



Diese Meldung wurde von [presstext.austria](http://www.presstext.at/pte.mc?pte=080908026) ausgedruckt und ist unter <http://www.presstext.at/pte.mc?pte=080908026> abrufbar.

## Mini-Programm macht Facebook zu Riesen-Botnetz Web-2.0-Plattformen sind Paradies für Cyberkriminelle

Athen/Wien (pte/08.09.2008/12:05) - IT-Securityspezialisten haben demonstriert, dass Social Networks im Handumdrehen in riesige Botnetze verwandelt werden können. Die Forscher des griechischen Institute of Computer Science (ICS) der Foundation for Research & Technology Hellas (FORTH) <http://www.ics.forth.gr> und des Institute for Infocomm Research in Singapur <http://www.i2r.a-star.edu.sg> haben dazu eine Applikation für die Web-2.0-Plattform Facebook entwickelt, die einen Rechner in ein Botnetz integriert, sobald das Mini-Programm auf dem PC installiert wird. "Photo of the Day", so der Name der Anwendung, verspricht ein täglich aktuelles Bild von National Geographic, schleust aber nebenbei Schadcode auf den Rechner.



Soziale Netzwerke als Paradies für Cyberangreifer

Das Problem bei dieser Form von Angriff ist, dass sie aktiv vom Opfer ausgeführt wird. Selbst die besten IT-Security-Produkte haben hier keine Chance, dies zu verhindern. "Es ist vergleichbar mit einem hohen Turm, der über modernste Sicherheitstechnik verfügt. Jedoch öffnet der Bewohner jedes mal sofort die Tür, wenn es klopft", meint Joe Pichlmayr, Geschäftsführer bei Ikarus Software, im Gespräch mit presstext. Web-2.0-Netzwerke seien ohnehin ein Paradies für Angreifer, wenn es darum geht, Informationen über ein potenzielles Opfer zu sammeln. Gezielte Attacken stellen schließlich auch Sicherheitssoftware vor ein Problem. "Einzelattacken passieren unter dem Radar der Software und werden dadurch schwer entdeckt", sagt Pichlmayr.

"Soziale Netzwerke bieten die idealen Voraussetzungen, um zu einer Plattform für Angriffe zu werden", stellen auch die griechischen Forscher in ihrem Bericht fest. Um ihren Schadcode an den PC-User zu bringen, verpackten sie diesen in eine harmlos aussehende Facebook-Applikation. Facebook-Mitglieder installieren die Anwendung schließlich selbst auf ihrem Rechner und öffnen dem Angreifer somit die Tür. Jedes Mal, wenn das Programm ein neues Foto lädt, wird der betroffene Rechner gezwungen, Daten zu senden. Im Hintergrund werden somit 600 Kilobyte Daten an den Server des Angreifers gesendet. Diese können allgemeine Informationen über den Rechner, Angaben zu offenen Ports oder Cookies sein. Ebenfalls möglich ist es, Malware über den derart gekaperten Rechner zu verschicken.

Die Studienautoren raten Betreibern von sozialen Netzwerken, große Vorsicht bei der Entwicklung ihre Programmierschnittstellen walten zu lassen. Vor allem sollten die Interaktionsmöglichkeiten zwischen den Applikationen und dem Internet begrenzt werden. "Anwendungen für soziale Netzwerke sollten ausschließlich in einer geschlossenen Umgebung laufen. Kontakte mit anderen Hosts abseits des eigenen sozialen Netzwerks sollten gänzlich unterbunden werden", schreiben die Spezialisten in ihrem Papier.

Pichlmayr rät im Umgang überhaupt zur Vorsicht, wenn private Informationen angegeben werden: "MySpace, XING und Co sind die idealen Plattformen für Angreifer. Auf keiner anderen Web-Plattform können Informationen so leicht abgestaubt werden wie hier. So einfach wie im Web 2.0 lassen sich nirgendwo persönliche Daten verknüpfen und komplette Profile von Menschen erstellen." Die Fülle an Daten, die freiwillig online gestellt werden, wirke sich auch auf die Qualität von Spam aus. "Die Option, E-Mail-Adressbücher online zu stellen und mit Freunden abzugleichen und zu verlinken, trägt nicht unwesentlich dazu bei, dass Spammer reale E-Mail-Adressen einsammeln können, sondern in Verbindung mit anderen Daten auch, dass Spam immer zielgerichteter zum Einsatz kommt", führt Pichlmayr aus. (Ende)



Aussender: [presstext.austria](http://www.presstext.austria)