Chapter 1: Malware

The term malware refers to any computer program written with the sole intent of

a) Performing an un-authorized actions
b) Causing harm to data and programs
c) Causing unwanted system behavior
d) Intrude and Invade privacy
e) Identifying vulnerabilities in the system and exploit them

Malware are classified into various types. Figure 1 presents details the broad classification of malware.

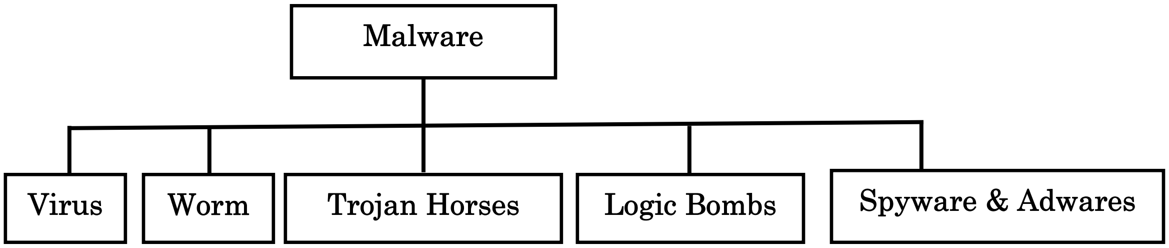

Figure 1: Malware classification

We shall examine all these classifications in detail.

1.1 Virus

Dr Frederick Cohen, a mathematician, in 1984, introduced the term of 'Computer Virus" and is known as the "father" of computer viruses. According to Cohen, a computer virus is: *"A virus is a program that is able to infect other programs by modifying them to include a possibly evolved copy of itself."*

Webster's Collegiate Dictionary explains a computer virus as "a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action (such as destroying data)".

1.1.1 Structure of a computer virus

Any virus has the following components.

a) Vector: Refers to what is to be infected. If the vector refers to a network, one can classify the malware as a worm.
b) Payload: Refers to what actions have to be done when the virus infects the target.
c) Replicator: An important part of the virus which helps in multiplication of the virus
d) Concealer: Refers to the portion of the virus which prevents the anti-virus software or integrity checkers from seeing or discovering the virus. Based on the level of concealment, we have encrypted, oligomorphic, polymorphic and metamorphic viruses.

1.1.2 Types of computer viruses

There are various types of viruses. They being

1. Boot sector viruses
2. File-infector viruses
3. Macro viruses
4. Memory resident viruses
5. Stealth viruses
6. Self-Protecting Viruses
7. Vulnerability-Exploiting viruses
8. Archive attacking viruses
9. Viruses for Pocket PCs
10. Retroviruses
11. Multipartite virus

1.1.2.1 Boot-Sector viruses

Boot-sector viruses infect the boot-sector portion of the system. Every media has a boot-sector which provides information about the drive or disk structure. A boot-sector virus attacks this area, and either resides there or changes the Master Boot Record (MBR). If a system is infected with a boot-sector virus, the system will not boot at all. Typical examples for boot-sector viruses are Stoned virus and Denzuko virus.

1.1.2.2 File-infector viruses

File-infector viruses infect files of various categories. Table 1 gives the types of viruses, what they infect and typical examples of them.

Table1: File-infector viruses

TYPE	INFECTS	SUGGESTIVE EXAMPLES
COM viruses	Infects .com files	Cascade, Virdem
Device Driver Viruses	Infects device drivers	W95/Opera
Dynamic Link Library Viruses	Infects a Dynamic Link Library file.	Happy99 worm
EXE viruses	Infects .exe files	W16/Winvir
LX (Linear Executable) viruses	Infects OS-2	OS2/Jiskefet
Native Viruses	Infects the Native DLL file NTDLL.DLL in Windows	W32/Chiton
NE (New Executable) viruses	Infects 16-bit windows and OS-2	W16/Winvir, W16/Tentacle_II
Object Code Viruses	Infects object files	Shifter viruses
PE (Portable Executable) Viruses	Infects 32-bit windows	W95/Boza, MSIL/Impanate virus

1.1.2.3 Macro-Viruses

Macros, by definition, refer to a series of commands written and stored by the user and when these macros are executed, all the commands are executed in one stroke. Macro viruses, written in macro languages, are a special type of virus that infects document files, electronic spreadsheets and databases instead of computer programs. They cling on to the application's macro programming language for propagating. To illustrate, in MS-Word, *normal.dot* is the template on which all MS-Word documents are created. Once this template is infected by the virus, all documents that use this template will also be infected. Note that macro-viruses are not platform specific. They are found in all kinds of environments. Table 2 provides a tentative list of Macro-viruses.

Table 2: List of Macro-Viruses

MACRO-VIRUS TYPE	INFECTS	SUGGESTIVE EXAMPLES
ABAP Viruses on SAP	Infects scripts written in ABAP, a scripting language for the ERP package SAP	ABAP/Rivpas
Adobe PDF Viruses	Infects Adobe Portable Data Format files	{ W32,PDF} /Yourde
AppleScript Virus	AppleScript which is used for in scripting Apple machines are infected.	AplS/Simpsons@mm
AutoLisp Script Viruses	Infects AutoLisp Script, a scripting language of AutoCAD	Pobresito, ALS/Burstead
Corel Script Viruses	Infects CorelScript files, a scripting language for products from Corel Corporation	CSC/CSV virus
DCL (DEC Command Language) Viruses for DEC/VMS	Infects VAX/VMS system	Father Christmas
Help File Viruses	Infects the scripts written in Windows Help section. Executes when F1 is pressed	W95/SK
Hive Viruses	Infects Microsoft Windows Registry	W32/PrettyPark
HTML (Hypertext Markup Language) virus	Infects the VBScript or Jscript embedded in a HTML page	W32/Nimda
JScript Viruses	Infects Java Scripts	Virus.JS.Fortnight
Lotus 1-2-3 macro virus	Infects the macros of Lotus 1-2-3 files	BAT/Ramble virus
Lotus Word Pro Macro Viruses	Infects Lotus Word Pro files	LWP/Spenty virus
Macromedia Flash virus	Infects ActionScript of Macromedia Flash	SWF/LFM-926Flash
MS-Office Macro viruses	MS-Office product	XM/Laroux, WM/DMV
Perl Viruses	Infects scripts written in Perl language	Virus.Perl.DirWorm
PHP Viruses	Infects scripts written in PHP language	PHP/Caracula
REXX Viruses on IBM Systems	Infects REXX command script language	CHRISTMA EXEC
Shell Script Viruses	Infects Shell scripts in UNIX	SH/Renepo
VBScript (Visual Basic Script) Viruses	Infects Windows Systems	VBS/LoveLetter.A@mm
Windows Installation Script Virus	Infects the installation script language of 32-bit Windows.	INF/Vxer

1.1.2.4 Memory resident viruses

Belonging to the category of TSR (Terminate - and Stay - Resident), memory resident viruses infects the system, occupies a portion of the memory, executes from that portion of memory and finally propagates by infecting files and system areas.

In Microsoft Disk Operating System (DOS), there exist various interrupts which are used for programming. Some examples of interrupts are INT 09 (Keyboard BIOS), INT 10h (Video BIOS), INT 12h (Get Memory Size BIOS), INT 20h (Terminate Program DOS Kernel), and INT 27h (Terminate-and-Stay Resident (DOS Kernel)). Virus developers exploit these interrupts and develop memory resident viruses.

Stupid virus, Darth_Vader virus, Jerusalem virus, Brain virus, and Filler virus are typical examples of TSR virus.

1.1.2.5 Stealth viruses

Viruses that can hide its virus code and protects itself from being discovered from scanners and integrity checkers is termed as a stealth virus. Most of the modern day viruses are stealth in nature.

1.1.2.6 Self-Protecting Viruses

Developers of viruses are developing techniques by which viruses can protect themselves from being detected from anti-virus software and integrity checkers. Viruses that can protect themselves are termed as self-protecting viruses. Self-protecting viruses are further classified as encrypted, oligomorphic, polymorphic, and metamorphic computer viruses.

a) Encrypted viruses

One way to hide what the virus does is to encrypt its functionality. The virus code is encrypted and only during the execution, the decryption process takes place. One typical example for an encrypted virus is the Cascade virus for DOS. The architecture of the virus begins with a decryptor, followed by the encrypted virus code.

b) Oligomorphic viruses

Detecting an encrypted virus using an anti-virus software was not difficult the anti-virus software was able to identified and detect the decryptor.

Oligomorphic viruses overcame this issue by creating a mutation of decryptors. The virus code remained the same but the set of decryptors were more than one.

For example, the W95/Memorial virus has 96 different decryptor patterns and randomly chooses one among them.

c) Polymorphic viruses

Polymorphic viruses are an extension to Oligomorphic viruses. Here, the decryptors can mutate and can take millions of different forms. Moreover, with the development of The Dark Avenger Mutation Engine and Trident Polymorphic Engine, polymorphic virus development became a simple task. W95/HPS virus and W95/Marburg virus are typical examples of polymorphic viruses.

d) Metamorphic viruses

The most feared type of computer viruses today belong to the metamorphic classification. W95/Zmist and W32/Simile viruses are typical examples for metamorphic viruses.

The main characteristics of metamorphic viruses are:

a) Metamorphic viruses can reprogram themselves. The virus body keeps changing in different generations.
b) Metamorphic viruses do not have a decryptor or a constant virus body.

Detection of W95/Zmist and W32/Simile metamorphic viruses is a real challenge for anti-virus softwares.

1.1.2.7 Vulnerability-Exploiting viruses

Vulnerability-Exploiting viruses exploit the various vulnerabilities present in the system.

Some of the typical vulnerabilities are buffer overflows, heap overflows, and format string vulnerabilities.

Typical examples of Vulnerability-Exploiting viruses include Morris Internet worm, Linux/Slapper and W32/CodeRed.

1.1.2.8 Archive Attacking viruses

The viruses of this category infects archive files which have an extension names of .ZIP, .ARJ, .RAR, and .CAB. One good example is the Zhengxi virus and W32/Beagle@mm virus

1.1.2.9 Viruses for Pocket PCs

Recently, viruses have been developed and released that infects Pocket PCs. A typical example is WinCE/Duts.1520 virus.

1.1.2.10 Retroviruses

A retrovirus is a special kind of computer virus that has the ability to bypass or circumvent the operation of an antivirus or a personal firewall, or any other installed security program.

Some of the common actions performed by a retrovirus include disabling antivirus programs, bypassing firewalls, deleting / modifying the integrity-checking database files, and preventing infected systems from downloading updates from antivirus Web sites.

Typical examples of retroviruses include IDEA.6155 virus, Varicella virus, HybrisF virus and W32/Beagle@mm virus.

1.1.2.11 Multipartite viruses

Multipartite viruses are a combination of boot-sector viruses and file viruses. A typical example for multipartite virus is Ywinz.

1.2 WORMS

Worms are malware whose vector is always the network. A worm, which is a stand-alone program, does not need a host to carry it. It self-replicates itself through a network. While worms harm the network by consuming bandwidth, viruses infect or corrupt files.

1.2.1 Classification of worms

Worms are classified as:

a) Rabbits
b) E-mail worms
c) Mobile worms

1.2.1.1 Rabbits

A rabbit is a kind of worm whose main line of activity is to self-replicate limitlessly, fill the hard-disk and exhaust all computer resources. Apart from self-replicating, rabbits, generally, do not cause any harm to data and programs.

1.2.1.2 E-mail worms

E-mail worms primarily use e-mail as the main vehicle for propagation. Mass-mailer worms belong to this class of worms. Mass-mailers worms such as VBS/Loveletter.A@mm, sends multiple e-mails including a copy of them once it is executed. Another worm, W32/SKA.A@m (also known as the Happy99 worm) sends a copy of itself every time the user sends a new message.

1.2.1.3 Mobile worms

Recently worms have appeared in mobiles also. The SymbOS/Cabir worm infects Nokia 60 series and also blue-tooth enabled mobiles running the Symbian operating system.

1.2.2 Techniques adopted by worms to propagate and replicate

Table 3 shows the techniques adopted by worms to propagate and replicate.

Table 3: Techniques adopted by worms to replicate and propagate

ATTACKING TECHNIQUES	METHOD	SUGGESTIVE EXAMPLES
Forging e-mail headers	Replaces the header of the e-mail with addresses of well-known firms and thus deceiving the users	W32/Parvo, W32/Hyd
IRC (Internet Relay Chat) worms	Propagates through Instant Messaging	W32/Choke worm
NNTP (Network News Transfer Protocol) Attacks	The worm infects one of the host in a network newsgroup and thus infects all those who are connected to the network news.	Happy99
Peer-to-Peer (P2P) Network Attacks	Worms creates a copy of themselves to a shared P2P folder on the host. When any user on the P2P network logs on to the P2P host, the worm copies itself to the target.	W32/Maax worm
SMTP (Simple Mail Transfer Protocol) Proxy Based worms	The e-mail client instead of directly connecting to the SMTP server is re-directed to the proxy from where the worm propogates.	W32/Taripox

1.3 TROJAN HORSES

Trojan horses derive their name from the Greek mythology story wherein the Greek soldiers, in order to sneak into the impregnable city of Troy, hid themselves into a wooden horse. The wooden horse was pulled into the city of Troy and the soldiers came out of the horse and opened the gates of the city.

Very similarly, Trojans are also a form of malware that sneak into the computer of a victim computer disguised as harmless software. They hide inside another program so that when the original innocent program is installed and executed, the Trojan program also gets installed and executes as well.

The main difference between a Trojan and a virus is that Trojans

a) Do not infect host files
b) Do not have the capability to self-replicate.

However, Trojans can do a lot of malicious act such as create back doors so that computer hackers can hack into the system to gain access to passwords, and other private information stored on a computer.

For a Trojan horse to infect, any user must run a program that has a Trojan embedded in it.

One of the popular Trojan horse recorded in history is the AIDS TROJAN DISK. The Trojan scrambled the names of almost all the files and filled the empty areas of the disk completely.

1.4 LOGIC BOMBS

A logic bomb is a class of malware that "explodes" when a specified condition occurs. The specific condition could be date, time or any specific logical condition. Logic bombs may reside within standalone programs, or they may be part of worms or viruses.

Typical examples of actions performed by logic bombs are:

a) Infect the system with a particular strain of virus and execute the virus until it has infected a certain number of hosts.
b) Perform a malicious act on a particular date and/or time. Example of such a logic bomb is 'Friday the 13th' virus.

1.5 SPYWARES & ADWARES

Internet is becoming ubiquitous and lots of users are browsing the web pages hosted by companies and sellers on the Internet. On account of this trend, sellers are interested in knowing what people like and look for and what kinds of products consumers might buy.

To obtain information about a potential customer sellers install small applications called spyware. When a naïve user browses the Internet, spywares collect information and personal preferences of the user and passes this information to the sellers. With the help of this information, sellers create and display customized advertisements in pop-up messages.

Adwares is a special type of spyware. While spywares get themselves installed into the system without seeking the consent of the user, adwares usually seeks permission of the user before it is installed.

Spammer programs, a kind of spyware, are used to send unsolicited messages to newsgroups, or to e-mail accounts through e-mails.

Yet another kind of spyware is the Keylogger. A keylogger captures keystrokes punched-in by an user and transmits the sequence of punched keystrokes to hackers. Keyloggers help in collecting sensitive information such as passwords, credit card numbers and their PINs.

Spywares and adwares, even though are not malicious in nature, they are obviously malware for they invade and intrude into the privacy of individuals.

1.6 HOW ARE VIRUSES DETECTED & IDENTIFIED

Every virus is identified by a unique pattern of bits. These unique patterns are termed as virus signatures. Just like fingerprints of humans are unique to individuals and can be used for identification, virus signatures for every virus is unique and are used by anti-malware programs to locate and either destroy or quarantine them. However, the task is not so simple for most of the modern day viruses are metamorphic in nature.

1.7 VIRUS DETECTION METHODS

Viruses are generally detected using any of the five methods of:

a) Checksumming
b) Interrupt Monitoring
c) Memory Detection
d) Signature Scanning
e) Heuristics/Rules-based Scanning

Table 4 provides information on these five methods and their limitations.

Almost all Anti-Virus solutions adopt any one of these methods or a combination of these methods to efficiently tackle the menace of malware.

Table 4: Major Virus Detection Methods

NAME	HOW IT WORKS	LIMITATIONS
Checksumming	Checks whether the virus has changed the characteristics of a file.	• Needs a virus-free checksum database • Cannot detect passive and active stealth viruses
Interrupt Monitoring	Attempts to locate and prevent a virus' "interrupt calls"	• Slows down the system. • Legal system calls may also be branded as malicious • Obtrusive in nature.
Memory Detection	Recognizing a known virus by its code and location while in memory.	• Can slow down the system • Can interfere with valid operations.
Signature Scanning	Recognizes a virus' unique "signature,"	• One has to maintain the signature files • May make false positive detection in valid file.
Heuristics based Scanning	Uses heuristics to efficiently identify viruses	• Obtrusive • May cause false alarms

1.8 ANTI-MALWARE POLICIES TO BE ADOPTED

a) Procure and use a good anti-virus program.
b) Update anti-virus software regularly.
c) Write protect all source diskettes and use a good anti-virus program to scan them before write-protecting it.
d) Scan all disks brought from outside
e) Educate users on the consequences of malware attack, caution them and inform users the procedures to be followed in case of a malware attack.
f) Have in place a Disaster Recovery Plan and a Business Continuity Plan
g) Have in place a good recording mechanism which records all activities during and after a malware attack
h) As far as possible, dedicate a stand-alone machine for connecting to the Internet. After downloading anything from the Internet, scan them using anti-virus software.
i) If possible, removable media may be disabled.
j) Using the firewall in the organization, prevent downloading of some types of files from the Internet.
k) If possible, disable macros.
l) Usage of Viewers can be encouraged (if the activity involves no modification) rather than full applications. For example use Microsoft Power-Point Viewer instead of Microsoft Power Point.
m) Any data that is downloaded from the Internet has to first pass through the firewall and the network intrusion detection software before they are used by people.

1.9 LIST OF MALWARE

The number of malware is so large and is fast expanding. Hence it is difficult to provide a complete list of all malware.

The following sources provide an updated list of all malware.

a) http://www.cert.org/other_sources/viruses.html#III

b) http://www.viruslist.com/en/viruses/encyclopedia

c) http://en.wikipedia.org/wiki/List_of_computer_viruses

2.0 COMPANIES DEVELOPING ANTI-MALWARE SOFTWARE

As the number and strength of malware increases day-by-day, the numbers of anti-malware software developers are also on the rise. Table 5 provides a suggestive list (no means exhaustive) of companies that develop anti-malware software.

Table 5: Suggestive list of companies that develop anti-malware software

NAME OF THE COMPANY	URL OF THE COMPANY
Aladdin Knowledge Systems	http://www.aladdin.com
Cat Computer Services	http://www.quickheal.com
Computer Associates	http://www.ca.com/etrust
Cybersoft	http://www.cyber.com
Doctor Web Ltd.	http://www.drweb.com
F-Secure	http://www.f-secure.com
Frisk Software	http://www.f-prot.com
Grisoft	http://www.grisoft.com
Kaspersky Labs	http://www.kaspersky.com
McAfee Inc.	http://www.mcafeeb2b.com
Microsoft Corporation	http://www.windowsonecare.com/
Panda Software	http://www.pandasoftware.com
Softwin	http://www.bitdefender.com
Symantec Corporation	http://www.symantec.com
Trend Micro Incorporated	http://www.trendmicro.com