Definitions of Malware

Adware - BOT - BOTNET - Hoax - Malware - Payload - Phishing - Rootkit - Scam - Spyware - Trojan horses - Virus – Worm

Adware

A type of Advertising Display Software, specifically certain executable applications whose primary purpose is to deliver advertising content potentially in a manner or context that may be unexpected and unwanted by users. Many **adware** applications also perform tracking functions, and therefore may also be categorized as Tracking Technologies. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for. (Source: Anti-Spyware Coalition)

BOT

Short for "Robot" a **bot** is a program that is designed to automate tasks. Initially bots were used in the UNIX world to automate dull tasks that system administrators frequently perform. Some **bots** will automatically chat with a user, simulating a human response to questions. Bots can also be used maliciously to allow a remote attacker to control a victims PC. The nature of many bots is such that it is as easy to control one PC as one hundred thousand PCs. Bots can be used to send spam, download and store illegal files, such as some types of porn, or to make computers participate in attacks on other computers. A **bot** can be made to search the victim's hard drive and send confidential information to a remote site on the internet in order to perform identity theft. Computers that are infected with bots are often called drones or zombies.

BOTNET

A botnet is a group of bot infected PCs that are all controlled by the same "command and control center". Recently peer-to-peer (P2P) botnets have been used. These botnets do not have a traditional command and control center but they are all part of the same "army".

Hoaxes

Hoaxes are usually silly pranks, and are a form of chain mail, and are often also Urban Legends.
Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an 'undetectable virus' on their system (how can it be undetectable if you can detect it?). Some have actually been malicious in content, causing the recipient to delete files from their systems. They should simply be deleted. There is no good luck from sending them to 20 of your friends, nor are they a way in which you will learn anything about the security of your computer.

Malware

Malware stands for MALicious SoftWARE. Terms such as Virus, Trojan, Worm, and Bot all have specific meanings. Malware is used to generically describe any malicious software, regardless of its technical category.

Payload

The additional functionality, for instance data stealing, file deletion, disk overwriting, BIOS flashing etc that may be included in a Virus, Worm or Trojan Horse. Note that the payload does not necessarily have to be damaging - for instance the payload of the Form-A virus was to make the keyboard make clicking noises on one day a month - it did no damage other than that. In the case of a Trojan, it is the 'secret' function that the programmer wanted to achieve.

Phishing

Phishing (pronounced in the same way as fishing) is a social engineering attack which attempts to fraudulently acquire sensitive personal information, such as passwords and/or credit card details. Usually this is achieved by sending e-mail (or similar communication) masquerading as a trustworthy person or business with an apparently legitimate request for information. The most common Phishes look as though they come from popular high-street banks, and usually contain some sort of threat of discontinuation of service, or other undesirable consequence if the instructions are not followed. Sometimes a the mail will look very genuine, and will contain branding and content which may have originally come from the source that it is impersonating. Usually there will be a link in the mail that will take the recipient to a website (which also may look very much like the legitimate site), and this site will be used to capture the details being 'phished'. It is important to remember that banks, and legitimate companies like Ebay or PayPal will never request usernames and passwords in unsolicited email. It is also worth bearing in mind that the links in phishing emails although they may look legitimate, will almost always point to a different site underneath. Always open a new browser session and type the correct address into the Address bar when you are trying to get to your internet bank or other online services.

Rootkit

A rootkit is a collection of one or more tools designed to covertly maintain control of a computer. Initially rootkits appeared on the UNIX operating systems (including Linux) and were a collection of one or more tools which allowed an attacker to gain and keep access to the most privileged user on the computer (on UNIX systems this user is called 'root' - hence the name) On Windows based systems, rookits have more commonly been associated with tools used for hiding programs or processes from the users. When installed a Windows rootkit uses functions in the operating system to hide itself, so as not to be detected, and is often used to hide other malicious programs such as keystroke loggers. The use of rootkits is not necessarily malicious, but they have come to be increasingly associated with undesirable behavior and malicious software.

Scams

Scams are very similar to phishing, but are not usually interested in obtaining your details, they often appeal to a sense of compassion or to human greed. For instance, almost every disaster (earthquake, flood, war, famine) has generated large amounts of scams, usually in the form of appeals for charitable aid for a 'worthy' cause. Advanced Fee Frauds (sometimes called 419 scams) offer you the opportunity to get a large amount of money by supposedly helping the scammer to transfer even larger sums of money out of a country (often an African country such as Nigeria). These scams always result in you being asked to send the scammer some money to cover "administration" costs (often this is several thousands of dollars). Sometimes, these scams have resulted in the person being scammed disappearing, either killed or kidnapped after traveling to another country to meet their 'benefactor'. In less extreme cases, many people have lost thousands and thousands of dollars to these frauds. Some tips for avoiding such scams:

- Legitimate charities usually only send appeal emails to people who have explicitly chosen (opted in) to receive emails from the organization. Unsolicited, such emails are almost always fraudulent - particularly ones that appear quickly after a disastrous event.
- Don’t be fooled by appearance. E-mails can appear legitimate by copying the graphics and language of a legitimate organization. Many include tragic stories of victims of the disaster. Don’t click through to links: links in emails can lead to “spoofed” Web sites that mirror the look and feel of a genuine organization.
- There's no such thing as a free lunch - If it looks too good to be true, it almost always is.

Spyware

The term Spyware has been used in two ways.
In its narrow sense, Spyware is a term for Tracking Software deployed without adequate notice, consent, or control for the user.
Often the tracking is done by reporting information (anything from browsing history to credit-card or personal details) to a third party.
Some Spyware is delivered as part of another program (much the same way as a Trojan Horse), but some is delivered as a **Payload** to a **Worm**, or via websites which exploit vulnerabilities in browsers to silently install the programs in the background. There are also many programs which pretend to be Anti-Spyware programs, but are themselves Spyware. In its broader sense, Spyware is used as a synonym for what the Anti-Spyware Coalition calls “Spyware and Other Potentially Unwanted Technologies.” This can include some types of cookies, commercial keyloggers and other tracking technologies.

Trojan Horse

A Trojan Horse, often referred to as just a Trojan, is a program which purports to do one thing, but actually does another. Not always damaging or malicious, they are often associated with things like deleting files, overwriting hard-drives, or being used to provide remote access to a system for an attacker. Classical Trojans include keyloggers being delivered as game files, or file deleters masquerading as useful utilities. Trojans can be used for many purposes including

- Remote Access (sometimes called Remote Access Tools or RAT's, or Backdoors)
- Keylogging and password stealing (Most spyware falls into this category)

Virus

A virus is a program which replicate by copying itself, either exactly, or in a modified form, into another piece of executable code. Viruses can use many types of hosts, some of the most common are:

- executable files (such as the programs on your computer)
- boot sectors (the parts of code that tell your computer where to find the instructions it uses to 'boot' or turn on)
- scripting files (such as Windows Scripting, or Visual Basic script)
- macros within documents (this is much less common now, as macros in, for instance Microsoft Word, will not execute by default)

When a virus inserts itself into other executable code, this ensures it is run when that other code is run, and the virus spreads by searching for other 'clean' hosts every time it is run. Some viruses overwrite the original files, effectively destroying them, but many simply insert themselves in a way that they become part of the host program, so that both survive. Depending on the way they are coded, viruses can spread across many files in the system, across networks via file shares, in documents, and in the boot sectors of disks. Although some viruses are spread by email, this does not make them viruses, and in-fact, most of the things that spread in email are actually **worms**. To be a virus, the code simply has to replicate, it does not need to do a lot of damage, or even spread very widely (See Payload).

Worm

In computer terms, worms are really a subset of **viruses** , but they have the ability to replicate by themselves, they do not require a host file.
Simply put, viruses infect hosts, and worms infest systems. Often worms exploit a vulnerability in services in network facing services. Such worms can spread very quickly across networks of vulnerable systems, as they do not require any intervention from users to run. However, the commonest type of worms are carried in emails (it is important to note that it is not the email which is infected, but that they carry the worm files). In the case of the email borne worm, the recipient of the email is the vulnerability that is exploited, usually with an enticing subject or message.
Usually worms are much easier to remove from a system than viruses, because they do not infect files. Worms often try to add themselves to the startup folder, or modify registry keys to ensure that they are loaded every time the system starts. Again, worms do not necessarily have to do any damage.