BigSur und (die nicht vorhandene) Privacy…

Beitrag von „5T33Z0“ vom 16. November 2020, 08:01

Ganz erhellender Artilel zum Thema Privacy unter BigSur…

"On modern versions of macOS, you simply can’t power on your computer, launch a text editor or eBook reader, and write or read, without a log of your activity being transmitted and stored.

[…]

Now, it’s been possible up until today to block this sort of stuff on your Mac using a program called Little Snitch (really, the only thing keeping me using macOS at this point). In the default configuration, it blanket allows all of this computer-to-Apple communication, but you can disable those default rules and go on to approve or deny each of these connections, and your computer will continue to work fine without snitching on you to Apple.

The version of macOS that was released today, 11.0, also known as Big Sur, has new APIs that prevent Little Snitch from working the same way. The new APIs don’t permit Little Snitch to inspect or block any OS level processes. Additionally, the new rules in macOS 11 even hobble VPNs so that Apple apps will simply bypass them.

[…]

@patrickwardle lets us know that `trustd`, the daemon responsible for these requests, is in the new `ContentFilterExclusionList` in macOS 11, **which means it can’t be blocked by any user-controlled firewall or VPN.** In his screenshot, it also shows that CommCenter (used for making phone calls from your Mac) and Maps will also leak past your firewall/VPN, potentially compromising your voice traffic and future/planned location information."

https://sneak.berlin/20201112/your-computer-isnt-yours/

Beitrag von „Aluveitie“ vom 16. November 2020, 08:18

Gibt noch einen guten Artikel zu OCSP und Apple: https://www.security-embedded.…rd-but-

apple-does-it-well

Beitrag von „Sascha_77“ vom 16. November 2020, 08:23

Und wieder ein Grund mehr solange es geht auf 10.15.x zu bleiben. Bin mal gespannt ob es eine Lösung geben wird das auszuhebeln.

Beitrag von „radartomx“ vom 16. November 2020, 08:50

Lässt sich das mit PiHole aushebeln?

Beitrag von „Sascha_77“ vom 16. November 2020, 08:53

Stimmt. Wenn du die Adresse/n dort blacklistet sollte es eigtl. gehen.

Dann wirds wohl bald irgendwo auf github oder so eine Apple-Sperr-Liste geben.

Beitrag von „toasta“ vom 16. November 2020, 08:54

Aber starten dann nicht die Programme alle wieder so langsam, weil die Server nicht gefunden werden, wenn man die Adresse blockt?

Das war ja das Problem vor ein paar Tagen bei Apple.

Beitrag von „Sascha_77“ vom 16. November 2020, 08:57

Auch wieder wahr ... hm. Vor allem starten dann auch nicht Apple Apps langsam weil die Signierung nicht geprüft werden kann.

Auf der anderen Seite ... wenn man den Netzwerkstecker rauszieht gehts ja auch wieder schnell. Vllt. kann man dem System bei gewissen Prüfungen vorgaukeln es wäre kein Netz vorhanden. Eine Art Network-Stealth-Mode.

Scheint ja dieses "trustd" für verantworlich zu sein für die Überprüfun

```
T440:~ luigi$ ps ax |grep trustd
  150   ??  Ss     0:11.77 /usr/libexec/trustd
  205   ??  S      0:00.12 /usr/libexec/trustd --agent
  288   ??  S      0:07.94 /usr/libexec/trustd --agent
  580   ??  S      0:00.32 /usr/libexec/trustd --agent
```

EDIT:

Hab mir gerade mal die Binary angeschaut ...

```
1ED7 I \A<ΔÖPÏÖ◆Y ÅËñËjÃ≥«FøÅH-  °s ◊
1604 Ë'®IH¢ A      £Ç z0Ç v0   U
FF04  Y∏+î: ∫Ò ÆÓPR#3…Y√Tò0   U    ˇ
5052  0   ˇ0   U #  0 Ä Y∏+î: ∫Ò ÆÓPR
2A86 #3…Y√Tò0Ç    U   Ç  0Ç  0Ç    *Ü
2F2F HÜ˜cd  0ÅÚ0*  +         https://
0505 www.apple.com/appleca/0Å√  +
6966    0Åð Å≥Reliance on this certif
6570 icate by any party assumes accep
7461 tance of the then applicable sta
7573 ndard terms and conditions of us
6966 e, certificate policy and certif
```

Wenn man derlei Adressen da drin einfacht verbiegt? "https://www.apple.com/applexx/" z.B. und schon wäre Ruhe? Wobei ... dann ist man ja im Grunde da wo man mit Pihole wäre. Er versucht die URL zu erreichen und hängt solange fest.

Beitrag von „toasta“ vom 16. November 2020, 09:13

war das nicht auch ocsp.apple.com was die Probleme verursachte.

UPDATE:

habe gerade das hier per Zufall gefunden:

https://support.apple.com/en-us/HT210060

Beitrag von „wmb“ vom 16. November 2020, 09:17

Habe gelesen, wenn man ocsp.apple.com auf 127.0.0.1 leitete, also blockierte, ging es wieder.

Ich würde technikaffinen Leuten generell PiHole ans Herz legen, nicht nur wegen Apple. Es gibt ja kaum noch ein Gerät im Haushalt das nicht gefühlt alle 5 Millisekunden nach Hause telefoniert... Denkt zB. mal ans Wohnzimmer.

Beitrag von „Sascha_77“ vom 16. November 2020, 09:21

Jo alles auf den localhost leiten über /etc/hosts wäre auch ne Möglichkeit. Ich glaube ich teste das mal nachher bei meiner BS Test Installation wo ich dann alle Adressen die unter Certificate validation stehen mal umleite. Sehe im Pihole Log ja dann ob noch was rausgehen will wenn ich ne App starte.

Beitrag von „wmb“ vom 16. November 2020, 09:23

Vorsicht: Was wenn die Zertifikate ablaufen und erneuert werden müssen? Bin damit nicht im Detail vertraut, aber eventuell starten die Apps dann gar nicht mehr?

Beitrag von „Sascha_77“ vom 16. November 2020, 09:32

Wenn "spctl --master-disable" durchgeführt wurde müsste das eigtl. egal sein. ?

Beitrag von „Heiko77“ vom 16. November 2020, 09:33

Blocken von `ocsp.apple.com` über den Router sollte ebenfalls zum Erfolg führen, oder sehe ich das falsch?

Beitrag von „Sascha_77“ vom 16. November 2020, 09:42

Wenn man das über /etc/hosts macht könnte das eher den Effekt haben, dass der Daemon denkt das System ist offline. Macht man das über den Router geht ja auf jeden Fall schonmal eine Verbindung zu diesem raus.

Beitrag von „karacho“ vom 16. November 2020, 09:44

Die Server sind doch in der Datei `ContentFilterExclusionList` gelistet. Was, wenn man die Server darin auskommentiert und die Datei dann Schreibgeschützt wieder speichert? 🤔

> Zitat von Sascha_77
>
> Wenn man das über /etc/hosts macht

Die soll wohl in einer der nächsten Versionen verschwinden.

Beitrag von „Sascha_77“ vom 16. November 2020, 09:46

> Zitat von karacho
>
> Die soll wohl in einer der nächsten Versionen verschwinden.

Na super. Aber warum wundert mich das nicht.

Beitrag von „wmb“ vom 16. November 2020, 09:55

> Zitat von Sascha_77
>
> Wenn "spctl --master-disable" durchgeführt wurde müsste das eigtl. egal sein. ?

Ich glaube dass bezahlte Apps aus dem App Store damit dennoch ein Problem haben könnten. Nur eine Vermutung.

Beitrag von „Sascha_77“ vom 16. November 2020, 09:56

Wobei ich zu befürchten ist, dass sie diesen Befehl demnächst auch abschaffen werden. Zutrauen würde ich denen das. Geht halt immer mehr hin zur Verkapselung wie bei iOS. ich denke bei den ARM Rechnern wird man dann demnächst auch eine Art Jailbreak machen müssen wenn man das System "offen" haben möchte.

Beitrag von „Obst-Terminator“ vom 16. November 2020, 10:13

Also oscp.apple.com lasse ich schon immer von der PiHole mitblocken (wegblocken) und das hat bisher noch nie Probleme gegeben. Zumindest keine die mich in der Nutzung und Funktion eingeschränkt hätten. Wenn es da noch mehr URL‘s in Richtung Apple, würde ich die ebenfalls wegblocken. Solange bis tatsächlich irgendwelche Funktionsbeeinträchtigungen aufschlagen.Je weniger Traffic in diese Richtung, desto lieber ist mir das.

Beitrag von „5T33Z0“ vom 16. November 2020, 10:21

https://twitter.com/itsluncht1me/status/1326996963649175553

~~Ich denke, mann knnte die REgel auch in die Blacklist vom Router einbauen.~~

Beitrag von „DSM2“ vom 26. November 2020, 12:01

Ein bisschen was zur Thematik :

https://eclecticlight.co/2020/…-online-for-over-2-years/