Stolen bank account with Trojan Banking

Today with the development of the digital age, online banking transactions are no longer strange. And the malware developer has released a kind of trojan used to steal users' bank accounts.

Hackers are no longer satisfied with using their skills to destroy computers. After all, they are still considered a cybercrime when only causing minor damage to computer users. This is why today's malware developers are trying to create viruses, malware, ransomware, trojans, etc. to steal users' money.

1. Distinguish malware, viruses and Trojan horses

Today with the development of the digital age, online banking transactions are no longer strange. And the best way to make money is to access someone's bank account. And malware developers have released a kind of trojan used to steal users' bank accounts. Let's see what this kind of trojan bank is and how to protect it from it.

Stealing bank accounts with Trojans

1. What is Banking trojan?
2. How to keep safe from banking trojans?
    1. Update security toolkit
    2. Download applications and files only from trusted sources
    3. Consider carefully when logging in to the banking application
    4. Use two-factor authentication if possible

What is Banking trojan?

Banking trojan disguised as a genuine application or software for users to download and install it to the device. Once downloaded, it will find itself accessing and stealing your bank information. After obtaining the necessary login information, it can bring this information back to the malware developer so that they can access your bank account easily.

Each trojan uses different attack methods. For example, Zeus malware installs itself on Windows computers via spam emails and downloads by drive (files downloaded from legitimate websites have been infected). Once installed, it uses a keylogger (capable of reading the user's keyboard input) to record the bank login information and return it to the hacker. It also connects itself to a botnet to receive additional instructions.

However, Marcher malware is designed for use on mobile phones. It uses a few different attack methods but mainly forged official banking application screens. When users open the banking application, Marcher will cover a fake screen on it so that users can enter their login information and steal them.

This type of attack can also be done on browsers on a PC. This type of attack is also known as 'man in the browser', the type of attack in which malware redirects users to a fake login page and causes them to enter login information into a fake website.

Unfortunately, Banking trojans have been growing in recent months. In June, Checkpoint reported that Trojan Trojans were up to 50% and Kaspersky Lab also claimed that Trojan banking reached the highest number ever in the second quarter of 2018.

How to keep safe from banking trojans?

Here are some preventive measures to keep your bank account safe.

Update security toolkit

If you use anti-virus software, you should regularly update to get the latest virus definitions from which to take timely precautions. When new trojans appear or old variants, security companies record what happens and update the virus definition to determine the tactics when they enter the device. Therefore, you should update regularly to get the latest banking trojan definitions.

Download applications and files only from trusted sources

The most common way for malware to get into your computer or phone is through downloading infected files. Therefore, you should check carefully before downloading anything anywhere. On mobile devices, you should download the app from the official app store and make sure not to download the fake application by checking the number of downloads, reviews, app's name, etc.

Consider carefully when logging in to the banking application

Does your bank login page look different than usual? Suddenly ask for personal information that you don't want to share? If you see the above signs, you should check carefully before entering any information.

Use two-factor authentication if possible

Most banks recognize the seriousness of hackers attacking online banking accounts, so they have implemented two-factor authentication to add a second layer of protection in addition to passwords. If your bank uses two-factor authentication, turn this feature on to protect your account.

See more:

1. 7 kinds of ransomware you didn't expect
2. How to remove Trojan, Virus, Worm or Malware?
3. Remove root malware (malware) on Windows 10 computers