

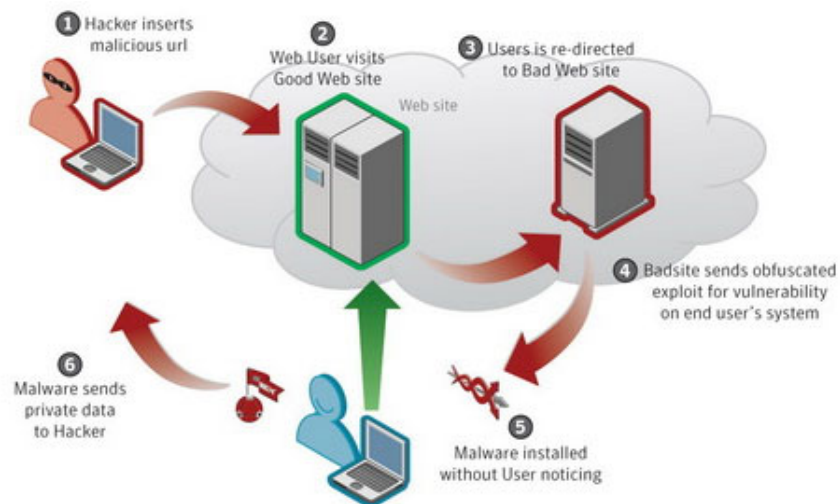
6 ways to prevent Drive-by Download

In the first quarter of 2011, business users faced an average of 274 web-based malicious attacks, an increase of 103% compared to 2010.

TipsMake.com - **In the first quarter of 2011, business users faced an average of 274 web-based malicious attacks, an increase of 103% compared to 2010** . This is a significant increase. One of the main causes is the growing development of Drive-by Download - Attack by automatically downloading. Drive-by Download is a particularly dangerous attack method, which is used to install viruses and spyware onto the user's computer, thereby completely controlling the computer.

Drive-by Download attack method

Drive-by Download works through the exploitation of browser vulnerabilities and plug-in components in the browser. They can happen in a number of different ways and you can still browse the web while malware is automatically downloaded to your computer. The site of the source of the infection can be created by the hackers themselves, or it can be legitimate websites hacked by hackers through web vulnerabilities. Dasient - a company that produces software to prevent malicious attacks via the website - says there are more than 400,000 websites infected with malware each month.



Another way Drive-by Download works is through the ad network. In 2009, *The New York Times* site was tricked into running an ad for fake antivirus software, which bombarded people who clicked on pop-up ads to make them pay for fake programs. . Andrew Brandt, director of threat research at Solera Network Laboratory, said criminals are still trying to use ad networks to distribute malware because it is easy to do and trick users. than.

Sometimes, Drive-by Download also prompts users to accept an action that allows malware to work on the computer. The most common example is installing and using fake malware. You visit a website and suddenly a pop-up window that looks like a legitimate antivirus program appears on your computer, it indicates that a virus has been detected and asks you to click here to Free virus scan.

While business users can through IT management teams to prevent these dangers, independent users face it. Whatever object you are, you should start protecting yourself and your company network.

6 ways to protect against Drive-by Download

1. Encouraging employees (and themselves) to keep the software up to date.

The most important measure for users to protect themselves and the corporate network is to keep all software up to date with the latest versions, especially anti-virus software, browsers, add-ons and plugs. -in browser including Java, Flash and Adobe Acrobat .

Ensuring the use of the latest version of the browser and extension components is important because with an older browser version, the vulnerabilities can be exploited.

The IT department must ensure that anti-virus software is always updated at least once a day (either at the end or the beginning of each working day) to always have the latest virus database to protect computers and networks.

2. Install web filtering software

Web filtering software has the ability to prevent users from visiting websites that have been marked as harmful. Software of this type has the mechanism to detect an unsafe web site, thereby preventing users from being timely.

3. Install NoScript on your browser

NoScript is a free, open-source add-on that allows only trusted sites that you have marked to run JavaScript, Java or Flash.

Running the browser with NoScript for **Firefox** helps you prevent many Drive-by Download.

4. Disable Java

Experts recommend that you disable Java immediately even uninstall Java out of the system, at least until the patch is released to solve the problem **CVE-2011-3544** . This is a malicious Java Applet code stored in a Java Archive file, allowing an unregistered applet to have unlimited access to arbitrary Java code.

5. Keep tabs always BLADE

BLADE stands for Block All Drive-By Download Exploits - Preventing the full exploitation of Drive-by Download - is a new Windows prevention system that can prevent Drive-by Download from infecting Windows computers. through holes. It is being developed by research specialists at Georgia Tech and SRI International.

BLADE v1.0 will be a free sample and will soon be available to users.

6. Do not use Admin account for all jobs

For business users, IT professionals should refrain from providing admin accounts to users. As for independent users, it is possible to create more regular accounts to use when working daily, admin accounts are only used when needed.

Limiting the use of admin rights will help mitigate damage when problems occur.

You finished reading the article "**6 ways to prevent Drive-by Download**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.