Security rootkits check - wie?

Beitrag von „Wolfe“ vom 5. November 2022, 11:41

Liebes Forum,

ich würde gerne meinen Rechner auf rootkits prüfen. Dazu gibt es im Netz viele Hinweise, insbesondere auf chkrootkit und rkhunter, die im Terminal gestartet werden sollen. Ventura kennt diese Programme von Haus aus nicht und ich werde nicht irgendetwas aus dem Internet herunterladen, das mir eine Lösung verspricht, aber womöglich ein rootkit installiert.

Wie gehe ich am Besten vor?

Beitrag von „ozw00d“ vom 5. November 2022, 12:55

Wegen den Tools musst du dir keine Sorgen machen. Ohne wirst du allerdings mal keine Möglichkeit bekommen dein System daraufhin zu prüfen.

Beitrag von „Wolfe“ vom 5. November 2022, 13:02

ozw00d
"Wegen den Tools musst du dir keine Sorgen machen." Was meinst du mit diesem Satz?

"Ohne wirst du allerdings mal keine Möglichkeit bekommen dein System daraufhin zu prüfen."
Mir ist schon klar, dass ich kein Programm einsetzen kann, wenn ich es nicht habe. Oder meintest du etwas anderes?

Beitrag von „ozw00d“ vom 5. November 2022, 13:15

Ok anders ausgedrückt die Tools sind zur freien Verfügung zb. Auf GitHub.

klar gibt es dort auch schwarze Schafe, aber ich wollte damit sagen die Tools hatte ich selbst schon in Verwendung und sie schaden nicht.
und ja ohne das du dir diese lädst wirst du keinen Check starten können.

Ich würde sogar noch weiter gehen, insofern du die Vermutung hast kompromittiert zu sein, installier dir ein Test System, darauf solche Tools, erstelle ein Image von deinem kompromittierten System und scanne das mit den Tools auf Herz und Nieren.

Beitrag von „talkinghead“ vom 5. November 2022, 14:34

Zur Be(un)ruhigung: "OpenCore is an open-source, unconventional, first-in-class piece of software designed to intercept kernel loading to insert a highly advanced rootkit,[...]"

Quelle: https://github.com/khronokernel/OpenCore-Desktop-Guide

Eigentlich bräuchtest Du ein Tool, was Opencore auf deinem Hacky anmeckert.

rkhunter und chrootkit z.B suchen auch nur nach bekannten IOCs. Ähnlich ist es bei rootkit-detection-Frameworks für Smartphone-OS.

Rootkits sind m.E. eine andere Klasse von Malware, die generisch schwer erkennbar ist im Vergleich zu Malware, die aktiv z.B. lateral Movement, Persistenz, Verschlüsselung,RAT durchführen und dadurch vorhersagbarer in den Aktivitäten ist.

MacOS scheint offensichtlich kein Problem mit opencore zu haben.

Um Rootkits auszuschließen, geht m.E. nur der Weg über nahtlos verkette Vertrauensanker von Hardware, Bios, Bootloader, Betriebssystem.

Beitrag von „Wolfe“ vom 5. November 2022, 14:39

talkinghead Der Grund meiner Anfrage ist die Aktualisierung meines Bios, um Sicherheitslücken zu schließen. Da ich nun schon seit einem Jahr einen Rechner mit diesen Lücken in Betrieb habe, würde ich gerne prüfen, ob sie ausgenutzt werden.
Außerdem rechne ich damit, dass die Mehrheit der Nutzer des Designare z390 als Hackintosh diese Aktualisierung noch nicht durchgeführt haben, da eine Rückkehr zur vorigen Biosversion ausgeschlossen wird.

Beitrag von „mhaeuser“ vom 6. November 2022, 09:25

talkinghead Weder OC noch Lilu sind Rootkits, weil sie die Privilegien anderer Software nicht bis kaum erweitern.