

## **Malicious code:**

Is software designed to infiltrate a computer system without the owner's informed consent? The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

## **Examples of malicious codes**

- Mellisa
- Explore.zip
- Freelinks
- Email worms

## **A hoax:**

Is a deliberate attempt to deceive or trick people into believing or accepting something which the hoaxer (the person or group creating the hoax) knows is false. Hoax E-mail messages distribute false, often disturbing, information designed to trick recipients into passing the same note onto other E-mail users. On the surface this does not sound like a terribly threatening or bothersome practice, but hoaxes, and those who choose to distribute them, can do real damage, both physical and mental. Each message sent from a user's E-mail account, practical or superfluous, requires the expenditure of resources on the computer of origination and on every computer network it happens to pass through or into

Example include Red Alert hoax

This is a warning of a nasty hoax that has been distributed on several mailing lists and in usenet news. The hoax message is falsely attributed to Mikko.Hypponen@F-Secure.com from F-PROT Professional Support.

## **A backdoor:**

Is a mechanism surreptitiously introduced into a computer system to facilitate unauthorized access to the system. While backdoors can be installed for accessing a variety of services, of particular interest for network security are ones that provide interactive access. These are often

installed by attackers who have compromised a system to ease their subsequent return to the system.

Backdoors are, by design, difficult to detect. A common scheme for masking their presence is to run a server for a standard service such as Telnet, but on an undistinguished port rather than the well-known port associated with the service, or perhaps on a well-known port associated with a *different* service

Backdoors can be detected by inspecting network traffic using an intrusion detection system (IDS), where we presume that there is a large volume of legitimate traffic which must be distinguished from the illegitimate traffic

## **Password cracking:**

Is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crack able passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

.Passwords can sometimes be guessed by humans with knowledge of the user's personal information. Examples of guessable passwords include:

- blank (none)
- the name of a significant other, a friend, relative or pet
- their birthplace or date of birth, or a friend's, or a relative's

## **Brute force:**

(also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard DES keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach

Brute force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute force attack against it.

A classic example is the *traveling salesman problem (TSP)*. Suppose a salesman needs to visit 10 cities across the country. How does one determine the order in which cities should be visited such that the total distance traveled is minimized? The brute force solution is simply to calculate the total distance for every possible route and then select the shortest one. This is not particularly efficient because it is possible to eliminate many possible routes through clever algorithms.

## **Dictionary:**

.A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password.

An e-mail spamming technique in which the spammer sends out thousands or millions of e-mails with randomly generated addresses using combinations of letters added to known domain names in the hopes of reaching a percentage of actual e-mail addresses. May can be used by the dictionary cracker For example, a dictionary attack list might begin with john@webopedia.com, john1@webopedia.com, john2@webopedia.com, and so on until all possible combinations of letters and numbers has been exhausted.

## **DOS:**

Is an abbreviation for Disk Operating System. Historically, not all operating systems ran off of floppy disks or hard drives, so ones that included this functionality often had "DOS" in their name.

Examples include:

Apple DOS

Atari DOS

Commodore DOS,

Nowadays, most operating systems are run off of a disk, so the term DOS is no longer widespread.

## **Man-in-the-middle attack:**

Abbreviated as MITM, a *man-in-the-middle attack* is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers. MITM attacks are associated with 802.11 security, as well as with wired communication systems.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle).

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send - most of the costs are paid for by the recipient or the carriers rather than by the sender.

There are two main types of spam, and they have different effects on Internet users. Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "lurkers", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the

newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming is universally reviled, and has been the subject of legislation in many jurisdictions

### **E-mail bombing:**

In Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

An email message consists of two components, the message *header*, and the message *body*, which is the email's content. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually additional information is added, such as a subject header field.

### **A sniffer:**

Is a piece of software that grabs all of the traffic flowing into and out of a computer attached to a network. They are available for several platforms in both commercial and open-source variations. Some of simplest packages are actually quite easy to implement in C or Perl, use a command line interface and dump captured data to the screen. More complex projects use a GUI, graph traffic statistics, track multiple sessions and offer several configuration options. Sniffers are also the engines for other programs. Intrusion Detection Systems (IDS) use sniffers to match

packets against a rule-set designed to flag anything malicious or strange. Network utilization and monitoring programs often use sniffers to gather data necessary for metrics and analysis.

## **A buffer overflow:**

Is when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability

Programming languages commonly associated with buffer overflows include C and C++ which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows

Technically a buffer overflow occurs when data written to a buffer, due to insufficient bounds checking corrupts data values in memory addresses adjacent to the allocated buffer. Most commonly this occurs when copying strings of characters from one buffer to another.

15 An occurrence or event; The regulation of the pace of e.g. an athletic race, the speed of an engine, the delivery of a joke, or the occurrence of a series of events; The time when something happens; The synchronization of the firing of the spark plugs in an internal combustion engine;

**References:**

<http://virusall.com/hoaxes/examples/redalert.php>

<http://www.itg.ias.edu/whatarehoaxmessages>

<http://www.icir.org/vern/papers/backdoor/>

[http://en.wikipedia.org/wiki/Buffer\\_overflow](http://en.wikipedia.org/wiki/Buffer_overflow)