

Anleitung zur Abwehr von Spyware, Dialern und Spam-Emails

Autoren: Colin van Loo, Grigory Pavlov
Datum der Erstellung: 04.06.2021
Letzter Autor: Grigory Pavlov
Datum der letzten Bearbeitung: 28.06.2021

Inhaltsverzeichnis

Inhaltsverzeichnis	1
Projektdeklaration	1
Spyware	2
Was ist Spyware?	2
Erkennen von Spyware	2
Präventiv gegen Spyware vorgehen	3
Spyware effektiv entfernen	3
Abbildungsverzeichnis	4
Quellenangabe	4

Projektdeklaration

Modul: M214 Benutzer im Umgang mit Informatikmitteln instruieren
Auftraggeber: Christoph Jäger
Abgabetermin: 29.06.2021

Über das gewählte Thema soll Stoff aufbereitet werden der mittels dieser Anleitung dem Benutzer präsentiert wird (bspw. in Form von Schritt-für-Schritt-Anleitung). Der Benutzer sollte den Stoff im Selbststudium einfach erlernen können.

Spyware

Was ist Spyware?

Sogenannte "Spyware" (vom engl. *spy* (Spion) + ware) ist Software, deren Absicht es ist, Informationen über eine Person oder Organisation zu sammeln und diese Informationen an eine Drittpartei, meistens den Hersteller der Software, zurückzusenden, beispielsweise indem die Sicherheit des Geräts beeinträchtigt. Dieses Verhalten kann sowohl in Malware als auch in vertrauenswürdiger Software vorhanden sein. Auch Websites können Spyware-Verhalten aufweisen, wie zum Beispiel Web-Tracking.

Erkennen von Spyware

Da es verschiedene Arten von Spyware gibt, ist es schwierig, definitive Indikatoren niederzulegen, jedoch kommen folgende Symptome oft vor:

- erhöhte CPU-/RAM-Nutzung, deutlich höher als von offenen Applikationen gebraucht
- unerklärliche Netzwerkaktivität
- Antivirus (falls installiert) zeigt Warnungen
- es werden Programme ohne Einwilligung des Nutzers installiert, modifiziert oder deinstalliert
- **"Browser Hijacking"**: Browser läuft langsamer, Standardsuchmaschine wurde geändert, verdächtige [Extensions](#), Werbe-Pop-Ups

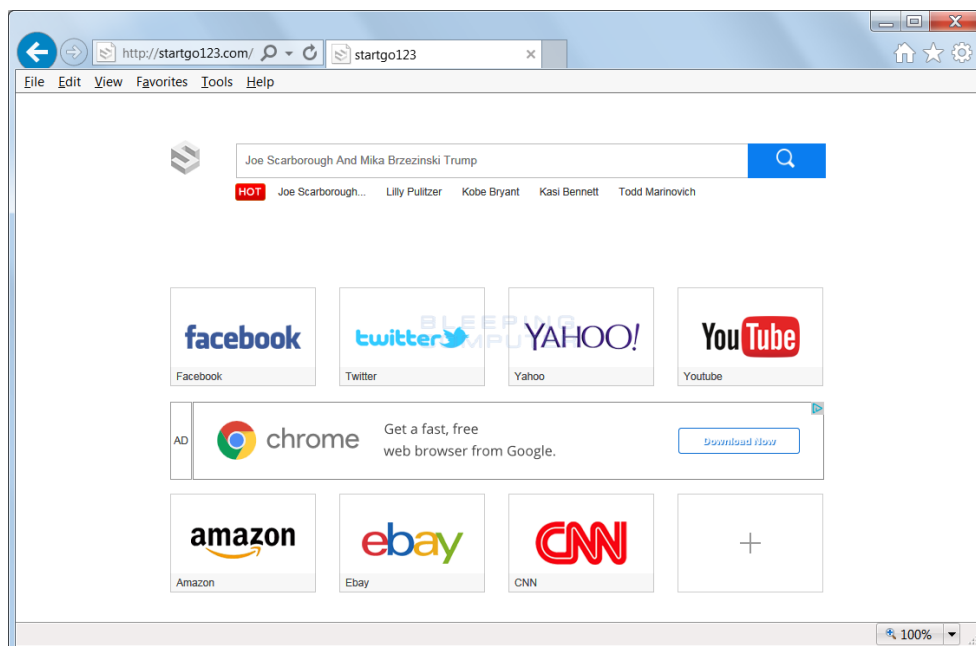


Bild 1: Browser eines mit Spyware infizierten Geräts nach Hijacking

Präventiv gegen Spyware vorgehen

Man kann verschieden gegen Spyware oder Malware (Schadsoftware) allgemein vorgehen. Beispielsweise gibt es spezielle Anti-Spyware-Applikationen mit Echtzeitschutz:

- Norton 360
- Bitdefender
- TotalAV
- ...viele andere

Zu beachten ist jedoch, dass auch sogenannte "Trügeantivirusprogramme" im Umlauf sind. Falls Sie unsicher sind, überprüfen sie zuerst auf einem anderen Gerät via das Internet, ob der Antivirus auch wirklich einer ist.

Ausserdem kann seitens Nutzer das Verhalten an die Möglichkeit einer Infizierung angepasst werden. Solches sollte man vermeiden:

- deaktivieren des Antivirus-Programms zur Installation eines Programms
- veralteter Browser oder Windows-Version (die meiste Spyware ist auf Windows-Systeme vorbereitet)
- neuen, unbekannte Applikationen mit Adminrechten ausführen

Zusätzlich kann eine Firewall oder ein Werbeblocker wie [uBlock](#) eingerichtet werden, um Netzwerkverkehr zu filtern.

Spyware effektiv entfernen

Falls die präventiven Massnahmen nicht eingesetzt wurden, kann man versuchen, so gut wie möglich Spyware vom Gerät zu entfernen:

1. Einen Malware-Scanner installieren (falls möglich via anderes Gerät herunterladen)
2. jegliche Internet-Verbindung (per Kabel oder WLAN) trennen um weiteren Schaden zu vermeiden
3. PC neustarten
4. Schnellstmöglich einen Scan durchführen
5. weiteren Anweisungen des Malware-Scanners folgen

Abbildungsverzeichnis

Bild 1: Browser eines mit Spyware infizierten Geräts nach Hijacking

2

Quellenangabe

[pcmag.com - Windows Computers Were Targets of 83% of All Malware Attacks in Q1 2020](#)