Drive-By Download

Simply visiting an infected website is sufficient to infect your device. Websites affected often contain reputable offers and have been compromised beforehand to distribute malware. But you can protect yourself.

Protect yourself against drive-by downloads by...

- always using the most current version of your browser and all plug-ins (Adobe Flash Player, Java, etc.).
- always keeping your operating system and all programs installed (Office, Adobe Acrobat Reader, etc.) up to date.
- always updating your virus scanner and regularly checking your hard drive for viruses.

Drive-by-infections threats

Hackers often systematically exploit websites by exploiting their vulnerabilities. Website operators often remain unaware of this for some time.

The following items will explain what it is that makes drive-by downloads so dangerous and unpredictable:

1. A device is infected by simply visiting an infected website containing malicious code, i.e. it is not necessary for visitors to start any download or explicitly install anything.
2. The malware download is started automatically in the background once you visit a website. This bypasses firewalls, which don't offer any protection against this.
3. And it is not only pages with dubious contents which are affected; respectable, well-known and frequently visited websites can also become infected with malicious code.

Counter-measures

To protect yourself, you should also use the latest version of your browser including any plug-ins (utilities expanding browser functionality) you use.

Another important protective measure is to always keep your anti-virus software up-to-date. Since many viruses are downloaded as a zipped file and are only unzipped once on a user device, virus scanners are not always able to detect them. It is therefore vital to run regular complete virus scans of your hard drive (for instance every week).

Checking websites

Norton (Symantec) offers a service on their website which enables you to find out the security status (and inherent potential threats) of well-known websites.

To do so, visit Norton Safe Web (https://safeweb.norton.com/?ulang=deu) and enter the address of the required website into the field provided. You will then be given a website assessment by Norton.

"Drive-by download" (also called "drive-by infection") is the term used for a device which becomes infected with malware (for instance viruses, Trojans) solely by visiting a website. In the process, browser or browser plug-in vulnerabilities are exploited.

Further information for those interested

Technologies

Nowadays, websites frequently contain dynamic functions implemented via technologies such as JavaScript, Java, Adobe Flash, etc. These technologies allow for browsers and web servers to continuously communicate with each other for the duration of a session (the time period visitors spend on a website), without visitors having to do anything specific. This is for instance used to exchange banner ads, load lists, or transfer data to the web server.

These actions are generally run in a browser's so-called "sandbox". A sandbox is a standard component of browsers or plug-ins serving to reduce the risk potential on the Internet. In the process, unknown scripts are provided with a contained area where they can be run safely (i.e. they only have limited access, for instance to a local hard drive).

If a browser or plug-in has a vulnerability though, such scripts can access user devices directly. It is therefore possible for malware go get from the web server to the browser and then onto a user device via such a vulnerability, without any conscious action by a user.

Protection provided by script language deactivation?

There are no really effective protective measures against drive-by downloads to date. To increase security further, you can deactivate script languages. However, this is not really a solution feasible in practice, since 95% of all websites rely on the technologies mentioned above, so that a large number of websites can no longer be displayed properly this way.