Downloads

Gängige Betrugsmaschen erkennen

Das Internet ist eine unerschöpfliche Quelle von Schätzen jeglicher Art, die man entweder beim Surfen entdecken, oder direkt herunterladen kann.

Dank effizienten Internetverbindungen können Downloads immer schneller und einfacher getätigt werden. Wer ein Informationsblatt oder ein PDF-Formular von einer offiziellen Seite herunterlädt, wird wohl kaum auf ein Problem stoßen.

Einige Webseiten bieten jedoch Dateien an, deren einziges Ziel darin besteht, den Computer zu schädigen. Auch bekannte Computerprogramme, die schon seit langer Zeit heruntergeladen werden, können problematisch werden, wenn sie Sicherheitslücken aufweisen, die nicht korrigiert wurden.

Die Bedrohungen

Schadprogramm

Schadprogramme, egal ob es sich um Viren, Würmer oder Trojaner handelt, können sich in jeder möglichen Dateiform verstecken: Dokument, Bild, Video, Musik,... Sie können den Computer auf unterschiedlichste Weise am korrekten Funktionieren hindern, bzw. ihn sogar komplett lahmlegen. Schadprogramme dienen entweder der Zerstörung von Daten oder der Spionage.

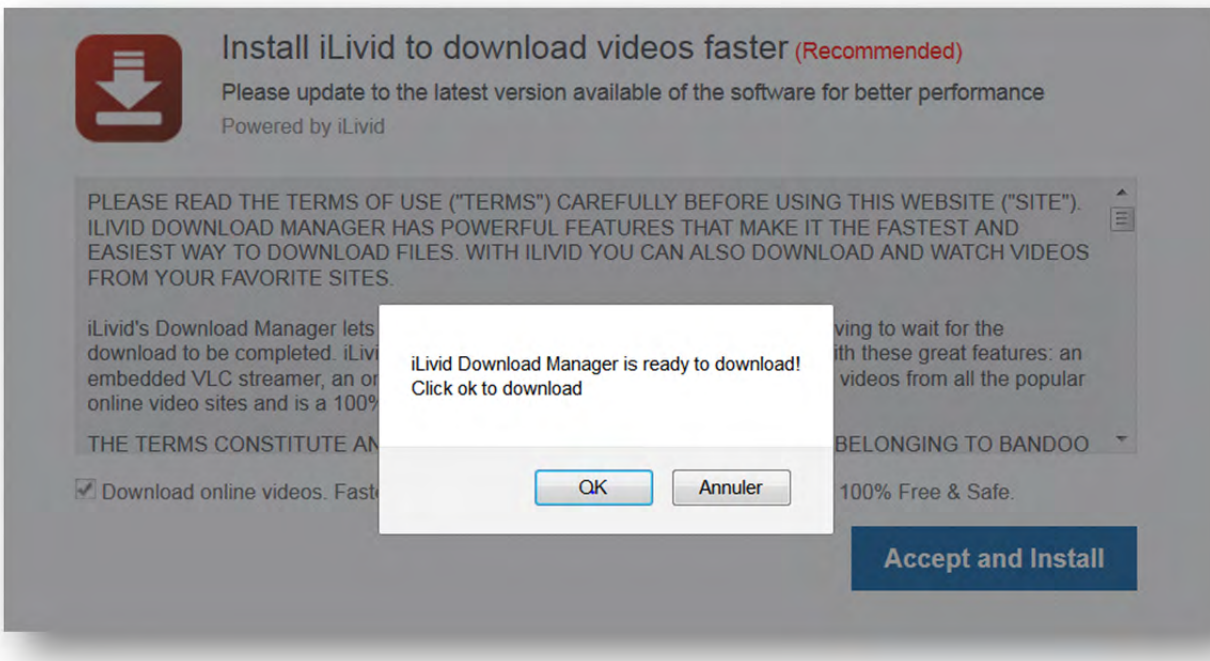
Falsche Viren und Antiviren

Falschmeldungen tauchen auf dem Bildschirm auf und nutzen die Angst ihres Opfers aus, um es zum Download eines tatsächlichen Schadprogramms zu bewegen. Auf einer gefälschten Webseite kann zum Beispiel eine Warnung aufleuchten, die behauptet, der Computer sei mit Viren infiziert. Indem es auf den Link klickt, lädt das Opfer automatisch das vermeintliche Antivirenprogramm herunter...das in Wahrheit ein Trojaner, also ein Schadprogramm ist. Ist der Download komplett, installiert sich der Trojaner auf dem Computer, ohne dass der Benutzer etwas davon mitbekommt. Der Angreifer hat nun die Möglichkeit, jederzeit die Kontrolle des infizierten Geräts zu übernehmen.

Videos und Player

Player sind Programme, welche die Wiedergabe von Audio- oder Video-Dateien erlauben. Es gibt sie in vielen verschiedenen Ausführungen. Die meiste Zeit funktionieren sie einwandfrei. Allerdings können zwei Arten von Problemen auftreten:

1. Alte oder nicht aktualisierte Player können Sicherheitslücken aufweisen, die von heruntergeladenen Video- oder Audiodateien ausgenutzt werden.
2. Illegale Download-Sites verpflichten ihre Benutzer, einen spezifischen Player oder ein spezifisches Programm zu benutzen, um die Videodatei schneller herunterzuladen. Diese Player sind meist schon infiziert. Darüber hinaus muss man wissen, dass Dateien, die auf illegalen Seiten heruntergeladen werden, nicht selten selbst ein Virus beherbergen. Alleine deshalb sollte man illegale Downloads vermeiden.



Plugins

Plugins an sich sind in der Regel ungefährlich. Man muss sich nur bewusst sein, dass es sich dabei um Programme wie andere handelt, und dass diese auch Sicherheitslücken und Schwachstellen haben können. Es liegt also auf der Hand, während des Downloads eines Plugins zu prüfen, ob es legitim ist und so funktioniert, wie beschrieben. Anschließend müssen Plugins regelmäßig aktualisiert werden, genauso wie der Browser, auf dem sie installiert sind.

Plugins, die nicht mehr benötigt werden, sollte man einfach löschen. Kurzum: Um Infektionen zu vermeiden, müssen Plugins, so wie jedes andere Programm auf Ihrem Computer, immer sauber bleiben.

Adware

Manchmal versteckt sich in einem Programm oder Plugin, das man herunterlädt, eine „Adware“ (Reklame-Software), die auf schädliche Art und Weise Werbung auf den Computer schickt, sei es auf Ebene der Browserleisten, mithilfe von Popup-Fenstern oder durch Systemnachrichten. Auch wenn Adware nicht wirklich bösartig ist, so kann sie doch den Computer stark verlangsamen und anfällig für andere Schadprogramme machen.

Zombies

Einige schädliche Dateien können Ihren PC in einen „Zombie“ verwandeln, der dann von Piraten benutzt werden kann, um Angriffe durchzuführen, ohne dass diese auf sie selbst zurückgeführt werden können.

Ransomware

Andere „infizierte“ Dateien führen wiederum dazu, dass Daten auf Ihrem Harddisk verschlüsselt werden. Sie haben fortan keinen Zugriff mehr darauf, und werden dazu aufgefordert, eine gewisse Summe Geld zu zahlen, um wieder normal auf Ihre eigenen Daten zugreifen zu können. Die fieseste aller Betrugsmaschen!

Wie kann man sich schützen?

„Clever klicken“ ist im Hinblick auf die Risiken, die mit Downloads einhergehen, besonders wichtig! Deshalb sollte man wissen, wie man sich verhalten soll, um nicht auf die gängigen Maschen hereinzufallen.

Verhaltensmaßnahmen

- Seien Sie skeptisch bei E-Mails, die Sie nicht erwartet haben sowie bei Angeboten im Internet, die sich zu gut anhören, um wahr zu sein. Vorsicht auch bei Datei-Anhängen in nicht angeforderten E-Mails oder sonstigen Webnachrichten: Nicht immer ist die Datei sauber! Lernen Sie, Social Engineering die Stirn zu bieten.
- Wenn Sie Zweifel haben, fragen Sie die Kontaktperson nach einer Bestätigung, bevor Sie eine Datei blind herunterladen.

- Es ist wichtig zu wissen, wie es aussieht, wenn Ihr Antivirenprogramm Alarm schlägt. Viele schädliche Webseiten ködern ihre Opfer mit falschem Virenalarm, um sie dazu zu bewegen, ein vermeintliches Antivirenprogramm herunterzuladen. Letzteres ist in Wahrheit selbst mit einem Schadprogramm infiziert.
- Berücksichtigen Sie Warnmeldungen von Suchmaschinen oder von Ihrem Browser, wenn diese Sie darauf aufmerksam machen, dass eine bestimmte Seite unsicher ist.

Technische Maßnahmen

- Benutzen Sie einen Browsing-Filter wie Web of Trust (WOT) oder aktivieren Sie direkt die Filter Ihres Browsers:
  - Smart screen von Microsoft
  - Phishing-Filter von Mozilla Firefox
  - Google Chrome und Browser-Sicherheit
- Installieren Sie für Ihr Unternehmen oder Ihr Zuhause einen Web-Filter, der automatisch viele schädliche Webseiten blockiert.
- Sie können auch auf ein Sandkastenprogramm (z.B. Sandboxie), oder andere Programme zur Systemvirtualisierung zurückgreifen, um eventuelle Bedrohungen im Vorfeld in einer Pufferzone aufzuspüren, ohne dass Ihr Computer dabei zu Schaden kommt.)

Sollten Sie Fragen zum Thema Online-Betrug oder zur Internetnutzung generell haben, kontaktieren Sie die BEE SECURE Helpline:

BEE SECURE HELPLINE
BERATUNG & HILFE
8002-1234

Union Luxembourgeoise des Consommateurs (ULC)

Wenn Sie online bei einem in Luxemburg ansässigen Unternehmen einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie die ULC.

www.ulc.lu

Centre Européen des Consommateurs (CEC)

Wenn Sie online in einem anderen Land der EU einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie das CEC.

Tel. 26 84 64-1 www.cecluxembourg.lu

Institut Luxembourgeois de Régulation (ILR)

Wenn Sie bei Ihrem Telekommunikationsanbieter eine Beschwerde eingereicht haben, können Sie sich, bei einer nicht zufriedenstellenden Lösung des Problems, kostenfrei an die Schlichtungsstelle des ILR wenden.

www.ilr.lu/consommateurs

Police Grand-Ducale

Sie wollen Anzeige wegen Betrugs erstatten?

Schreiben Sie eine E-Mail an contact@police.etat.lu und informieren Sie sich über die genaue Prozedur.

www.police.lu

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+ 352) 46 41 86
bee-secure@snj.lu · www.bee-secure.lu

Co-funded by the European Union