Inhalt

Ransomware lautet die Bezeichnung für eine inzwischen recht weit verbreitete Art von Trojanern. Entweder sperrt die Schadsoftware den kompletten Rechner oder den Zugang zu wichtigen Daten wie E-Mails, Datenbanken, Fotos und den „Eigenen Dateien“. Dabei setzt Ransomware sogar Verschlüsselung ein. Ein Zugriff auf die „entführten“ Dateien ist also, sofern die Verschlüsselung ordentlich umgesetzt wurde, tatsächlich nicht mehr möglich. Wie nicht anders zu erwarten, verspricht der Trojaner, den Zugang zu den Daten wieder frei zu geben, wenn man ein „Lösegeld“ an die Kriminellen überweist. Meist wird als Zahlungsmethode **Ukash** verwendet. Ein Bezahlsystem, bei dem der Empfänger anonym bleibt.

Unnötig zu erwähnen, dass nach der Zahlung nichts geschieht. Die Dateien bleiben „gekidnappt“ und sind verloren.

„Es ist die ungesetzliche Tätigkeit enthüllt“ *

So der etwas holprige Hinweis des **BKA-Trojaners**, der sich bereits Anfang 2011 in diesem Umfeld einen Namen machte. Diese inzwischen in zahlreichen Varianten verbreitete Schadsoftware behauptete, den Rechner zu sperren, weil sich auf ihm Raubkopien und kinderpornografische Inhalte befänden. Die Freigabe des Rechners erfolge nach Zahlung.

Das entführte Facebook Konto *

Jetzt schlägt eine Variante des **Trojaners Carberp** zu und erpresst **Facebook** Nutzer. Dieser Schädling gibt vor, den Zugang zum Facebook-Konto gesperrt zu haben. In Wahrheit fängt er einfach alle Anfragen an Facebook-Server lokal im Browser ab und gibt eine Warnmeldung mit einem Hinweis aus. Bei Carberb ist man bereits mit 20 EURO dabei. Natürlich soll die Zahlung auch hier via Ukash erfolgen. Ich muss es

eigentlich nicht erwähnen, nach Zahlung geschieht nichts. Leider hat Carberp zusätzliche Waffen mit an Bord. Er kann ferngesteuert werden und dient damit als Werkzeug, mit dem die kriminellen Betreiber des Botnetzes den Rechner beliebig kontrollieren können.

Als Verbreitungsmedium kommen anscheinend vor allem manipulierte PDF und Office Dokumente zum Einsatz.

Leider kann man in diesem Zusammenhang nur die folgenden allgemeinen Empfehlungen geben:

1. Sichern Sie Ihre Daten regelmäßig
2. Halten Sie Ihr Betriebssystem auf dem neusten Stand
3. Halten Sie Ihren Browser auf dem neusten Stand
4. Öffnen Sie nicht wahllos E-Mails und klicken Sie nicht unbedacht auf Links in E-Mails. Gesundes Misstrauen ist angebracht.
5. Investieren Sie etwas Geld in eine ordentliche Anti-Viren Software, die regelmäßige Updates zur Verfügung stellt.
6. Zahlen Sie nicht, wenn Ihre Daten gekidnappt werden. Finden Sie sich mit dem Verlust ab.

Die Seite http://www.bundespolizei-virus.de/ hat es sich zur Aufgabe gemacht, speziell diesen Trojaner zu thematisieren, seine Hintergründe näher zu beleuchten und Mittel und Maßnahmen bereitzustellen, mit denen sich diese lästige und gefährliche Art von Computerschädling beseitigen lässt.

Quellen:
http://bka-trojaner.de/

http://winfuture.de/news,67661.html

