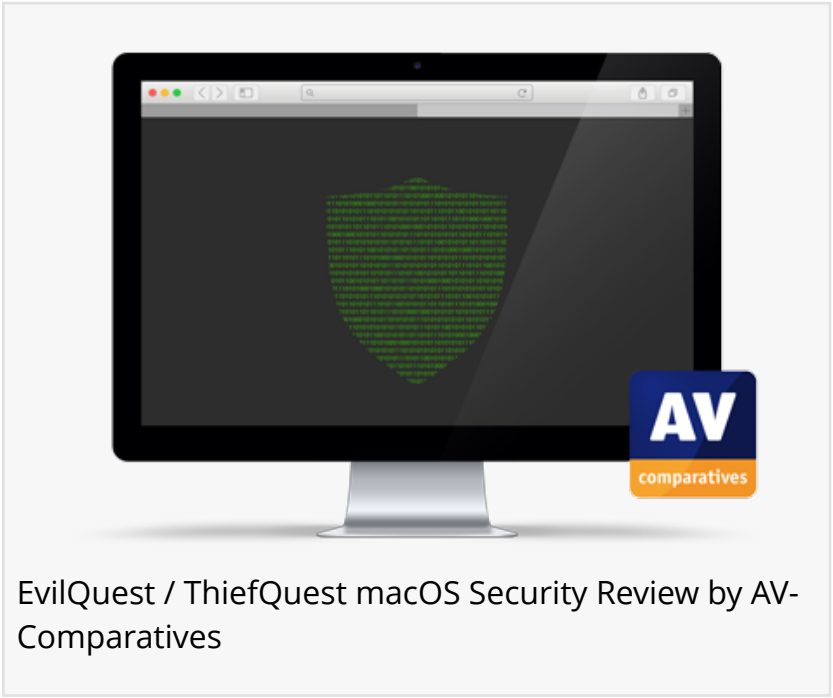
EvilQuest / ThiefQuest Ransomware für macOS zeigt die wie wichtig unabhängige Mac Antivirus Software Tests sind

EvilQuest / ThiefQuest ransomware wird nun von Avast ; AVG Avira; Bitdefender Crowdstrike Fireeye; Kaspersky; Trend Micro.

INNSBRUCK, TIROL, ÖSTERREICH, July 8, 2020 /EINPresswire.com/ -- Erste Sichtung

Am 29. Juni twitterte K7-Sicherheitsforscher Dinesh Devadoss @dineshdina04 über die Entdeckung eines neuen macOS-Ransomware -Programms (https://twitter.com/dineshdina04/status/1277668001538433025?lang=en).



EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Als EvilQuest / ThiefQuest bekannt, nicht zu verwechseln mit dem gleichnamigen Spiel, erscheint es auf den ersten Blick als ein eher übliches Ransomware-Programm, das Benutzerdateien verschlüsselt und gegen einen Entschlüsselungsschlüssel eine Bezahlung verlangt. Es stellt sich jedoch heraus, dass es besonders lästig ist.

> Macht ein Backup, bezahlt nicht das Lösegeld! Das Backup-Medium muss danach von Computer getrennt werden, um eine Verschlüsselung des Backup zu vermeiden!"
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

Obwohl die Ransommail eine Bitcoin-Adresse für die Zahlung enthält, gibt es für die Opfer keine Möglichkeit, sich mit den Angreifern in Verbindung zu setzen oder nachzuweisen, dass sie bezahlt haben.

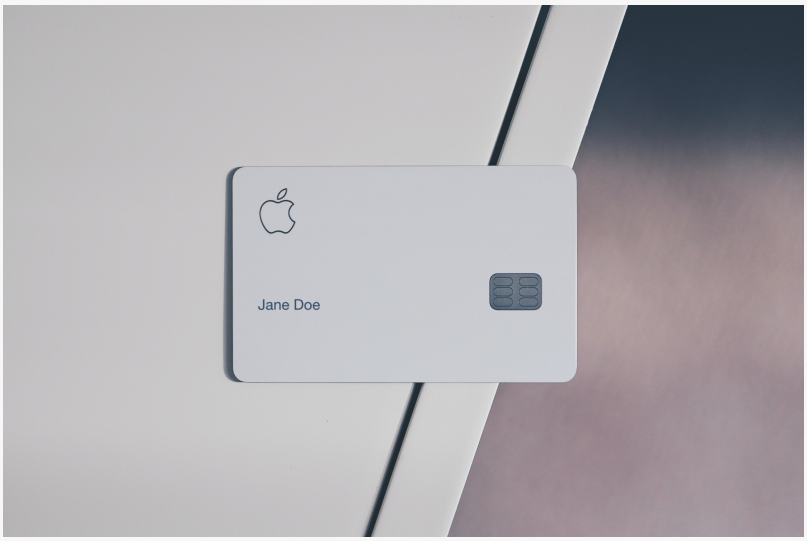
Was mach EvilQuest / ThiefQuest?

Schlimmer noch, EvilQuest / ThiefQuest hat noch andere böse Tricks auf Lager. Es installiert einen Keylogger, um jeden Tastenanschlag des Opfers aufzuzeichnen, und

verbindet das Zielsystem mit einer Kommando- und Kontrollzentrale, wodurch die Angreifer weitere Befehle ausführen können. Schließlich wird die Ransomaware versuchen, bestimmte Dateien in Bezug auf CryptoWallets auszufiltern, um mehr Geld zu stehlen.

EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Die Autoren von EvilQuest scheinen sich bemüht zu haben, zu verhindern, dass Malware-Forscher das Programm analysieren. Es scheint, dass es nicht auf virtuellen Rechnern - die häufig für die Malware-Analyse verwendet werden - oder auf dem System installiert sein kann (https://www.macworld.co.uk/news/mac-software/mac-ransomware-evilquestthiefque-3791288/).



EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Good News / Bad News

Die gute Nachricht über EvilQuest ist, dass es ziemlich schwierig ist, infiziert zu werden. Als eigenständiger Installer wird die Ransomeware nun von den eingebauten Sicherheitsmechanismen in macOS blockiert, vorausgesetzt, diese haben Zugang zu Apples Cloud-Diensten. Es scheint, dass Infektionen nur aufgetreten sind, wenn Benutzer kompromittierte Installer für gecrackte Versionen legitimer Anwendungen wie Little Snitch und Mixed in Key8 heruntergeladen haben, über torrenting Dienste. Selbst dann wird es den Mac nur infizieren, wenn die Sicherheitswarnungen von macOS blind durchgeklickt werden.

Soll ich das Lösegeld zahlen?

Die Bezahlung von Schutzgeld für die Entschlüsselung Ihrer Dateien ist in fast allen Fällen eine

Lotterie, aber in den meisten Fällen scheint es mehr oder weniger sicher, dass die verschlüsselten Daten für immer verloren gehen, selbst wenn Sie zahlen.

Was kann ich tun?

Macht ein Backup, bezahlt nicht das Lösegeld! Die beste Option ist, ein Backup häufig auszuführen. Aber man muss sicherstellen, dass das Backup-Medium danach von Computer getrennt wird, um eine Verschlüsselung des Backup zu vermeiden!

Verwendung von Antivirus-Software für macOS

Für Mac-Benutzer, die das Risiko eingehen, indem sie Software aus potenziell riskanten Quellen ausführen, wird deutlich, wie wichtig es ist, effektive, unabhängig getestete und zertifizierte Antivirensoftware für macOS zu betreiben.

Logo AV-Comparatives

EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Sie können sich auf unabhängige Vergleichstests verlassen, nicht aber auf Online-Vergleichswerkzeuge, z. B. Virustotal. Diese Tests sind oft falsch. Während diese Online-Scanner für andere Zwecke ihre Berechtigung haben, verlassen sie sich ausschließlich auf Kommandozeilenscanner, um hochgeladene Dateien auf Malware zu prüfen, die aber kein Real-World Szenario simuliert. Zusätzlich können einige Mac-Malware auf VT nur erkannt werden,wenn sie die richtige Dateierweiterung haben.

Ein komplettes Antivirusprogramm, das auf dem lokalen System läuft, hat eine ganze Reihe anderer Schutzmechanismen, wie URL-Blocker, Reputationsdienste und Verhaltensblocker, die die Chancen des Schutzes des Systems vor Infektionen erheblich erhöhen. Eine solche Sicherheitssoftware kann auch eine dynamische Analyse eines Programms bei der Ausführung durchführen und so Verschlüsselungstechniken (wie proprietäre Packer) umgehen, die in einem einfachen Scan des inaktiven Installers nicht erkannt werden können.

Wo findet man einen zuverlässigen macOS Antivirus Test?

Die von AV-Comparatives in ihrem Mac Malware Test verwendete Testmethodik erlaubt es den getesteten Programmen, eine Vielzahl von Schutzmechanismen, einschließlich cloud-basierter Dienste, zu nutzen, um das System vor, während oder nach der Ausführung bösartiger Programme zu schützen. Eine große Anzahl verifizierter Malware-Samples stellt auch die statistische Relevanz der Ergebnisse sicher.

Neben Mac-Malware überprüft der Test zusätzlich den Schutz gegen Mac PUA - eine zunehmende Belästigung - und die Erkennung von Windows-Malware-Samples. Letztere stellt sicher, dass macOS-Benutzer böswillige Programme nicht versehentlich an Freunde, Verwandte oder Kollegen weitergeben, die das Windows-Betriebssystem benutzen. Ein falsch-positive Test überprüft zusätzlich, dass die getesteten Mac-Antivirusprogramme Benutzer nicht mit falschen Alarmen auf legaler Software plagen.

Die in diesem Jahr geprüften und zertifizierten Programme sind in alphabetischer Reihenfolge:

Avast Security für Mac; AVG Internet Security für Mac; Avira Antivirus Pro für Mac; Bitdefender Antivirus für Mac; Crowdstrike Falcon Prevent für Mac (Enterprise Produkt); Fireeye Endpoint Security für Mac (Enterprise Produkt); Kaspersky Internet Security für Mac; Trend Micro Antivirus für Mac. Der Bericht enthält auch eine Handhabungstest, so dass die Leser ein Bild davon bekommen, wie jedes Programm in alltäglichen Situationen zu verwenden ist.

Wie alle öffentlichen Berichte von AV-Comparatives wird der 2020 Mac Security Test and Review kostenlos für jedermann zur Verfügung gestellt. Es kann hier heruntergeladen werden: https://www.av-comparatives.org/tests/mac-security-test-review-2020/

Peter Stelzhammer
AV-Comparatives
+43 720 115542
email us here