Erpressungs-Trojaner VirLocker mit Fleißarbeit auf die Matte schicken

27.01.2017

Die Ransomware VirLocker verbreitet sich wurmartig. Doch verschlüsselte Dateien kann man mit 64 Nullen und vielen Mausklicks retten.

VirLocker treibt schon seit 2014 immer mal wieder sein Unwesen, infiziert Windows-Computer, verschlüsselt Dateien und fordert Lösegeld. Aktuell ist der Schädling wieder in Umlauf, berichten Sicherheitsforscher von Malwarebytes.

Der Erpressungs-Trojaner ist besonders heimtückisch: Er verschlüsselt nicht nur Daten, sondern bettet diese in ausführbare .exe-Dateien ein, die wiederum auch den Schädling enthalten. Führt man eine derartige Datei auf einem anderen Computer aus, infiziert sich auch dieser mit VirLocker.

Umsonst entschlüsseln

Wer sich den Trojaner eingefangen hat, muss aber nicht verzweifeln: Opfer bekommen ohne das Lösegeld zu zahlen und sogar ohne Entschlüsselungstool wieder Zugriff auf ihre Daten. Bevor man die folgenden Tipps befolgt, sollte man den infizierten Computer vom Netzwerk trennen, damit VirLocker sich nicht weiter verbreiten kann.

Um wieder Zugriff auf verschlüsselte Daten zu bekommen, muss man Malwarebytes zufolge lediglich 64 Zeichen im Feld "Transfer ID" des Lösegeldformulars eingeben. In ihrem Beispiel funktionierte das eigenen Angaben zufolge mit 64 Nullen. Aufgrund eines Bugs ist das Lösegeld nach der Eingabe beglichen und VirLocker gibt die Daten wieder frei. Wie lange das auf diesem Weg noch funktioniert, ist derzeit unbekannt. Den Malware-Entwicklern ist natürlich daran gelegen, diesen Fehler zügig auszubessern.

Klick für Klick

Nach dem Vortäuschen der Lösegeldzahlung muss man jede .exe-Datei von Hand anklicken, damit die Original-Datei wiederhergestellt wird. In diesem Fall wird nicht die Ransomware ausgeführt, sondern die eingesperrte Datei entpackt.

Anschließend sollte man die wiederhergestellten Daten auf eine externe Festplatte kopieren und den infizierten Computer komplett neu aufsetzen. Das Opfer sollte in jedem Fall darauf achten, keine der infizierten .exe-Dateien mitzuschleppen; ansonsten infiziert sich ein frisch installierter Computer gleich wieder. (des)