

# Security term

Internet hacking and hacking activities have become a part of the computer industry. Despite the changes and expansions, but as people often say, 'where technology goes, hackers go there'. The best measure against c & aa

**Internet hacking and hacking activities have become a part of the computer industry. Despite the changes and expansions, but as people often say, 'where *technology goes, hackers go there* '. The best measure against these risks is to understand them. We have compiled a list of common Internet security terminology that aims to help network users cope with threats from A to Z.**

## **ActiveX control**

These controls link to any traditional object with dynamic content such as tables, site activation buttons via mouse click. They are often embedded in a Web page. Although ActiveX controls help the site 'spring', malicious programmers can easily use them as a convenient means to download spyware. Installing strong browsers and firewalls can protect you from ActiveX controls. Download them carefully, only accept ActiveX from trusted websites.

## **Adware ( Adware )**

Usually adware components are installed next to shareware applications or free software. These ads are profitable for software developers and are provided only with the user's initial consent. Adware displays web-based ads through pop-up windows or banner ads within the program's interface.

## **Antispyware software ( Antispyware software )**

This is a broad term for programs that protect computers against adware and spyware. Almost all antispyware applications have a scanner that detects suspicious elements and removes them. Some antispyware applications have real-time protection modules. It is a shield that warns the user whenever a program is trying to install itself and allows the user to reject them.

## **Backdoor program ( Backdoor program )**

This is a software program that allows an attacker to remotely control a device, hiding all authentication. Software vendors and users themselves are the most popular authors of backdoor programs. They use them to perform tests. Backdoor Trojan horse is a spyware program that destroys a computer. These Trojan horses put the backdoor program on your computer and access it to gather information or install spyware spyware.

## **Bot**

An Internet robot, or 'bot' for short, is an automated program that performs the timesaving function in place of human activity. It could be a spider dragging websites to collect market research data. Secret spyware bots are installed secretly through worms, Trojan horses and download components to the hard drive. Most of them are used in remote attacks such as DoS attacks (denial-of-server) or other similar types.

## **Botnet**

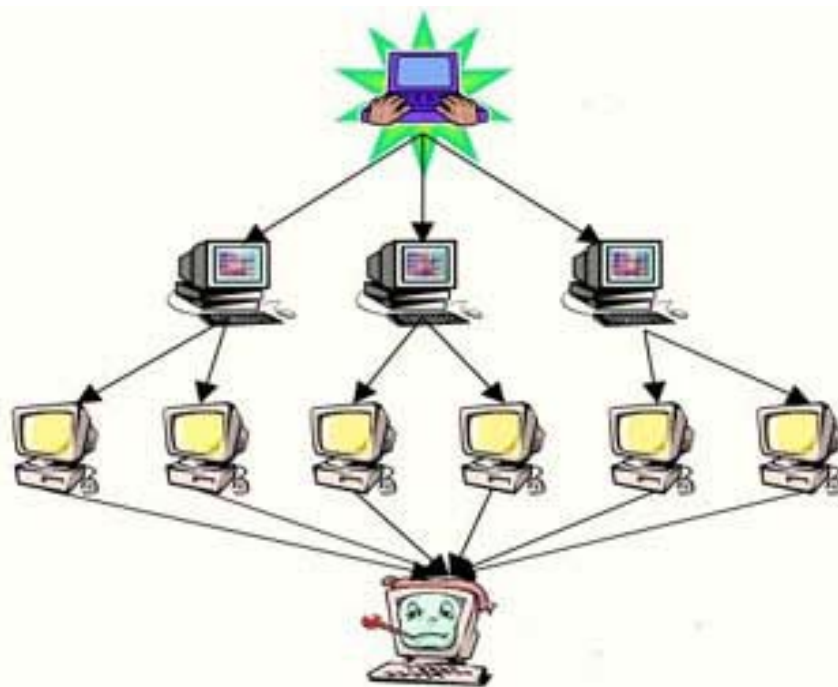
A botnet is a bot network installed on many computers, each running an identical malware. A botnet can be remotely controlled via Internet Relay Chat (IRC) or peer-to-peer application.

### **Browser-helper object (BHO)**

BHOs are files (mostly DLLs) that can add additional functionality to Internet Explorer. Although there are many useful programs like Adobe Acrobat deploying BHO, these files are also often used for unhealthy purposes. BHOs associated with adware or spyware can monitor browser activity, take control of the home page or replace certain advertisements with other ads.

### **Cracker**

Cracker is the short name for 'Criminal Hacker'. Usually just called hackers.



### **Denial-of-server attack (DoS)**

Denial-of-server is a form of attack that blocks access to a user's website or network through phishing with false information (including many requests). This information will overload the website and the network's ability to execute the program. The result is that users cannot access Internet services and appear inaccessible messages. The DoS attack threatens performance, causing high damage, although the main purpose of hackers is usually to disrupt, not to steal.

### **Distributed denial-of-service (DDoS) attack**

This is a variant of DoS, attacking multiple machines at once to deceive a single target with fake information. A hacker can take control of the computer and force it and some other machines to perform a DoS attack on multiple computers, multiple users and multiple networks.

### **Dialer**

Traditional modems use a program called 'dialer' to connect computers to the Internet but dialers are perhaps the most well known of illegal activities. A destructive dialer causes your phone to call more long-distance phone numbers or numbers that pay more than your ISP. The result made most users receive terrible phone bills, while dialer organizers earned very little profit.

**Drive-by**

This term is often used loosely for sneaky software installed on users who are not proficient. In some cases it is simply that visiting a website can download malicious programs to the computer that the user does not know. Some other cases may be pop-up ads that were initially defaulted when installed via the hard drive.

**Evil twin**

Evil twin as a "ghost of the living" (doppelganger) deceives the legal wireless access point. Usually built in a family style, evil twin hotspots provide wireless access to the purpose of collecting user data for exploitation or sale.

**False positive** ( *error of authentication* )

The false positive has several types. When selling software, some of the anti-spyware programs drop that make users mistakenly believe their device is attacked by spyware, but there is practically no problem. The term 'false positive' can also be used when legitimate anti-spyware applications are mistakenly evaluated as a threat.

**Firewall**

Firewall is an important key component in computer protection fences. Because firewalls prevent unauthorized services or programs from accessing computers or network resources. Although almost every virtual network has its own firewall, personal computers should also equip themselves with a firewall. Personal firewalls can be a standalone product or a built-in component of a security suite.

**Hackers**



'Hacker' is a fairly broad term. Hackers can operate with intentions and consequences from profit purposes to sabotage. To hack a file or program simply rebuild or interrupt its execution program. Hackers also have extra meaning that only the creators of computer programs have no purpose of vandalism, but due to being dishonest, they should become malicious programs. Hackers can be original computer programmers, security researchers or criminal hackers (also known as crackers). They seek the ability to harm computers, increase data storage or control remote computers. People classify hacking activities by color. White hat hackers (harmless), black hat hackers (malicious) and gray hat hackers (there are many different purposes).

**Hijacker** ( *Operator of hijacking* )

Often conducting the installation as a useful toolbar of the browser, the Hijacker can edit the settings in the browser or change the homepage default with other websites.

**Keylogger**

Keyloggers are programs that record all keyboard actions performed on a computer. Although some of the original control applications use Keyloggers to monitor, most of them are bundled with spyware. Keyloggers then send sensitive information to the remote computer. From there, thieves can access data such as credit card numbers, bank accounts or passwords and social security codes.

**Malware**

Malware is often used to describe a piece of exploiting software or harass users. It often refers to almost all types of malware such as adware or spyware.

### **Man-in-the-middle attack** ( *Attack type to be an intermediary* )

In this type of attack, operations in the third group will insert a valid user privilege, increasing unacceptable access in the computer or the network. Man-in-the-middle attack (MITM) exploits a one-way authentication process of a wireless access point (WAP). MITM does this by blocking a valid one-way authentication granted by a network for any Media Access Connection (MAC) connection. With the user's legitimate access to the shield, MITM has full access to the data in and out of the user's computer.

### **Pharming**

Like phishing, pharming also acts socially, enticing to get sensitive information from victims. But while phishers disguised as legitimate organizations, pharers took control of the domain to redirect traffic to other places. In this way, a visitor to an online bank's website may be transferred to another replicated website and prompted to provide personal data for the cracker to collect and use.

### **Phishing**

A form of forging a legitimate organization to entice users to provide sensitive data, is the preferred technique of cybercrime. Users often receive the same e-mail as from trusted organizations. It may be mail sent by your bank, collected, stored and edited into the organization they need. Users are also tempted to follow embedded links to a persuasive website that requires them to log in and use personal account information.

During phishing, spear phishing activities targeted at specific users such as gamers. In VoiIP phishing, users can directly verify account information via phone instead of website.

### **Phreaking**

As a combination of the words 'phone' and 'freak', phreaking refers to a large group of hacking activities including manipulation and exploitation of telecommunications systems.

### **Phishing antispayware software**

Placed as legitimate antispayware applications, these malware scans the computer and uses false positives to make users buy products. Rogue often disperses itself through pop-up ads that indicate that the computer is about to be attacked or infected. These programs can be very difficult to remove.



### **Rootkit**

Although there is no exact definition of rootkits, it is often interpreted as part of software that allows intruders to hide malicious files and programs from users and system administrators. Rootkits can be extremely difficult to remove and allow troublemakers to perform many undetectable illegal jobs.

### **Spam**

Starting from the large number of unwanted messages flooded user accounts in the form of e-mail (mostly e-mail advertising), in which the sender tries to attract users to buy their products. So far spam has expanded to expand into instant message messages (called spim), blog comments (splogs), mobile messages (SMS spam), forums, etc . Not just stop at The annoying level of annoying, the attached spam also contains viruses, malware or links to malicious websites. Spam is the basic means for phishing scams.

### **Spoof ( Phishing activity )**

Spoof activities such as phishing to address websites, distribute spam, fake IP addresses are often done by malicious hackers. They use these activities to search and collect materials from legal organizations. Spoof activity is used to detect user traces through a warning response from trusted organizations such as banks. Users responding to fake requests and making this emergency look will be asked to provide private data. Spoof activity is usually phishing, pharming and phreaking.

In pharming, usually a fake IP address of legitimate organizations is used to make users trust that the website is valid.

### **Spyware ( Spyware )**

Spyware are programs that collect and transmit personal information or activities of third parties without the user's permission. Like adware, it is usually installed as a third party component embedded in free software (freeware) or shareware. But there is no difference between the two.

### **Tracking cookies ( Cookies detect )**

Internet browsers record and read cookies and files with small amounts of data (such as passwords and settings on a website) based on the structure of the website. In many cases cookies are beneficial to users. However,

some cookies are used to merge and detect user activity on many different websites. That helps market researchers gather personal information of users.

### **Trojan horses**

Trojan horses are usually dropped into and run in a personal computer without the user's knowledge. They have many functions such as using a computer modem to make long distance calls, generating huge phone bills. Unlike viruses and worms, Trojan horses do not replicate themselves.



### **Viruses**

Like human viruses, computer virus variants include malicious code, which can spread easily on many hosts. Viruses are notorious for destroying hardware, software and personal files. Viruses cannot spread on their own but require users to share infected files via e-mail attachments, portable hard drives, disks, P2P networks, websites or any other file transfer mechanism.

### **Worm ( Deep )**

Usually a couple with viruses, worms are also self-replicating programs. But they multiply independently of user interaction, via a shared network connection, or directly connected to the network. Worms can destroy data on personal computers but mostly threaten bandwidth or automatically shut down users.

### **Zombie ( Computer hijacked )**

Using viruses, Trojan horses and worms, criminal hackers can control malicious activity remotely on a computer that users don't know. Zombie computers are often forced by a remote control program to join the bot network (called botnets) to launch DDoS attacks.

### **Zero-day vulnerability**

Malicious hackers discovered that they could increase the level of vandalism by cracking the product protection fence on the same day the news of a new vulnerability had occurred or the next patch was released. This forces software and security firms to publicly disclose the vulnerability to the rapid operation of exploiters. The result of zero-day attacks will affect users who do not update the patch to fix the vulnerability.

You finished reading the article "**Security term**" 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.

---