Opening a Word file might get you infected!

Source: blog.360totalsecurity.com

You probably wouldn't believe that simply opening a Microsoft Word document could compromise your system. But it's real.

Security researchers recently discovered a serious vulnerability named CVE-2017-0199 in MS Word. By exploiting such flaw, an attacker can take fully control of the computer when a user opens a Word file containing a booby-trapped OLE2 link object which downloads a malicious HTML app.

Since January, the vulnerability has been used by cyber criminals to distribute malware like Dridex banking trojans and Latenbot through Emails, and by government-sponsored hackers to spy on Russian targets, according to The Hacker News. Massive spam emails were still discovered last Monday targeting at millions of users globally while most of them located in Australia. Once your computer get infected, these malware will steal users' credential details, erase data, and even control your PC.

Luckily, Microsoft has released a new patch last Tuesday to prevent more damages. All the Word users, pretty much everyone, are strongly recommended to patch this flaw from:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

How to prevent this type of attack that most likely will happen in the future?

It's difficult to stop these financially-driven cyber criminals but it's not hard to protect yourselves.

These attackers usually use Emails with scary or urgent subjects to prompt users to open the email, such as "hire_form", "urgent!!", "invoice", etc. Then you may download an attachment named "invoice_8393373.doc" or "hire_form", which looks harmless.

Yet your PC may be infected right when you open this file.

Here are a few actions you can take:

1. Pay attention to the Email sender and see if it's someone that you know of, and the attachment is something that you are expecting. Sometimes your friends or colleagues' emails are manipulated by bad guys.

2. If you already downloaded the file, check the extension (the letters after dot) before you open it. Malware often fakes its file type. Don't open an .exe, .js, .com, or other weird file types. (Within the case above, it's simply a word doc, so read the next tip.)

3. If you are not sure, run 360 Total Security Antivirus program to exam the file first or run the file in Sandbox to guard your PC's safety.

4. Once you open the document which is fully blank, and it tells you to enable editing to see the content. Don’t enable macros or editing function as instructed.

5. Always update to the latest version of your computer software and programs.

6. Do Full Check in 360 Total Security regularly.

We certainly despise these cyber criminals who are hiding behind the computers but taking advantage of innocent people- all of us. However, we believe that if all the people actively and constantly care about cyber security, there will be less and less victims or crimes.