How malicious code breaks into a user's PC

Although very careful, most users sometimes still do not understand why malicious code can easily infect their PC.

Although very careful, most users sometimes still do not understand why malicious code can easily infect their PC. The article will partly provide answers to users' questions .

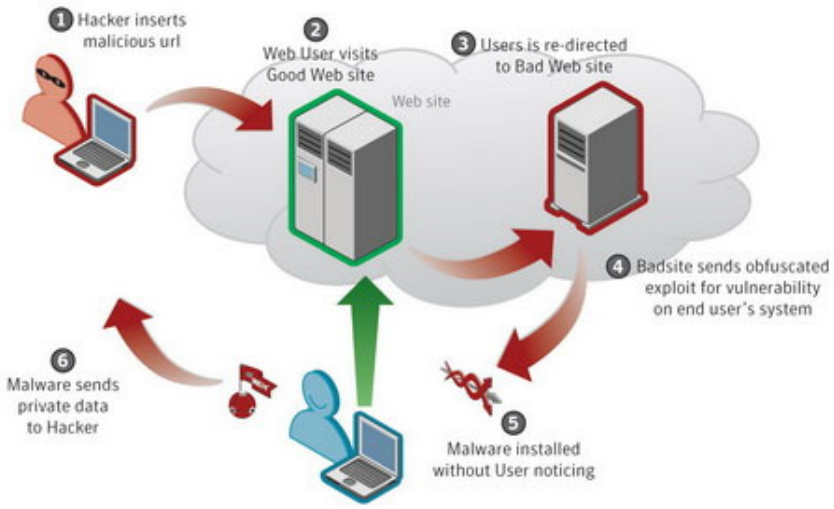
As mentioned in the article 'Web is a favorite target of hackers', the website is a very favorite target for hackers. The ultimate purpose of doing this is just to attack the end user because that is the main benefit for hackers.

Therefore, the website can be said to be the form of malicious code infection on the most popular PC users today. This attack method gives hackers the ability to actively find users. While other forms of infection such as USB memory sticks, hackers must rely too much on users as well as waiting for the opportunity of users to connect USB containing malicious code to uninfected PCs.

Drive-by Download

It can be said that this is the most dangerous form of malicious infection. This form of attack allows malicious code to break into a PC without users knowing it at all. The method of attack is also extremely simple, only if users access a website of hackers, they have been infected with malicious code.

Below is a model that illustrates in detail the steps in the 'drive-by download' attack process.



Abducting a legitimate website. The attack process begins with hackers abducting a legitimate website. Readers can refer to the previous article to learn more about typical website attacks. The purpose of this step is to insert a

malicious website or malicious code on a legitimate website. On the surface of malicious content can be displayed as a simple ad or a frame that users can hardly recognize.

Users access the kidnapped website. This is a step where hackers lose their activeness and have to sit and wait for users to access the websites they kidnap and hope that on the PC of users still have software that has not been fixed security errors. Full like multimedia supplement application error or text editing application error .

Secrets of downloading malicious content. When users access kidnapped websites, the hacked code will automatically activate content downloads or redirect users to malicious hackers' websites. The goal of this step is to determine what operating system the user is using, what web browser, and whether a security error has not been fixed.

Download malicious code to PC. Having such information, hackers will immediately know where to attack. For example, a malicious website that identifies a multimedia add-on application on a user's browser will immediately send a multimedia content. When this content is played back on the website the user is accessing, that's when the malicious code is downloaded to the user's PC.

Activate malicious code infection. The advantage of security vulnerabilities in multimedia add-on applications such as on the malicious code built into the content that the malicious website sent will automatically be activated to infect the user's PC.

Malicious activity. After successfully infecting the PC the malicious user will perform the tasks that the hacker has assigned to it, such as hijacking the PC to turn it into a tool to help hackers perform dark or steal purposes. personal information of users .

It is long, but the entire attack process is almost instantaneous with the website being loaded and displayed in the browser. Users are unaware that they have been infected with malicious code when accessing legitimate websites.

Software security error

As mentioned above, software security error is a prerequisite to ensure the success of 'drive-by-download' attack.

Security errors are loopholes in the software. If an attacker successfully exploits these loopholes, they can completely control the software to do what it does not have the functionality to do.

Specifically, successfully exploiting the security error, hackers can control the software that makes mistakes on the user's PC:

- Activate a script that hackers send
- Download files from the Internet
- Open a file on the user's PC
- Disable and make the application hang completely

Starting in 2003 malicious code began taking advantage of security flaws to attack users. Specifically, it was the computer worm Blaster and Sasser. Successfully exploiting the vulnerability of Windows operating system, these two computer worms have gained the ability to automatically infect and spread. And most recently, the outbreak of Conficker also through another security error in Microsoft's Windows operating system.

Today hackers also target both web browser security bugs, ActiveX Control, browser applications, multimedia applications, file content browsing applications . Just a security error has not been The fix is ??completely malicious code can easily break into the PC without the user knowing.

Notably, the statistics show that the majority of users have not paid attention to installing security updates for the software even though developers have tried to develop features that allow The software is automatically corrected.

Attack tool kit

Finding a security error that can be used to attack a user's PC is not a simple task. But hackers have the support of web attack toolkits.

These are software designed to help identify security flaws present on the user's PC system. These software are widely available on the Internet such as Neosploit, MPack, Icepack, El Fiesta, or Adpack. Hackers have taken advantage of these tools to help them simplify the determination of errors on users' PCs for attack purposes.

Usually in the above tools, there are many codes that exploit different software bugs. Not only that, it is constantly updated with the latest error information so it can be said that this is a very dangerous tool for users.

(*Continued*)

You finished reading the article "**How malicious code breaks into a user's PC**" 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.

© 2019 TipsMake.com