SCRUTIL STATUS merkwürdige Meldung

Beitrag von „WITON“ vom 27. April 2023, 22:52

Hallo Freunde, ich wollte prüfen ob mein SIP aktiviert ist und erhalte eine andere Meldung... Da müsste doch bloß enabeld oder disabled stehen. Was bedeutet das. Hat jemand eine Ahnung ?

Beitrag von „Maulwurf“ vom 27. April 2023, 23:14

Das ist die Vollumfängliche Ausgabe.

Hatte ich letztens auch. Zur Zeit aber nur disabled oder enabled.

Hat was mit den HExwerten zu tun die du unter NVRAM ----> CSR-Active Config einstellen kannst.

Das hier ist die Empfehlung von griven

csr-active-config DATA 67F00000

Ansonsten das hier.

csr-active-config DATA 00000000 ——> SIP Completely Enabled

Schau mal bei Dortania vorbei und Guck was noch für andere Werte möglich sind.

Wenn du wie ich Toggle SIP benutzt kommt nur die Disabled oder enabled Ausgabe.

Wenn du manuell die Hexwerte setzt, zeigt er dir das Potpourri an was alles enabled oder eben disabled ist.

Toggle SIP macht halt absolute Werte.....Also Stumpf An oder AUS.

Mit den Zwischenkonfigs zeigt es dir halt detailierter an.

Beitrag von „WITON“ vom 27. April 2023, 23:51

Maulwurf , ich dachte schon ich hab mir einen Virus eingefangen. Safari brachte nämlich laufend Nachrichten das ich gehackt worden bin, Mein Konto wird angegriffen usw. der Störenfried nennt sich ASK YOU und sitzt wahrscheinlich in Safari. Ich habe das gesamte System scannen lassen Mit Spyhunter.. Nichts gefunden. Auch Clean my Mac zeigt nach ausführlichem Scan nichts an. Habe gesehen das in der Mitteilungszentrale das Viech ASK YOU sich einquartiert hat. Frage mich wo das herkommt. Habe es entfernt. Mal sehen ob nun Ruhe ist. De Safari Browser auf Werkseinstellung zu setzen und alles im Browser zu löschen geht wahrscheinlich nicht.Diese SIP Meldung in Verbindung mit den Meldungen von ASK YOU hat mich schon bisschen erschreckt. Gott sei dank habe ich für alle Fälle eine komplette Sicherung. So wie ich Dich verstanden habe bedeutet diese TERMINAL Antwort keine Gefahr und ich könnte es auch ignorieren ? Habe gerade über Bootstick gebootet und SIP aktiviert. der Befehl wird ordentlich übernommen. Nach Systemstart gibt aber das Terminal wieder diesen erweiterten Bericht.Wenn das kein Problem darstellt müsste ich doch nichts ändern Oder ?

Beitrag von „griven“ vom 28. April 2023, 00:02

Nope stellt kein Problem dar und tut exakt das was es tun soll

Die SIP kennt eben nicht nur an oder aus sondern auch so manches zwischen an und au
Man kann die SIP sehr fein einstellen und ziemlich genau bestimmen was erlaubt und was verboten sein soll aber für den normalen Betrieb ist es eigentlich ratsam die SIP einfach aktiv zu lassen. Es gibt, auch auf dem Hackintosh, eigentlich keinen Grund (mehr) daran rum zuschrauben. Dieses ASK ME Dingen ist so ein Spaß den man sich gerne mal einfängt wenn man auf dubiosen Seiten unterwegs ist oder dubiose Programme ausführt. Mein Tipp an der Stelle einfach die Finger weg lassen von allem was nicht vertrauenswürdig ist bzw. aus Quellen stammt denen man nicht zu 100% vertraut andernfalls frei nach Stoppok:

https://www.youtube.com/watch?v=XLgdXFR49GQ

Beitrag von „WITON“ vom 28. April 2023, 00:26

griven , danke für die Lektion.... schmunz .Dubiose Programme nicht, aber neugierig machende Internetseiten schon. Man googelt ja nicht nur nach Kochrezepten Gott sei dank war nur Safari betroffen. Schön mit Dir und den anderen zu quasseln

---

Beitrag von „ozw00d“ vom 28. April 2023, 07:29

WITON wenn sich etwas eingenistet hat, am Client, nicht lange Fackeln und neu aufsetzen. Du weißt nie wo sich sonst noch was eingenistet hat.

Beitrag von „WITON“ vom 28. April 2023, 15:44

ozw00d , um Gottes Willen.. Die Installation würde wieder Tage dauern. Da müsste doch eine Backup Sicherung von Time Machine auch sicher sein. Das würde vielleicht ne viertel Stunde

dauern. Sollte die Meldung wiederkommen muss ich das auch machen. Oder reicht die Rücksicherung nicht ?

Beitrag von „user232“ vom 28. April 2023, 16:04

ozw00d hat den richtigen Tipp gegeben, alles andere ist Murks und fahrlässig.

ASK YOU hab ich nie zuvor was gelesen, gefunden hab ich jetzt das hier.

Auch würde ich die Finger von CleanMyMac u.ä. lassen.

Beitrag von „ozw00d“ vom 29. April 2023, 06:00

WITON mal ein wenig deutsche Lektüre https://www.bsi.bund.de/DE/The…e.html#doc507166bodyText4

abgesehen davon, bist du jemand der scheinbar nicht wirklich viel davon versteht.

Time Machine Wiederherstellung klingt erst mal super, allerdings kann dir niemand garantieren das der Schurke sich nicht auch dort eingenistet hat ohne forensische Untersuchungen an zu stellen.

Mit anderen Worten nein das reicht nicht.

Die allermeisten Schadsoftware zielt erstmal darauf ab sich ein zu nisten ohne das der normale Anwender eine Möglichkeit hat diese zu entfernen.
der zweite Schritt ist dein System so zu kompromittieren das weitere Schadsoftware nachgeladen wird.

Bei so einer Software würde ich immer erst das Netzwerkkabel ziehen, damit das viech sich nicht weiter verbreiten kann.

Dann würde ich neu aufsetzen. Und erst mal alle Kennwörter ändern.

Man weiß nie was nicht bereits geloggt oder kopiert wurde.

Beitrag von „Maulwurf“ vom 29. April 2023, 11:52

WITON da stimme ich dem ozw00d voll und ganz zu!

Wenn du Software ausprobieren möchtest, dann richte dir doch eine Testpartition ein.

Ich habe das jetzt so gemacht. Das ich ein 13.3.1 Produktiv System habe.

Und eine Dynamische zweite 13.3.1 Testpartition. Da ist erstmal nur Das MAcOS drauf.

Da kann ich dann erstmal in Ruhe zukünftige macOS Updates Testen und prüfen.

Sowie Software installieren und Kompatibilitätsproblemen Probleme Testen usw.

Hatte letztens auch gedacht das ein Time Maschine Backup reicht.

Hat nur leider zur hälfte geklappt.

NI- MAschine hat die bereits installierten/ zurück gespielten Plugins nicht alle erkannt.

So konnte ich trotzdem wieder alles neu Installieren.

Deswegen arbeite ich jetzt mit einem Super Duper Klon.

Den würde ich aber erst anlegen, wenn du zu 100 Prozentig sicher sein kannst, das da nichts verdächtiges drauf ist.

Beitrag von „iPhoneTruth“ vom 29. April 2023, 12:31

Ich hatte diese Meldung "ASK YOU" auch mal bei mir auf dem MacBook.

Zwei Virenscanner habe ich drüber laufen lassen, beide haben nichts erkannt, konnten damit auch nichts entfernen.

Auch Lulu hat da nichts angezeigt, daß da wer nach außen funkt (da kann so was wie Lulu dann doch mal interessant sein).

Hier fand ich dann die Methode, diese "Notification" in Safari zu enfernen:

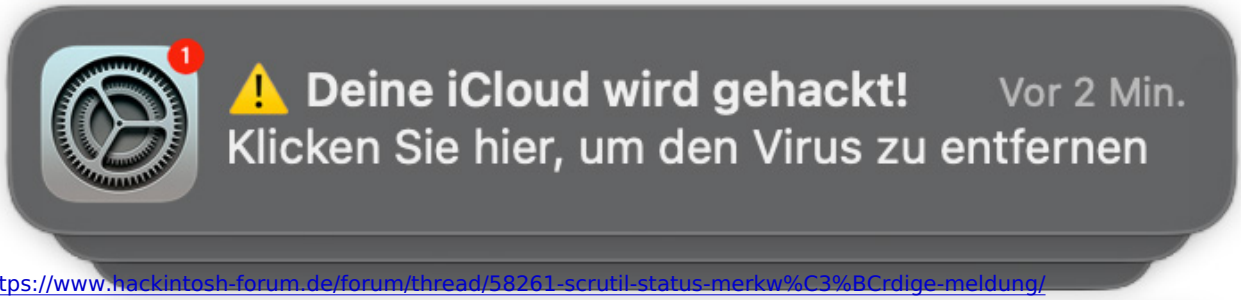
https://discussions.apple.com/thread/254511125

Nach diesen Angaben habe ich "ASK YOU" entfernt und seither habe ich Ruhe.

Deswegen glauben ich nicht, daß es sich hierbei um eine echte Gefahr handelt.

Meines Erachtens würde ein echter Virus oder Trojaner sich nicht so plakativ geben wie diese einfache Meldung, die in Safarie nur die Erlaubnis hat, Mitteilungen durchzugeben.

Beitrag von „WITON“ vom 29. April 2023, 12:57



Hallo

Wenn man drauf klickt, wird man auf bösartige Websites gelenkt

Gemeinde, ich habe ASK YOU entfernt. Habe meine Windows Lizenz von ESET auf MAC CYBER SECURITY PRO erweitert. Hat 19 Euro gekostet.Nach dem Tiefenscan aller !! Laufwerke hat ESET das Vieh gekillt. Es war nicht als Virus deklariert sondern als bösartige Website Verlinkung (Malware) in Safari. Nun ist gut.. Ich verwende ESET schon in Windows seit vielen Jahren und es hat immer sofort angeschlagen wenn auf einer Website was verdächtiges oder gar gefährliches ist.Kack auf die 19Euro.. Ich lass den jetzt mit werkeln im OS.

Beitrag von „user232“ vom 29. April 2023, 13:45

Ausgangslage:

- Zeitpunkt des Einfangens von Malware, Viren, Programminstallation etc. bekannt
- Time Machine aktiviert

ToDo wenns ganz schnell gehn soll:

- Recovery booten
- "Aus Time Machine wieder herstellen" wählen
- SSD auf dem das macOS installiert ist auswählen
- gewünschtes Backup zurückspielen
- ...dauert ein paar Sekunden, neustarten

Lokale Snapshots können im FDP angeguckt werden. (Darstellung/APFS-Schnappschüsse einblenden)

Beitrag von „WITON“ vom 29. April 2023, 14:07

user_232 , jetzt muss ich mal ganz dumm fragen... Wie boote ich am Hacky in den Recovery Mode ? Über einen Bootstick

---

Beitrag von „user232“ vom 29. April 2023, 14:08

Während der Bootpicker angezeigt wird, Leertaste drücken.

Beitrag von „WITON“ vom 29. April 2023, 14:16

user_232 , vielen Dank gerade mal probiert.. Man lernt nie aus