Dennis Schirrmacher

TeslaCrypt 2 geknackt

Dechiffrierte Dateien mit TeslaDecoder lesbar machen

Kriminelle machen oft Fehler bei kryptografischen Operationen von Verschlüsselungstrojanern – zum Glück für die Opfer. Allerdings fixen neue Versionen Unachtsamkeiten und lassen die Bedrohung erneut aufflammen. Doch es gibt Tipps und Vorgehensweisen, wie man seiner Daten wieder habhaft wird.

Malware-Entwickler haben es heutzutage nicht ausschließlich auf Nutzerdaten abgesehen, sondern erpressen Opfer auch mit Verschlüsselungstrojanern, welche Dateien chiffrieren. Den Schlüssel wollen Kriminelle nur gegen Lösegeld rausrücken. Opfer von TeslaCrypt 2 können nun aber aufatmen: Aufgrund mangelnder Sorgfalt der Malware-Entwickler bei der Umsetzung kryptografischer Verfahren können Betroffene ihre persönlichen Daten mit dem kostenlosen Tool TeslaDecoder dechiffrieren. Doch der ausgebesserte Nachfolger TeslaCrypt 3 ist bereits im Umlauf. Der erstellt Dateien mit den Endungen .micro, .mp3, .ttt, oder .xxx und die lassen sich derzeit nicht retten.

TeslaDecoder funktioniert aktuell nachträglich bis zur Version TeslaCrypt 2.2.0, die verschlüsselte Dateien mit den Endungen .aaa, .abc, .ccc, .ecc, .exx, .vvv, .xyz und .zzz erzeugt. Wer also geduldig war und seine verschlüsselten Dateien aufbewahrt hat, kann sich glücklich schätzen. Die Erpresser fordern für die Entschlüsselung umgerechnet über 400 Euro; mit TeslaDecoder geht es auch ohne Lösegeld.

Die Drahtzieher hinter der Malware schüchtern Opfer mit der Behauptung ein, ihre Daten wären mit starker Verschlüsselung wie RSA-2048 oder sogar RSA-4096 chiffriert. Doch das ist nicht der Fall. Würde TeslaCrypt RSA richtig einsetzen, könnte man sich daran lange die Zähne ausbeißen.

Dateien verschlüsselt die Ransomware mit symmetrischen AES-Schlüsseln. Damit die geschützt sind, kommt eine Form der Public-Key-Verschlüsselung zum Einsatz, um die AES-Schlüssel zu chiffrieren. Doch bei TeslaCrypt 2 haben die Kriminellen an dieser Stelle offensichtlich gepfuscht: Im Kopf jeder verschlüsselten Datei findet sich das Produkt zweier Schlüssel. Dieses setzt sich aus dem geheimen AES-Schlüssel und einem geheimen ECDH-Schlüssel zusammen. Bei ECDH handelt es sich um Diffie Hellman auf elliptischen Kurven. Dieses Verfahren wird eigentlich nicht zur Verschlüsselung eingesetzt, sondern zum Schlüsselaustausch.

Der ECDH-Einsatz kommt Opfern zugute, denn Kryptografie auf elliptischen Kurven setzt vergleichsweise sehr kurze Schlüssel ein. Das Produkt aus dem AES- und ECDH-Schlüssel ist demzufolge keine sonderlich große Zahl und lässt sich schon auf herkömmlichen Desktop-Systemen mit Open-Source-Software wie YAFU in endlicher Zeit in seine Primfaktoren zerlegen.

Dateien enträtseln

Das Tool TeslaDecoder zum Dechiffrieren von Dateien wurde von der Community der IT-Webseite BleepingComputer entwickelt und ist über den c't-Link abrufbar. Dort finden sich neben weiteren Tools noch Anleitungen. Obacht: Beim Download von TeslaDecoder kann sich ein Viren-Wächter mit einer Warnung melden. Auf unserem Test-System konnten wir keine bösartigen Aktivitäten beobachten; wir vermuten einen Fehlalarm. Wer TeslaDecoder nicht traut, kann sein Glück mit dem Open-Source-Kommandozeilen-Script TeslaCrack auf Github versuchen.

TeslaDecoder kommt zusätzlich noch mit den Anwendungen TeslaRefactor und TeslaViewer. Um den Prozess der Dechiffrierung einzuleiten, füttert man TeslaViewer mit einer verschlüsselten Datei. Anschließend wird das Produkt aus Shared Secret und Private Key extrahiert: Darin versteckt sich der gesuchte AES-Schlüssel. Auf der Webseite www.factordb.com kann man prüfen, ob das Produkt bereits faktorisiert wurde. Das ist der Fall, wenn beim Status FF steht. Mit den Faktoren lässt sich der private Schlüssel via TeslaRefactor ohne weitere Zwischenschritte errechnen. Alle anderen Statuswerte machen eine Faktorisierung unumgänglich.

Das übernimmt YAFU auf Basis des Dezimalwerts des Produkts „SharedSecret1*PrivateKeyBC“, das man der Ausgabe von TeslaViewer entnehmen kann. Der Prozess war im Test mit einem Core-i5-Prozessor bereits nach 20 Sekunden erfolgreich abgeschlossen. Das ging so schnell, weil unsere Zahl viele kleine Primfaktoren enthielt, die sehr schnell gefunden wurden. Unter Umständen kann dieser Vorgang den Entwicklern von TeslaDecoder zufolge auch mehrere Tage dauern. Mit den Faktoren füttert man nun die Refactor-Batchdatei. Als Ergebnis spuckt TeslaRefactor den privaten Schlüssel aus, bei dem nicht ganz klar ist, ob das schon der AES- oder der zum Public Key gehörende Schlüssel ist. Die Entwickler verwenden zum Teil sehr eigenwillige Bezeichnungen. Auf Basis des Schlüssels kann TeslaDecoder jedenfalls verschlüsselte Dateien dechiffrieren. Im Test gelang das erfolgreich mit .vvv-Dateien. Anschließend ließ sich eine mit TeslaCrypt verschlüsselte PDF-Datei problemlos öffnen.

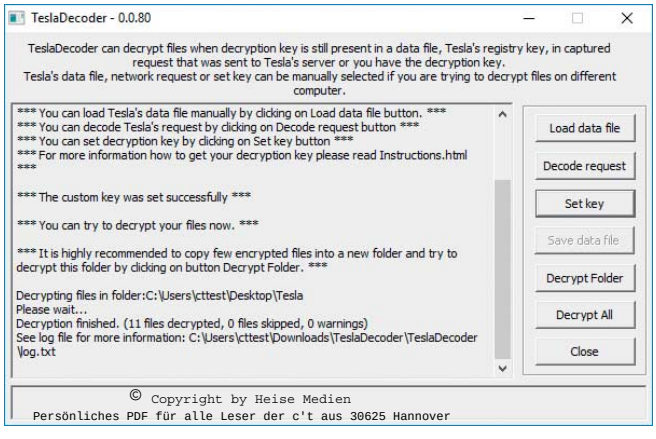
Die Ransomware nutzt zur Laufzeit für alle Dateien den gleichen AES-Schlüssel, sodass man in einem Rutsch gleich mehrere Dateien dechiffrieren kann. Bei einem Neustart erzeugt TeslaCrypt aber einen neuen AES-Schlüssel. In so einem Fall muss man die hier dokumentierten Schritte erneut durchführen.

Nach einer Infektion

Wen es erwischt hat, der sollte umgehend alle externen Datenträger und Netzwerklaufwerke trennen, denn der Verschlüsselungstrojaner macht vor diesen nicht Halt. Sind bereits Dateien chiffriert, gibt es die Hoffnung, dass schon ein Entschlüsselungstool existiert (siehe c't-Link). Ist das nicht der Fall, sind hoffentlich Backups vorhanden. Wer keine Backups hat, kann versuchen, die betroffene Festplatte mit Tools wie ShadowExplorer nach Schattenkopien der ursprünglichen Dateien zu durchsuchen. Auch Datenrettungsprogramme wie Recuva sind einen Versuch wert. Doch in der Regel schieben Verschlüsselungstrojaner derartigen Hilfsmitteln einen Riegel vor und verschlüsselte Dateien sind vorerst verloren. Chiffrierte Daten sollte man auf jeden Fall aufbewahren. Noch besser ist es, ein Image der gesamten Platte zu sichern. Denn oft werden zur nachträglichen Entschlüsselung zusätzliche Informationen etwa aus der Registry benötigt.

Wer dringend auf seine Daten angewiesen ist und überlegt, das Lösegeld zu bezahlen, sollte aufpassen: Die Zahlung an die Erpresser ist keine Garantie, dass diese den Schlüssel zur Dechiffrierung rausrücken oder dass die Entschlüsselung funktioniert. Wer auf der sicheren Seite sein will, sollte im Computer-Alltag stets wachsam sein, zyklisch Sicherheitspatches einspielen und wichtige Daten regelmäßig auf einen nicht permanent am Computer angeschlossenen Datenspeicher ablegen. (des@ct.de)

c't Anleitungen und Tools: ct.de/yaay



TeslaDecoder kommt schlicht daher, ist für Opfer von TeslaCrypt 2 aber die letzte Rettung, eigene Dateien wieder öffnen zu können.