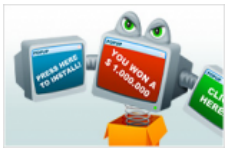
Parasiten nach Kategorien:

Rogue Anti-Spyware (623) Was ist ROGUE ANTI-SPYWARE? Als Rogue Anti-Spyware bezeichnet man die Software, die Malware oder andere bösartige Tools verwendet, um zu werben, sich auf Ihrem Computer zu installieren oder die Computerbenutzer zum Kauf der vorgeblichen Software zu verleiten. Rogue Anti-Spyware kann häufig ein Trojanisches Pferd installieren oder anderen Schaden verursachen. Die Hersteller von Rogue Anti-Spyware streben danach, ihre nutzlose Produktion zu verkaufen. Auf dem Bildschirm werden vorgebliche Windows-Dialogfenster eingeblendet. Es wird auch dauernd eine Meldung angezeigt, wie beispielsweise “Warnung! Ihr Computer ist mit Spyware infiziert! Kaufen Sie SpyHunter, um Spyware zu entfernen!” Sobald man OK anklickt, wird der Benutzer auf die Webseite der Software verwiesen. Manchmal, wenn man auf die Schaltfläche X auf der oberen rechten Seite anklickt, um das Dialogfenster zu schliessen, entweder es passiert dasselbe oder die Software-Installation aktiviert wird (wenn man Alt+F4 drückt, kann man das umgehen). Falls die Rogue Anti-Spyware auf Ihrem PC installiert wurde, kann es sehr schwierig sein, sie zu entfernen.

Adware (177) Was ist ADWARE? Als Adware bezeichnet man Software (Adware ist die Abkürzung für Advertising Software“), die die Benutzer mit unerwünschter Werbung belastet. Anders als z.B. bei Viren oder Würmern werden Ihre Daten durch Adware in der Regel nicht zerstört oder manipuliert. Die Hersteller von dieser Anwendung haben einen zusätzlichen Code zugefügt, der die Ads liefert, die in Form von Pop-up-Fenster oder Leisten auf dem Bildschirm erscheinen, und manchmal in Form von Textlinks oder integrierten Suchergebnissen. Adware wird in Verbindung mit Shareware- oder Freewareprogrammen, wie Filesharing-Anwendungen, Suchhilfen, Informationsprogrammen und Software wie Screensaver, Cartoon-Cursor, Hintergründe, Töne, etc. verteilt. Manche Adware-Anwendungen können auch Ihre Aktivitäten im Internet überwachen und gezielte Werbung anzeigen, wie Pop-up, Pop-Under u.a. Bemerken Sie, dass, falls Sie sich zum Entfernen der Adware entscheiden, können manche Sheware-Programme, die Sie installiert haben, nicht mehr funktionieren.



Browser Helper Object (148) Was ist BROWSER HELPER OBJECT? Browser-Helper-Object oder BHO ist nur ein kleines Programm, dass automatisch ausgeführt wird, indem Sie Ihr Internet-Browser starten. Technisch gesehen ist BHO eine Objektbibliothek (DLL), die jedes Mal geladen wird, wenn der Internet Explorer läuft. Normalweise dienen BHOs der Erweiterung der Funktionalität des IEs. Da die BHOs Zugriff auf alle Objekte und Ereignisse des Internet Explorers haben, können sie das Verhalten des Browsers manipulieren, und somit als Spionage-Tools dienen. BHOs können alles machen, was andere Programme auch können. Deswegen ist es nicht einfach, die BHOs, die auf einem PC installiert sind, aufzuspüren. Viele BHOs werden heimlich installiert. Es reicht nur, dass die Programmdatei, eine DLL- oder Exe-Datei, auf die Festplatte gespeichert wird. Die Hacker verwenden BHOs, um das Benutzerverhalten im Internet zu überwachen und die gesammelten Informationen beispielsweise an Marketing-Unternehmen zu übermitteln. Es können auch verschiedene Informationen sein, die der Web-Browser an einen Internet-Server übermittelt. Deswegen können die Hacker auch auf Ihre persönlichen Informationen zugreifen, einschließlich Benutzernamen, Kennwörter oder Kreditkarteninformationen .

Browser Hijackers (209) Was ist BROWSER HIJACKERS? Browser-Hijacker ist eine Art von Spyware, welche die Einstellungen Ihres Browsers manipulieren kann. Die Einstellungen des Browsers werden so verändert, dass beim Start des Browsers die Werbeseiten angezeigt oder eingegebene Adressen auf andere Seiten umgeleitet werden. Viele Browser-Hijacker erwirtschaften die Einkommen für Hackern, indem sie die Suchanfragen auf bestimmte Webseiten umleiten. Somit können die Inhaber den Web-Traffic ihrer Webseiten optimieren. Browser-Hijacker kann die Leistung Ihres Computers senken und sogar Systemabstürze hervorrufen.

Browser Plugins (105) Was ist BROWSER PLUGINS? Browser-Plugin ist ein Programm, das handelsüblichen Web-Browser um Funktionen erweitern, die er standardmäßig nicht enthält. Es kann die Daten auf Webseiten verarbeiten, die nicht in browsertypischen Dateiformaten vorliegen. Doch stellen die Browser-Plugins durch das automatische Starten ein gewisses Risiko der Manipulation der eigenen Daten dar. Diese Programme können Ihren Webbrowser auf verschiedene Weise auswirken. Manche Plugins können die Windows-Fenster erstellen, um Zusatzinformationen auf der Webseite zu zeigen oder Werbebanner mit eigener Werbung ergänzen. Doch gibt es Browser-Plugins, die Ihre Aktivitäten im Internet überwachen und die gesammelten Informationen an Parent-Server senden. Daher sollten Sie vor dem Installieren von Zusatzprogrammen abwägen oder muss in Ihrem System ein wirksamer Schutz gegen Spyware vorhanden sein.

Dialers (1784) Was ist DIALERS? Dialer sind kleine Programme, die eine Wählverbindung zum Internet oder anderen Computernetzwerken über das analoge Telefon- oder das ISDN-Netz aufbauen können. Normalweise sind Dialer legal und dienen dazu, Dienstleistungen im Internet abzurechnen. Es kann aber passieren, dass sich Dialer versteckt und unbemerkt vom Nutzer einwählen. Das hat zu Folge, dass die Benutzer riesige Telefonrechnungen bekommen. Ähnlich wie viele Spyware können Dialer in Freeware eingebettet sein, und sobald sie installiert werden, funktionieren sie ohne Ihr Wissen. Manche Dialer können auch sich auf einem PC einnisten und dann mittels Suchmaschinen kostenpflichtige Webseiten aufrufen. Da nur die Benutzer von Dialer betroffen sind, die sich über DSL mit dem Internet verbinden, kann man bei der Telefongesellschaft eine Sperrung aller 0190-Nummer für eigenen Anschluss beantragen.

Keyloggers (214) Was ist KEYLOGGERS? Keylogger ist ein Typ von kontrollierender Software, die alle Eingaben des Benutzers an einem Computer mitzuprotokollieren kann. Keylogger kann Instant-Nachrichten, E-Mail und jede Information speichern, die Sie mit Hilfe der Tastur eingeben. Die Log-Datei, die Keylogger erstellt, kann an einem bestimmten Empfänger geschickt werden. Manche Keyloggers speichern auch die E-Mail-Adressen, die Sie verwenden oder URL-Adressen der Webseiten, die Sie besuchen. Keyloggers werden häufig von den Arbeitsgebern verwendet,um zu gewährleisten, dass die Mitarbeiter die Arbeitscomputer nur für Geschäftsziele verwenden. Leider können Keyloggers in Spyware eingebettet, was erlaubt, Ihre persönliche Informationen an Drittperson zu senden.

Malware (424) Was ist MALWARE? Als Malware (engl. bösartige Software) bezeichnet man Software, die vom Benutzer unerwünschte und ggf. schädliche Funktionen ausführen. Zu Malware zählen beispielsweise Viren, Würmer und die Programme, die unerwünschte Fernwartung auf Ihrem Computer ermöglichen. Malware kann auch Spyware oder Programme enthalten, die Ihre Internetaktivitäten überwachen oder die Browser- oder Einwahleinstellungen ändern. Schadfunktionen können zum Beispiel die Senkung der Computerleistung, Bombardieren mit störenden Pop-up-Fenstern, oder Pop-up-Ad, das Löschen von Dateien u.s.w. sein.

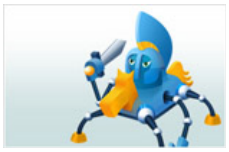
Spyware (601) Was ist SPYWARE? Unter der Spyware versteht man ein Computerprogramm, das über Internet auf Ihren Rechner gelangt. Nach der Installation beginnt Spyware die Internet-Aktivitäten der Benutzer zu überwachen und persönliche Daten zu sammeln. Danach werden die Informationen normalerweise an die Programmhersteller oder Werbefirmen weitergeleitet. Dort werden sie meist dazu genutzt, Werbung zielgerichtet zu den potenziellen Käufern zu bringen: mittels Hauspost, E-Mail-Werbung, Browserfenster (Pop-Ups) u.a. Es ist auch möglich, dass die Startseite Ihres Browsers durch Zusatzprogramme verändert werden kann oder die Favoritenordner durch die Spyware um

Aktuelle Parasiten-Modifikationen:

Zusatzseiten ergänzt werden. Wenn die Werbefenster plötzlich Ihren Bildschirm überfluten, Ihre Startseite geändert wird, der Rechner außergewöhnlich langsam funktioniert, im Favoritenordner die Links stehen, die Sie nicht gespeichert haben, ist es wahrscheinlich, dass Ihr Rechner mit Spyware befallen ist. Um Ihren Computer von Spyware zu befreien, benötigen Sie Anti-Spyware-Software. Anti-Spyware-Software funktioniert ähnlich wie Anti-Virus-Software und manche von ihnen enthalten einen Wächter, und die Definitionen-Dateien, die man ständig aktualisieren muss, um zu gewährleisten, dass der Benutzer gegen die neuesten Bedrohungen geschützt sind. Heutzutage gibt es viele kostenlose Anti-Spyware-Anwendungen. Seien Sie aber vorsichtig! Vertrauen Sie jeder Anti-Spyware-Anwendung nicht, weil manche Anti-Spyware-Tools so genannte “rogue” Anti-Spyware sind.

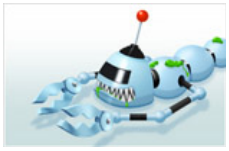
Tracking Cookie (1115) Was ist TRACKING COOKIE? Tracking Cookies oder verfolgende Cookies sind kleine Textdaten, die dazu dienen, die Einblicke in das Surfverhalten des Benutzers zu erlangen. Sie können die Informationen über die Webseiten oder Werbungen, die Sie gesehen haben, oder andere Aktivitäten im Internet sammeln. Verschiedene Webseiten können Tracking Cookies freigeben, und eine Webseite kann mit demselben verfolgenden Cookie die Information speichern oder ablesen. Normalerweise werden Cookies dazu benutzt, den Benutzer zu merken, um den entsprechenden Inhalt ihm zu zeigen. Manche Webseiten können ohne dieses nicht funktionieren. Wenn Sie ein Kennwort auf der Webseite eingeben, wird Cookie dazu benutzt, um festzustellen, dass Sie sich angemeldet haben. Die Problematik bei verfolgenden Cookies ist generell die, das die Einstellungen, Präferenzen, Aktionen, oder ähnliche personenbezogene Daten des Benutzers erfasst und gespeichert werden können. Diese Informationen können an Marketingunternehmen und Werbemailversender gelangen. Somit wird Nutzerprofil gebildet, um gezielte Werbung zu liefern, was störend sein kann. Außerdem können verfolgende Cookies eine Belastung von Verbindung, Netz und Festplatte verursachen.

Trojans (588) Was ist TROJANS? Der Name „Trojaner“ oder „Trojanisches Pferd” ist ursprünglich auf den Troja-Krieg zurückzuführen: die



Spartaner haben den Trojanern ein riesiges hölzernes Pferd geschenkt, in dem die Soldaten sich versteckt haben. In der Nacht stiegen die Soldaten heimlich aus dem Inneren des Holzpferdes aus und die Festung einnahmen. Die Hackers haben die Idee des Trojanischen Pferdes entnommen. Doch heute werden nicht die hölzerne Pferder verschenkt, sondern die Programme, die schädliche Funktionen aufweisen. Es gibt hauptsächlich zwei Arten von Trojaner. Die eine sind scheinbar nützliche Software, die den von den Hackern eingefügten bösartigen Code aufweisen, und die anderen sind die Programme, die maskiert sind (z. B. als Bilderdateien), und dienen dazu, den Benutzer zu betrügen und Ziele des Programms auszuführen. Die häufig vorkommende Möglichkeit für Trojaner, einen Computer zu befallen, ist die manuelle Aktivierung der Programmdatei, die mindestens einmal manuell gestartet werden muss, um gefährlich zu werden. Deswegen ist es empfehlenswert, die unerwartete E-Mail-Anhänge nicht öffnen, selbst wenn sie in attraktiver Form vorliegen (z.B. ein sexy Bild, das einen Trojaner oder Wurm enthalten kann). Das infizierte Programm kann auch an Sie in einer Instant-Message geschickt oder von einem Web-Server herunterladen werden. Normalweise gibt Trojanisches Pferd dem Angreifer die Möglichkeit, die Steuerung über Ihren Rechner zu bekommen. Diese Steuerung kann dem Angreifer erlauben, Ihren Rechner ohne Ihr Wissen entfernt zugänglich zu machen. Außerhalb der Privatsphäre können auch andere Gefahren durch Trojanische Pferde entstehen: beim Befall mit Trojanischen Pferden wird der Schutz vertraulicher Daten auf vernetzten Computern nicht mehr gesichert. Um die Trojanische Pferde zu vermeiden, muss man nicht nur Vorsichtig beim Anklicken von verschiedenen Anhängen oder Links sein, sondern auch wäre es empfehlenswert, ein Schutzprogramm zu erwerben. Da täglich neue Trojanische Pferde erscheinen, muss man beachten, dass die Definitionen der Bedrohungen ständig aktualisiert werden.

Worms (21) Was ist WORMS? Computer-Würmer sind böswillige Software-Anwendungen, die sich über Computernetzwerke verbreiten.



Computer-Wurm ist ein spezifischer Virus-Typ, der dadurch gekennzeichnet, wird, dass er sich mittels infizierter E-Mails, IRC-, Peer-to-Peer- und Instant-Messaging-Programme oder über Dateifreigaben verbreitet. Der Wurm ist eine gefährliche Viren-Form, weil es vorkommen kann, dass er von einem Freunden geschickt werden kann. Ob ein Computer-Wurm sich verbreiten wird, hängt davon ab, ob die Person leichtgläubig ist, die das E-Mail bekommen hat. Der E-Mail-Anhang kann aussehen, als wäre er legitim, oft kommt er von Ihrem ISP oder von einem Freund. Sobald der Anhang geöffnet wird, kann er auf verschiedene Weise beeinflussen Ihren Computer beeinflussen. Die Würmer suchen die Adresslisten und Kontakte des E-Mail-Programms durch und versenden automatisch eine E-Mail (meist mit infiziertem Anhang) an alle gefundene Adressen. Somit werden Ihre Freunde und Kollegen auch Opfer eines Computerwurms. Ein Wurm kann auch mit anderen Viren gebündelt sein, die verschiedenen Schaden verursachen können. Die meisten Anti-Spyware-Programme können die bekannteste Computerwürmer aufspüren. Sie können auch die Würmer entfernen.