COMPUTER VIRUSES

- Definition.
- A computer virus is a type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them.
- Infecting computer programs can include as well, data files, or the "boot" sector of the hard drive.

Historical Development.

Early academic work on self-replicating programs. The first academic work on the theory of self-replicating computer programs[18] was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the «Theory and Organization of Complicated Automata». The work of von Neumann was later published as the «Theory of self-reproducing automata». In his essay von Neumann described how a computer program could be designed to reproduce itself.[19] Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical «father» of computer virology.[20] In 1972, Veith Risak, directly building on von Neumann's work on self-replication, published his article «Selbstreproduzierende Automaten mit minimaler Informationsübertragung» (Self-reproducing automata with minimal information exchange).[21] The article describes a fully functional virus written in assembler programming language for a SIEMENS 4004/35 computer system. In 1980 Jürgen Kraus wrote his diplom thesis «Selbstreproduktion bei Programmen» (Self-reproduction of programs) at the University of Dortmund.[22] In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.First examples.The MacMag virus 'Universal Peace', as displayed on a Mac in March 1988The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s.[23] Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.[24] Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system.[25] Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The Reaper program was created to delete Creeper.[26] In fiction, the 1973 Michael Crichton sci-fi movie Westworld made an early mention of the concept of a computer virus, being a central plot theme that causes androids to run amok.[27] Alan Oppenheimer's character summarizes the problem by stating that "...there's a clear pattern here which suggests an analogy to an infectious disease process, spreading from one...area to the next." To which the replies are stated: "Perhaps there are superficial similarities to disease" and, "I must confess I find it difficult to believe in a disease of machinery."[28] (Crichton's earlier work, the 1969 novel The Andromeda Strain and 1971 film were about a biological virus-like disease that threatened the human race.)In 1982, a program called "Elk Cloner" was the first personal computer virus to appear "in the wild"—that is, outside the single computer or [computer] lab where it was created.[29] Written in 1981 by Richard Skrenta while in the ninth grade at Mount Lebanon High School near Pittsburgh, it attached itself to the Apple DOS 3.3 operating system and spread via floppy disk.[29][30] This virus, created as a practical joke when Skrenta was still in high school, was injected in a game on a floppy disk. On its 50th use the Elk Cloner virus would be activated, infecting the personal computer and displaying a short poem beginning "Elk Cloner: The program with a personality." In 1984 Fred Cohen from the University of Southern California wrote his paper "Computer Viruses – Theory and Experiments".[31] It was the first paper to explicitly call a self-reproducing program a "virus", a term introduced by Cohen's mentor Leonard Adleman. In 1987, Fred Cohen published a demonstration that there is no algorithm that can perfectly detect all possible viruses.[32] Fred Cohen's theoretical compression virus[33] was an example of a virus which was not malicious software (malware), but was putatively benevolent (well-intentioned). However, antivirus professionals do not accept the concept of "benevolent viruses", as any desired function can be implemented without involving a virus (automatic compressio

A viable computer virus must contain a search routine, which locates new files or new disks which are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program which the search routine locates.[42] The three main virus parts are:Infection mechanism-Infection mechanism (also called 'infection vector'), is how the virus spreads or propagates. A virus typically has a search routine, which locates new files or new disks for infection.[43]Trigger-The trigger, which is also known as logic bomb, is the compiled version that could be activated any time an executable file with the virus is run that determines the event or condition for the malicious "payload" to be activated or delivered[44] such as a particular date, a particular time, particular presence of another program, capacity of the disk exceeding some limit,[45] or a double-click that opens a particular file.[46]Payload-The "payload" is the actual body or data that perform the actual malicious purpose of the virus. Payload activity might be noticeable (e.g., because it causes the system to slow down or "freeze"), as most of the time the "payload" itself is the harmful activity,[43] or some times non-destructive but distributive, which is called Virus hoax.[47]Phases-Virus phases is the life cycle of the computer virus, described by using an analogy to biology. This life cycle can be divided into four phases:Dormant phase-The virus program is idle during this stage. The virus program has managed to access the target user's computer or software, but during this stage, the virus does not take any action. The virus will eventually be activated by the "trigger" which states which event will execute the virus, such as a date, the presence of another program or file, the capacity of the disk exceeding some limit or the user taking a certain action (e.g., double-clicking on a certain icon, opening an e-mail, etc.). Not all viruses have this stage.[43]Propagation phase-The virus starts propagating, that is multiplying and self-replicating itself. The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often "morph" or change to evade detection by IT professionals and anti-virus software. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.[43]Triggering phase-A dormant virus moves into this phase when it is activated, and will now perform the function for which it was intended. The triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.[43]Execution phase-This is the actual work of the virus, where the "payload" will be released. It can be destructive such as deleting files on disk, crashing the system, or corrupting files or relatively harmless such as popping up humorous or political messages on screen.

OPERATIONS AND FUNCTIONS

INFECTION TARGETS AND REPLICATION TECHNIQUES.

Computer viruses infect a variety of different subsystems on their host computers and software.[48] One manner of classifying viruses is to analyze whether they reside in binary executables (such as .EXE or .COM files), data files (such as Microsoft Word documents or PDF files), or in the boot sector of the host's hard drive (or some combination of all of these).[49][50]Resident vs. non-resident viruses-A memory-resident virus (or simply "resident virus") installs itself as part of the operating system when executed, after which it remains in RAM from the time the computer is booted up to when it is shut down. Resident viruses overwrite interrupt handling code or other functions, and when the operating system attempts to access the target file or disk sector, the virus code intercepts the request and redirects the control flow to the replication module, infecting the target. In contrast, a non-memory-resident virus (or "non-resident virus"), when executed, scans the disk for targets, infects them, and then exits (i.e. it does not remain in memory after it is done executing).[51][52][53]Macro viruses-Many common applications, such as Microsoft Outlook and Microsoft Word, allow macro programs to be embedded in documents or emails, so that the programs may be run automatically when the document is opened. A macro virus (or "document virus") is a virus that is written in a macro language, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer. This is one of the reasons that it is dangerous to open unexpected or suspicious attachments in e-mails.[54][55] While not opening attachments in e-mails from unknown persons or organizations can help to reduce the likelihood of contracting a virus, in some cases, the virus is designed so that the e-mail appears to be from a reputable organization (e.g., a major bank or credit card company).Boot sector viruses-Boot sector viruses specifically target the boot sector and/or the Master Boot Record[56] (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.).[49][57][58]Email virus-Email virus – A virus that specifically, rather than accidentally, uses the email system to spread. While virus infected files may be accidentally sent as email attachments, email viruses are aware of email system functions. They generally target a specific type of email system (Microsoft's Outlook is the most commonly used), harvest email addresses from various sources, and may append copies of themselves to all email sent, or may generate email messages containing copies of themselves as attachments.

VULNERABILITIES AND INFECTION VECTORS

- Software bugs-Because software is often designed with security features to prevent unauthorized use of system resources, many viruses must exploit and manipulate security bugs, which are security defects) in a system or application software, to spread themselves and infect other computers. Software development strategies that produce large numbers of "bugs" will generally also produce potential exploitable "holes" or "entrances" for the virus.Social engineering and poor security practices-In order to replicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to executable files that may be part of legitimate programs (see code injection). If a user attempts to launch an infected program, the virus' code may be executed simultaneously.[75] In operating systems that use file extensions to determine program associations (such as Microsoft Windows), the extensions may be hidden from the user by default. This makes it possible to create a file that is of a different type than it appears to the user. For example, an executable may be created and named "picture.png.exe", in which the user sees only "picture.png" and therefore assumes that this file is a digital image and most likely is safe, yet when opened, it runs the executable on the client machine.[76]Vulnerability of different operating systems-The vast majority of viruses target systems running Microsoft Windows. This is due to Microsoft's large market share of desktop computer users.[77] The diversity of software systems on a network limits the destructive potential of viruses and malware.[78] Open-source operating systems such as Linux allow users to choose from a variety of desktop environments, packaging tools, etc., which means that malicious code targeting any of these systems will only affect a subset of all users. Many Windows users are running the same set of applications, enabling viruses to rapidly spread among Microsoft Windows systems by targeting the same exploits on large numbers of hosts.[6][7][8][79]While Linux and Unix in general have always natively prevented normal users from making changes to the operating system environment without permission, Windows users are generally not prevented from making these changes, meaning that viruses can easily gain control of the entire system on Windows hosts. This difference has continued partly due to the widespread use of administrator accounts in contemporary versions like Windows XP. In 1997, researchers created and released a virus for Linux—known as "Bliss".[80] Bliss, however, requires that the user run it explicitly, and it can only infect programs that the user has the access to modify. Unlike Windows users, most Unix users do not log in as an administrator, or "root user", except to install or configure software; as a result, even if a user ran the virus, it could not harm their operating system. The Bliss virus never became widespread, and remains chiefly a research curiosity. Its creator later posted the source code to Usenet, allowing researchers to see how it worked.

STEALTH STRATEGIES

- In order to avoid detection by users, some viruses employ different kinds of deception. Some old viruses, especially on the MS-DOS platform, make sure that the "last modified" date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date cyclic redundancy checks on file changes.[60] Some viruses can infect files without increasing their sizes or damaging the files. They accomplish this by overwriting unused areas of executable files. These are called cavity viruses. For example, the CIH virus, or Chernobyl Virus, infects Portable Executable files. Because those files have many empty gaps, the virus, which was 1 KB in length, did not add to the size of the file.[61] Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them (for example, Conficker). In the 2010s, as computers and operating systems grow larger and more complex, old hiding techniques need to be updated or replaced. Defending a computer against viruses may demand that a file system migrate towards detailed and explicit permission for every kind of file access.

THANK YOU FOR YOUR ATTENTION!