Some ways to avoid the risk of computer attacks

Symantec Vietnam has just released some guidelines for domestic users to handle computer security risks

Symantec Vietnam has released a number of guidelines for domestic users to handle computer security risks, such as stealing personal information, phishing and phishing networks (botnets) in the context. The scene of threats and damage from computer attacks is increasing .

Ghost computer network

What is a botnet?

Bots are robots on the network that sneak into computers, especially unprotected machines or weak security systems, turning them into ghost computers. A ghost computer can attack and turn other computers into ghost computers and eventually, they gather into a powerful army.

Who controls the botnet?

Botmaster (who owns / holds bot) will control botnet computer network. Botmaster can crash websites with data, copy and steal software. The botmaster also hired other Internet bad guys to hire armies of their ghost computers, and in fact, 40% of spam (spam) comes from the botnets of computer ghosts. According to statistics, there are about 320 million junk emails every day.

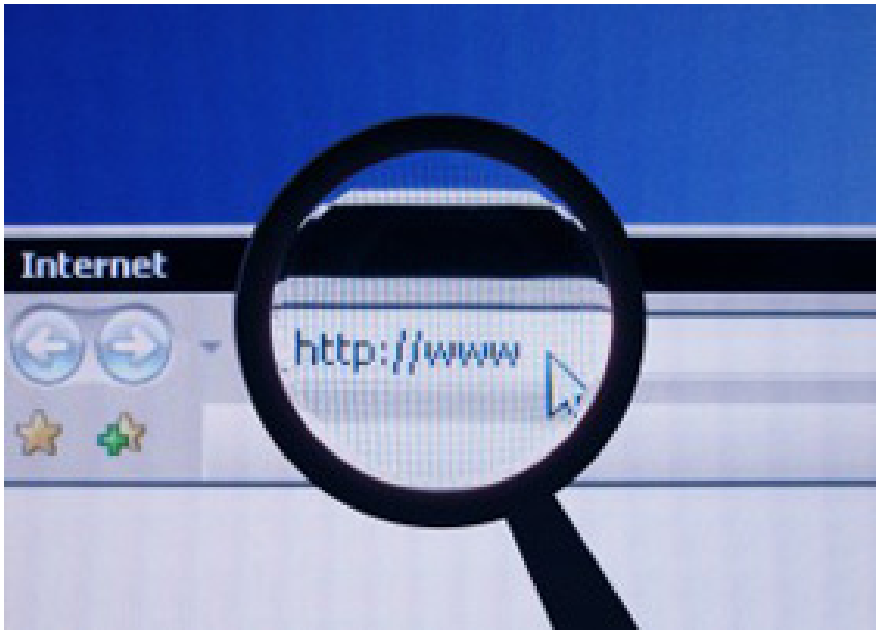
How it works

Botmaster can record your typing. In other words, whenever you log in to your bank's website or make an online transaction, the Botmaster can see exactly what you are typing. Botmasters are often tied to cybercrime by stealing passwords, taking account details and taking over your computer. Now you can be attacked, or your computer can be a ghost computer. You should be alert if your computer starts to operate slowly, or you get a message about suspicious connections.

Prevention

Do not open email attachments that originate from unclear or unreliable. Make sure you have and have the firewall enabled for your system, and make sure your Windows is up to date, your security software has a "live" update feature (auto update online).

Stealing personal information



This is just one of the micro-activities of the underground economy (operated by hackers). So what is underground economy (Underground Economy)?

As everyone knows, supermarkets often sell items like dumplings, breaded fish slices and soap. However, in the Internet world, it is not a market or a supermarket, but a black market, which we often call "The Crime of Cyber ??Crime"! The cybercrime world sells stolen items like credit card information, bank accounts, personal information, passwords, PINS, and now you can sell yourself!

How does the underground economy operate?

First, bad guys steal information such as personal information, bank accounts, credit card information. They sell all this information in the underworld of cybercrime. They use Trojans viruses, fake phishing sites, and get the help of ghost computer networks (zombie botnet) to steal your private information. After that, they are for sale! Bank accounts are particularly popular goods in this underground world. Your bank account is worth only a few pounds, a few US dollars or even a few hundred dollars, it can be sold within 15 seconds. Meanwhile, credit card numbers are for sale for £ 150 or a few hundred dollars.

You cannot close this underground market either because servers are constantly being moved. In the underworld cybercrime, bad guys are everywhere; Thieves, brokers, money launders, and they link together to carry out illegal actions against you. So be wary!

Never open any email without your knowledge.

Phishing attacks (phishing)

What is phishing?

"Phishing" sounds like "Fishing" means going fishing. Phishing is a way that bad guys use to trick your personal information like passwords or bank account numbers. The bait they use is "LIE".

How it works

Basically, this type of fraud stems from the fact that you receive an email (email) that seems to be sent from someone you trust, such as your bank. But the reality is not from your bank. That email requires that you confirm your bank details or your account may be closed. Obviously, that makes you nervous. Therefore, when you click on a link to a web page, like a real banking site - but not really, you fill in the details and the bad guys will steal that information, use It to buy goods with your money.

A few tips to avoid the risk of phishing - this scam

- Your bank NEVER asks you to confirm details via an email. That is the easiest way to recognize a phishing style. If you receive an email like that, DON'T CLICK ON IT!

- See your name. The phishing message is usually "Dear Valued Customer" (Dear Customer). If it doesn't specify your name, DO NOT CLICK ON IT!

- Pay attention to the link (URL) when you visit. If the URL is different from the name of the company you know, DO NOT CLICK IT!

- To get the mouse pointer on the link, it will show the actual web address. If the address is not the same as the name of a suitable company, DO NOT CLICK IT!

- Note the misspellings. If the e-mail has many spelling errors, it doesn't look professional, DO NOT CLICK IT!