

vor einem Jahr

in IT/Hightech und Internet

## G Data macht aktueller Windows Schwachstelle den Garaus

### Neuer Hotfix kostenlos als Download erhältlich

(ddp direct) Die gravierende Sicherheitslücke bei Dateiverknüpfungen in Microsoft Windows Produkten wird inzwischen durch mehrere Schädlingen ausgenutzt und es zeichnet sich ab, dass der Exploit schnell Einzug in weitere, neue Malware findet. Wie in den Medien berichtet, waren erste Ansätze, das Sicherheitsleck zu schließen, nicht sehr erfolgreich. Die G Data-Spezialisten haben jetzt mit dem G Data LNK-Checker einen Hotfix entwickelt, der die automatische Ausführung von Schadcode bei der Betrachtung von LNK-Dateien unterbindet, reguläre Icons aber normal darstellt. Der Anwender ist so vor gefährlichen LNK-Dateien geschützt. Das Programm steht gratis auf der G Data Webseite zum Download bereit.

„Die aktuelle Schwachstelle eröffnet Cyber-Kriminellen viele neue Wege, um Rechner zu infizieren. Sie müssen nur dafür sorgen, dass eine LNK-Datei auf dem Rechner angezeigt wird. Die Datei, auf die verwiesen wird, muss nicht einmal auf dem Rechner vorliegen, diese kann auch im Internet hinterlegt sein“, erklärt Ralf Benzmüller, Leiter der G Data SecurityLabs. „Nicht nur Nutzer von USB-Sticks sind betroffen. In Unternehmensnetzwerken reicht eine präparierte und abgelegte Datei auf dem Netzlaufwerk aus. Selbst einige Standard-Programme, wie z.B. Textverarbeitung und E-Mail-Clients, ermöglichen die Anzeige von Dateiverknüpfungen. Das Missbrauchspotenzial ist immens. Wir rechnen damit, dass diese Sicherheitslücke in Kürze massiv ausgenutzt wird.“

#### Der G Data LNK-Checker im Detail

G Data hat schnell reagiert und veröffentlicht mit dem G Data LNK-Ckecker ein kostenloses Sicherheits-Tool. Das Programm arbeitet unabhängig vom installierten Virenschutz und ergänzt ihn um einen generischen Schutz. Nach der Installation überwacht der G Data LNK-Checker im Hintergrund die Erstellung von Dateiverknüpfungssymbolen und unterbindet die automatische Ausführung von Programmcode.

Desktopsymbole mit gängigen und ungefährlichen Mechanismen werden wie gewohnt dargestellt. Wenn jedoch der schädliche Mechanismus erkannt wird, erscheint ein rotes Warnsymbol und unterbindet so die Infektion des Computers.

Achtung: Es gibt legitime Anwendungsbereiche für den aktuell missbrauchten Mechanismus. Ein Doppelklick auf eine als gefährlich markierte Dateiverknüpfung liegt daher weiterhin in der Hand der Anwender. Generell ist der Einsatz einer leistungsstarken Virenschutzlösung auf einem System nötig.

Sobald Microsoft die Sicherheitslücke geschlossen hat und der Nutzer das dazugehörige Windows-Update durchgeführt hat, kann das Programm „G Data LNK-Checker“ wie jede andere Software komplett deinstalliert werden. Der Hotfix funktioniert bei allen Windows Betriebssystemen ab Windows XP, sowohl in den 32-bit und den 64-bit Varianten. Geschützt sind auch Windows XP-Systeme mit Service Pack 2, obwohl der Support von Microsoft kürzlich eingestellt wurde.

Der G Data LNK-Checker ist unter folgendem Link erhältlich:  
<http://www.gdata.de/support/downloads/tools>

#### Hintergrund

Jeder PC mit einem Windows-Betriebssystem hat Verknüpfungen auf dem Desktop, mit einem Klick hat man so Zugriff auf die wichtigsten Programme und Dateien. Diese nützliche Funktion wird immer wieder von Malware missbraucht. So auch in einem gerade von Microsoft bestätigten Zero-Day-Exploit, der auf alle aktuellen Windows-Versionen zutrifft. Dabei wird der Mechanismus zur Anzeige von Icons auf eine spezielle Art ausgenutzt, um Schadcode auszuführen und letztlich die volle Kontrolle über den Rechner zu erlangen. Damit das funktioniert muss ein Nutzer lediglich die präparierte Dateiverknüpfung z.B. im Explorer, auf dem Desktop oder in einer Anwendung anzeigen.

Microsoft hatte umgehend reagiert und einen Lösungsvorschlag (Hotfix) erstellt, der aber dazu führt, dass alle Dateiverknüpfungen ihre Icons verlieren. Für den Anwender ist dies jedoch äußerst nachteilig.



Ralf Benzmüller, Leiter G Data SecurityLabs  
Detailansicht



G Data Software AG, Logo Detailansicht

#### Pressekontakt

Frau Kathrin Beckert

G Data Software AG  
Königsallee 178b  
44799 Bochum  
Deutschland

Email: [Kontakt aufnehmen](#)  
Website: [www.gdata.de](http://www.gdata.de)  
Telefon: +49.234.9762.376

#### Schlagworte

gdata sicherheitslücke hotfix  
dateisymbole viren trojaner  
schwachstelle windows

#### Permanenterlink

<http://www.themenportal.de/it-hightech/g-data-macht-aktueller-windwos-schwachstelle-den-garaus-76301>

