c't - Magazin für Computertechnik, 07/2016, S. 82

Schädlinge eliminieren, Daten retten

Erste Hilfe für Opfer

Wenn Locky & Co. zugeschlagen haben, ist die Katastrophe komplett und der Zugriff auf persönliche Daten versperrt. Doch es gibt zumindest einen Lichtschimmer am Ende des Tunnels: Mit verschiedenen Tools und Vorgehensweisen können Opfer ihre Daten unter Umständen zurückerobern, ohne Lösegeld zu zahlen.

Seit Anfang dieses Jahres kontaktieren c' t zunehmend verzweifelte Leser und fragen, ob sie ihre von Erpressungs-Trojanern verschlüsselten Daten auf irgendeinem Weg zurückbekommen können, ohne Lösegeld zu zahlen. Wenn gewisse Voraussetzungen erfüllt sind, kann man diese Frage durchaus mit Ja beantworten.

Unsere Erfahrungen mit infizierten Systemen zeigen aber, dass die Aussichten nicht rosig sind. Das bestätigt auch Stephan Bäcker vom IT-Dienstleister Trebaxa, der regelmäßig infizierte Computer von Kunden bereinigt und versucht, Daten zu retten. Erfolg hat er dann, wenn es Backups gibt, aus denen er zuvor gesicherte Daten nach der Infektion zurückspielen kann. Nur sehr selten gelang es ihm, ohne Backups Daten zu retten.

Über die Zahlung des Lösegelds sollte man vorerst nicht nachdenken. Betroffenen empfiehlt das Landeskriminalamt (LKA) Niedersachsen, in jedem Fall Anzeige zu erstatten; das geht in manchen Bundesländern sogar online.

Im ersten Schritt müssen Opfer herausfinden, welcher Krypto-Trojaner ihren Computer befallen hat. Dabei hilft die Tabelle auf Seite 85. Dort finden sich Informationen zu den meistverbreiteten Erpressungs-Trojanern. Der Schädling lässt sich meist an den Namenszusätzen der verschlüsselten Dateien identifizieren: In der Tabelle sieht man auf einen Blick, ob es dafür ein kostenloses Entschlüsselungs-Tool gibt.

Schädling loswerden

Vor einer Datenrettung muss man sich den Schädling erst mal vom Hals schaffen. Oft geschieht das sogar von selbst, denn Erpressungs-Trojaner beenden sich nach getaner Arbeit nicht nur automatisch, sondern löschen sich auch direkt - um Spuren zu verwischen. Das ist zum Beispiel bei Locky der Fall, wie wir bei Test-Infektionen beobachten konnten. Ein Scan mit einem Virenschutzprogramm ist dennoch obligatorisch, um auf Nummer sicher zu gehen.

Verschlüsselungs-Trojaner auf frischer Tat zu ertappen, gestaltet sich als schwierig: Die Macher der Malware veröffentlichen regelmäßig aktualisierte Versionen. Demzufolge kann es durchaus Stunden oder sogar Tage dauern, bis Viren-Wächter den Schädling vor oder während einer Infektion erkennen. Erschwerend kommt hinzu, dass ein Verschlüsselungs-Trojaner vergleichsweise wenig im System anrichtet, weshalb die Heuristik und Verhaltensanalyse des Wächters oft nicht zuschlagen.

Hat man den Verdacht, dass der Trojaner gerade aktiv ist, sollte man den Computer umgehend hart ausschalten und vorerst nicht neu starten. Stattdessen empfiehlt es sich, ein Live-System zu booten und von dort aus die Windows-Partitionen zu scannen. Den lokalen Viren-Wächter sollte man nicht nutzen: Dafür müsste das infizierte System gestartet werden, was die Situation weiter verschlimmern könnte. Als Live-System eignet sich etwa Desinfec' t [1]. Damit geht die Suche besonders komfortabel vonstatten, da sich Desinfec' t gleich mit vier Viren-Scannern auf die Jagd begibt. Alternativ können Betroffene auch ein Boot-Medium eines Antiviren-Herstellers nutzen. Ist der Schädling eliminiert, kann man sich einen Überblick verschaffen, ob der Erpressungs-Trojaner sein Werk vollenden konnte oder Dateien verschont hat.

Beste Lösung: Backup

[Seitenwechsel auf Seite: 83]Wer seine Daten regelmäßig auf einer nicht dauerhaft am Computer angeschlossenen Festplatte sichert, kommt relativ glimpflich davon. Denn das Zurückspielen eines kompletten System-Backups oder einzelner Daten geht vergleichsweise leicht von der Hand. Anschließend hat man wieder Zugriff auf den zuletzt gesicherten Zustand; verloren sind allenfalls danach hinzugekommene Dateien.

Übrigens: Wenn man ein Backup zurückspielt, sollte man dies am besten aus einem frisch installierten Betriebssystem heraus tun. Denn wenn trotz aller Reinigungsaktionen noch Teile des Erpressungs-Trojaners auf dem Computer schlummern, kann dieser die ganze Arbeit in Sekunden vernichten und verschlüsselt im schlimmsten Fall noch das Backup-Speichermedium.

Entschlüsselungs-Tools

Es ist bereits vorgekommen, dass Malware-Entwickler die Segel gestrichen haben und die Schlüssel vom Trojaner an die

Öffentlichkeit gelangt sind. Das war etwa im Sommer 2015 bei Locker der Fall. Dabei wurden nicht nur die Schlüssel veröffentlicht: Der Verschlüsselungs-Trojaner erhielt von den Machern sogar den Befehl, alle Daten wieder zu dechiffrieren. Darauf können Locky-Opfer nicht hoffen, da sich diese Malware selbstständig löscht.

Es gibt auch Einzelfälle, in denen Ermittlungsbehörden Erpresser-Banden hochnehmen und Schlüssel beschlagnahmen. So wurden im April 2015 die Drahtzieher hinter Bitcryptor und Coinvault verhaftet. Kaspersky hat alle Schlüssel in sein kostenloses Dechiffrierungs-Tool Ransomware Decryptor gepackt. Damit können Opfer verschlüsselte Dateien mit der Endung .clf wieder lesbar machen.

Bei TeslaCrypt ist noch niemand an die geheimen Schlüssel gekommen; das Dechiffrierungs-Tool TeslaDecrypt kann diese aber rekonstruieren. Das funktioniert mit Dateien, die mit TeslaCrypt bis Version 2.2 verschlüsselt wurden.

Derartige Werkzeuge sollten Betroffene aber nur mit Kopien der chiffrierten Dateien ausprobieren. Wenn hier etwas schiefgeht, driften die Daten endgültig ins digitale Nirwana ab. Bei TeslaDecoder greifen verschiedene Tools ineinander: Als erstes öffnet man mit TeslaViewer eine verschlüsselte Datei. Anschließend wird das Produkt zweier Schlüssel angezeigt, in dem sich der AES-Schlüssel versteckt. Den ermittelten Wert reicht man an Yafu weiter, das ihn in seine Primfaktoren zerlegt. Das dauert auf Desktop-Systemen typischerweise ein paar Minuten, kann bei einem sehr großen Wert aber auch mehrere Tage in Anspruch nehmen. Aus den errechneten Faktoren kann TeslaRefactor den benötigten Schlüssel rekonstruieren. Dieser landet schließlich im TeslaDecoder, der damit mehrere Dateien in einem Rutsch entschlüsselt.

Weisen verschlüsselte Dateien jedoch die Endungen .micro, .mp3, .ttt oder .xxx auf, hilft TeslaDecoder nicht weiter. Diese Dateien wurden mit TeslaCrypt 3 chiffriert, dessen Verschlüsselung bisher nicht geknackt wurde.

Selbst wenn es noch kein Entschlüsselungs-Tool gibt, sollte man die chiffrierten Daten unbedingt aufbewahren. Am besten sichert man das komplette System als Image. Denn in Einzelfällen müssen Entschlüsselungs-Tools auf die Registry oder bestimmte Dateien eines infizierten Systems zurückgreifen. Zur Erstellung von Images kann man Acronis True Image, Paragon Partition Manager oder das kostenlose Clonezilla einsetzen.

Alle in diesem Abschnitt und in der Tabelle erwähnten Recovery-Werkzeuge sind über den c' t-Link abrufbar. Dort finden sich auch Schritt-für-Schritt-Anleitungen.

Helfen Schattenkopien?

Immer wieder stolpern Opfer von Erpressungs-Trojanern über den Begriff Schattenkopien, wenn sie nach Hilfe suchen. Über den Volume Shadow Copy Service (VSS) legt [Seitenwechsel auf Seite: 84]Windows Schattenkopien bestimmter Dateien an. Bei VSS handelt es sich um einen Systemdienst, der Versionsstände erzeugt. Die standardmäßig aktivierte Systemwiederherstellung greift auf solche Schattenkopien zurück. Auf diesem Weg kann man Windows zwar auf einen Zeitpunkt vor der Infektion zurücksetzen, doch verschlüsselte Nutzerdaten bleiben chiffriert. In Einzelfällen hilft das kostenlose Tool ShadowExplorer weiter: Damit können Ransomware-Opfer die angelegten Wiederherstellungspunkte in einer Explorer-Ansicht durchsuchen. Diese Punkte legt Windows zwar automatisch, aber nicht regelmäßig an; etwa bei einer Treiber-Installation. Im schlimmsten Fall sind die Schattenkopien mehrere Wochen alt und veraltet. Wiederherstellungspunkte kann man aber auch manuell anlegen. Wählen Betroffene in ShadowExplorer ein Datum vor der Infektion aus, tauchen unter Umständen alte, unverschlüsselte Versionen von Dateien auf, die sich exportieren lassen. Praktisch jeder Erpressungs-Trojaner löscht jedoch als Teil seines Zerstörungswerk alle Schattenkopien. Das kann im Fall von Locky sogar im Verborgenen passieren, ohne dass eine UAC-Nachfrage auftaucht.

In unseren Tests konnten wir mit dem Tool keine Dateien wiederherstellen. In einem Fall existierten nach einer Infektion zwar noch Schattenkopien; die mit ShadowExplorer exportierten Dateien waren aber defekt. Für Ransomware-Geschädigte kann zudem der Punkt " Vorgängerversionen" in den Eigenschaften einer Datei hilfreich sein. Darüber können einzelne Dateien von einem Zeitpunkt vor der Infektion wiederhergestellt werden. Diesen Dateiversionsverlauf gibt es seit Windows 8; er ist auch in Windows 10 implementiert.

Der Versionsverlauf ist im Gegensatz zur Systemwiederherstellung jedoch nicht standardmäßig aktiviert. Wer vor der Infektion daran gedacht hat, den Dateiversionsverlauf einzuschalten, hat womöglich die Option, zu unverschlüsselten Datei-Versionen zurückzukehren. Das Problem dabei: Der Backup-Mechanismus sichert Dateien zwar auf Wunsch auch auf externe Datenträger. Ist dieser während des Infektionsvorgangs mit dem Computer verbunden, schlägt der Verschlüsselungs-Trojaner jedoch auch dort zu.

Forensik-Tools In der Regel verschlüsseln Erpressungs-Trojaner die Dateien und löschen anschließend die Originale. Beim Entfernen markiert das Betriebssystem die Dateien lediglich als gelöscht, sie sind aber nach wie vor auf dem Datenträger vorhanden. Prinzipiell sollte also durchaus eine Chance bestehen, die unverschlüsselten Originalversionen mit einem Datenrettungsprogramm zu rekonstruieren. Bewährte kostenlose Undelete-Tools sind Autopsy, PhotoRec und Recuva (siehe c' t Link).

IT-Dienstleister Bäcker konnte damit allerdings bei keinem Verschlüsselungs-Trojaner-Befall wichtige Daten retten, sondern nur etwa temporäre Internetdateien. Er hat die Datenrettung mit Autopsy & Co. nach mehreren Versuchen komplett aufgegeben. Auch unsere Tests sind gescheitert.

Das Gelingen hängt hier von mehreren Faktoren ab. Für eine höhere Erfolgsquote gilt: Umso größer die Festplatte ist, desto

länger bleiben als gelöscht markierte Dateien liegen. Es ist also eine Frage der Zeit, bis diese überschrieben werden. SSD-Nutzer haben schlechtere Karten, denn in der Regel ist die Speicherkapazität dort kleiner, weshalb die Daten schneller überschrieben werden. Erschwerend kommt die TRIM-Funktion hinzu, die Schreibzugriffe möglichst gleichmäßig verteilt. Somit werden gelöschte Dateien bei SSDs schnell überschrieben. Um kein Risiko einzugehen, sollte man die Festplatte mit den verschlüsselten Daten an ein nicht infiziertes System hängen. PhotoRec lässt sich zum Beispiel auch über ein Linux-Live-System nutzen. Nach dem Start eines Datenrettungsprogramms wählt man die Festplatte mit den verschlüsselten Daten aus. Anschließend kann man auf Wunsch festlegen, ob das Tool nur nach bestimmten oder allen Dateitypen suchen soll.

Letzter Ausweg Lösegeld?

Wenn alle Stricke reißen und keine andere Methode hilft, bleibt noch eine letzte Option: das Lösegeld zu zahlen. c' t rät nicht dazu, sich auf die Forderungen der Verbrecher einzulassen. Diese Entscheidung muss das Erpressungsopfer selbst treffen. Für viele ist der Bezahlvorgang abstrakt und ohne Vorwissen ist es schwierig, Bitcoins zu [Seitenwechsel auf Seite: 85]kaufen. Ein c' t-Artikel beschreibt, wie der Einkauf über www.bitcoin.de vonstatten geht. Diesen kann man online über den c' t-Link lesen.

IT-Dienstleister Bäcker hat sich mit verzweifelten Kunden zweimal auf die Forderung eingelassen. In beiden Fällen ließen sich alle Daten wiederherstellen. Nachdem das Lösegeld mit Bitcoins beglichen wurde, stellten die Gauner ein Dechiffrierungs-Tool inklusive passendem Schlüssel zur Verfügung.

Die Zahlung des Lösegelds garantiert allerdings nicht, dass Opfer tatsächlich wieder Zugriff auf ihre Daten bekommen. So sind Fälle bekannt, in denen Kriminelle nach Erhalt des Lösegelds in der Versenkung verschwanden und den Schlüssel nicht rausrückten. Nachverfolgen kann man das nicht, da sich die Server im Tor-Netz verstecken.

Es kann auch schlimmer kommen: Ein Leser schilderte c' t, wie er rund 500 Euro Lösegeld gezahlt hatte; anschließend habe er eine Batch-Datei zur Entschlüsselung erhalten. Doch durch einen Fehler bei der Übergabe des Laufwerksbuchstabens an die Dekodierungsroutine hat das Skript die Dateien nicht entschlüsselt, sondern gelöscht. Erst nachdem der Leser die Batch-Datei angepasst hatte, funktionierte das Skript wie versprochen.

Anlaufstelle für Opfer Dieser Artikel spiegelt unseren aktuellen Kenntnisstand über erste Hilfe für Opfer von Verschlüsselungs-Trojanern wider - weitere Infos stehen uns aktuell nicht zur Verfügung. Bitte haben Sie Verständnis, dass c' t keine Einzelfall-Beratung leisten kann. Betroffene können sich im Forum" Hilfe bei Erpressungs-Trojanern" auf heise online austauschen, das über den c' t-Link erreichbar ist. (des@ct.de)

Alle Tools: ct.de/yh5v Literaturverzeichnis

[1] Jürgen Schmidt, Desinfec' t 2015, Schädlinge einfach und zuverlässig aufspüren, c' t 14/15, S. 91

Webcode: ct.de/yh5v

Anzeige erstatten
Wie alle Behörden orientiert sich auch die Polizei bei ihrer Ressourcen-Planung am Bedarf. Diesen ermittelt sie unter anderem aus dem Aufkommen an Anzeigen zu bestimmten Straftaten. Mehr Anzeigen bedeuten, dass sich mehr Beamte mit der Verfolgung der Täter und dem Schutz beziehungsweise der Betreuung der Opfer befassen. Im Idealfall bildet die Polizei spezielle Ermittlungsgruppen für Erpressungs-Trojaner wie in Niedersachsen.
Betroffene Firmen können sich derzeit an die Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) der einzelnen Bundesländer wenden und erhalten dort Hilfe. Privatpersonen erhalten zwar keine Unterstützung bei der Datenrettung, aber Beratung. Ansprechpartner gibt es in jeder örtlichen Polizeidirektion in der Abteilung für Cyber-Kriminalität.

Dennis Schirrmacher

Quelle:	c't - Magazin für Computertechnik, 07/2016, S. 82
ISSN:	0724-8679
Dokumentnummer:	20160319160319102

Dauerhafte Adresse des Dokuments: https://www.wiso-net.de/document/PMGC__20160319160319102