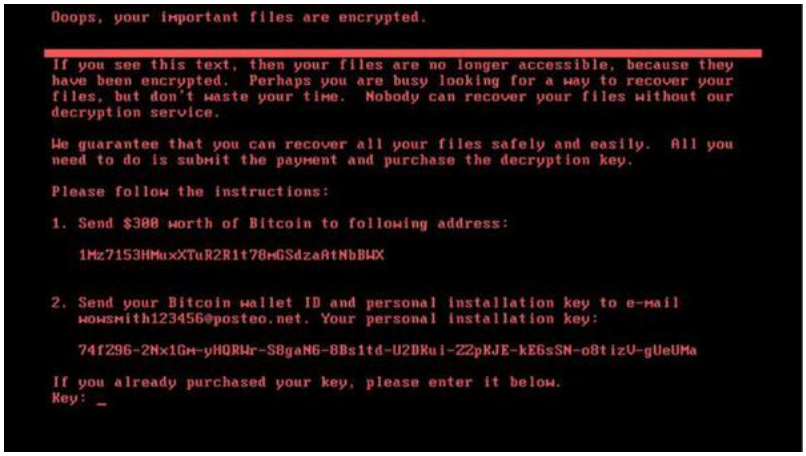
Verschlüsselung knackbar: Hoffnung für (manche) NotPetya-Opfer

11.07.2017 13:36 Uhr – Fabian A. Scherschel vorlesen



NotPetya-Erpressungsbildschirm

Die Entwickler des Verschlüsselungstrojaners NotPetya haben entscheidende Fehler bei der Umsetzung ihrer Verschlüsselung gemacht. Unter bestimmten Umständen lässt sich diese knacken. Automatische Tools wird es aber wohl erst einmal nicht geben.

Nachdem die Autoren der Goldeneye-Trojanerfamilie, zu der auch Petya gehört, den Masterschlüssel für diese Erpressungstrojaner veröffentlicht haben, gibt es Hoffnung für Opfer, deren Festplatten verschlüsselt wurden. Da es sich bei NotPetya aber um keinen Abkömmling dieser Familie sondern um das Werk eines Trittbrettfahrers (ob Cyberkrimineller oder Cyberterrorist sei dahingestellt) handelt, kann dieser Schlüssel nicht verwendet werden, um den Opfern des neuesten Ransomware-Ausbruchs zu helfen. Laut Sicherheitsforschern von Positive Technologies gibt es aber dennoch Hoffnung – unter bestimmten Umständen.

Trojaner mit Admin-Rechten: In diesem Fall ein gutes Zeichen

Wird ein Rechner mit NotPetya infiziert, versucht der Trojaner sich Administrator-Rechte zu verschaffen. Schlägt dies fehl, verschlüsselt der Nutzerdaten mittels AES. Das Betriebssystem funktioniert dann weiterhin, aber die wichtigsten Daten sind futsch. Um diese Daten zu retten, braucht man den geheimen RSA-Schlüssel, den die Kriminellen angeblich in Untergrundforen für horrende 100 Bitcoin verkaufen. Ob das wirklich funktioniert, ist unbekannt. Bisher haben Sicherheitsforscher auch keine Möglichkeit gefunden, die Verschlüsselung der Daten zu knacken.

Hat es NotPetya allerdings beim Einbruch in den Rechner geschafft, Administrator-Rechte zu ergattern, verschlüsselt der Trojaner die gesamte Festplatte mit Salsa20 und verhindert so, dass das Betriebssystem gebootet werden kann. Zwar gilt der Salsa20-Algorithmus ähnlich wie AES als sicher, allerdings scheint es so, als hätten die Malware-Schreiber bei der Umsetzung entscheidende Fehler begangen. Diese führen unter anderem dazu, dass aus dem 256 Bit langen Schlüssel nur 128 Bits für die eigentliche Verschlüsselung verwendet werden. Das reicht aber leider noch nicht, um die Verschlüsselung knackbar zu machen.

Virenschreiber machten Fehler bei der Verschlüsselung

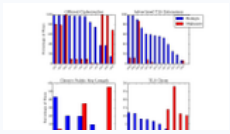
Die NotPetya-Macher haben aber eine ganze Reihe weiterer Fehler begangen, die die resultierende Verschlüsselung angreifbar machen. Der Hebel für die Datenrettung ist eine sogenannte Known-Plaintext-Attacke. Anhand bekannter Daten, die auf Windows-Partitionen immer gleich sind, kann die falsch implementierte Salsa20-Verschlüsselung so gebrochen werden. Das bedeutet allerdings eine Menge Aufwand und ist mit automatischen Entschlüsselungstools nicht zu leisten, erklären die Forscher. Allerdings sind sie zuversichtlich, dass professionelle Datenretter und Forensik-Teams die Verschlüsselung innerhalb einiger Stunden knacken können. Vor allem für Firmen, denen sehr wichtige Geschäftsdaten abhanden gekommen sind, ist das immerhin ein kleiner Hoffnungsschimmer.

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

Artikel

Cisco analysiert verschlüsselten Traffic, um Malware zu erkennen



Mit Hilfe von Machine Learning gelang es einer Forschergruppe, den verschlüsselten Netzwerk-Verkehr von Malware von regulärem zu unterscheiden – und das, ganz ohne ihn zu entschlüsseln.

Windows-Diagnose: Programme und Prozesse meistern

Wer mehr über das wissen will, was unter der Haube von Windows so vorgeht, kommt weder am Task-Manager noch am Sysinternals-Tool ProcMon vorbei.

Analysiert: Alte Masche, neue Verpackung – Infektion durch PDFs

Manipulierte Word-Dokumente sind bei Kriminellen beliebt, um Computer mit Malware zu infizieren. Dass auch PDF-Dateien ausführbaren Code enthalten können, ist hingegen ein wenig in Vergessenheit geraten. Eine unlängst grassierende Spam-Kampagne ist ein guter Grund, sich diese Gefahr anhand eines frischen Samples in Erinnerung zu rufen.

Aber auch andere Opfer sollten ihre NotPetya-verschlüsselten Platten aufbewahren. Es ist nicht ausgeschlossen, dass Sicherheitsforscher in Zukunft weitere Schwachstellen in der Verschlüsselung der Trojaners finden. Immerhin haben dessen Entwickler bereits mehrere Fehler beim Bau ihrer Verschlüsselungsroutinen gemacht. (fab)

Kommentare lesen (9 Beiträge)

Forum zum Thema: **Viren & Würmer**

https://heise.de/-3768889 Drucken

Mehr zum Thema **Datenrettung** **Ransomware** **Malware** **Verschlüsselung**

Neueste Forenbeiträge

Re: Tolle Wurst!

SomeoneYouKnow schrieb am 12.07.2017 13:41: Zeitmaschine :-D Ich bin da schon etwas neidisch. Ob er auch morgen die Lottozahlen schon am…

Forum: Patchday bei Microsoft: Erneut SMB-Sch…

von DAC324; 12.07.2017 14:16

Unter Windows 8.1...

...sollte sich ja der MS Updater um das Flash-Update kümmern. Aber schon seit 1 Monat meldet mir Secunias PSI, dass mein Flash veraltet wäre.

Forum: Patchday bei Microsoft: Erneut SMB-Sch…

von hurgaman2; 12.07.2017 14:12

Re: Direkter Download (Deep Links)

You are the hero we don't deserve. Danke!

Forum: Patchday: Adobe stopft kritische Flash-L…

von flixs; 12.07.2017 14:09

Der Kommentar

1 2 3 4 5

Warum wir Forward Secrecy brauchen

Der SSL-GAU zeigt nachdrücklich, dass Forward Secrecy kein exotisches Feature für Paranoiker ist. Es ist vielmehr das einzige, was uns noch vor einer vollständigen Komplettüberwachung aller Kommunikation durch die Geheimdienste schützt.