Infection par « drive-by download »

Le simple fait de se rendre sur un site contaminé suffit pour infecter son dispositif. Il s'agit pour la plupart de sites sérieux ayant été piégés par des cybercriminels dans le but de propager leurs malwares. Mais des solutions existent...

Pour vous protéger contre les infections par « drive-by download »...

- utilisez toujours la dernière version du navigateur et de ses plugins-(Adobe Flash Player, Java etc.).
- effectuez régulièrement les mises à jour de votre système d'exploitation et des programmes installés (Office, Adobe Acrobat Reader, etc.).
- actualisez constamment votre antivirus et procédez régulièrement à un scan de votre disque dur.

Le danger des infections par « drive-by download »

Les hackers peuvent pirater des sites web en exploitant certaines failles, la plupart du temps sans que les propriétaires des sites en question ne remarquent rien pendant longtemps.

Les points suivants montrent à quel point une infection par drive-by download peut être dangereuse et les conséquences incalculables qu'elle peut avoir :

1. Il suffit de visiter un site web contaminé pour infecter son dispositif. En d'autres termes, l'infection se produit sans que l'utilisateur n'ait à télécharger ni à installer quoi que ce soit.
2. Le téléchargement du malware démarre automatiquement en arrière-plan au moment où l'utilisateur se connecte au site. Les pares-feux sont dans ce cas parfaitement impuissants et n'offrent donc aucune protection sur ce point.
3. À noter que les sites « louches » ne sont pas plus susceptibles de représenter un risque que les sites sérieux, connus et très visités, qui peuvent également être infestés par des codes malicieux.

Contre-mesures

Pour vous protéger, la première chose à faire est d'utiliser toujours la dernière mise à jour du navigateur et des plug-ins (assistants d'application qui étendent les capacités du navigateur).

Autre mesure préventive importante, disposer d'un antivirus parfaitement à jour. Sachant que les virus sont souvent téléchargés sous une forme comprimée avant d'être extraits sur le dispositif de la victime, ceux-ci ne sont pas toujours détectés par l'antivirus. Il est par conséquent indispensable d'effectuer régulièrement (une fois par semaine par exemple) un scan antivirus complet.

Contrôler les sites web

Sur son site Internet, Norton (Symantec) met à la disposition des internautes un service qui vous permettra de vérifier la sécurité (et la présence éventuelle de menaces) de sites connus.

Il suffit d'ouvrir la page Norton Safe Web (https://safeweb.norton.com/?ulang=deu) et de taper l'adresse du site que vous

souhaitez contrôler dans le champ prévu à cet effet pour obtenir l'estimation de Norton.

Une infection par « drive-by download » désigne l'infection d'un appareil par un maliciel (ex. : virus, cheval de Troie) lors d'une simple visite sur un site web. Dans ce type d'attaque, les cybercriminels exploitent généralement les failles du navigateur ou de ses plugins.

Pour aller plus loin

Fonctionnement

Les sites Internet contiennent aujourd'hui le plus souvent des fonctions dynamiques basées sur des langages tels que JavaScript, Java, Adobe Flash, etc. Ces technologies assurent la communication constante entre le navigateur et le serveur web pendant une session (la durée pendant laquelle un internaute reste sur une page Internet), sans que l'internaute n'ait aucune action à exécuter. Elles sont utilisées p. ex. pour échanger des bannières publicitaires, charger des listes ou transmettre des données au serveur web.

Habituellement, ces opérations sont effectuées dans ce que l'on appelle la « sandbox » (bac à sable) du navigateur. Une sandbox est en règle générale un composant du navigateur ou d'un plugin qui sert à réduire les risques de sécurité liés à l'exécution d'une application web. Les scripts inconnus disposent ainsi d'un emplacement restreint dans lequel ils peuvent s'exécuter en toute sécurité (accès limité au disque dur local par exemple).

Or, si le navigateur ou un plugin présente une faille de sécurité, ces scripts malicieux peuvent attaquer directement le dispositif de l'utilisateur. C'est ainsi que les malwares peuvent exploiter la faille, passer du serveur web au navigateur et s'installer sur le dispositif de l'internaute et ce, à son insu.

Désactiver les scripts pour se protéger ?

À l'heure actuelle, il n'existe aucune mesure de sécurité vraiment efficace contre les infections par « drive-by download ». Pour encore plus de sécurité, il est possible de bloquer l'exécution des scripts. Mais dans la pratique, cette solution peut s'avérer difficile à mettre en œuvre dans la mesure où 95% des sites Internet se basent sur les technologies mentionnées plus haut, ce qui signifie que la désactivation des scripts empêcherait nombre d'entre eux de s'afficher correctement.