Trojanerjagd

Ganz früher gab es mal HijackThis.
Das wird auch noch weitergeführt, allerdings als Fork, und das von einem Ukrainer. Wegen des Krieges mit Russland bitte vorsichtig sein: https://github.com/dragokas/hijackthis (bei Sicherheit zählt halt auch sowas …)
Dort ist Krieg und keiner kann garantieren dass Hijackthis millitärisch durch Russland genutzt wird.

FRST – oder das Farbar Recovery Scan Tool – macht das Gleiche. BleepingComputer-Downloadlink, weil Originaldownload hinter Adblock-Gemecker.

Wichtig ist, dass weder HijackThis noch FRST irgendwas tut, das erstellt euch ein File mit allen Daten aus allen relevanten Bereichen in denen Trojaner und Viren drin sein könnten. Dienste, laufende Prozesse, etc.

Früher gab es mal die berühmte Logfileauswertung, da konnte man dann alle Treffer mit Anomalien (z. B. Dienste deren Prozesse in einem anderen Speicherort liegen etc.) easy erkennen und die Dienste dann abschießen. Die gibts leider nicht mehr.

Wenn man also selbst die Zeit nicht investieren will – die Logs sind umfangreich, weil halt alle Details zu allen relevanten Bereichen – kann man stattdessen das https://www.trojaner-board.de damit nerven.

Dort scheints i. d. R. folgender Prozess zu sein:

1. https://www.malwarebytes.com/solutions/rootkit-scanner
2. adwCleaner und Anleitung dazu
3. neues Logfile vom FRST fürs Forum.

Die Logfiles von FRST oder HijackThis enthalten wie gesagt sämtliche Einträge, die relevant sein könnten. Ob diese Einträge dort richtig sind oder eine Anomalie darstellen ist dann eure Aufgabe.

Das bedeutet in der Regel umfangreiche Recherchearbeit, um festzustellen, ob Einträge von Windows stammen, zu einem bestimmten Programm gehören oder von Drittanbieter-Software gewollt sind. Also ziemliche Fummelarbeit.

Version #4
Erstellt: 2023-10-23 21:52:01 UTC von Konstantin
Zuletzt aktualisiert: 2024-07-05 09:16:40 UTC von Konstantin