Erledigt „EvilOSX“ wird es Zeit für ein AV Programm?!

Beitrag von „revunix“ vom 24. Februar 2018, 20:47

Hey,

ich habe da gerade was bei Github gefunden...
Früher dachte ich immer das es RAT (Remote Administration Tool) nur für Windows gibt, aber der folgende Link hat mich stutzig gemacht: https://github.com/Marten4n6/EvilOSX

Wie seht ihr das ganze?

Grüße,
alex

Beitrag von „al6042“ vom 25. Februar 2018, 14:01

In Bezug auf die ggf. damit aufdeckbaren Sicherheitslücken ist das natürlich ein gutes Tool, auf der anderen Seite ist es wie bei allen anderen Sachen.
Das Ganze ist mit Vorsicht zu geniessen, da sehr mächtig und leicht zu missbrauchen.

Beitrag von „Frankiee“ vom 25. Februar 2018, 14:39

Ich habe gerade das hier testweise im Betrieb: https://www.objective-see.com/products/blockblock.html

Was haltet Ihr davon? Sollte zumindest einige Versuche aufdecken, Software aller Art ("gut" wie auch "böse") persistent zu installieren.

Beitrag von „al6042“ vom 25. Februar 2018, 15:00

Klingt nach einem guten Plan.

Beitrag von „Frankiee“ vom 25. Februar 2018, 16:24

Zumindest "meckert" das Tool auch bei normalen Installationen, scheitn also zu tun, was es vorgibt zu tun. Der Betreiber der Site (Patrick Wardle) ist auch ein relativ bekannter Sicherheitsexperte, der schon auch die eine oder andere macOS Lücke aufgedeckt hat.

Also ich denke das taugt durchaus was, und ich werde es mal aktiv lassen. Natürlich ist bei so Dingen auch Little Snitch potentiell nützlich, was ja ebenfalls "verdächtige" Aktivitäten anzeigen kann (aber auch dazu führen kann, dass Dinge nicht wie gewünscht funktionieren).