Inhaltsverzeichnis

Der HDD-Low Trojaner/Malware/Virus

Vorgeschichte

Wie man sich diese Malware an Land zieht, kann ich bisweilen nicht nachvollziehen. Höchstwahrscheinlich wird sie durch Banner mit der Aufschrift "Ihr Computer ist gefährdet" verbreitet. Installiert wird es anscheinend auch nicht richtig, aber eine deutliche Desktopverknüpfung, mit buntem Logo ist erkennbar. Bei genauerem Hinsehen mündet diese Verknüpfung im systemeigenen Temp-Ordner in einer [zufallszahlen].exe

Die Erscheinung

Das Programm selbst versteckt sich nicht, es agiert offensiv nach dem Systemstart mit einem programm-ähnlichen Fenster, welches sich aber im Gegensatz zu "normalen" Anwendungen nicht schließen lässt. Wenn man dieses ignoriert, so wird man ständig mit verschiedensten Fehlermeldungen belästigt. Diese reichen von "Ihr System ist gefährdet", über "Defragmentieren Sie Ihr System, um den Fehler zu beheben" bis hin zu "Es kann nicht vom Datenträger gelesen werden" oder**"Bitte sichern sie Ihr System auf einen externen Datenträger."**Letzeres sollte keinesfalls durchgeführt werden, da sich das Programm auf diesem Wege gern vermehrt.

Vorgehensweise

Das Programm befindet sich im Ordner:

C:\Users\User\AppData\Local\Temp

und heißt**[zufallszahlen].exe**

In meinem Versuch hieß das Programm 2165983.exe ... oder so :-).

Haben wir herausgefunden wie das Programm in unserem Falle heißt, so können wir:

- es über den Task-Manager ersteinmal stoppen

- Das Programm im o.g. Temp-Ordner löschen

- Im Ordner **C:\Programme** nachschauen, ob dort ein Ordner HDD-Low existiert, wenn ja ... löschen

- ggf. C:\Users\User\AppData\Local\Temp\dfrg löschen
- ggf. C:\Users\User\AppData\Local\Temp\dfrgr löschen
- Den Programmpfad in der Registry mit löschen, das geht so:

Registry

Start -> Ausführen -> **regedit** eingeben

Dann im Fenster nach:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ?[random].exe?

suchen und den Eintrag entfernen.

Danach das System neu starten und das ganze sollte funktioniert haben. ggf. von oben nochmal wiederholen.