Ronald Eikenberg

Erpresser-Schutz

Windows und Daten gegen Erpressungs-Trojaner wappnen

Wenige Vorkehrungen reichen, damit Ihnen Krypto-Trojaner kaum etwas anhaben können. Bringen Sie Ihre Daten rechtzeitig in Sicherheit – und sorgen Sie dafür, dass Schädlinge gar nicht erst ausgeführt werden können.

Trotz aller Vorsichtsmaßnahmen kann es passieren, dass ein Krypto-Trojaner zuschlägt und alles verschlüsselt, was er erreichen kann: Daten auf der Platte des Rechners, USB-Speicher, Netzwerkfreigaben. Der einzig sichere Weg, noch etwas zu retten, sind Backups, die außerhalb der Reichweite des Schädlings aufbewahrt wurden. Im einfachsten Fall kopiert man die wichtigsten Daten auf eine USB-Platte, die man nur gezielt mit dem Rechner verbindet, wenn man Dateien sichern oder wiederherstellen möchte. Dateien, die sich nicht mehr ändern, bieten optische Datenträger wie CDs oder DVDs für einige Jahre einen Trojaner-geschützten Unterschlupf. Aktuelle Daten kann man mit Cloud-Speichern wie Dropbox, Google Drive und OneDrive abgleichen. Schlägt ein Krypto-Trojaner zu, werden die durch ihn verschlüsselten Dateien zwar möglicherweise mit in die Cloud synchronisiert. Die meisten Cloud-Speicher halten jedoch alte Dateiversionen vor, zu denen man leicht zurückfindet.

Grundsätzlich eignet sich auch ein NAS oder eine Fritzbox mit USB-Platte als Backup-Speicher. Da viele Verschlüsselungs-Trojaner jedoch routinemäßig auf Netzwerkfreigaben zugreifen, sollte man es dem Schädling so schwer wie möglich machen, diese Sicherungskopien zu erreichen. Wenn ein angemeldeter Nutzer mit dem Explorer auf die Freigaben zugreifen kann, dann schaffen es auch Locky & Co. Im Idealfall konfigurieren Sie das NAS so, dass der Backup-Ordner nicht über SMB erreichbar ist. Übertragen Sie die zu sichernden Dateien zum Beispiel per FTP mit einem eigenständigen Client wie FileZilla. Bietet das NAS eine Nutzerverwaltung, sollten Sie für diesen Zweck einen speziellen Backup-Nutzer anlegen, der nur auf den Sicherungsordner zugreifen darf. Allen anderen Nutzern räumen Sie maximal Lesezugriff auf diesen Ordner ein.

Automatisch sichern

Backup-Tools, die sich automatisch um das Wegsichern kümmern, gibt es wie Sand am Meer. Möglicherweise setzen Sie bereits ein Programm ein, das Ihnen gute Dienste leistet. Beim Autor dieses Artikels hat sich das Open-Source-Tool Duplicati bewährt (siehe c't-Link). Es ist leicht zu bedienen und sehr flexibel: Es kopiert die zu sichernden Daten auf Datenträger, FTP-, SFTP- und WebDAV-Server oder zu diversen Cloud-Diensten. Vor dem Upload verschlüsselt Duplicati die Dateien lokal mit AES-256, auf Wunsch nutzt es auch GnuPG – ein Angreifer, der sich Zugriff auf das Speicherziel verschafft, kann also nichts mit den Backups anfangen. Die Ziele lassen sich beliebig kombinieren. So landet etwa der Dokumente-Ordner stündlich in der Cloud, wohingegen das große Rundumsorglos-Paket mit Foto- und Musiksammlung, Programmierprojekten und ähnlichem nur einmal täglich via FTP auf die an der Fritzbox hängende USB-Platte geschaufelt wird.

Duplicati arbeitet inkrementell, speichert also nur die Änderungen zum vorherigen Stand, was Zeit und Platz spart. Man legt selbst fest, wie lange das Tool Zwischenstände aufheben soll. Unabhängig davon, womit man sein digitales Hab und Gut sichert, ist es sinnvoll, mehrgleisig zu fahren und mehrere Backups an verschiedenen Orten aufzubewahren. Duplicati macht diese Vorgehensweise leicht: man legt einfach mehrere Jobs an. Zudem ist es ratsam, von Zeit zu Zeit die gesamte Systemplatte zu sichern, damit man sie nach einer Infektion auf einen sauberen Stand bringen kann. Ab Windows 8 geht das mit dem c't-Tool WIMage [1] leicht von der Hand. Nachdem Sie Ihre individuelle Backup-Lösung

eingerichtet haben, sollten Sie unbedingt einen Testlauf der Wiederherstellung vornehmen – am besten auf eine leere Platte.

Infektion verhindern

Mit Backups sind Sie bestens auf den Fall vorbereitet, dass sich ein Krypto-Trojaner über Ihre Dateien hermacht. Wer die Verbreitungsmaschen der Schädlinge kennt, kann mit relativ wenig Aufwand dafür sorgen, dass es erst gar nicht so weit kommt. Online-Ganoven verteilen ihre Erpressungs-Trojaner vor allem über Mails mit Dateianhängen und über sogenannte Exploit-Kits, die Sicherheitslücken im Browser und dessen Plug-ins ausnutzen. Vor beiden Angriffswegen kann man sich schützen: Per Mail verbreitete Schädlinge werden erst beim Öffnen des Dateianhangs ausgeführt. Seien Sie also skeptisch, wenn Sie einen Anhang erhalten, die Sie nicht erwarten. Fragen Sie im Zweifel beim Absender nach, ob er die Datei tatsächlich verschickt hat und was es damit auf sich hat. Handelt es sich um ein Office-Dokument, sollten Sie darin enthaltene Makros auf keinen Fall ausführen, wenn Sie der Datei nicht hundertprozentig vertrauen. Das Starten von Office-Makros ist genauso gefährlich wie das Ausführen von .exe-Dateien! Makros können beliebigen Code aus dem Internet nachladen und ausführen. Das gilt auch für an Mails angehängte Batch- und Skript-Dateien wie .bat, .cmd, .js, .vbs und .wsf. Ebenfalls gefährlich sind unter anderem .com, .scr sowie .pif. Auch in PDF-Dateien kann sich Schadcode verstecken. Häufig stecken die eigentlichen Trojaner-Skripte in Zip-Archiven. Einige Archive sind verschlüsselt, um eventuell vorhandene Virenfilter auszutricksen. Das dazugehörige Passwort steht dann in der Mail.

Makros zähmen

Damit Makros nicht versehentlich gestartet werden, sollten Sie in den Office-Einstellungen sicherstellen, dass deren automatische Ausführung deaktiviert ist. Bei Office 2016 finden Sie das entsprechende Stellrad unter „Datei / Optionen / Trust Center / Einstellungen für das Trust Center… / Alle Makros mit Benachrichtigung deaktivieren“. So wird Makro-Code nur noch ausgeführt, wenn man eine gelbe Benachrichtigungsleiste oberhalb des Dokuments anklickt. Geht es darum, den Rechner von weniger technisch versierten Personen abzusichern, wählen Sie am besten die Option „Alle Makros ohne Benachrichtigung deaktivieren“. Einige verseuchte Dokumente weisen nämlich ausdrücklich darauf hin, man solle auf die gelbe Leiste klicken – wo aber keine Leiste ist, kann auch niemand drauf klicken. Für viele Office-Formate bietet Microsoft kostenlose Viewer an, die keine Makros unterstützen (siehe c’t-Link). Bei OpenOffice und LibreOffice stehen aufgrund der eingeschränkten Kompatibilität mit Microsoft-Office-Makros die Chancen gut, dass ein Trojaner-Downloader nicht vollständig ausgeführt wird.

Um zu verhindern, dass man in einem unaufmerksamen Moment doch mal ein gefährliches Skript ausführt, kann man die oben genannten Skript-Formate mit dem Windows-Editor verknüpfen. Im Fall der Fälle öffnet sich dann Notepad mit dem Quellcode und es wird kein Code ausgeführt. Per Registry lässt sich zudem der Windows Script Host deaktivieren, der die meisten Skript-Formate ausführt. Legen Sie unter „HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings“ eine Zeichenfolge namens „Enabled“ an und setzen Sie deren Wert auf „0“. Kommt es anschließend zu Komplikationen, etwa weil ein genutztes Programm ohne den Host nicht funktioniert, aktivieren Sie ihn mit dem Wert „1“ wieder.

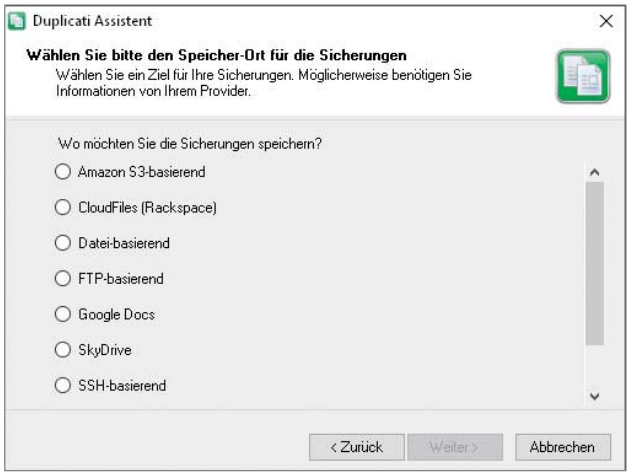
Damit Sie sich beim Surfen keinen Schädling einfangen, müssen Sie System und Programme aktuell halten. Installieren Sie Windows-Updates, sobald sie angeboten werden und kümmern Sie sich insbesondere um die Anwendungen, die am häufigsten angegriffen werden: nämlich Browser, Flash, Java und Adobe Reader. Am wenigsten Stress hat man mit Google Chrome: Der Browser bringt sich zuverlässig selbst auf den aktuellen Stand und integriert den Flash-Player direkt, um ihn ebenfalls frisch zu halten. PDF-Dokumente rendert Chrome selbst, ohne auf einen potenziell veralteten Adobe Reader angewiesen zu sein.

Virenbremse

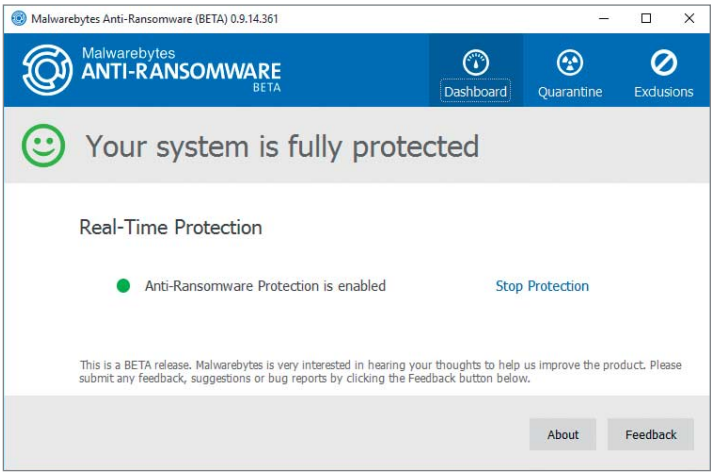
Ein Virenscanner gehört nach wie vor auf jeden Windows-Rechner, der mit Dateien aus dem Internet hantiert. Sie dürfen sich allerdings nicht darauf verlassen, dass der Wächter jede Bedrohung abwendet: Es kann mehrere Stunden dauern, ehe ein Schädling, der gerade frisch per Mail serviert wurde, vom Virenschutzprogramm erkannt wird. Online-Ganoven testen ihre Schädlinge mit diversen Virenscannern und verändern ihn so lange, bis sie an allen vorbeikommen. Erst wenn der Trojaner nicht mehr erkannt wird, geht er an die potenziellen Opfer raus.

Manche Hersteller von Virenschutz-Software wie Bitdefender und Kaspersky werben damit, dass ihre Produkte Ransomware allein anhand ihres Verhaltens identifizieren und anschließend blockieren können. Wie effektiv das ist, konnten wir bisher nicht isoliert testen, da stets auch die anderen Schutzfunktionen der Virenwächter aktiv sind. Man kann eine solche Erkennung auch nachrüsten – unabhängig davon, welches Virenschutzprogramm installiert ist.

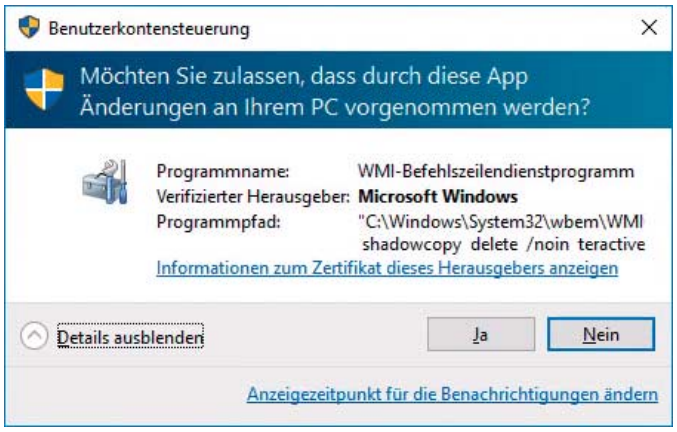
Um die Chance zu erhöhen, dass eine Ransomware frühzeitig ertappt wird, kann man dem Virenschutz spezialisierte Wächter wie Malwarebytes Anti-Ransomware (siehe c’t-Link) zur Seite stellen. Das Tool versucht, Krypto-Trojaner anhand typischer Handlungen zu erkennen. Bei einem Test mit einem aktuellen TeslaCrypt 3 wurde tatsächlich keine einzige Datei verschlüsselt. Bei Locky mussten immerhin nur etwa 20 von mehreren Hundert Dateien dran glauben, ehe Anti-Ransomware den Prozess stoppte. Noch ist



Duplicati erstellt automatisch AES-verschlüsselte Kopien Ihrer Dateien. Diese überträgt die Freeware zum Beispiel auf USB-Platten, FTP-Server oder in die Speicher-Cloud.



Das Tool Malwarebytes Anti-Ransomware identifiziert Krypto-Trojaner anhand ihres Verhaltens, um sie rechtzeitig zu blockieren.

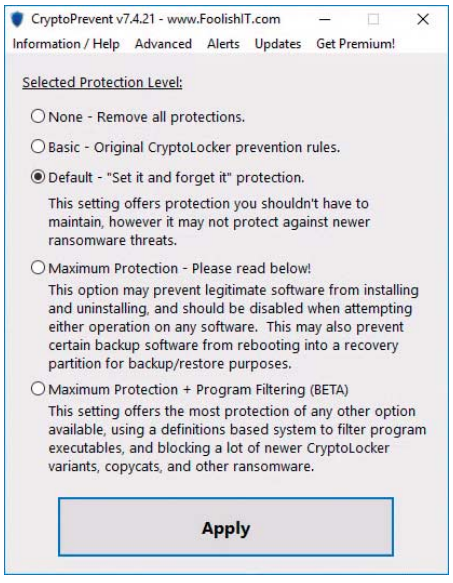


Bei einigen Krypto-Trojanern kann man das Löschen von Schattenkopien verhindern, indem man den UAC-Dialog von vssadmin.exe nicht bestätigt.

das Programm nur mit Vorsicht zu genießen, da es sich um eine Beta-Version handelt. Der Hersteller rät ausdrücklich vom Einsatz auf Produktivsystemen ab. Während unseres Tests erlebten wir jedoch keine Komplikationen oder Fehlalarme. Das Tool ist aktuell kostenlos – soll in Zukunft aber in den kostenpflichtigen Schutzprogrammen des Herstellers aufgehen.

UAC ernst nehmen

Zum Verschlüsseln reichen den Krypto-Trojanern die Rechte des angemeldeten Nutzers. Um es den Opfern so schwer wie möglich zu machen, ihre Dateien ohne Zahlung des Lösegelds zu retten, eliminieren einige Schädlinge wie Locky und TeslaCrypt auch die sogenannten Schattenkopien, welche Windows periodisch automatisch anlegt. In manchen Fällen kann man aus diesen Kopien die Originale retten (siehe S. 83). Zum Löschen nutzen die Trojaner das Windows-Tool vssadmin.exe, das erhöhte Rechte voraus-



CryptoPrevent setzt einige Richtlinien für Softwareeinschränkungen um, die Erpressungs-Trojaner an der Ausführung hindern sollen.

setzt. Diese Rechteausweitung führt normalerweise zu einer UAC-Abfrage der Benutzerkontensteuerung (UAC). Wenn die Schädlingsentwickler clever sind, kann die Abfrage allerdings auch ausbleiben: So bedient sich etwa Locky eines bekannten Tricks, um das Tool ohne Einwilligung des Nutzers mit erhöhten Rechten auszuführen. Die bei Redaktionsschluss aktuelle TeslaCrypt-Ausgabe war hingegen noch nicht so weit. Wer hier nicht nach der Infektion leichtfertig den UAC-Dialog abnickt, kann das Löschen der eventuell vorhandenen Schattenkopien verhindern.

Begegnet Ihnen eine unerwartete UAC-Abfrage, sollten Sie diese also auf keinen Fall auf die leichte Schulter nehmen und im Zweifel lieber ablehnen. Wenn Sie die Details ausklappen, verrät Windows, was genau passieren soll. Beim Löschen von Schattenkopien nennt der Dialog meistens das Systemtool vssadmin.exe; Parameter wie „shadowcopy delete“ sind ebenfalls höchst verdächtig. Die Angaben „Programmname“ und „Verifizierter Herausgeber“ sind hier wenig aussagekräftig: Da die Trojaner System-Tools einspannen, steht hier meist nur, dass es sich um verifizierte Microsoft-Programme handelt. Damit der UAC-Dialog im Fall der Fälle überhaupt erscheint, sollten Sie sicherstellen, dass Sie die Benutzerkontensteuerung mindestens auf der zweithöchsten Stufe betreiben. Sie finden die entsprechenden Einstellungen über eine Startmenü-Suche nach „UAC“.

Tipps für Experten

Windows bietet mit den Richtlinien für Softwareeinschränkungen (Software Restriction Policies, SRP) ein mächtiges Werkzeug, um die Ausführung von Schädlingen zu verhindern. Wer diesen Schutzwall aktivieren will, sollte jedoch genau wissen, was er tut – sonst besteht die Gefahr, dass man damit nicht nur Trojaner, sondern auch sich selbst vom System aussperrt. Mit den SRP kann man so weit gehen, dass nur noch Programme ausgeführt werden dürfen, die zuvor auf eine Whitelist gesetzt wurden. So würde Windows alltäglich genutzte Anwendungen starten lassen, ein frisch heruntergeladenes Programm aber blockieren – ganz gleich, ob es sich um einen Trojaner oder erwünschte Software handelt. Dieser Whitelisting-Ansatz ist aufwendig und deshalb vor allem im Firmenumfeld verbreitet: Hier kann der Admin die Positivliste zentral pflegen. Alternativ kann das Unternehmen einen von zahlreichen Dienstleistern konsultieren, die sich um das Whitelisting kümmern. Privatkunden ist damit aber nicht geholfen.

Eine abgeschwächte Form ist die Blockade von Programmen in bestimmten Ordnern. Das Download-Skript von Locky etwa speichert den Schädling im Temp-Ordner. Blockiert eine Software-Richtlinie den Start von hier, kann der Krypto-Trojaner nicht ausgeführt werden. Das hat aber auch Nebenwirkungen: Ein Software-Updater, der die Aktualisierung im Temp-Ordner zwischenspeichert, läuft ebenso gegen die Wand. Wer mit Software-Richtlinien experimentieren will, sollte vorher einen Systemwiederherstellungspunkt anlegen, für den Fall, dass das System nach einer Fehlkonfiguration nicht mehr sauber startet.

Das in der Basisversion kostenlose Tool CryptoPrevent (siehe c’t-Link) erstellt einige grundlegende Richtlinien, die Ransomware blockieren sollen. Auf Wunsch erleichtert es auch das Whitelisting und blockiert System-Tools wie vssadmin.exe, mit denen Schädlinge größeren Schaden anrichten können. Wer eine Windows-Domäne administriert, sollte einen Blick auf die AppLocker-Funktion des Betriebssystems werfen. Damit kann man im Detail steuern, welche Programme die Windows-Clients ausführen dürfen. Auf den Clients muss mindestens Windows 7 in der Ultimate- oder Enterprise-Version laufen. Admins von Linux-Fileservern können infizierte Windows-Clients im Netz mit dem Tool Fail2ban daran hindern, die Daten auf dem Server zu verschlüsseln. Eine konkrete Anleitung haben wir auf heise Security veröffentlicht (siehe Link). Für Windows-Server gibt es einen ähnlichen Ansatz, zu dem der c’t-Link ebenfalls führt.

Unerpressbar

Die drei wichtigsten Tipps zum Schutz vor Erpressungs-Trojanern lauten: Backups, Backups, Backups. Wählen Sie eine Backup-Lösung, die Ihren persönlichen Bedürfnissen gerecht wird, damit Sie Ihr digitales Hab und Gut stressfrei wiederherstellen können, falls ein Krypto-Trojaner zuschlägt. Mit den oben beschriebenen Schutzvorkehrungen haben Sie zudem gute Karten, dass es erst gar nicht so weit kommt. Eine hundertprozentige Garantie gibt es freilich nicht – Cyber-Erpressung ist ein lukratives Geschäft und die Ganoven denken sich immer wieder neue Tricks aus. Falls Sie das Gefühl haben sollten, dass ein Erpressungs-Trojaner auf Ihrem System wütet, schalten Sie den Rechner sofort aus und lesen Sie auf Seite 82 weiter. (rei@ct.de)

Literatur

[1] Hajo Schulz, Versicherungsfall, Systemwiederherstellung mit c’t-WIMage, c’t 5/16, S. 132

c’t Tools gegen Krypto-Trojaner ct.de/ytxm

Sind Mac-Nutzer automatisch sicher?

Bis vor Kurzem konnten sich Mac-Nutzer beruhigt zurücklehnen – Erpressungs-Trojaner waren ein reines Windows-Phänomen. Dann tauchte Anfang März mit KeRanger der erste voll funktionsfähige Trojaner auf, der die Daten von Mac-Anwendern verschlüsselte und die Zahlung von Lösegeld in Form von Bitcoins einforderte.

Ungewöhnlich war nur der Verbreitungsweg. Anders als bei Windows, wo man sich Ransomware über Mails oder durch Drive-by-Downloads einfängt, kam KeRanger als angeblich neue Version des beliebten BitTorrent-Clients Transmission daher. Offenbar hatten die Erpresser die Web-Seiten der Entwickler gehackt und verbreiteten ihre trojanisierte Version darüber. Wer zwischen dem 4. und 5. März die Transmission-Version 2.90 installiert hat, holte sich damit unter Umständen den Erpressungs-Trojaner ins System. Um die Selbstschutz-Mechanismen von OS X zu umgehen, war der Code mit einem gültigen Entwickler-Zertifikat digital signiert, das vermutlich schlicht gestohlen wurde.

Der Rest funktioniert ähnlich wie bei Windows: Nach der Installation wartet KeRanger 72 Stunden und verschlüsselt dann die erreichbaren Dateien des Anwenders. Der Trojaner arbeitet mit normalen Benutzerrechten; ins Visier nimmt er Dokumente (.doc, .docx, .ppt, pptx, .xls, …), Bilder, Audio- und Video-Dateien, Archive, Datenbanken und einiges mehr.

Mittlerweile hat Apple das verwendete Entwickler-Zertifikat gesperrt und auch die Signaturen seines rudimentären Virenschutzes XProtect aktualisiert. Damit geht von dieser KeRanger-Version keine akute Gefahr mehr aus. Doch prinzipiell kann so etwas jederzeit wieder passieren.

Schutz für OS X

Auch unter OS X helfen eigentlich nur Backups, um im Ernstfall nicht zahlen zu müssen. Das Schöne ist, dass OS X mit Time Machine eine sehr komfortable Backup-Möglichkeit mitbringt. Wer sie nutzt, kann auch nach einem Ransomware-Vorfall ältere, unverschlüsselte Versionen seiner Dateien wiederherstellen.

KeRanger enthält zwar bereits Funktionen, um diese Backups zu zerstören. Die sind aber in der aktuellen Version nicht aktiv. So ganz einfach kann man mit normalen Benutzerrechten auch keine Time-Machine-Backups löschen. Grundsätzlich ist es aber durchaus möglich: Im Netz kursieren dazu Anleitungen, die wir testweise nachvollziehen konnten. Somit könnte also auch ein Erpressungs-Trojaner wie KeRanger die Backups zerstören.

Wer auf Nummer sicher gehen will, speichert seine Backups deshalb außer Reichweite der Schädlinge. Im einfachsten Fall sichert man seine Daten dazu auf eine externe Platte, die nur zu diesem Zweck an das System angeschlossen wird und sonst sicher im Schrank liegt. Um zu verhindern, dass während des Sicherns ein bereits infizierter Rechner die Backup-Platte schreddert, kann man mit rotierenden Backups auf mehreren Platten arbeiten oder zusätzlich zu den täglichen Backups monatliche Sicherungen auf einer zweiten Platte verwahren.

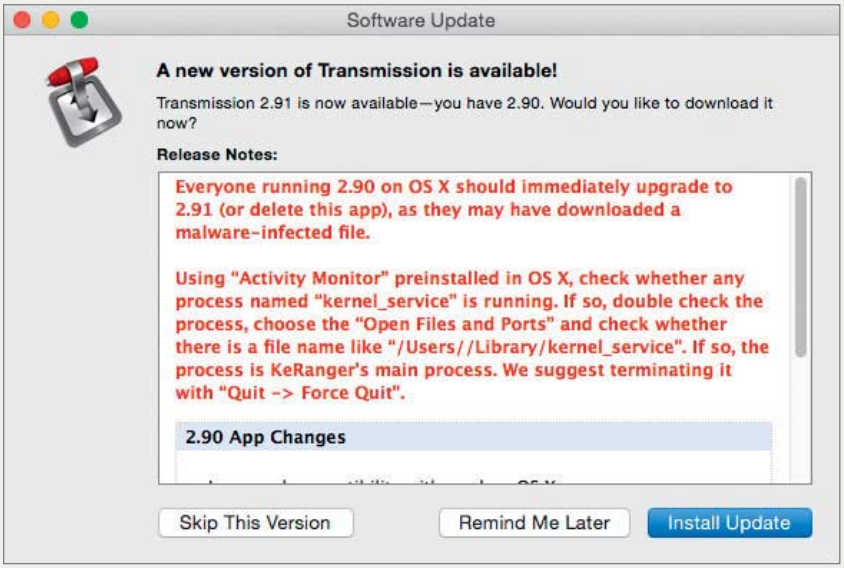
Alternativ kann man seine Daten auch auf externe Systeme sichern, zu denen ein Erpressungs-Trojaner keinen (Schreib-)Zugang erlangen kann. Time Machine kann verschlüsselte Backups erstellen, die man getrost etwa bei Freunden oder in die Cloud hochladen kann. Das im Haupttext beschriebene Backup-Tool Duplicati mit seinen universellen Sicherungsfunktionen gibt es übrigens auch für Macs. Gänzlich immun gegen Erpressungs-Trojaner sind Backup-Lösungen, die nach dem Pull-Prinzip arbeiten und meist im Enterprise-Umfeld anzutreffen sind. Dabei holt sich der Backup-Server die Daten vom Client. Der stellt dazu entweder Freigaben bereit oder hat einen speziellen Agenten installiert, bei dem der Server die Daten abholen kann. In dieser Situation kann sich ein Trojaner auf dem Client-Rechner keinen Zugang zu den gesicherten Daten verschaffen.

Antiviren-Schutz

Wer sich fragt, ob er sich vorsorglich einen Virenscanner auf seinen Macs installieren sollte: Nach unserem Kenntnisstand hätte keines der existierenden AV-Programme die Infektion mit KeRanger verhindert. Die greifen erst ein, nachdem sie passende Signaturen erhalten haben, mit denen sie den Erpressungs-Trojaner erkennen. Da Apple parallel mit dem Widerruf des Zertifikats und aktualisierten XProtect-Signaturen reagiert hat, waren Macs ohne Virenscanner genauso gut geschützt.

Wie das bei zukünftigen Erpressungs-Trojanern aussehen wird, ist natürlich offen. Doch die Erfahrung bei Windows zeigt, das AV-Software vor neuen Bedrohungen nicht sonderlich gut schützt. Es mag sein, dass die jetzt ausgelieferten Signaturen die nächste KeRanger-Version ebenfalls erkennen; darauf verlassen sollte man sich nicht. Existierende Signaturen lassen sich mit überschaubarem Aufwand umgehen, und bis neue kommen, ist der Schaden vielleicht schon angerichtet.

Ob sich bei Mac-Usern wie bei Windows-Anwendern tatsächlich ein Millionen-Geschäft machen lässt, ist mehr als fraglich. Ohne das Geld fehlt aber der wichtigste Anreiz zur Serienproduktion von Erpressungs-Trojanern. Wahrscheinlicher ist es, dass weitere, vereinzelte Versuchsballons wie der KeRanger-Trojaner auftauchen, Erpressungs-Trojaner für OS X aber auf absehbare Zeit kein Massenphänomen werden. (Jürgen Schmidt)



Über den offiziellen Mac-Installer des beliebten BitTorrent-Clients Transmission wurde ein perfider Verschlüsselungs-Trojaner verteilt.