Erledigt Virus-Meldung OpenCore

Beitrag von „bob7“ vom 13. Juni 2020, 00:40

hi ich habe eine frage die nicht zum Thema passt, ich habe Viren in driver gefunden, meine uefi orner lade ich hoch, ich habe über die seite virustotal (https://www.virustotal.com/gui/)

entdeckt. weis vielleicht wie man sie loss wird? in opencore gibt es auch viele! ❗

Beitrag von „sn0wleo“ vom 13. Juni 2020, 00:40

mach bitte ein eigenen Thread auf.

Beitrag von „bob7“ vom 13. Juni 2020, 00:43

akay, vielen dank 🙂

Beitrag von „g-force“ vom 13. Juni 2020, 00:44

g-force: bob7 Ich habe deine Frage in einen eigenen Thread abgetrennt.

Beitrag von „bob7“ vom 13. Juni 2020, 00:46

ich habe Viren in driver gefunden, meine uefi orner lade ich hoch, ich habe über die seite

virustotal (https://www.virustotal.com/gui/)

entdeckt. weis vielleicht jemand, wie man sie loss wird? in opencore gibt es auch viele! 

Beitrag von „g-force“ vom 13. Juni 2020, 00:52

Wenn Du ein bißchen aufpasst und mitliest, dann hättest Du bemerkt, daß ich deinen ersten Post schon in ein eigenes Thema abgetrennt habe.

Nun habe ich deinen neuen (Doppel-)Post hier mit rein geschoben.

Beitrag von „bob7“ vom 13. Juni 2020, 00:55

Entschuldigung, du warst viel zuschnell für mich, da war ich schon an meinen thema schreiben 

Beitrag von „Sascha_77“ vom 13. Juni 2020, 00:58

Das heisst nix. Ich habe im Kext Updater auch mal ein Element mit drin gehabt was angeblich potentiell gefährlich ist (PCI Geräte auflisten). Ist aber Fehlalarm. Würde dem Ergebnis keine große Bedeutung beimessen. Diese ganzen Scanner machen die Pferde mehr scheu als alles Andere (was macOS angeht). So zumindest meine Meinung. Da muss ja nur jemand der so Sachen in Viren-Datenbanken einpflegt denken: "Och, das könnte aber gefährlich sein, dann markieren wir das mal direkt als Malware. Kann ja nicht schaden." Und schwupps denken die Leute ihr Rechner sei infiziert.

Beitrag von „bob7“ vom 13. Juni 2020, 01:00

gibt vielleicht ein tool, der den Trafik analysiert?

Beitrag von „Sascha_77“ vom 13. Juni 2020, 01:01

Auf Bootloaderebene? Nein. Das wäre mir neu.

Beitrag von „bob7“ vom 13. Juni 2020, 01:03

okay, danke für info  , ich überlege ob ich beim Hakentosh bleibe

---

Beitrag von „Sascha_77“ vom 13. Juni 2020, 01:04

?? Von was machst Du das abhängig? Von der Warnung des Scanners?

Beitrag von „bob7“ vom 13. Juni 2020, 01:06

ich habe angst, dass alle Passworte, Überweisungen, Konten, alle Daten gestohlen werden!

Beitrag von „Sascha_77“ vom 13. Juni 2020, 01:12

Aber nicht durch Hackintosh Bootloader. Sowas kann höchstens durch Unachtsamkeit eines Users passieren der z.b. einfach irgendein dubioses Programm aus noch dubioserer Quelle in macOS installiert was nach dem Root Passwort fragt und dann "böse" Sachen macht. Dazu ist dann aber die Interaktion des Benutzers nötig. Kurz gesagt: Bei solchen Sachen sitzt zumeist

der größte Unsicherheitsfaktor vor dem Bildschirm. Und das betrifft somit jedes Betriebssystem.

Beitrag von „bob7“ vom 13. Juni 2020, 01:28

okay vielen dank 

Beitrag von „g-force“ vom 13. Juni 2020, 01:29

bob7 Wir haben doch schon alle notwendigen Info aus deiner EFI. Du bist mit deiner IP im Hackintosh-Forum angemeldet, dein PC steht bim Profil.

Wird Zeit für eine Alu-Hut.

Wenn ein bestimmtes (von privat entwickeltes) Programm Scripte enthält, die dem User 1000 Eingaben ersparen, dann könnte ein Virenwächter Alarm schlagen.

Warum ich einen Virenwächter mit so hohem Level auf einem Hackintosh betreibe, auf dem ich dann Programme ausführe, die nicht von Apple stammen...

Überdenke mal deine Einstellung zu Apple und Hackintosh.

Beitrag von „bob7“ vom 13. Juni 2020, 01:50

welchen Virenwächter benutzt du?

Beitrag von „Sascha_77“ vom 13. Juni 2020, 02:02

Ich z.b. gar keinen. macOS ist ja nicht Windows. Es gibt zwar Malware für den Mac aber in den

ganzen Jahren (angefangen mit OSX in 2001) hatte ich keine Probleme mit sowas. Aber die Frage Antivirus für Mac, ja oder nein ist zumeist eh eine Geschmacksfrage.

Unter Windows hingegen möchte auch ich **nicht** ohne Schutz unterwegs sein. Und wenn es nur der eingebaute Defender ist.

Beitrag von „bluebyte“ vom 13. Juni 2020, 08:24

bob7 ... ganz viele Viren in Opencore? Mal hören was Opencore-Entwickler mhaeuser dazu meint.
Seriöse Hackintosh-Entwickler stehen uns hier im "Hackintosh-Forum" mit Rat zur Seite.

So mal nebenbei gesagt. Habe selbst schon viel mit der Script-Sprache "Auto-IT" experimentiert und programmiert. Gab damit auch immer Warnungen, sobald man beim Kompilieren die UPX-Kompression ausgewählt hat. Manchmal sind es nur ungünstige Einstellungen des Compilers, die aus einem harmlosen Programm eine Malware zaubern.

Beitrag von „griven“ vom 13. Juni 2020, 08:34

Eine klare Empfehlung für einen Virenscanner kann und will ich nicht aussprechen dafür aber eine deutliche gegen einige Vertreter dieser Zunft

Von Programmen wie dem ehemalig gutem AVIRA zum Beispiel lässt man besser die Finger denn die sind gerade in den kostenfreien Varianten inzwischen eher selbst eine Malware/Bloatware als das sie einen sinnvollen Nutzen hätten. Verwende Deinen Mac/Hack einfach mit Bedacht und gib Dein Passwort zum Beispiel nur dann ein wenn Du weißt was passiert oder die Installation von Software selbst angestoßen hast. Was sogn. false Positives angeht also Falschmeldungen von Virenscanner so ist es an der Stelle schon so wie bluebyte schreibt. Viele Scanner sind zudem auf die typischen Windows Muster optimiert und in dem Kontext sind Dinge die unter macOS oder Unix/Linux zum Tagesgeschäft gehören gerne schon mal unter Generalverdacht gestellt weil sie in Systemnahe Abläufe eingreifen. OpenCore zum Beispiel ist eine Erweiterung für die Firmware also in den Augen vieler Virenscanner schon mal per se verdächtig einfach weil OpenCore per Definition VOR dem Betriebssystem ausgeführt

wird und in dieser Phase natürlich Dinge implementieren könnte die unerwünscht sind oder eine potentielle Bedrohung darstellen. Viele der Dinge die wir tun/tun müssen um einen Hackintosh zu betreiben sind in der Tat mit der Arbeitsweise von Viren vergleichbar denn wir nehmen unter anderem Änderungen am Bootprozess (Bootloader, EFI Treiber usw.) vor und greifen an diversen Stellen sehr tief ins System ein um macOS dazu zu bewegen auf unserer Hardware überhaupt einen Mucks von sich zu geben.

Beitrag von „mhaeuser“ vom 13. Juni 2020, 09:29

bluebyte Seit 0.5.2 aktualisieren wir nur noch die Viren in OC, weil Apple nachlegt. /s

Was ich dazu meine? Manche Leute sollten besser Windows benutzen und nicht nur ein AV sondern auch eine Kindersicherung aktivieren.