

## **Falsche Virenschutz-Programme zocken Anwender ab - Betrügerische Scanner lassen Kasse von Online-Kriminellen klingeln**

Bochum (pts/24.09.2008/15:12) - In einer weltweiten Kampagne versuchen internationale Cyber-Banden ahnungslose Anwender mit falschen Security-Lösungen zu überrumpeln. Die Experten des G DATA Security-Labs <http://www.gdata.de> verzeichneten in den vergangenen Wochen eine explosionsartige Zunahme dieser sog. "Rogue-Antispyware". Die Masche der Täter ist dabei äußerst aufwendig und ausgeklügelt: Auf gehackten Webseiten wird Schadcode hinterlegt, der PCs unbemerkt per Drive-by-Download infiziert und ein vermeintliches Virenschutz-Programm installiert. Dieses meldet dann umgehend vorgetäuschte Infektionen. Eine "Desinfektion" ist angeblich nur nach Kauf und Registrierung des nutzlosen und schädlichen Programms möglich. Die Täter haben es bei dieser aufwendigen Inszenierung u. a. auf Kreditkarteninformationen, persönliche Daten und den Rechner selbst abgesehen. Der PC wird im nächsten Schritt mit weiterem Schadcode versehen und als Zombie zur Spam-Schleuder umfunktioniert. Mit mehr als 1.000 verbreiteten Varianten ist "Trojan-Downloader.FraudLoad" bei diesem eCrime-Konzept die aktivste Malware-Familie.

Ralf Benz Müller, Leiter G DATA Security Lab: "Online-Kriminelle entwickeln nur erfolgversprechende eCrime-Produkte und Konzepte weiter. Das gesamte Handeln ist auf Gewinnoptimierung ausgerichtet - "Poor Dogs" werden schnell aus den Portfolios entfernt. Die Verbreitung von Security-Blüten muss für die Täter in der Vergangenheit daher äußerst erfolgreich gewesen sein. Der Anstieg der letzten Wochen und Monate ist hierfür ein eindeutiger Beleg. Opfer dieser Attacken sind meist Anwender, die leichtsinnigerweise auf leistungsstarke Security-Lösungen verzichten und den Browser und das Betriebssystem nicht auf den neuesten Stand halten."

### **Aufwendige Datenjagd**

Die recht aufwendige Vorgehensweise, mit vorgetäuschter Malware-Infektion und angeblicher Abwehrsoftware, soll potenzielle Opfer im ersten Schritt zur Herausgabe ihrer persönlichen Daten bewegen. Im Fokus der Datenjäger: Kreditkarteninformationen, Telefonnummern und E-Mail-Adressen. Viele Varianten der eingesetzten "Rogue-Antispyware" gehen noch einen Schritt weiter und führen quasi "im Huckepack" reale Infektionen durch, um den PC komplett unter ihre Kontrolle zu bringen. Dieser wird als Zombie in Botnetze integriert und anschließend gewinnbringend als Spam-Schleuder vermietet.

### **Vier Tipps der G DATA Experten**

1. Setzen Sie ausschließlich Security-Lösungen mit aktuellen Virensignaturen ein. Abgelaufene Testversionen oder Security-Software ohne Signatur-Updates bieten keinen ausreichenden Schutz vor Schadcode.
2. http-Filter bieten einen effektiven Schutz vor Drive-by-Downloads. Der gesamte Datenverkehr wird vor Erreichen des Browsers nach Schadcode untersucht. Diesen niemals ausschalten!
3. Betriebssystem und Browser immer auf den neuesten Stand halten und Updates regelmäßig installieren.
4. Empfehlenswert: Aktive Inhalte im Browser deaktivieren. Active-X und andere Komponenten werden häufig zur Einschleusung von Schadcode verwendet.

Weitere Informationen finden Sie im G DATA Whitepaper "Fehlalarm 2.0 - Funktionsweise von Rogue-AntiSpyware". (Ende)

Aussender: G DATA Software AG Ansprechpartner: Thorsten Urbanski Email: [Thorsten.Urbanski@gdata.de](mailto:Thorsten.Urbanski@gdata.de) Tel.: +49-234-9762-239

Quelle: <http://presstext.com/pte.mc?pte=080924037>

© presstext Nachrichtenagentur GmbH <http://www.presstext.de> - Die inhaltliche Verantwortung für redaktionelle Meldungen (pte) liegt bei presstext, für Pressemitteilungen (pts) beim jeweiligen Aussender. Weitere Informationen erhalten Sie bei unserem Redaktionsservice unter [info@presstext.com](mailto:info@presstext.com) oder Tel.

+43-1-81140-300.

[\[dowjones.de\]](#) • [24.09.2008](#) • [13:20 Uhr](#) • [155 Views](#)

[0 Kommentare]