



Pressemitteilung – Freigegeben zur sofortigen Veröffentlichung

Emsi Software warnt: Falschparken löst neue Virenattacke aus!

Emsi Software, Anbieter der Schutz-Software a-squared Anti-Malware 4.0, warnt vor einer neuen Virenattacke, die bislang nur in den USA zum Einsatz kommt. Hier finden immer mehr Autofahrer nach dem Einkauf einen Strafzettel hinter ihrer Windschutzscheibe vor. Details zum eigenen Falschparken und zum Bußbescheid sollen sich die Fahrer im Web abholen. Autofahrer, die dem abgedruckten Link folgen, holen sich aber nur neue Malware auf den PC.

Salzburg, Februar 2009 - Viele Besucher einer Shopping Mall in Grand Forks (ND), USA, staunten nicht schlecht, als sie mit Tüten beladen zu ihrem Auto zurückkehrten. Hinter dem Scheibenwischer ihrer Windschutzscheibe klebte ein Strafzettel - fürs Falschparken. Auf den Zetteln stand zu lesen:

"PARKING VIOLATION This vehicle is in violation of standard parking regulations. To view pictures with information about your parking preferences, go to website xxx."

Übersetzt bedeutet dies: Das Auto steht im Parkverbot. Um ein Foto der Straftat einzusehen und um sich über die Strafe zu informieren, sollten die Autofahrer eine Internet-Verbindung herstellen und im Web eine bestimmte Seite aufrufen.

Auf der angegebenen Web-Seite bekamen die Besucher Fotos von anderen Parksündern präsentiert, aber nicht das eigene. Um es zu finden, sollte erst eine Picture Search Toolbar heruntergeladen und installiert werden. Diese richtete aber ungewollt eine Malware-DLL im System ein, die sich als Internet Explorer Helper Object (BHO) etabliert. Über diese Verbindung wird dann eine weitere DLL-Datei bezogen, die bereits einschlägig als Malware bekannt ist. Sie richtet sich ebenfalls als BHO ein und öffnet nach einiger Zeit ein Popup-Fenster mit einer gefälschten Sicherheitsmeldung. Sie möchte den Anwender dazu veranlassen, einen so genannten Rogue-Anti-Spyware-Scanner zu installieren - also ein Schutzprogramm, das keins ist, und das selbst nur wieder weitere Malware-Manipulationen am System vornimmt.

Social Engineering: Kontaktaufnahme zu den "Opfern" nun auch offline

Dies ist ein gutes Beispiel für das Social Engineering der Malware-Autoren. Auch offline werden nun Anwender mit Schad-Software konfrontiert, ohne dass Sicherheitslücken im Browser oder komplizierte Infektionswege zum Einsatz kommen müssen.

Christian Mairoll, Geschäftsführer von Emsi Software: "Mit der Malware, die hier zum Einsatz kommt, kommen Schutzprogramme wie unser a-squared Anti-Malware 4 problemlos klar. Überraschend und auch schockierend ist für uns, dass die Online-Mafia inzwischen völlig neue und mitunter auch sehr aufwändige Wege beschreitet, um die ahnungslosen Anwender zu überlisten. Der Trick mit den gefälschten Strafzetteln ist in den USA inzwischen bereits mehrfach zum Einsatz gekommen. Die Lehre daraus ist, dass man als Bürger noch misstrauischer sein muss, sobald eine Web-Adresse zum Einsatz kommt. Hierzulande gilt: Kein Polizist fordert im Strafzettel dazu auf, doch bitteschön eine Homepage zu besuchen. Das ist Humbug."



Pressemitteilung – Freigegeben zur sofortigen Veröffentlichung

a-squared Free 4.0 ist für Privatanwender zur kostenfreien Nutzung freigegeben. Das Programm arbeitet unter Windows XP, 2003/2008 Server und Vista. Es läuft nicht mehr auf Windows 98, ME und 2000. Der große Bruder a-squared Anti-Malware 4.0 kostet 29,90 Euro im Jahr. Die Verhaltensanalyse von a-squared Anti-Malware meldet übrigens aktiv die Installation von schädlichen Browser Helper Objekten (BHOs).

Homepage Emsi Software: <http://www.emsisoft.de/>

a-squared Free 4.0: <http://www.emsisoft.de/de/software/free/>

a-squared Anti-Malware 4.0: <http://www.emsisoft.de/de/software/antimalware/>

SANS Internet Storm Center zum Thema: <http://isc.sans.org/diary.html?storyid=5797>

ÜBER EMSI SOFTWARE

Emsi Software ist ein privat geführtes Unternehmen mit Sitz in Österreich. Das schnell wachsende Unternehmen ist ein führender europäischer Anbieter für Verhaltensanalyse-Technologie zum Analysieren von Software, insbesondere Malware.

Gegründet wurde das Unternehmen 2003 von Christian Mairoll, der damit seine Vision einer virtuellen Firma umsetzt: Die 15 Mitarbeiter der Firma sind auf der ganzen Welt verteilt, arbeiten aber über das Internet so zusammen, als würden sie nebeneinander im echten Büro sitzen. Um die technischen Visionen kümmert sich Georg Wicherski, der als Mitbegründer des "Nepenthes" Honeypot Projekts sowie der mwcollect Alliance (Zusammenschluss von Honeypot Netzen zum automatisierten Einfangen von Schadsoftware aus dem Internet) ein großes Ansehen in der Sicherheitsbranche genießt. Zur Produktpalette von Emsi Software gehören die Sicherheitsprogramme a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer und seit Ende 2007 Mamutu.

PRESSEKONTAKT

Thomas Günther

PR-Manager

Mail: tg@emsisoft.com

Fon: +43 664 344 60 68

Fax: +43 6235 200 53