Andere voorbeelden van exploits**

### **Dubbele extensie**

Virussen: Klez, Netsky en Lovegate.

Werkwijze: Kwaadaardige bestanden worden voorzien van een dubbele extensie (bijvoorbeeld filename.txt.exe) om de gebruiker ertoe te verleiden het bestand te openen.

### **URL spoofing exploit**

Virussen: er zijn nog geen virussen/wormen gevonden die van deze methode gebruik maken. URL spoofing exploits zijn echter wel gebruikt om achterdeuren op Windowscomputers te installeren.

Werkwijze: Stelt spammers en phishers (mensen die aan vertrouwelijke informatie proberen te komen) in staat om gebruikers kwaadaardige websites te laten bezoeken.

### **Object data file execution**

Virussen: Bagle Q

Werkwijze: Stelt aanvallers in staat om ongepatchte versies van Internet Explorer/Outlook (Express) automatisch te infecteren door code van een HTTP site te downloaden en uit te voeren.

## De 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 mshhtml.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

### Configuratie van de exploit engine van GFI MailSecurity

GFI MailSecurity is het eerste e-mailbeveiligingsproduct dat bescherming biedt tegen exploits die via e-mail worden verspreid. Dit product bevat verschillende soorten bescherming tegen e-maildreigingen, waaronder een engine voor de detectie van exploits. Deze unieke engine detecteert handtekeningen van bekende email exploits en blokkeert berichten die deze handtekeningen bevatten. De meeste gevaren die door de exploit engine van GFI MailSecurity worden geïdentificeerd, worden niet gedetecteerd door andere antivirusoplossingen. GFI MailSecurity bevat controles voor alle belangrijke email exploits en kan tevens automatisch nieuwe exploitcontroles downloaden zodra ze beschikbaar zijn.

Naast de email exploit detection engine beschikt GFI MailSecurity ook over: verschillende virusscan-engines voor een hogere detectiekans en snellere reacties; controle van de inhoud van e-mailberichten en bijlagen, waarbij gevaarlijke bijlagen en inhoud in quarantaine worden geplaatst; exploitbeveiliging voor bescherming tegen huidige en toekomstige virussen op basis van exploits; een engine die HTML-scripts uitschakelt; een Trojan & Executable Scanner die kwaadaardige uitvoerbare bestanden opspoot; en meer. Kijk voor meer informatie en een trialversie op <http://www.gfi.nl/nl/mailsecurity/>.

---

## Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

