

F-Secure warnt vor falschem Doktor: Ransom-Trojaner bittet zur Kasse!

München, 26. Januar 2010 – Die Idee ist nicht neu – ein Computerprogramm zu entwickeln, mit dessen Hilfe Online-Betrüger sensible Daten auf den Rechnern ihrer Opfer verschlüsseln und erst nach der Zahlung einer horrenden Summe wieder freigeben. Doch nun ist mit W32/DatCrypt ein neuer Trojaner aufgetaucht, der sich nicht als solcher ausgibt. Das Opfer wird lediglich darüber informiert, dass eine Datei beschädigt sei und eine Reparatur (gegen einen geringen Obolus) dieses Problem beheben könnte. Die finnischen Sicherheitsexperten von F-Secure raten deswegen: Der wirkungsvollste Schutz gegen diese Form der Online-Erpressung besteht in der Sicherung der Daten mittels Backup. Im Falle einer Attacke können die verschlüsselten Daten relativ einfach und bei regelmäßiger Sicherung nahezu verlustfrei wieder gewonnen werden.

Mikko Hyppönen, Chief Research Officer bei F-Secure zu der Problematik mit Ransomware: „Der W32/DatCrypt-Trojaner infiziert den PC und gaukelt seinem Benutzer vor, dass Dokumente, Videos, Musik und Bilder beschädigt seien. In Wahrheit aber arbeitet der Schädling bereits im Hintergrund, verunsichert den User mit täuschend echt aussehenden Windowsbotschaften und fordert zum Download einer ‚Reparatursoftware‘ namens Data Doctor 2010 auf.“

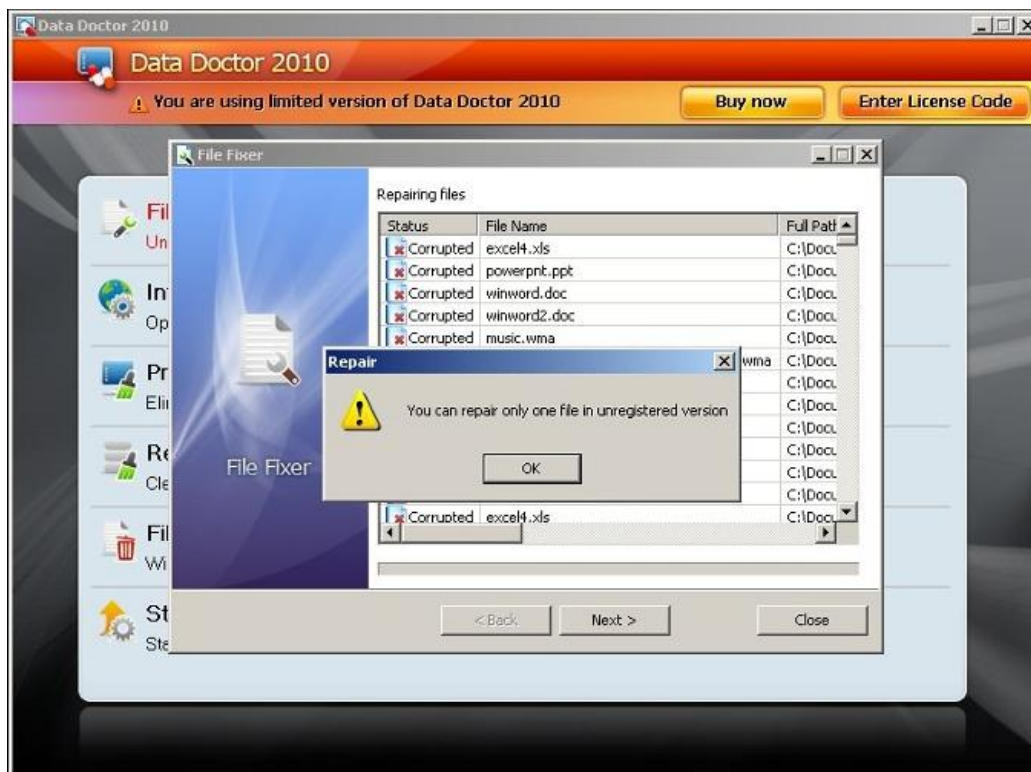
Kontakte für die Presse:

Sandra Proske
F-Secure GmbH
 Zielstattstraße 44
 81379 München

Tel.: +49 89 787 467-22
 Fax: +49 89 787 467-99
sandra.proske@f-secure.com
www.f-secure.de

Berk Kutsal / Jürgen Rast
Trademark PR GmbH
 Goethestraße 66
 80336 München

Tel.: +49 89 444.467-461
 Fax: +49 89 444.467-479
f-secure@trademarkpr.eu
www.trademarkpr.eu



Einmal heruntergeladen und installiert erhält der User folgende Nachricht: „Eine nicht registrierte Version berechtigt nur zum Reparieren einer Datei. Um weitere Dateien entschlüsseln zu können, benötigen Sie die Vollversion zum Preis von 89,95 US-Dollar. Sobald das Geld bezahlt worden ist, wird der Zugriff auf sämtliche Dateien wieder freigegeben.“

Mikko Hypponen führt weiter aus: „Der Trojaner geht dabei äußerst hinterhältig vor. Der Benutzer setzt in der Regel alle Hebel in Bewegung, um an seine Daten zu kommen, vergisst dabei aber, dass er gerade im Begriff ist, teures Geld zu bezahlen. Einige User empfehlen das Produkt sogar im Freundeskreis weiter, ohne sich über die Konsequenzen bewusst zu sein. Vergleichbare Ransomware setzt dabei auf einen seit Jahren bekannten Trick – File Fix Pro Utility.“ Einer der ersten Angreifer, der Ransomware zur Verbreitung über das Internet einsetzte, war der Trojaner TROJ_PGPCODER.A, der nach seiner Infizierung mehrere hundert US-Dollar zur Entschlüsselung forderte.

Der kriminelle Beutezug gelingt allerdings nur dann, wenn der Benutzer seine wichtigen Dateien nicht regelmäßig sichert. Die finnischen Sicherheitsexperten empfehlen daher, Dokumente, Videos, Musik und Bilder turnusmäßig mittels Backup zu archivieren. F-Secure bietet seinen Kunden beispielsweise ein bequemes und unbegrenztes online Backup an.

Screenshots zum DatCrypt-Trojaner sind unter folgendem Link zu finden:

<http://www.f-secure.com/weblog/archives/00001850.html>

Über F-Secure

Innovation, Zuverlässigkeit und Schnelligkeit – diese drei Qualitäten haben F-Secure seit der Gründung 1988 zu einem der führenden IT-Sicherheitsanbieter weltweit gemacht. Heute vertrauen sowohl Millionen Privatanwender als auch Unternehmen auf die mehrfach ausgezeichneten Lösungen von F-Secure. Der effektive Echtzeitschutz arbeitet zuverlässig und unbemerkt im Hintergrund und macht das vernetzte Leben von Computer- und Smartphone-Nutzern sicher und einfach.

Die Lösungen von F-Secure sind als Service-Abonnement über mehr als 200 Internet Service Provider und Mobilfunkbetreiber weltweit zu beziehen. Die umfangreichen Partnerschaften machen F-Secure zum Marktführer in diesem Bereich. Seit 1999 ist das Unternehmen an der Börse in Helsinki notiert. Seitdem wächst F-Secure schneller als viele andere börsennotierte Mitbewerber.

Ständig aktuelle Informationen über die neuesten Viren finden sich im Weblog des „F-Secure Antivirus Research Teams“ unter der Internetadresse www.f-secure.com/weblog.