Viren

GEMA / BKA / BUNDESPOLIZEI / BKA - Trojaner entfernen

Sehr viele werden diesen Virus bereits kennen. Zur Zeit tun sich die Anti-Viren-Programme immer noch recht schwer gegen "Drive-By-Download". Hierbei reicht der reine Besuch einer Webseite, am häufigsten betroffen sind bisher Sicherheitslücken in den älteren Flash-Playern bzw. in älteren Java-Versionen. Ich habe noch eine Alternative zum ausdrucken erstellt, diese kann hier heruntergeladen werden. Vorweg: Auf keinen Fall bezahlen, da das Geld ansonsten unwiderbringlich weg ist und der PC weiterhin von dem Virus blockiert wird.

Hier möchte ich einmal einen schnellen und recht einfachen Lösungsweg aufzeigen. Es gibt mittlerweile mehrere Versionen dieses Virus, die auch alle unterschiedlich tief ins System eingreifen.

Lösung:

1. Schritt
Abgesicherten Modus starten
Windows XP / Vista / Windows 7
Den abgesicherten Modus können wir aufrufen, indem wir beim starten die F8-Taste drücken und dann abgesicherter Modus auswählen und mit Enter bestätigen. Dies ist wichtig, damit die erste Version des Virus nicht gestartet wird!

2. Schritt

Windows XP / Vista / Windows 7

Als Benutzer anmelden und sofort den Task-Manager starten, dafür mit einem Rechtsklick auf die Task-Leiste und Task-Manager starten oder STRG+ALT+ENTF drücken. Dies ist bei den neueren Viren wichtig, da diese auch im abgesicherten Modus gestartet werden. Im Task-Manager erscheint eventuell eine Datei z.B. gema.exe, diese wird als normaler Benutzer ausgeführt und kann recht einfach mittels "Prozess beenden" gestoppt werden.

3. Schritt

MSConfig aufrufen

Windows XP:

Start --- Ausführen --- msconfig eingeben und Enter betätigen Unter Systemstart nach Dateien suchen, die aus dem Ordner "Dokumente und Einstellungen" gestartet werden Zum deaktivieren einfach den zugehörigen Haken unter Systemstartelement entfernen Nun noch nach exe-Dateien suchen, die aus dem Ordner "Windows\System32\" aufgerufen werden Auch hier den zugehörigen Haken entfernen

Windows Vista & Windows 7:

Start-Button --- Programme/Dateien durchsuchen --- msconfig eingeben und den Eintrag msconfig.exe anklicken Unter Systemstart nach Dateien suchen, die aus dem Ordner "Dokumente und Einstellungen" gestartet werden Zum deaktivieren einfach den zugehörigen Haken unter Systemstartelement entfernen Nun noch nach exe-Dateien suchen, die aus dem Ordner "Windows\System32\" aufgerufen werden Auch hier den zugehörigen Haken entfernen

4. Schritt

Windows XP / Vista / Windows 7

Den Rechner wieder im normalen Modus starten und hoffen, dass alle Einträge entfernt wurden. Sollte dies nicht der Fall sein, dann nochmal bei Schritt 1 anfangen. Und nach weiteren eigenartigen Einträgen in MSConfig suchen. Leider gibt es eine Version, die man auf diesem Wege nicht los wird, hier kann man nur noch mit einer speziellen Rettungs-CD eine Lösung erzielen.

Eindeutige ID: #1001
Verfasser: Björn Graunke
Letzte Änderung: 2015-09-13 21:57