BKA-Trojaner / GEMA-Trojaner

02.07.2025 08:57:25

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit::Trojaner, Viren, etc.	**Bewertungen:**	2
Status:	öffentlich (Alle)	**Ergebnis:**	100.00 %
Sprache:	de	**Letzte Aktualisierung:**	20:10:48 - 21.02.2024

Schlüsselwörter

BKA-Trojaner, GEMA, Trojaner, BKA, Virus, UKash, Sperren

Symptom (öffentlich)

Nach Hochfahren eines Rechners wird der Bildschirm vermeintlich durch das Bundeskriminalamt oder die GEMA gesperrt, mit der Aufforderung binnen kurzer Zeit Geld zu überweisen, damit der PC entsperrt wird.

Ein gesperrter Bildschirm könnte z.B. so aussehen:

Problem (öffentlich)

Eine Schadsoftware blockiert den Desktop und verhindert das Ausführen sämtlicher Befehle (z.B. die Tastenkombination für den Task-Manager), selbst nach Neustart tritt das Problem wieder auf.

In einigen Fällen hilft selbst die Arbeit im abgesicherten Modus als Administrator nicht weiter, da sich einige Varianten "tief" in die Registry und Autostart schreiben und auch dort den Bildschirm blockieren.

Antivirensoftware ist meist nicht in der Lage diese Schadprogramme vorab zu erkennen und zu blockieren.

Auffallend sind meist unsinnig klingende Sätze und viele Rechtschreibfehler.

Lösung (öffentlich)

Plötzlich ist der Computer gesperrt und es erscheint eine Meldung auf dem Bildschirm, die einem mitteilt, man hätte eine Straftat im Internet begangen. Gegen die Zahlung von 100 Euro per Ukash-Karte, soll die Sperre wieder aufgehoben werden. Die Ukash Karte ist jedoch lediglich ein Zahlungsmittel, bei dem es möglich ist, einem anonymen Zahlungsempfänger Geld zukommen zu lassen. Das diese Karten bei Tankstellen erhältlich sind, steht meist auch in dem Hinweis. Normalerweise wird jedoch trotz der Eingabe des Codes der Bildschirm nicht entsperrt und das Geld ist weg.

Diese Schadsoftware gibt es mittlerweile in vielen unterschiedlichen Varianten, mal als Meldung der Bundespolizei, mal als GVU- oder GEMA Meldung oder auch als vorgetäuschte Sicherheitswarnung. Das schlimme daran ist, dass es sich nicht um einen Virus sondern eine Schadsoftware handelt. Daher ist auch nicht zu erwarten, dass ein Virenscanner diese Software findet. Meist läßt sich auch nicht nachvollziehen, wo man sich diese Schadsoftware eingefangen hat, denn sie aktiviert sich in aller Regel erst ein paar Tage später.

Nun stellt sich zunächst die Frage: „Wie beseitige ich die Schadsoftware?“ Wer eine ganz einfache Grundregel beachtet hat, hat es hier relativ leicht: Wenn man als „eingeschränkter Benutzer“ arbeitet, nistet sich die Software meist im Temp-Verzeichnis des Benutzerprofils (%TEMP%) ein, also unter C:\Dokumente und Einstellungen\<Benutzername>\Temp\ bei WinXP oder C:\Users\<Benutzername>\AppData\Local\Temp unter Windows Vista/7. Alles was in dem Verzeichnis liegt, kann in der Regel ohne Probleme gelöscht werden, zumindest wenn ein anderer Benutzer angemeldet ist. Verwendet man eine Software, die bereits beim Einloggen das Temp-Verzeichnis löscht, kann es sein, dass man sich die Software mal eingefangen hat, diese jedoch noch gelöscht wird, bevor sie jemals aktiviert werden kann. Es kann dann natürlich sein, dass in der Systemregistrierung noch der Eintrag zum Starten der Schadsoftware existiert. Wer mit regedit unter HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run schaut, findet möglicherweise einen mysteriösen Eintrag, wie z.B. %TEMP%\234756234675923756938247569283.exe. Dieser Eintrag ist schon sehr verdächtig und sollte entfernt werden.

Alle, die mit administrativen Rechten arbeiten haben jetzt ein Problem. Durch die administrativen Rechte, kann sich die Software an jeder beliebigen Stelle im System verstecken und ist so kaum zu finden – erstrecht, weil es so viele Varianten der Software gibt.

Meistens ist der Benutzer mit dem gearbeitet wird der einzige im System vorhandene Benutzer. Es gibt also auch keine Möglichkeit mehr, sich mit einem anderen Benutzer anzumelden und die Schadsoftware zu suchen.

Auf der Internetseite der [1]Bundespolizei gibt es eine Übersicht der unterschiedlichen Varianten. Diese Seite wird immer wieder mal aktualisiert. Ausserdem gibt es auf der Seite Hinweise, wie die jeweilige Variante zu entfernen ist.

Insbesondere stellt sich die Frage Wie schütze ich mich?

-

Ganz wichtig ist, dass man auch wenn man der einzige Benutzer eines Rechners ist, mindestens einen eingeschränkten Benutzer haben sollte, mit dem man arbeitet und mindestens einen administrativen Benutzer, der nur dann verwendet wird, wenn es gar nicht anders geht, also beispielsweise bei Softwareinstallationen.

-

Man sollte einen aktuellen Virenscanner installiert haben und diesen regelmäßig aktualisieren, auch wenn er die eigentliche Schadsoftware nicht erkennt, verhindert er Viren, die das System für Schadsoftware anfällig machen könnte.

-

Für den Internetbrowser sollte man einen Adblocker installieren. (z.B. uBlock Origin unter
(Firefox) [2]https://addons.mozilla.org/de/firefox/addon/ublock-origin/ oder
(Chrome) [3]https://chrome.google.com/webstore/detail/ublock-origin/.
Häufig verstecken sich Viren und Schadsoftware in irgendwelchen Ads, die beim Aufrufen einer Webseite zusätzlich ausgeführt werden.

-

Automatisches Leeren des Temp Verzeichnis im Benutzerprofil schon beim Einloggen.
(z.B.: ccleaner ([4]www.ccleaner.de/)

Und durch keine Software zu ersetzen ist der Grundsatz:

„erst denken dann klicken“, denn: „This machine has no brain! Use your own!“

[1] https://www.bundespolizei.de/Web/DE/02Sicher-im-Alltag/05Weitere-Themen/02_BKA-Trojaner/BKA-Trojaner_node.html
[2] https://addons.mozilla.org/de/firefox/addon/ublock-origin/
[3] https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm
[4] http://www.ccleaner.de/