

ADWARE

Unwanted programs that, once installed, bombard users with unwanted adverts. Often those pushing the aware programs get paid for every machine they manage to recruit. Some adware poses as fake computer security software. Can be very hard to remove.

BLACKHAT

A hacker that uses his or her skills for explicitly criminal or malicious ends. Has been used to mean the writers of destructive viruses or those that use attacks to knock websites offline. Now as likely to refer to those that steal credit card numbers and banking data with viruses or by phishing.

BOT

The name given to an individual computer in a larger botnet and which is more than likely a home PC running Windows. The name is an abbreviation of "robot" to imply that it is under someone else's control.

BOTNET

A large number of hijacked computers under the remote control of a single person via net-based command and control system.

The machines are often recruited via a virus that travels via e-mail but increasingly drive-by downloads and worms are also used to find and recruit victims.

The biggest botnets can have tens of thousands of hijacked computers in them. Research suggests they can be hired from as little as 4 cents per machine.

BOTNET HERDER

One of the names for the controller or operator of a botnet.

BULLET-PROOF HOSTING

A company that guarantees that its servers will not be shut down even when the request to do so comes from law enforcement agencies.

These hosting companies are often located off-shore or in nations where computer crime laws are lax or non-existent and where extradition requests will not be honoured.

CARDER

Someone who steals or trades exclusively in stolen credit card numbers and their associated information.

CASH-OUT

A euphemism that means to steal money from a bank account or credit card to which someone has gained illegal access.

Hackers who grab credit card data often do not possess the skills or contacts to launder the money they can steal this way.

CHANNEL

A virtual "room" on the IRC text chat system. Most channels are usually dedicated to a single topic.

CROSS-SITE SCRIPTING

A sophisticated phishing attack that exploits weaknesses in the legitimate sites of financial institutions to make attempts to trick people into handing over confidential details more plausible.

A successful use of Cross-site scripting will make it look like all the transactions are being done on the website of the real bank or financial institution.

DEAD-DROP

A hijacked PC or server used to store all the personal data stolen by keyloggers, spyware or viruses.

Criminal hackers prefer to keep their distance from this data as its possession is incriminating. Dead drops are usually found and shut down within a few days of the associated phishing e-mails being sent out.

DDoS

Abbreviation for Distributed Denial of Service. This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net.

DDoS attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid.

DRIVE-BY DOWNLOAD

Malicious programs that automatically install when a potential victim visits a booby-trapped website. The vast majority exploit vulnerabilities in Microsoft's Internet Explorer browser to install themselves. Sometimes it is obvious that a drive-by download has occurred as they can lead to bookmarks and start pages of the browser being replaced. Others install unwanted toolbars. Increasingly criminals are using drive-bys to install keyloggers that steal login and password information.

EXPLOIT

A bug or vulnerability in software that malicious hackers use to compromise a computer or network. Exploit code is the snippet of programming that actually does the work of penetrating via this loophole.

FIREWALL

Either a program or a feature built into hardware and which sits between a computer and the internet. Its job is to filter incoming and outbound traffic.

Firewalls stop net-borne attacks such as worms reaching your PC.

HONEYPOT

An individual computer or a network of machines set up to look like a poorly protected system but which records every attempt, successful or otherwise, to compromise it.

Often the first hints of a new rash of malicious programs comes from the evidence collected by honeypots.

Now cyber criminals are tuning their malware to spot when it has compromised a honeypot and to leave without taking over.

IP ADDRESS

The numerical identifier that every machine attached to the internet needs to ensure the data it requests returns to the right place. IP stands for Internet Protocol and the technical specification defines how this numerical system works.

IRC

Abbreviation for Internet Relay Chat - one of the net's hugely popular text chat systems.

The technology is also used by botnet herders to keep tabs on and control their flock of machines.

KEYLOGGER

Program installed on a victim's machine that records every keystroke that a user makes.

These tools can obviously be very useful for stealing login and password details. However, the data that is stolen often has to be heavily processed to make it intelligible and to extract names and numbers.

MALWARE

Portmanteau term for all malicious software covers any unwanted program that makes its way on to a computer.

Derived from **Mal**icious soft **ware** .

MAN-IN-THE-MIDDLE

A sophisticated attack in which a criminal hacker intercepts traffic sent between a victim's computer and the website of the organisation, usually a financial institution, that they are using.

Used to lend credibility to attacks or simply steal information about online accounts. Can be useful to defeat security measures that rely on more than just passwords to grant entry to an account.

PACKET SNIFFING

The practice of examining the individual packages of data received by a computer to find out more about what the machine is being used for.

Often login names and passwords are sent in plain text within data packets and can easily be extracted.

PHISHING

The practice of sending out e-mail messages that look as if they come from a financial institution and which seek to trick people into handing over confidential details.

Often they direct people to another website that looks like that of the bank or financial institution the e-mail purports to have come from. Anyone handing over details could rapidly have their account plundered.

PORT

The virtual door that net-capable programs open to identify where the data they request from the net should be directed once it reaches a computer.

Web browsing traffic typically passes through port 80, e-mail through port 25.

ROOTS

A slang term for networks that have been hacked into by criminal hackers. Derives from the deep, or root, access that system administrators typically enjoy on a network or computer.

The login details to get root access are often sold to spammers and phishing gangs who then use these networks to send out millions of e-mail messages.

SCRIPT KIDDIE

An unskilled hacker who originates nothing but simply steals code, techniques and attack methods from others.

Many viruses and worms on the web today are simply patched together from other bits of code that malicious hackers share.

SPYWARE

Malicious program that, once installed on a target machine, steals personal and confidential information. Distinct from adware.

Spyware can be contracted many different ways. Increasingly it arrives on a PC via a web download. Often uses a keylogger to grab information. Some are now starting to record mouse movements in a bid to foil the latest security measures. Some fake security programs pose as spyware cleaners.

TCP

Abbreviation for Transmission Control Protocol - the series of specifications which define the format of data packets sent across the internet.

TROJAN

Like the wooden horse of legend this is a type of program or message that looks benign but conceals a malicious payload. Many of the attachments on virus-bearing e-mail messages carry trojans.

VIRUS

A malicious program - usually one that requires action to successfully infect a victim. For instance - the malicious programs inside e-mail attachments usually only strike if the recipient opens them.

Increasingly the word is used as a portmanteau term for all malicious programs - those that users must set off or those that find their own way around the net.

WHITEHAT

A hacker that uses his or her skills for positive ends and often to thwart malicious hackers.

Many whitehat security professionals spend their time looking for and closing the bugs in code that blackhats are keen to exploit.

WORM

Self-propelled malicious program that scours the web seeking new victims - in the past this has been used to distinguish it from a virus that requires user action to compromise a machine.

Worms can infect and take over computers without any help, bar lax security, from a victim.

ZERO DAY

A Zero day vulnerability is one on which code to exploit it appears on the first day that a loophole is announced.

As most of the damage done by exploiting bugs occurs in the first few days after they become public, software firms usually move quickly to patch zero day vulnerabilities.