Trojaner auf dem Mac: So schützt man OS X vor Malware

von Sebastian Trepesch, giga.de

KeRanger, wohl der „gelungenste“ Verschlüsselungs-Trojaner, hat es auf Macs geschafft. Wie kann man sich vor Ransomware, vor **Erpressungs-Trojanern**, schützen? Wir nennen die wichtigsten Punkte, die es zu beachten gilt.

Erst letzte Woche haben wir über Locky berichtet – der gefährliche Trojaner treibt aktuell nur auf Windows-Systemen sein Unwesen. In „Mac als Locky-freie Zone: Bei Windows ist die Hölle los“ haben wir aber bereits ein paar Tipps mitgegeben, die Mac-Nutzer zum Schutz von Schadsoftware beherzigen sollten. Da mit KeRanger nun ein Verschlüsselungs-Trojaner auf OS X entdeckt wurde, möchten wir noch ausführlicher auf das Thema eingehen.

Ein Geschenk, das eine böse Überraschung beinhaltet – das Trojanische Pferd aus der griechischen Mythologie steht Pate für Schadsoftware, die es getarnt auf den Rechner schafft. Meistens sind Trojaner in Mailanhängen versteckt, in einem bekannten Dateiformat a la PDF, Excel, ZIP oder ähnliches. Erst mit dem Öffnen der Datei wird es gefährlich. Ein anderer Weg führt über die Installation einer anderen Software auf den Mac. KeRanger hat sich im BitTorrent-Client Transmission (Version 2.90) versteckt.

Erpressungs-Trojaner wie Locky und KeRanger verschlüsseln die persönlichen Dokumente auf dem Rechner und angeschlossenen Laufwerken. Die Freigabe der Dateien erfolgt erst nach einer Lösegeldzahlung des Nutzers über das Internet. Locky verlangt knapp 200 Euro, KeRanger rund 370 Euro in Form von Bitcoin.

Schutz gegen Trojaner auf dem Mac: Vorsicht im Alltag

Die klassischen Wege für Trojaner auf den Computer laufen über Mails und infizierte Webseiten. Ein paar simple Regeln können die Gefahr maßgeblich reduzieren:

- **Mail-Anhänge** vor dem Öffnen prüfen: Stammen sie von einem bekannten Absender? Da auch die eingeblendete Mailadresse gefälscht sein kann: Ist das Thema relevant und passt die angehängte Datei zum Inhalt der Mail?
- Ähnliches gilt für Links in Mails. Achtung, sie können maskiert sein und nicht sofort das wahre Ziel verraten. Ist der Absender vertrauenswürdig?
- Downloads von Webseiten beinhalten die selben Gefahren wie bei Mails. Unseriöse Webseiten meiden, Sicherheitstools des Browsers aktivieren, bei Software-Downloads auf Mac App Store, Entwicker-Webseiten oder zumindest sehr bekannte Anbieter zurückgreifen.

Einstellungssache: Mac und Software richtig konfigurieren

„Sicherheit schon integriert“, bewirbt Apple OS X. Mehrere Funktionen sind hierfür im Betriebssystem verantwortlich, zum Beispiel Sandboxing, Laufzeitschutz, Antiphishing in Safari und: Gatekeeper will schädliche Software vom Mac fernhalten.

- In den *Systemeinstellungen -> Sicherheit* darf der App-Download nur aus dem **Mac App Store**, oder noch verifizierten Entwicklern, erlaubt sein. (Im Falle KeRanger konnte sie sich dennoch einschleichen, bis Apple das Entwickler-Zertifikat deaktivierte.)
- FileVault 2 in OS X verschlüsselt die Festplattendaten, auch von externen Laufwerken. *Systemeinstellungen -> Sicherheit -> FileVault*.
- Trojaner benutzen oft **Makros** – sie sind für viele Nutzer irrelevant und können deshalb deaktiviert werden. Siehe Word, Excel und Outlook im *Sicherheitscenter* (*Trust Center*) *-> Einstellungen/Optionen*.
- Software-Updates stopfen bekannte Sicherheitslücken. Neben OS X und den Browsern sollte auch der FlashPlayer, Adobe Reader, QuickTime und – falls überhaupt nötig – Java aktuell gehalten werden. **Automatische Updates** erledigen die Arbeit zügig. *Systemeinstellungen -> App Store*, bzw. in den jeweiligen Einstellungen der Software.
- Das Bundesamts für Sicherheit in der Informationstechnik (BSI) empfiehlt, neben dem **Admin-Konto** sich für die normale Mac-Nutzung ein Benutzerkonto mit eingeschränkten Rechten anzulegen. Online-Banking solle sogar in ein weiteres Konto ausgelagert werden.

Backups gegen Erpressung

Wer die von Ransomware verschlüsselten Daten auf einem Backup-Laufwerk besitzt, wird nicht in Verlegenheit kommen, Lösegeld zu zahlen. Also:

- Regelmäßig **Backups** anlegen.
- Backup-Laufwerke ausschalten oder **abstecken**, wenn sie nicht benötigt werden, damit sie nicht auch verschlüsselt werden können.
- Gleiches gilt für Cloud-Laufwerke wie Dropbox etc.: Trennen, wenn sie nicht benötigt werden.

Wer es ganz genau nimmt, beherzigt die 3-2-1-Regel: Drei Sicherheitskopien von wichtigen Dokumenten anlegen, davon zwei auf unterschiedlichen Medien und eines an einem anderen Ort beziehungsweise in der Cloud lagern.

Anti-Viren-Software für Mac gegen Trojaner – sinnvoll?

Ein heiß diskutiertes Thema ist, ob Anti-Viren-Software auf dem Mac sinnvoll ist oder nicht. Selbst das BSI sah es zumindest unter OS X Mountain Lion (PDF) nicht notwendig an, Anti-Viren-Software zu installieren. Klar sehen das die Entwickler von Kaspersky & Co anders (sie rechtfertigen ihre Produkte zudem über Zusatzfunktionen*). Aber:

Eine **Firewall** prüft, welche Programme eine Internetverbindung aufnehmen. Eventuell für einen Trojaner notwendige Downloads können so nicht ohne weiteres nachgeladen werden. Die OS X-eigene Firewall wird unter *Systemeinstellungen -> Sicherheit -> Firewall* aktiviert (zum Bearbeiten vorher unten auf das Schloss klicken).

Trojaner auf dem Mac: Kein Grund zur Panik

Auch nach dem Fund von KeRanger müssen sich Mac-Nutzer keine übertriebenen Sorgen machen: Schadsoftware auf OS X-Systemen ist aktuell eine große Seltenheit. Selbst die Verbreitung von KeRanger konnte durch die Entwickler des infizierten Torrent-Programms und durch Apple gestoppt werden.

Spätestens seit Flashback aus dem Jahre 2011 sollte aber bekannt sein: Generell kann auch ein Mac infiziert werden. Meistens ist das menschliche Handeln die Schwachstelle. Ein bisschen Umsicht kann nicht schaden.

Das im Artikel vermittelte Vertrauen, dass Backups nicht von „KeRanger" beeinflusst werden, verringert sich rasch, wenn man die nachstehende, gründlichere Analyse von Thomas Reed liest:

Erste Ransomware auf dem Mac

von Thomas Reed (malwarebytes.org), Übersetzung KJM

Am Samstag ergänzte Apple stillschweigend die XProtect-Anti-Malware-Definitionen in OS X um die Merkmale von etwas, was „KeRanger" genannt wird. Es wurde am Sonntag von Claud Xiao von Palo Alto Networks veröffentlicht, dass KeRanger die erste echte Mac-Ransomware ist, und das ist keine Theorie: sie ist tatsächlich in Umlauf.

Xiao zufolge wurde das Programm **Transmission** – ein BitTorrent-Client – infiziert, um diese Ransomware zu enthalten. Die infizierte App wurde von der offiziellen Transmission-Website verteilt, aber mit einer anderen Code-Signatur als der, die normalerweise zuvor verwendet wurde, um die App zu signieren, was bedeutet, dass die App selbst geändert wurde und vom Angreifer neu signiert wurde (obwohl dies noch nicht bestätigt wurde).

Die modifizierte Kopie von Transmission enthält eine Datei namens `General.rtf`, die in Wirklichkeit eine ausführbare Datei ist statt, wie sie vorgibt, ein Rich-Text-Dokument. Wenn die App gestartet wird, wird diese Datei in eine Datei namens `kernel_service` im Library-Ordner des Benutzers kopiert (der normalerweise in aktuellen OS-X-Versionen ausgeblendet ist).

Dieser `kernel_service` Prozess läuft dann weiterhin im Hintergrund und legt im Library-Ordner des Benutzers zusätzliche Dateien an namens `.kernel_pid` und `.kernel_time`. Letztere Datei enthält einen Zeitstempel, der benutzt wird, um festzustellen, wann drei Tage vergangen sind.

Nach drei Tagen „explodiert" die Malware und beginnt, Dateien zu verschlüsseln. Laut Xiao wird sie sowohl den gesamten Inhalt Ordners **/Users** verschlüsseln als auch Dateien, die übliche Dokumenten-Suffixe haben und sich im Ordner **/Volumes** befinden (mit anderen Worten: Dateien, die sich auf verbundenen

externen Festplatten, Servern usw. gespeichert sind). In jedem Ordner, in dem Dateien verschlüsselt wurden, wird eine Datei angelegt mit Namen `README_FOR_DECRYPT.txt`, die Anweisungen enthält, wie man für einen Entschlüsselung-Key bezahlen soll.

Die Tatsache, dass diese Malware externe Festplatten und angeschlossene Netzwerk-Volumes verschlüsseln will, bedeutet, dass sie auch Backups verschlüsseln kann, was auch Time Machine Backups beinhaltet, die auf einer Time Capsule gespeichert sind. Schlimmer noch: Es gibt in der App Code in einer Routine, die `_encrypt_timemachine` heißt – zur Zeit laut Xiao zwar noch ungenutzt. Das bedeutet, dass Ihre Backups, die Sie für den Fall einer Infektion mit Ransomware intakt halten wollen, dieser Malware ebenso zum Opfer fallen können.

Interessanterweise sieht es so aus, dass diese Malware keinen Mechanismus zum dauerhaften Verbleib enthält. Der `kernel_service` Prozess bleibt am Laufen, aber wenn man den Rechner neu startet, wird der Prozess nicht automatisch neu gestartet. Man muss schon die infizierte **Transmission** App erneut starten, um den Prozess zu reaktivieren.

Apple hat sowohl die Aufdeckung dieser Malware zu XProtect hinzugefügt als auch das Entwickler-Zertifikat widerrufen, das benutzt wurde, um die maligne Kopie von Transmission zu signieren. Das bedeutet, dass – ohne ein Update der Malware – keine neuen Infektionen mehr möglich sein sollten. Es ist aber wichtig, anzumerken, dass, wenn man bereits eine infizierte Kopie von Transmission heruntergeladen hat, dies natürlich nicht verhindern kann, dass man die App erneut öffnet … Der Mac wird sie dann nämlich als sicher ansehen, da sie ja zuvor schon einmal erfolgreich geöffnet wurde. Das bedeutet, dass Apples Maßnahmen denjenigen Anwendern nicht helfen, die bereits infiziert wurden und bei denen der 3-Tage-Countdown schon läuft.

Manche Leute mögen in Versuchung sein, auf die Lösegeldforderung einzugehen, um ihre Dateien wieder zurückzubekommen. Es ist aber wichtig, zu verstehen, dass dies eine extrem schlechte Idee ist. In der Windows-Welt hatte das Zahlen des Lösegelds machmal das gewünschte Ergebnis, dass man einen Key erhielt, der die Daten erfolgreich entschlüsseln kann. Genauso aber konnte das Resultat sein, dass man Geld an die Hacker schickte und nichts dafür bekam oder aber einen Schlüssel, der nicht funktionierte, weil die Ransomware schlecht programmiert war.

Wenn Sie die **Transmission** App kürzlich heruntergeladen haben, sollten Sie sie von ihrem Rechner löschen und Ihren Computer neu starten. Das sollte eine Reaktivierung der Malware verhindern. Sie können diese Malware auch mit **Malwarebytes Anti-Malware for Mac** entfernen. Bedenken Sie aber, dass alle Dateien, die vor dem Löschen verschlüsselt wurden, verloren sind, es sei denn, Sie haben Backups davon und die Backups sind noch intakt.

Bedenken Sie auch, dass dies nicht das erste Mal ist, dass Mac-Anwender nach dem Download eines Torrent-Clients infiziert wurden, wenngleich diese Infektionen in der Vergangenheit nur Adware waren. Seien Sie also vorsichtig, wenn Sie künftig mit Torrents umgehen.

Ergänzung:

Die infizierte Kopie der Transmission-App hatte die Versionsnummer 2.9.0.

*Der Entwickler hat inzwischen **Transmission 2.9.2** veröffentlicht, das nach seinen Angaben nicht nur sauber ist, sondern angeblich aktiv gegen die Infektion vorgeht und ihre installierten Dateien löscht.*