## Bitdefender E-Threat-Report für das zweite Halbjahr 2012: Adware und auf Java basierende Malware am gefährlichsten

Bitdefender E-Threat-Report für das zweite Halbjahr 2012: Adware und auf Java basierende Malware am gefährlichsten<br /><br />Top 10 Online-Bedrohungen in der DACH-Region <br />In seinem aktuellen E-Threat-Report stellt Antivirus-Softwarehersteller Bitdefender die zehn meistverbreiteten E-Threats des zweiten Halbjahres 2012 für die DACH-Region zusammen. In den Top 10 tauchen Adware und auf Java basierende Malware am häufigsten auf. Zudem spielen Exploits eine Schlüsselrolle, da sie in der zweiten Jahreshälfte für rund 6 Prozent aller Malware-Störfälle in der DACH-Region verantwortlich waren. <br />Platz eins des Rankings belegt JS:Trojan.Script.EY, ein verändertes JavaScript- Snippet, das in "saubere" Webseiten injiziert wird, um Benutzer auf Malware-infizierte Websites umzuleiten. Diese Seiten beinhalten Exploit-Codes, die den Browser oder deren Plugins wie Adobe Reader oder Adobe Flash angreifen. Die verschlüsselten Scripts werden in der Regel automatisch zu Webseiten hinzugefügt, indem sie Schwachstellen in der Plattform-Software ausnutzen.<br />Gleich dahinter auf Rang zwei befindet sich Generic.JS.Crypt1.C14787EE, ebenfalls ein Code-Fragment, das als JavaScript geschrieben wurde. Dieses Script lädt Bilder, die auf Werbebannern basieren, von bestimmten Webseiten herunter. Die Bilder sind dabei von aktuell auf diesen Servern laufenden Kampagnen abhängig. Das Script simuliert einen Klick auf das Banner, ohne die Zustimmung der User zu haben. Ein Mausklick ist dabei für Cyberkriminelle gleichbedeutend mit einer finanziellen Einnahme.<br />Den dritten Platz belegt Gen.Adware.Solimba. Diese Adware hat noch einen Ableger auf dem achten Platz der Top 10 Online-Bedrohungen. Beide sind Variationen des Solimba-Werbeprogramms. Sie erkennen vom User potenziell unerwünschte Installationen von Drittanbieter-Software nach dem Verhalten, zusammen mit dem Produkt, das der User zu installieren versucht. Typisch für Adware.Solimba ist eine exe-Datei, die als Downloader fungiert. Sie versucht, ausführbare Dateien aus dem Werbenetzwerk abzurufen. Diese Adware zeigt ein potenziell bösartiges Verhalten, da sie private Nutzerdaten sammelt. Adware.Solimba betrifft alle Windows-Betriebssysteme von Windows 2000 bis Windows 7.<br />Auf Position vier befindet sich Win32.Worm.Downadup. Im Jahre 2009 war der als Conficker bekannte Schädling einer der aggressivsten E-Threats, da er mehr als zwölf Millionen PCs innerhalb eines Tages kompromittierte. Der Wurm ist dazu fähig, per Fernzugriff Rechner zu infizieren, die sich im selben Netzwerk befinden. Dafür gelangt er mittels Brute-Force-Angriff an die Anmeldeinformationen. Gleichzeitig verweigert er den Zugriff auf Webseiten von Antivirensoftware-Herstellern, die seinen Übergriff verhindern könnten. Der Wurm wird verwendet, um unter anderem gefälschte Sicherheitssoftware auf dem infizierten Computer zu installieren. <br />Auf Platz 5 befindet sich die Bedrohung PDF:Exploit.PDF-JS.HN, die in PDF Dateien versteckt wird, welche sich im Anhang von Spam-Nachrichten befinden. Diese Dateien sind mit einem Exploit-Code ausgestattet, der Fehler in der Client Software (CVE-2010-0188) auslöst und anschließend einen beliebigen Code ausführt. Dies ist eine häufig auftretende Infektionsmethode, die von dem Blackhole Exploit Kit verwendet wird, um Malware auf den Computern der Nutzer zu installieren. Diese Methode wird auch von Exploit.TIFF.Gen (Rang sechs) und Exploit.PDF-JS.GW (Platz sieben) verwendet. Beide kompromittieren durch in Adobe Acrobat- und Adobe Reader-Versionen injizierte Codes die Systeme der Nutzer. <br />Neunter des Rankings ist Exploit.JS.Agent.AK: ein Exploit-Code, der versucht, einen "Heap Spray-Angriff" auf den Browser auszuführen. Auf Platz zehn liegt mit Trojan.AutorunInf eine bereits seit 2008 aktive Malware-Applikation. Dieser Trojaner fängt speziell entwickelte Autorun-Dateien ab. Diese sind stark verschlüsselt, damit die Nutzer sie beim Öffnen nicht lesen können. Bedrohungen wie Sality, Virtob, Downadup oder Stuxnet erstellen anschließend eine Kopie von sich selbst und eine Autorun.Inf Datei, die beide auf Wechseldatenträger übertragen werden. Sobald das Wechselmedium an einen PC angeschlossen wird, befällt die Malware das Betriebssystem. <br />Der komplette E-Threat Report für das zweite Halbjahr 2012 steht hier als PDF zum Download bereit.<br />Über Bitdefender<br />Bitdefender ist Hersteller einer der weltweit schnellsten und effektivsten Produktserien für international zertifizierte Internet-Sicherheits-Software. Seit dem Jahr 2001 ist das Unternehmen immer wieder ein innovativer Wegbereiter der Branche, indem es preisgekrönte Schutzlösungen einführt und weiterentwickelt. Mittlerweile setzen weltweit rund 400 Millionen Privat- und Geschäftsanwender auf die Bitdefender-Technologie, um ihre digitale Welt sicherer zu machen. Bitdefender hat vor kurzem eine Reihe wichtiger Empfehlungen und Auszeichnungen in der globalen Sicherheitsindustrie erhalten. Dazu gehört "Editors Choice des PC Mag für Bitdefender Antivirus Plus 2013 und die "GoldAward-Auszeichnung des TopTenREVIEW, die den Spitzenplatz der Software unter 25 getesteten Sicherheitslösungen bestätigt hat. Die Bitdefender Antivirus-Technologie hat diese Spitzenposition auch bei den führenden Industrietests von AV-TEST und AV-Comparatives belegt. Weitere Informationen zu den Antivirenprodukten von Bitdefender sind im Bitdefender Security Center der Unternehmenswebseite im Pressecenter verfügbar.<br />Über Bitdefender HOTforSecurity<br />Zusätzlich veröffentlicht Bitdefender das englischsprachige Blog "HOTforSecurity", welches rund um die aktuelle Sicherheitslage weltweit informiert. Es bietet eine prickelnde Mischung aus nebulösen Computersicherheitsgeschichten und sachlich fundierten Stories, die die schmutzige Welt der Internetbetrügereien, Spams, Scams, Malware und des Klatsches sichtbar macht. Bitdefender pflegt auch eine deutsche HOTforSecurity-Version, die sich insbesondere auf die Nachrichtenlage im deutschsprachigen Raum (Deutschland, Österreich, Schweiz) konzentriert.<br /><br />

### Pressekontakt

Bitdefender GmbH

59439 Holzwickede

ataflan@bitdefender.com

### Firmenkontakt

Bitdefender GmbH

59439 Holzwickede

ataflan@bitdefender.com

Über BitdefenderBitdefender ist Hersteller einer der weltweit schnellsten und effektivsten Produktserien für international zertifizierte Internet-Sicherheits-Software. Seit dem Jahr 2001 ist das Unternehmen immer wieder ein innovativer Wegbereiter der Branche, indem es preisgekrönte Schutzlösungen einführt und weiterentwickelt. Mittlerweile setzen weltweit rund 400 Millionen Privat- und Geschäftsanwender auf die Bitdefender-Technologie, um ihre digitale Welt sicherer zu machen. Bitdefender hat vor kurzem eine Reihe wichtiger Empfehlungen und Auszeichnungen

in der globalen Sicherheitsindustrie erhalten. Dazu gehört Editors Choice des PC Mag für Bitdefender Antivirus Plus 2013 und die GoldAward-Auszeichnung des TopTenREVIEW, die den Spitzenplatz der Software unter 25 getesteten Sicherheitslösungen bestätigt hat. Die Bitdefender Antivirus-Technologie hat diese Spitzenposition auch bei den führenden Industrietests von AV-TEST und AV-Comparatives belegt. Weitere Informationen zu den Antivirenprodukten von Bitdefender sind im Bitdefender Security Center der Unternehmenswebseite im Pressecenter verfügbar. Über Bitdefender HOTforSecurityZusätzlich veröffentlicht Bitdefender das englischsprachige Blog ?HOTforSecurity, welches rund um die aktuelle Sicherheitslage weltweit informiert. Es bietet eine prickelnde Mischung aus nebulösen Computersicherheitsgeschichten und sachlich fundierten Stories, die die schmutzige Welt der Internetbetrügereien, Spams, Scams, Malware und des Klatsches sichtbar macht. Bitdefender pflegt auch eine deutsche HOTforSecurity-Version, die sich insbesondere auf die Nachrichtenlage im deutschsprachigen Raum (Deutschland, Österreich, Schweiz) konzentriert.