Verschlüsselungstrojaner GPcode ein Schnippchen schlagen

Statt den RSA-Schlüssel zu knacken, empfiehlt Kaspersky betroffenen Anwendern, die gelöschten Originale zu restaurieren. Die erforderlichen Tools gibt es kostenlos im Internet. Kaspersky hat eine detaillierte Anleitung dazu veröffentlicht.

News die Meldung vom 17.06.2008

Da das Knacken des vom Verschlüsselungstrojaner GPcode benutzten RSA-Schlüssels nach einhelliger Meinung derzeit kaum zu bewerkstelligen ist, schlägt Kaspersky nun betroffenen Anwendern alternativ vor, die gelöschten Originale wieder zu restaurieren. Dazu empfehlen sie den Einsatz des kostenlosen Datei-Rekonstruktionstools PhotoRec (http://www.cgsecurity.org/wiki/PhotoRec). Anders als der Name es vermuten lässt, kann das Tool nicht nur gelöschte Fotos wiederherstellen, sondern eine Vielzahl weiterer Dateiformate wie .doc, html, .pdf. txt, .zip, .mp3 und so weiter. Eine vollständige Liste findet sich unter "File Formats Recovered By PhotoRec" (http://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec).

Die Rekonstruktion funktioniert, weil GPcode die verschlüsselte Version eines Dokuments in eine neue Datei schreibt und anschließend das Original löscht. Da Windows aber nur die Referenz im Dateisystem löscht, ist die Datei weiterhin vorhanden und lässt sich erfolgreich rekonstruieren – solange der Anwender nicht allzu viel weitere Änderungen auf der Festplatte vorgenommen hat.

PhotoRec stellt aber alle gelöschten Dateien wieder her, auch solche, die der Anwender selbst und nicht GPcode gelöscht hat. Da das Tool zudem keine Pfade restaurieren kann, müsste man sich mühsam durch ein große Liste von Dateien arbeiten. Um diese Arbeit zu erleichtern, hat Kaspersky das Tool "StopGPcoder" (http://www.kaspersky.com/downloads/misc/stopgpcode_tool.zip) veröffentlicht, das durch einen Vergleich der verschlüsselten und restaurierten Dateien die richtigen herauszufinden versucht. Kaspersky hat eine detaillierte Anleitung (http://www.viruslist.com/en/viruses/encyclopedia?virusid=313444) aller erforderlichen Schritte und Download-Links in der Rubrik "File Recovery" zu der Beschreibung von GPcode veröffentlicht.

PhotoRec dient aber nicht nur Windows-Anwendern zu Rettung ihrer Daten. Es läuft auch unter Linux, FreeBSD, NetBSD, OpenBSD, Sun Solaris sowie Mac OS X und unterstützt die Dateisysteme FAT, NTFS, EXT2/EXT3-Dateisysteme und HFS+ auf unterschiedlichen Medien.

Laut einem Bericht von SecurityFocus hätte der mutmaßliche Autor von GPcode nach dem erfolgreichen Knacken des RSA-Schlüssels in künftigen Versionen die Schlüssellänge auf 4096 Bit erhöht, womit erfolgreiche Angriffe vollends außer Reichweite gelangt wären. Allerdings wäre dann zu überlegen, ob man sich nicht lieber dem Knacken des RC4-Schlüssels widmet.

Die Dateien selbst sind mit dem auf XOR-Verknüpfungen beruhenden Stromchiffre RC4 verschlüsselt, nur der RC4-Schlüssel ist mit RSA geschützt. RC4 gilt zwar als hinreichend sicher, allerdings nur, wenn er korrekt initialisiert wird und keine schwachen Schlüssel verwendet. Der WLAN-Verschlüsselungsstandard WEP gilt aufgrund schwacher Initialisierungsvektoren als mittlerweile leicht angreifbar.