BitDefender entlarvt Trojaner der Woche

29.07.2008, 09:36 | IT, New Media & Software

Pressemitteilung von: *BitDefender GmbH*

Angelina Jolie, Britney Spears und Barack Obama sind Teil einer neuen Spam-Kampagne mit gefährlicherMalware

Holzwickede, 29. Juli 2008 – BitDefender-Antivirenspezialisten haben eine neue Art der Malware-Verbreitung entdeckt: Spam-Nachrichten, die Computerbenutzer austricksen und dazu bringen sollen, Schadsoftware herunterzuladen und auf ihren Rechnern zu installieren. Die Malware-Verbreitungsmethode basiert auf Nachrichtenfragmenten, die von Show-Stars wie Angelina Jolie, Britney Spears oder wichtigen amerikanischen Politikern wie Barack Obama handeln.

Die E-Mail-Nachrichten führen den unachtsamen Nutzer zu Internetseiten, auf denen vermeintlich Video-Clips zu sehen sind. Allerdings stellt sich beim Besuch der Seite heraus, dass dort lediglich ein Bild eines Video-Players zu sehen ist, welches mit einem ausführbaren Programm (ein EXE-File) verlinkt ist.

Um den Clip nun sehen zu können, werden die User angewiesen, ein vermeintliches Update für den weit verbreiteten Adobe Flash Player herunterzuladen. Dieses ist jedoch mit Trojan.Downloader.Tibs.GZM infiziert. Zu allem Überfluss beginnt das Programm automatisch mit dem Download weiterer unerwünschter Schadsoftware – ein Phänomen, welches als „Drive-by-download“ bekannt ist. Allein dies sollte als Warnung für den User genügen, die Legitimität der Datei in Frage zu stellen. Einmal ausgeführt, installiert der Trojaner weitere Malware, darunter den berüchtigten Trojan.Peed.JPU, der im Storm Botnet weit verbreitet ist.

Die neue Mail-Verbreitungskampagne hat hauptsächlich Computernutzer mit begrenztem Wissen hinsichtlich der Datensicherheit zum Ziel. Benutzer, die wohlwissentlich allgemeine Sicherheitsregeln ignorieren, um Zugang zu sensationellen Neuigkeiten zu bekommen, sind ebenfalls betroffen.

„Die E-Mail-Nachrichten sind Teil einer größeren Welle, die versucht, User mit diversen Trojanern zu infizieren. Diese Arten von Nachrichten haben vor zwei Tagen begonnen, die Postfächer der User zu füllen. Ursprünglich als Nachricht mit nur einer einzigen Struktur designt, entwickelten sich schnell drei Varianten: eine Kategorie mit einem einzigen, rein Text-basiertem Teil, eine zweite mit einem HTML-Teil sowie eine dritte, die sich die Templates des Opera Mail Clients zu Nutze macht“, erklärt Bogdan Dumitru, CTO bei BitDefender.

Um die Erfolgsquote der Angriffe zu erhöhen, bedienen sich die Spammer einer Reihe von packenden Schlüsselwörtern, die auf verschiedene Weise innerhalb des Nachrichtentextes angezeigt werden. Trotz der Tatsache, dass jede Nachricht unterschiedlich gefälschte News-Flashes und Headlines benutzt, wird der User immer an eine URL weitergeleitet, die mit „stream.html“ oder „watchit.html“ endet.

Wenn auch der Ansatz sehr an eine vorangegangene Spam-Kampagne erinnert, die Angelina Jolie und Michael Jackson als Aufhänger benutzte, haben sich die Malware-Komponenten und die Hosting-Server geändert. Um nicht erkannt zu werden, wurde der neue Trojaner zudem in einem anderen Utility-Programm neu verpackt.

Für ein sicheres und unbeschwertes Surfen im Internet ist man auf eine zuverlässige und stets aktuelle Anti-Malware-Schutzlösung angewiesen. Mit Bitdefenders professionellen Security-Produkten erhalten Internet-User einen wirksamen Schutz: Er filtert einerseits die Spam-Nachricht heraus und erkennt andererseits den schädlichen Code (Trojan.Downloader.Tibs.GZM), mit dem die Anwendung „install_flash_player_update“ infiziert ist.

Bildmaterial zu dieser Pressemitteilung kann unter bitdefender@sup-pr.de angefordert werden.

Portrait

Über BitDefender:
BitDefender ist ein führender, globaler Anbieter von international zertifizierten und proaktiv arbeitenden Sicherheitslösungen für Desktop PCs, Unternehmensnetzwerke und mobile Geräte. Das Unternehmen besitzt eines der schnellsten und effektivsten Portfolios von Security Software, das neue Maßstäbe für Gefahren-Prävention, zeitnahe Entdeckung und zuverlässige Beseitigung setzt. BitDefender hat mit B-HAVE, der neuen, proaktiven Virus Detection-Technology, die wohl zurzeit fortschrittlichste Waffe gegen unbekannte Viren in seine Produkte integriert. B-HAVE findet und beseitigt auch unbekannte Viren – unabhängig von Virensignaturen. BitDefender ist mit Niederlassungen in Deutschland, Spanien, Rumänien, UK sowie den USA vertreten. Mehr über BitDefender finden Sie unter: www.bitdefender.de.

News-ID: 230014 • Views: 996 (Stand: 23.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/230014/BitDefender-entlarvt-Trojaner-der-Woche.html