

E-Mail-Exploits und ihre Gefahren

Warum zum Erkennen von E-Mail-Exploits eine besondere Engine benötigt wird

In diesem White Paper erfahren Sie, worum es sich bei E-Mail-Exploits handelt und welche E-Mail-Exploits unter anderem verbreitet sind. Informieren Sie sich, warum bei E-Mail-Exploits eine auf Signaturen basierende Abwehr, z. B. durch Anti-Viren-Engines, nutzlos ist und daher ein effektiverer Sicherheitsansatz verfolgt werden muss.

Einführung

Viren-Programmierer verwenden immer komplexere und raffiniertere Techniken, um Anti-Viren-Software zu überlisten und ihre schädlichen Programme zu verbreiten. Bestes Beispiel hierfür war der berühmte Nimda-Virus, der sich mehrerer Methoden bedient hat, um sich zu verbreiten und keinen schadhaften Programmcode als Basis hatte, nach dem Anti-Viren-Lösungen

üblicherweise suchen, sondern einen Exploit. Obwohl Anti-Viren-Software unerlässlich ist, kann sie allein solche Angriffe jedoch nicht abwehren. Hierfür ist zusätzlich ein Tool erforderlich, mit dem sich E-Mail-Exploits erkennen lassen.

Einführung	2
Was ist ein Exploit?	2
Unterschied zwischen Anti-Viren-Software und Programmen zur Identifizierung von E-Mail-Exploits	2
Exploit-Engine ohne häufige Updates	3
Nimda, BadTransB, Yaha und Bugbear und ihre Konsequenzen	3
Weitere Beispiele für Exploits	4
Die Exploit-Engine von GFI MailSecurity	5
Über GFI	6

Was ist ein Exploit?

Ein Exploit nutzt bekannte Schwachstellen von Anwendungen oder Betriebssystemen aus, um ein Programm oder Code auszuführen. Hierbei wird eine Funktion eines Programms oder des Betriebssystems vom Exploit für böswillige Zwecke ausgenutzt, um z. B. beliebigen Code auszuführen, Dateien auf Festplatten zu lesen/schreiben oder unautorisierten Zugriff auf das System zu erlangen.

Was ist ein E-Mail-Exploit?

Ein E-Mail-Exploit ist ein Exploit, der per E-Mail übertragen und gestartet wird. Er ist meistens in einer E-Mail versteckt und wird auf dem Rechner des Empfängers ausgeführt, sobald der Anwender die Mitteilung öffnet oder auch nur empfängt. Mit dieser Methode können Hacker die meisten Firewalls und Anti-Viren-Produkte umgehen.

Unterschied zwischen Anti-Viren-Software und Programmen zur Identifizierung von E-Mail-Exploits

Anti-Viren-Software ist so konzipiert, dass sie bereits bekannten böswilligen Programmcode aufspürt und blockiert. Eine E-Mail-Exploit-Engine hingegen verfolgt bei der Virenabwehr eine andere Strategie: Sie durchsucht Mitteilungen nach potenziell sicherheitsgefährdenden

Exploits. Dadurch bietet sie nicht nur Schutz vor neuen Viren, sondern auch vor allem vor unbekanntem Code. Besonders bei unbekanntem Code, der speziell für einen Angriff auf ein bestimmtes Netzwerk konzipiert wurde, erweist sich diese Eigenschaft als äußerst nützlich.

Hierbei werden E-Mails im Hinblick auf Verfahren gescannt, mit denen sich ein Programm oder ein Befehl auf dem System des Anwenders ausführen lässt, um Schwachstellen des Betriebssystems, E-Mail-Clients oder Internet Explorer auszunutzen. Die Exploit-Engine prüft dabei jedoch nicht, ob das Programm/der Code bösartig ist oder nicht. Sie informiert Administratoren lediglich, dass ein potenzielles Sicherheitsrisiko vorliegt, sobald sie feststellt, dass eine E-Mail einen Exploit verwendet, mit dem sich ein Programm oder Code ausführen lässt.

Auf diese Weise arbeitet eine E-Mail-Exploit-Engine wie ein Zugangskontrollsystem (IDS – Intrusion Detection System) für E-Mails. Die E-Mail-Exploit-Engine löst unter Umständen zusätzliche Fehlalarme aus, bietet dafür aber einen zusätzlichen, neuen Schutz, der einen Sicherheitsaspekt berücksichtigt, der von vielen normalen Anti-Viren-Paketen bisher vernachlässigt wurde.

Anti-Viren-Engines bieten zwar Schutz vor einigen Exploits, aber sie suchen nicht nach allen Varianten und ähnlichen Angriffsmöglichkeiten. Eine Engine zur Exploit-Erkennung hingegen sucht nach allen bekannten Exploits. Zudem ist die E-Mail-Exploit-Engine für das Auffinden von Exploits in E-Mails optimiert und gewährleistet daher eine wesentlich effizientere Überprüfung als gängige Anti-Viren-Engines.

Exploit-Engine ohne häufige Updates

Exploit-Engines müssen nicht so oft wie Anti-Viren-Engines aktualisiert werden, da sie eine übergreifende Angriffsmethode und keine neuen Einzelviren bekämpfen. Obwohl Exploit- und Anti-Viren-Engines gleichermaßen auf dem neuesten Stand gehalten werden müssen, bestehen bei Exploit-Engines zusätzliche Vorteile: Nachdem ein neuer Exploit identifiziert und in die Datenbank einer Exploit-Engine aufgenommen wurde, besteht automatisch ein Schutz vor allen Virenvarianten, die auf diesem Exploit basieren. Ein neuer Virus ist somit längst von der Exploit-Engine abgefangen worden, bevor Anti-Viren-Hersteller überhaupt darauf reagieren und entsprechend modifizierte Signaturen anbieten können. Dies ist ein entscheidender Vorteil, wie folgende Beispiele aus dem Jahr 2001 belegen.

Nimda, BadTransB, Yaha und Bugbear und ihre Konsequenzen

Nimda und BadTrans.B sind zwei Viren, die im Jahr 2001 weltweit zweifelhafte Berühmtheit erlangten, weil sie in einem bis dahin unbekanntem Ausmaß Windows-Rechner, die mit dem

Internet verbunden waren, infiziert und außer Betrieb gesetzt haben. Forschungsergebnissen des US-Unternehmens Computer Economics vom November 2001 zufolge hat allein der Nimda-Virus weltweit schätzungsweise ca. 8,3 Millionen Netzwerke infiziert.

Nimda ist ein Wurm, der gleich mehrere Methoden verwendet, um automatisch andere Computer zu infizieren. Er kann sich mit Hilfe des MIME-Header-Exploits per E-Mail vermehren und verbreiten. Dieser Exploit war bereits Monate vor dem Erscheinen von Nimda öffentlich in Erscheinung getreten. BadTrans.B ist ein Mass-Mailing-Wurm, der sich ebenfalls mit Hilfe des MIME-Header-Exploits verbreitet. BadTrans.B wurde erstmals nach dem Ausbruch des Nimda-Wurms gesichtet.

Anti-Viren-Hersteller waren auf die schnelle Infektionsrate von Nimda und BadTrans.B nicht vorbereitet. Obwohl die Hersteller versuchten, nach dem Bekanntwerden der neuen Schädlinge ihre Definitionsdateien so schnell wie möglich zu aktualisieren, hatte der Virus bereits eine große Zahl von PCs infiziert, bevor die Anti-Virus Updates veröffentlicht werden konnten.

Obwohl beide Viren denselben Exploit verwendeten, mussten Anti-Viren-Hersteller für jeden Schädling eigene Definitionsdatei-Updates erstellen. Eine Exploit-Erkennungs-Engine hätte den verwendeten Exploit erkannt und den Versuch, mittels des MIME-Header-Exploits automatisch eine ausführbare Datei zu starten, identifiziert und beide Würmer automatisch blockiert und eine Infektion verhindert.

Weitere Beispiele für Exploits

Doppelte Dateierweiterung

Viren: Klez, Netsky und Lovegate.

Auswirkungen: Dateien mit böswilligen Inhalten werden mit einer doppelten Dateierweiterung versehen, z. B. filename.txt.exe, um Anwender dazu zu verleiten, die scheinbar harmlose Text-Datei zu öffnen.

URL-Spoofing-Exploit

Viren: Bisläng ist noch kein Virus/Wurm aufgetaucht, der diese Methode einsetzt. Sie ist jedoch bereits verwendet worden, um Hintertüren auf Windows-Rechner zu installieren.

Auswirkungen: Spammer und Phisher (Betrüger oder Personen, die an vertrauliche Informationen gelangen wollen) können Anwender mit diesem Exploit dazu verleiten, eine für Spionage-Angriffe präparierte Web-Site zu besuchen.

Object Data Remote Execution

Viren: Bagle.Q.

Auswirkungen: Der Exploit erlaubt es Angreifern, Rechner, auf denen nicht gepatchte Versionen von Internet Explorer/Outlook (Express) laufen, durch das Herunterladen und Ausführen von Code von einer HTTP-Seite automatisch zu infizieren.

Die Exploit-Engine von GFI MailSecurity

Exploit Description	Last Updated	Enabled	Exploit ID
CLS-ID File Extension (High alert)	2/15/2002	Enabled	1
Frame 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

Konfigurierung der Exploit-Engine von GFI MailSecurity

GFI MailSecurity for Exchange/SMTP ist die erste E-Mail-Sicherheitslösung, die Schutz vor per E-Mail übertragenen Exploits bietet. Neben der Engine zur Identifizierung von Exploits stehen weitere Abwehrmaßnahmen zur Verfügung, die umfassend vor E-Mail-basierten Bedrohungen schützen. Bei der Entwicklung der neuartigen Engine hat GFI auf sein umfangreiches Know-how in der Erforschung von E-Mail-Exploits zurückgreifen können. Mit der branchenweit einzigartigen Engine werden Signaturen aktueller bekannter E-Mail-Exploits identifiziert und Mitteilungen blockiert, die diese Signaturen enthalten. Viele der Gefahren, die von der in GFI MailSecurity integrierten Exploit-Engine identifiziert werden, bleiben von anderen gängigen Anti-Viren-Lösungen unerkannt. GFI MailSecurity überprüft Mitteilungen auf alle wichtigen E-Mail-Exploits und kann zudem neue Exploit-Sicherheitschecks automatisch herunterladen, sobald diese von GFI zur Verfügung gestellt werden.

Neben dieser innovativen Funktion bietet die Sicherheitslösung auch noch mehrere Anti-Viren-Engines für eine höhere Erkennungsrate und schnellere Gegenmaßnahmen bei neuen Viren; eine E-Mail Inhalts- und Anhangskontrolle, um potenziell gefährliche Inhalte und Anhänge unter Quarantäne zu stellen; eine HTML-Threats-Engine zur Deaktivierung von HTML-Skripten sowie einen Trojan & Executable Scanner zur Identifizierung böswilliger exe-Dateien. Weitere Informationen und eine kostenfreie Test-Version von GFI MailSecurity finden Sie unter <http://www.gfisoftware.de/de/mailsecurity>.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Netzwerk-Fax-Server GFI FAXmaker for Exchange/SMTP, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen sowie GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter <http://www.gfisoftware.de>.

© 2004 GFI Software Ltd. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema des White Papers wieder. Änderungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Dieses White Paper dient nur der Produktinformation. GFI ÜBERNIMMT KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE HAFTUNG FÜR DIE IN DIESEM DOKUMENT PRÄSENTIERTEN INFORMATIONEN. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity und die zugehörigen Produkt-Logos sind eingetragene Marken oder Marken von GFI Software Ltd. in den Vereinigten Staaten und/oder anderen Ländern. Alle in diesem Dokument aufgeführten Produkte oder Firmennamen sind Eigentum der jeweiligen Inhaber.

