

## Cyberkriminelle tarnen Spam als konkrete Job-Angebote

**Holzwickede, 09. März 2010 – Ein „alter Bekannter“ sorgt in der Welt der E-Threats wieder für Aufsehen. Die Sicherheitsexperten von BitDefender ([www.bitdefender.de](http://www.bitdefender.de)) registrierten jüngst vermehrt Infektionen durch Win32.Worm.Mabezat.J. Dieser verbreitet sich über englischsprachige Spam-Mails, die eine mit dem Wurm infizierte Datei „winmail.dat“ im Anhang enthält. Der neueste Trick: Die Mails wurden von Cyberkriminellen als konkrete Job-Angebote getarnt.**

Die weiterhin schwierige Wirtschaftslage bleibt ein beliebtes Lockmittel für Spam-Attacken. Ausgenutzt werden dabei vor allem die derzeitige hohe Arbeitslosenquote und die Hoffnung vieler Beschäftigungsloser auf neue Arbeit. So gehören gefälschte Job-Angebote zu den neuen Methoden der Malware-Autoren, um ihre verseuchten Nachrichten an den User zu bringen. Die auf englisch verfassten Mails werden mit Betreffzeilen betitelt wie z.B.: „Web designer vacancy“, „New work for you“, „Welcome to your new work“ oder „We are hiring you“.

Statt eines konkreten Job-Angebotes enthält die Mail einen scheinbar harmlosen Anhang namens winmail.dat. Der User wird gebeten, diese Datei zu entpacken. Anschließend erscheint die Aufforderung zum Öffnen eines Word-Dokuments mit dem Titel Readme.doc. Dieses erweist sich jedoch als eine ausführbare Datei, die mit Win32.Worm.Mabezat.J infiziert ist.

Einmal geöffnet, erstellt die angebliche Readme-Datei unter Nutzung des Windows Explorer ein eigenes Verzeichnis, das den Wurm enthält. Dieser erzeugt anschließend einen Eintrag in der „autorun.inf“ inklusive einer neuen Datei mit dem Namen zPharaoh.exe. Dabei handelt es sich um eine Kopie des Wurms. Besonders beunruhigend ist die Tatsache, dass Win32.Worm.Mabezat.J in der Lage ist, die ersten 1768 Bytes einer exe-Datei mit seinem eigenen verschlüsselten Code zu ersetzen, anstatt sich wie andere Schädlinge anzuhängen. Der Wurm infiziert den PC anschließend jedes Mal von Neuem, sobald eine solche Datei ausgeführt wird. Beispiele sind der Windows Media Player sowie einige Binär-Dateien in Outlook Express.

### Selbstständige Verbreitung via Massen-Spam

Die Mabezat-Familie ist extrem gefährlich: Neben dem Befall von Binär- und der Zerstörung von Systemdateien sammeln Varianten des Wurms auch E-Mail-Adressen aus einer Vielzahl von Dateiformaten. Nachdem der Wurm eine E-Mail-Liste erstellt hat, nutzt er seine eigene SMTP Engine, um sich via Massen-Mails selbstständig weiterzuverbreiten.

Um sich vor einem derartigen Angriff zu schützen, empfiehlt BitDefender den Download und die Installation einer kompletten Anti-Malware-Suite mit Antiviren-, Antispam-, Antiphishing- und Firewall-Schutz. PC-Nutzer sollten zudem davon absehen, in ihren E-Mails Dateien von unbekanntem Absendern zu öffnen oder verdächtig aussehende Links zu aktivieren.

Unter dem Link <http://quicksan.bitdefender.com/> können Anwender einen kostenlosen Malware-Scan durchführen, um sicherzugehen, dass sich Mabezat nicht bereits auf ihrem Rechner befindet.

Mehr unter [www.bitdefender.de](http://www.bitdefender.de).

### Über BitDefender®

BitDefender ist Softwareentwickler einer der branchenweit schnellsten und effizientesten Produktlinien international zertifizierter Sicherheitssoftware. Seit der Gründung des Unternehmens im Jahr 2001 hat BitDefender permanent neue Standards im Bereich des proaktiven Schutzes vor Gefahren aus dem Internet gesetzt. Tagtäglich schützt BitDefender viele Millionen Privat- und Geschäftskunden rund um den Globus und gibt ihnen das gute Gefühl, dass ihr digitales Leben sicher ist. BitDefender vertreibt seine Sicherheitslösungen in mehr als 100 Ländern über ein globales VAD- und Reseller-Netzwerk. Ausführlichere Informationen über BitDefender und BitDefender-Produkte sind online im [Pressecenter](http://Pressecenter) verfügbar. Zusätzlich bietet BitDefender in englischer Sprache unter [www.malwarecity.com](http://www.malwarecity.com) Hintergrundinformationen und aktuelle Neuigkeiten im täglichen Kampf gegen Bedrohungen aus dem Internet.

### Pressekontakt:

BitDefender GmbH  
Robert-Bosch-Str. 2  
D-59439 Holzwickede

Ansprechpartner:  
Hans-Peter Lange  
PR-Manager  
Tel.: +49 (0)2301 – 9184-330  
Fax: +49 (0)2301 – 9184-499  
E-Mail: [presse@bitdefender.de](mailto:presse@bitdefender.de)

### PR-Agentur:

Sprengel & Partner GmbH  
Nisterstraße 3  
D-56472 Nisterau

Ansprechpartner:  
Fabian Sprengel  
Tel.: +49 (0)2661 – 91260-0  
E-Mail: [bitdefender@sprengel-pr.com](mailto:bitdefender@sprengel-pr.com)