

## **Fortinet warnt vor tückischem Phishing-Angriff auf MySpace.com-Nutzer**

*Die portalübergreifende Attacke zielt auf Kreditkarteninformationen*

**München, 17. Oktober 2006 - Das auf IT-Sicherheitslösungen in Echtzeit spezialisierte Unternehmen Fortinet warnt vor bösartigen Phishing-Attacken in Zusammenhang mit dem Portal MySpace.com. Die Angreifer imitieren das Format der Benachrichtigungs-E-Mails von MySpace.com und locken die Nutzer so auf eine Phishing-Seite, die einzig und allein mit dem Ziel entworfen wurde, Kreditkarteninformationen abzugreifen. Dabei sind nicht nur MySpace.com-Nutzer betroffen: Spam-Versender schicken die falschen E-Mails an jeden in ihrer Reichweite, da sie davon ausgehen, dass sie auf diese Weise immer noch genug Leute mit einem MySpace-Profil erreichen.**

Um die Spam-Filter zu umgehen wird das E-Mail als Plain-Text verschickt und gelangt auf diese Weise in die Postfächer. Da das E-Mail wie eine Info-Mail von MySpace.com aussieht, gehen viele Empfänger bedenkenlos auf das Angebot ein, sich ein neues MP3-File eines Künstlers, einer Band oder eines Freundes anzuhören – der verhängnisvolle Klick auf den mitgelieferten Link, der eine täuschend echte MySpace-typische URL aufweist, erfolgt. Danach findet sich das Phishing-Opfer auf einer Seite wieder, die wie ein normales Musik-Downloadcenter mit verlockend preiswerten Angeboten aussieht. Nach der Auswahl der gewünschten Musiktitel ergeht die Aufforderung an den Nutzer, sein Konto auf einer verschlüsselten Bezahlseite auszugleichen und die Kreditkarteninformationen einzugeben – nur dass diese Seite, sobald dies geschehen ist, mit einem Time-out-Fehler schließt und der Betreiber sämtliche Informationen für mögliche betrügerische finanzielle Transaktionen besitzt.

Das MySpace-Portal war bereits mehrmals Angriffsziel von Hackern. Wie Fortinet vor einigen Monaten berichtete, waren die Seiten eine wahre Brutstätte von Malware-Aktivitäten, die vor allem auf die jüngeren, technisch nicht so versierten Nutzer des Portals abzielten. Dabei wurden anpassbare Avatare und Profilsucher-Software eingesetzt, die beide auf dem Rechner des Anwenders Adware installierten. In anderen Fällen übernahmen die Hacker

---

#### **Kontakte für die Presse:**

Manuel Hüttl  
markenzeichen GmbH  
Goethestr. 66  
D-80336 München  
Tel.: +49 (0)69 71 04 880-40  
Fax: +49 (0)69 71 04 880-79  
Mobil: +49 (0)179 -5097472  
[manuel.huettl@markenzeichen.eu](mailto:manuel.huettl@markenzeichen.eu)  
[www.markenzeichen.eu](http://www.markenzeichen.eu)

einfach Profile und posteten Nachrichten, die die Wirksamkeit ihrer bösartigen Links verlängerten.

Das Threat Research Team von Fortinet bietet im FortiGuard Center Informationen zur aktuellen Phishing-Attacke an, und zwar unter <http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-28.html>.

#### **Über Fortinet Inc.**

Fortinet entwickelt und produziert Echtzeit-Sicherheitslösungen für den Einsatz in Unternehmens-netzwerken. Das Unternehmen wurde vor sechs Jahren von Ken Xie, dem Gründer und früheren CEO von NetScreen, gegründet und ist laut IDC weltweiter Marktführer im Bereich Unified Threat Management (UTM). Für die FortiGate-Produktfamilie erhielt das Unternehmen bereits mehrfach Auszeichnungen. Die Anti-Threat-Lösung integriert unterschiedliche Netzwerksicherheits-Komponenten, die für Unternehmen wichtig sind, in einem Produkt. So werden Netzwerk-basierte Funktionalitäten von Firewall-, VPN- oder Intrusion Detection-Systemen ebenso im Produkt vereint wie Schutzmechanismen Content-basierter Attacken aus dem E-Mail- und Internetverkehr. Damit stellt die Lösung auch einen effizienten Viren- und Spam-Schutz dar und filtert darüber hinaus auch Content. Die Systeme basieren auf einer ASIC-Architektur – das heißt, dass sämtliche Sicherheitsfunktionalitäten auf einem Mikroprozessor integriert sind. Fortinet ist in privater Hand und hat seinen Stammsitz in Sunnyvale, Kalifornien. Weitere Informationen über Fortinet finden Sie unter [www.fortinet.com](http://www.fortinet.com)