G Data warnt vor Erpresser-Trojaner Spora

Die Ransomware Spora macht manches anders als andere Erpresser-Trojaner: So verbreitet sie sich wie ein Wurm und verlangt ein individuelles Lösegeld.

Der Antivirushersteller G Data hat den Erpresser-Trojaner Spora analysiert, der sich vor allem über verseuchte E-Mails und USB-Speicher verbreitet. Nach Angaben von G Data ist Spora eine besonders gefährliche Kombination aus Ransomware und Wurm. Zur Verbreitung setzt Spora Data auf Verknüpfungen. Ein ähnliches Verhalten haben bereits die Schädlinge Dinihou und Gamarue gezeigt. Vor kurzem hatte G Data seine Prognosen für das Jahr 2017 veröffentlicht und dabei bereits vor allem vor Ransomware gewarnt.

Gefährliche Verknüpfungen

Spora versteckt alle Dateien und Ordner auf dem Desktop sowie den Hauptverzeichnissen von Speichermedien und dem Systemlaufwerk mit dem Dateiattribut "Hidden". Um keinen Verdacht zu erregen, ersetzt die Malware die versteckten Elemente dann durch gleichnamige Verknüpfungen mit den gleichen Dateisymbolen.

Klickt ein Anwender auf eine der Verknüpfungen, öffnet er nicht nur die Originaldatei, sondern startet auch die Malware. Dadurch wird Spora ausgeführt, selbst wenn der Anwender nur eine vermeintlich harmlose Aktion wie etwa das Öffnen eines Ordners auf dem Desktop beabsichtigt.

Pfiffige Verschlüsselung

Hat Spora einmal einen Rechner infiziert, beginnt der Schädling mit der Verschlüsselung von Dateien. Dazu sucht die Ransomware nach Dateien mit den Endungen .backup, .7z, .rar, .zip, .tiff, .jpeg, .jpg, .accdb, .sqlite, .dbf, .1cd, .mdb, .cd, .cdr, .dwg, .psd, .pdf, .odt, .rtf, .docx, .xlsx, .doc und .xls. Bei der Verschlüsselung werden die Dateinamen nicht verändert. Als Schlüssel verwendet Spora ein RSA-Schlüsselpaar mit einer Länge von jeweils 1.024 Bit.

Dank einem relativ komplizierten Verschlüsselungsschema, das G Data in einem Blog-Post ausführlich erläutert, muss der Trojaner keinen Schlüssel von einem Command & Control-Server (C&C-Server) beziehen und kann deshalb autark arbeiten. Die Opfer sollen die KEY-Datei mit dem verschlüsselten privaten Schlüssel auf einer speziellen Webseite hochladen. Erst nach dem Upload berechnen die Kriminellen dann das geforderte Lösegeld. Es ist abhängig von der Zahl der verschlüsselten Dateien. Darin sehen die Analysten von G Data "eine Raffinesse, die das Schadprogramm zum neuen Locky machen könnte".