COMPUTER VIRUS

INTRODUCTION

Hex dump of the Blaster worm, showing a message left for Microsoft CEO Bill Gates by the worm's programmer

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Virus writers use social engineering and exploit detailed knowledge of security vulnerabilities to gain access to their hosts' computing resources. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit, desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore artificial life and evolutionary algorithms.

Computer viruses currently cause billions of dollars' worth of economic damage each year,[14] due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems. Even though no currently existing antivirus software is able to uncover all computer viruses (especially new ones), computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

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 (security defects) in a system or application software to spread and infect. Software development strategies that produce large numbers of bugs will generally also produce potential exploits.

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. If a user attempts to launch an infected program, the virus' code may be executed simultaneously.

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 an image and most likely is safe, yet when opened run the executable on the client machine.

Vulnerability of different operating systems to viruses

The vast majority of viruses target systems running Microsoft Windows. This is due to Microsoft's large market share of desktop users. The diversity of software systems on a network limits the destructive potential of viruses and malware. 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.

Only a few major viruses have hit Macs in the last years. The difference in virus vulnerability between Macs and Windows is a chief selling point, one that Apple uses in their Get a Mac advertising.

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 XP. In 1997, researchers created and released a virus for Linux—known as "Bliss". 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.

Infection targets and replication techniques

Computer viruses infect a variety of different subsystems on their hosts. 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).

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).

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 attachments in e-mails.

Boot sector viruses

Boot sector viruses specifically target the boot sector/Master Boot Record (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.).

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.

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.
Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them (for example, Conficker).

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.

Read request intercepts

While some antivirus software employ various techniques to counter stealth mechanisms, once the infection occurs any recourse to clean the system is unreliable. In Microsoft Windows operating systems, the NTFS file system is proprietary. Direct access to files without using the Windows OS is undocumented. This leaves antivirus software little alternative but to send a read request to Windows OS files that handle such requests. Some viruses trick antivirus software by intercepting its requests to the OS. A virus can hide itself by intercepting the request to read the infected file, handling the request itself, and return an uninfected version of the file to the antivirus software. The interception can occur by code injection of the actual operating system files that would handle the read request. Thus, an antivirus software attempting to detect the virus will either not be given permission to read the infected file, or, the read request will be served with the uninfected version of the same file.

The only reliable method to avoid stealth is to boot from a medium that is known to be clean. Security software can then be used to check the dormant operating system files. Most security software relies on virus signatures, or they employ heuristics.

Security software may also use a database of file hashes for Windows OS files, so the security software can identify altered files, and request Windows installation media to replace them with authentic versions. In older versions of Windows, file hashes of Windows OS files stored in Windows—to allow file integrity/authenticity to be checked—could be overwritten so that the System File Checker would report that altered system files are authentic, so using file hashes to scan for altered files would not always guarantee finding an infection.

Self-modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called *virus signatures*. Unfortunately, the term is misleading, in that viruses do not possess unique signatures in the way that human beings do. Such a virus signature is merely a sequence of bytes that an antivirus program looks for because it is known to be part of the virus. A better term would be "search strings". Different antivirus programs will employ different search strings, and indeed different search methods, when identifying viruses. If a virus scanner finds such a pattern in a file, it will perform other checks to make sure that it has found the virus, and not merely a coincidental sequence in an innocent file, before it notifies the user that the file is infected. The user can then delete, or (in some cases) "clean" or "heal" the infected file. Some viruses employ techniques that make detection by means of signatures difficult but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

Encrypted viruses

One method of evading signature detection is to use simple encryption to encipher the body of the virus, leaving only the encryption module and a cryptographic key in cleartext. In this case, the virus consists of a small decrypting module and an encrypted copy of the virus code. If the virus is encrypted with a different key for each infected file, the only part of the virus that remains constant is the decrypting module, which would (for example) be appended to the end. In this case, a virus scanner cannot directly detect the virus using signatures, but it can still detect the decrypting module, which still makes indirect detection of the virus possible. Since these would be symmetric keys, stored on the infected host, it is in fact entirely possible to decrypt the final virus, but this is probably not required, since self-modifying code is such a rarity that it may be reason for virus scanners to at least flag the file as suspicious.

An old, but compact, encryption involves XORing each byte in a virus with a constant, so that the exclusive-or operation had only to be repeated for decryption. It is suspicious for a code to modify itself, so the code to do the encryption/decryption may be part of the signature in many virus definitions.

Some viruses will employ a means of encryption inside an executable in which the virus is encrypted under certain events, such as the virus scanner being disabled for updates or the computer being rebooted. This is called Cryptovirology. At said times, the executable will decrypt the virus and execute its hidden runtimes infecting the computer and sometimes disabling the antivirus software.

Polymorphic code

Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which

remain identical between infections, making it very difficult to detect directly using signatures. Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called mutating engine or mutation engine) somewhere in its encrypted body. See polymorphic code for technical detail on how such engines operate.

Some viruses employ polymorphic code in a way that constrains the mutation rate of the virus significantly. For example, a virus can be programmed to mutate only slightly over time, or it can be programmed to refrain from mutating when it infects a file on a computer that already contains copies of the virus. The advantage of using such slow polymorphic code is that it makes it more difficult for antivirus professionals to obtain representative samples of the virus, because bait files that are infected in one run will typically contain identical or similar samples of the virus. This will make it more likely that the detection by the virus scanner will be unreliable, and that some instances of the virus may be able to avoid detection.

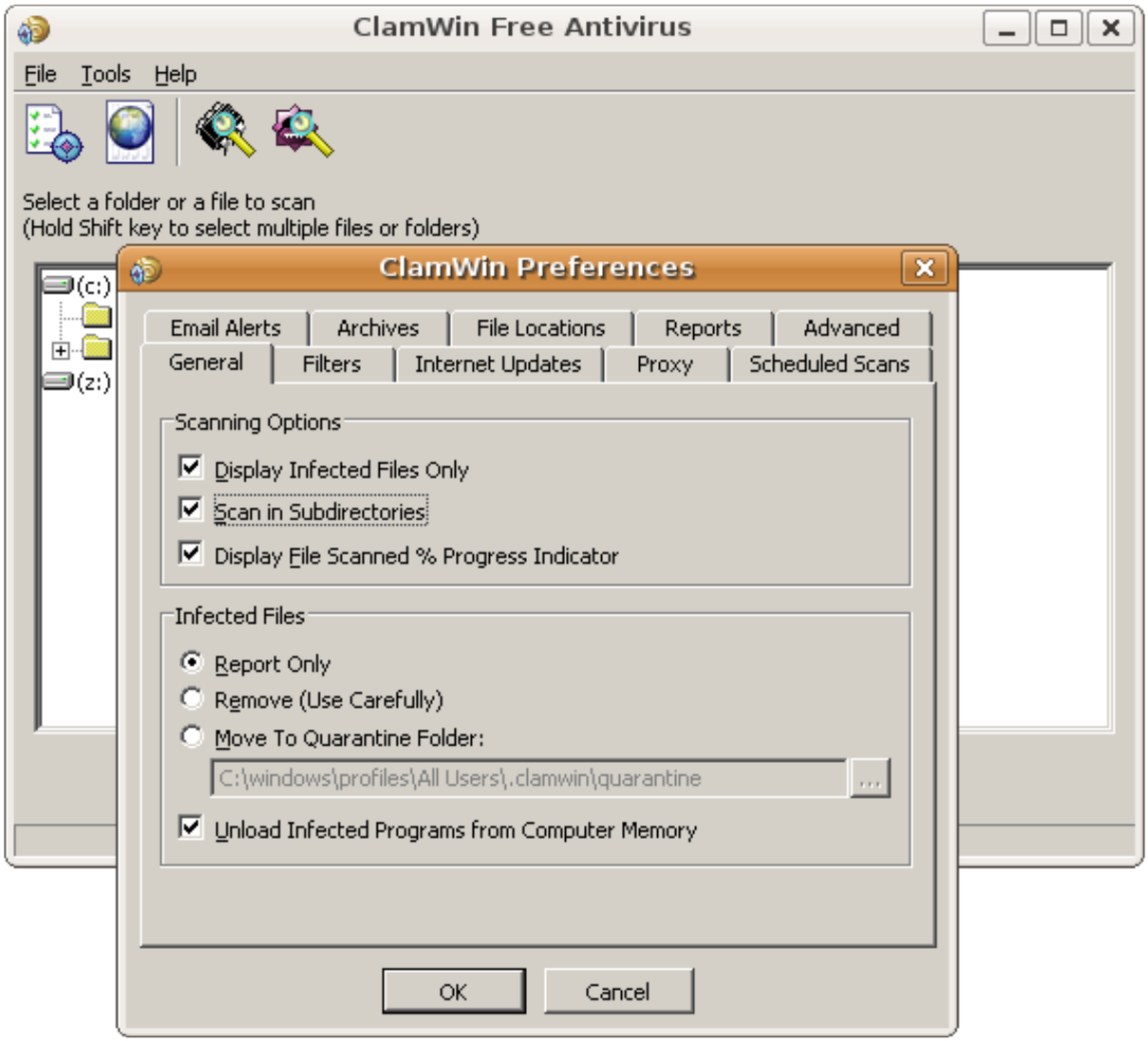
There has also been virus called undetectable virus (proposed in Yongge Wang). Undetectable virus is one kind of polymorphic virus that is static signature-free and whose dynamic signatures are hard to determine unless some cryptographic assumption fails.

Metamorphic code

To avoid being detected by emulation, some viruses rewrite themselves completely each time they are to infect new executables. Viruses that utilize this technique are said to be metamorphic. To enable metamorphism, a metamorphic engine is needed. A metamorphic virus is usually very large and complex. For example, W32/Simile consisted of over 14,000 lines of assembly language code, 90% of which is part of the metamorphic engine.

Countermeasures

Antivirus software



Screenshot of the open source ClamWin antivirus software running in Wine on Ubuntu Linux

Many users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable (which may be distributed as an email attachment, or on USB flash drives, for example). Some antivirus software blocks known malicious web sites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to patch security vulnerabilities ("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest threats. The German AV-TEST Institute publishes evaluations of antivirus software for Windows and Android.

Examples of Microsoft Windows anti virus and anti-malware software include the optional Microsoft Security Essentials (for Windows XP, Vista and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP). Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Some such free programs are almost as good as commercial competitors. Common security vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it. Ransomware and phishing scam alerts appear as press releases on the Internet Crime Complaint Center noticeboard.

Other commonly used preventative measures include timely operating system updates, software updates, careful Internet browsing, and installation of only trusted software. Certain browsers flag sites that have been reported to Google and that have been confirmed as hosting malware by Google.

There are two common methods that an antivirus software application uses to detect viruses, as described in the antivirus software article. The first, and by far the most common method of virus detection is using a list of virus signature definitions. This works by examining the content of the computer's memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a database of known virus "signatures". Virus signatures are just strings of code that are used to identify individual viruses; for each virus, the antivirus designer tries to choose a unique signature string that will not be found in a legitimate program. Different antivirus programs use different "signatures" to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that are detected by signatures in their most recent virus definition update, and not protected from new viruses (see "zero-day attack").

A second method to find viruses is to use a heuristic algorithm based on common virus behaviors. This method has the ability to detect new viruses for which antivirus security firms have yet to define a "signature", but it also gives rise to more false positives than using signatures. False positives can be disruptive, especially in a commercial environment.

Recovery strategies and methods

One may reduce the damage done by viruses by making regular backups of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which will hopefully be recent).

If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the CD/DVD). Likewise, an operating system on a bootable CD can be used to start the computer if the installed

operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable flash drives.

Virus removal

Many websites run by antivirus software companies provide free online virus scanning, with limited cleaning facilities (the purpose of the sites is to sell antivirus products). Some websites—like Google subsidiary VirusTotal.com—allow users to upload one or more suspicious files to be scanned and checked by one or more antivirus programs in one operation. Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Microsoft offers an optional free antivirus utility called Microsoft Security Essentials, a Windows Malicious Software Removal Tool that is updated as part of the regular Windows update regime, and an older optional anti-malware (malware removal) tool Windows Defender that has been upgraded to an antivirus product in Windows 8.

Some viruses disable System Restore and other important Windows tools such as Task Manager and CMD. An example of a virus that does this is CiaDoor. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking, and then using system tools or Microsoft Safety Scanner.[67] System Restore on Windows Me, Windows XP, Windows Vista and Windows 7 can restore the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files and does not exist in previous restore points.

Operating system reinstallation

Microsoft's System File Checker (improved in Windows 7 and later) can be used to check for, and repair, corrupted system files.

Restoring an earlier "clean" (virus-free) copy of the entire partition from a cloned disk, a disk image, or a backup copy is one solution—restoring an earlier backup disk image is relatively simple to do, usually removes any malware, and may be faster than disinfecting the computer—or reinstalling and reconfiguring the operating system and programs from scratch, as described below, then restoring user preferences.

Reinstalling the operating system is another approach to virus removal. It may be possible to recover copies of essential user data by booting from a live CD, or connecting the hard drive to another computer and booting from the second computer's operating system, taking great care not to infect that computer by executing any infected programs on the original drive. The original hard drive can then be reformatted and the OS and all programs installed from original media. Once the system has been restored, precautions must be taken to avoid reinfection from any restored executable files.

Historical development

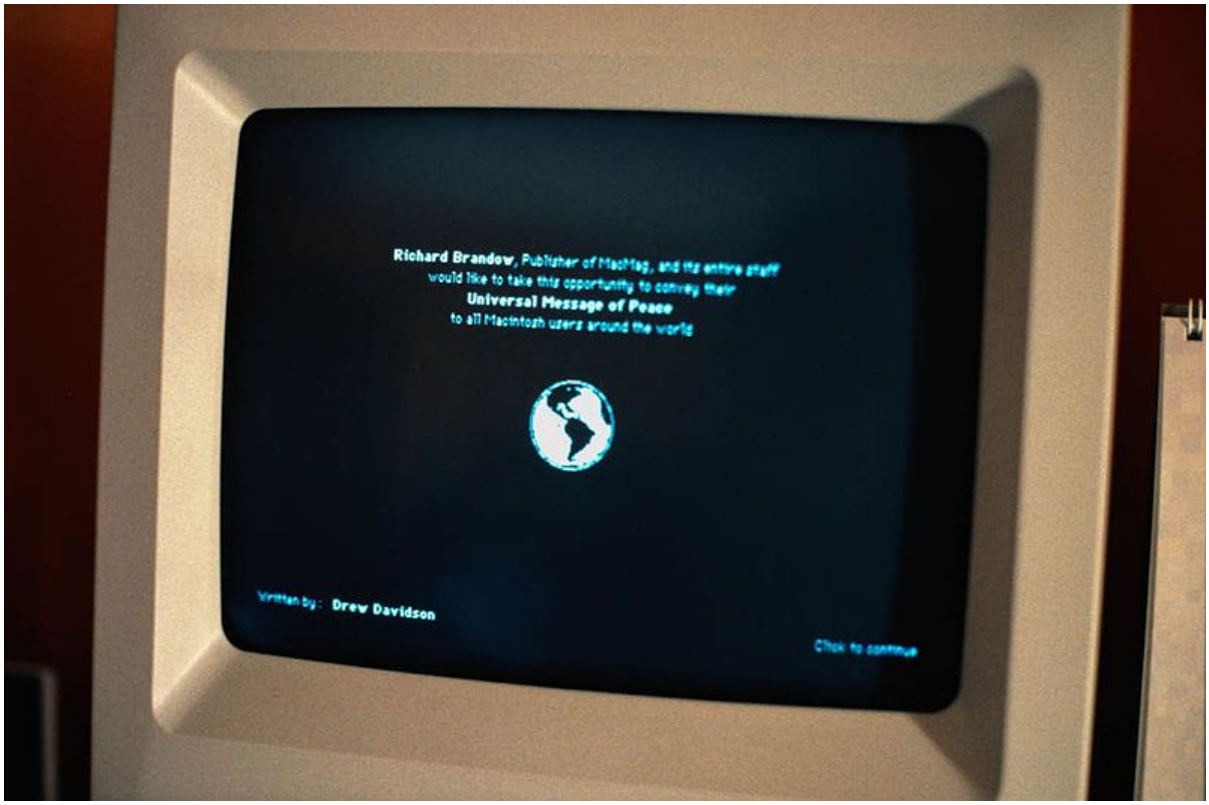
Early academic work on self-replicating programs

The first academic work on the theory of self-replicating computer programs 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. 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.

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). The article describes a fully functional virus written in assembler 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. In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.

The first computer viruses



The MacMag virus 'Universal Peace', as displayed on a Mac in March of 1988

The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s. Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971. Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system. 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.

In fiction, the 1973 Michael Crichton movie *Westworld* made an early mention of the concept of a computer virus, being a central plot theme that causes androids to run amok. 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 belief in a disease of machinery." (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 lab where it was created. Written in 1981 by Richard Skrenta, it attached itself to the Apple DOS 3.3 operating system and spread via floppy disk. 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". 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. Fred Cohen's theoretical compression virus was an example of a virus which was not malware, but was putatively benevolent. However, antivirus professionals do not accept the concept of benevolent viruses, as any desired function can be implemented without involving a virus (automatic compression, for instance, is available under the Windows operating system at the choice of the user). Any virus will by definition make unauthorised changes to a computer, which is undesirable even if no damage is done or intended. On page one of *Dr Solomon's Virus Encyclopaedia*, the undesirability of viruses, even those that do nothing but reproduce, is thoroughly explained.

An article that describes "useful virus functionalities" was published by J. B. Gunn under the title "Use of virus functions to provide a virtual APL interpreter under user control" in 1984.

The first IBM PC virus in the wild was a boot sector virus dubbed (c)Brain, created in 1986 by the Farooq Alvi Brothers in Lahore, Pakistan, reportedly to deter piracy of the software they had written.

The first virus to specifically target Microsoft Windows, WinVir was discovered in April 1992, two years after the release of Windows 3.0. The virus did not contain any Windows API calls, instead relying on DOS interrupts. A few years later, in February 1996, Australian hackers from the virus-writing crew Boza created the VLAD virus, which was the first known virus to target Windows 95. In late 1997 the encrypted, memory-resident stealth virus Win32.Cabanas was released—the first known virus that targeted Windows NT (it was also able to infect Windows 3.0 and Windows 9x hosts).

Even home computers were affected by viruses. The first one to appear on the Commodore Amiga was a boot sector virus called SCA virus, which was detected in November 1987.
The first social networking virus, Win32.5-0-1, Was created by Matt Larose on August 15, 2001. The virus specifically targeted users of MSN Messenger and bulletin boards. Users would be required to click on a link to activate the virus, which would then send an email containing user data to an anonymous email address, which was later found to be owned by Larose. Data sent would contain items such as user IP and email addresses, contacts, site history, and commonly used phrases. In 2008, larger websites used part of the Win32.5-0-1 code to track web users ad related interests.

Viruses and the Internet

Before computer networks became widespread, most viruses spread on removable media, particularly floppy disks. In the early days of the personal computer, many users regularly exchanged information and programs on floppies. Some viruses spread by infecting programs stored on these disks, while others installed themselves into the disk boot sector, ensuring that they would be run when the user booted the computer from the disk, usually inadvertently. Personal computers of the era would attempt to boot first from a floppy if one had been left in the drive. Until floppy disks fell out of use,

this was the most successful infection strategy and boot sector viruses were the most common in the wild for many years.

Traditional computer viruses emerged in the 1980s, driven by the spread of personal computers and the resultant increase in bulletin board system (BBS), modem use, and software sharing. Bulletin board–driven software sharing contributed directly to the spread of Trojan horse programs, and viruses were written to infect popularly traded software. Shareware and bootleg software were equally common vectors for viruses on BBSs. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.

Macro viruses have become common since the mid-1990s. Most of these viruses are written in the scripting languages for Microsoft programs such as Word and Excel and spread throughout Microsoft Office by infecting documents and spreadsheets. Since Word and Excel were also available for Mac OS, most could also spread to Macintosh computers. Although most of these viruses did not have the ability to send infected email messages, those viruses which did take advantage of the Microsoft Outlook COM interface.

Some old versions of Microsoft Word allow macros to replicate themselves with additional blank lines. If two macro viruses simultaneously infect a document, the combination of the two, if also self-replicating, can appear as a "mating" of the two and would likely be detected as a virus unique from the "parents".

A virus may also send a web address link as an instant message to all the contacts on an infected machine. If the recipient, thinking the link is from a friend (a trusted source) follows the link to the website, the virus hosted at the site may be able to infect this new computer and continue propagating.

Viruses that spread using cross-site scripting were first reported in 2002, and were academically demonstrated in 2005. There have been multiple instances of the cross-site scripting viruses in the wild, exploiting websites such as MySpace and Yahoo!.

Timeline of computer viruses and worms

This timeline of computer viruses and worms presents a chronology of noteworthy computer viruses, computer worms, Trojan horses, similar malware, related research and events.

1949

- John von Neumann's article on the "Theory of self-reproducing automata" is published.[1] The article is based on lectures given by von Neumann at the University of Illinois about the "Theory and Organization of Complicated Automata" in 1949.

1970–1979

1971

- The Creeper system, an experimental self-replicating program, is written by Bob Thomas at BBN Technologies to test John von Neumann's theory. Creeper infected DEC PDP-10 computers running the TENEX operating system. 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 later created to delete Creeper.

1974

- The Rabbit (or Wabbit) virus, more a fork bomb than a virus, is written. The Rabbit virus makes multiple copies of itself on a single computer (and was named "Rabbit" for the speed at which it did so) until it clogs the system, reducing system performance, before finally reaching a threshold and crashing the computer**.**

1975

- April: ANIMAL is written by John Walker for the UNIVAC 1108. ANIMAL asked a number of questions of the user in an attempt to guess the type of animal that the user was thinking of, while the related program PERVADE would create a copy of itself and ANIMAL in every directory to which the current user had access. It spread across the multi-user UNIVACs when users with overlapping permissions discovered the game, and to other computers when tapes were shared. The program was carefully written to avoid damage to existing file or directory structures, and not to copy itself if permissions did not exist or if damage could result. Its spread was therefore halted by an OS upgrade which changed the format of the file

status tables that PERVADE used for safe copying. Though non-malicious, "Pervading Animal" represents the first Trojan "in the wild".

1980–1989

1981

- A program called Elk Cloner, written for Apple II systems, was created by Richard Skrenta. The Apple II was seen as particularly vulnerable due to the storage of its operating system on floppy disk. Elk Cloner's design combined with public ignorance about what malware was and how to protect against it led to Elk Cloner being responsible for the first large-scale computer virus outbreak in history.

1983

- November: The term 'virus' is coined by Frederick Cohen in describing self-replicating computer programs. In 1984 Cohen uses the phrase "computer virus" – as suggested by his teacher Leonard Adleman – to describe the operation of such programs in terms of "infection". He defines a 'virus' as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." Cohen demonstrates a virus-like program on a VAX11/750 system at Lehigh University. The program could install itself in, or infect, other system objects.

1984

- August: Ken Thompson publishes his seminal paper, *Reflections on Trusting Trust*, in which he describes how he modified a C compiler so that when used to compile a specific version of the Unix operating system, it inserted a backdoor into the login command, and when used to compile itself, it inserted the backdoor insertion code, even if neither the backdoor nor the backdoor insertion code were present in the source code.

1986

- January: The Brain boot sector virus is released. Brain is considered the first IBM PC compatible virus, and the program responsible for the first IBM PC compatible virus epidemic. The virus is also known as Lahore, Pakistani, Pakistani Brain, and Pakistani flu as it was created in Lahore, Pakistan by 19-year-old Pakistani programmer, Basit Farooq Alvi, and his brother, Amjad Farooq Alvi.
- December: Ralf Burger presented the Virdem model of programs at a meeting of the underground Chaos Computer Club in Germany. The Virdem model represented the first programs that could replicate themselves via addition of their code to executable DOS files in COM format.

1987

- Appearance of the Vienna virus, which was subsequently neutralized—the first time this had happened on the IBM platform.
- Appearance of Lehigh virus (discovered at its namesake university), boot sector viruses such as Yale from USA, Stoned from New Zealand, Ping Pong from Italy, and appearance of first self-encrypting file virus, Cascade. Lehigh was stopped on campus before it spread to the wild, and has never been found elsewhere as a result. A subsequent infection of Cascade in the offices of IBM Belgium led to IBM responding with its own antivirus product development. Prior to this, antivirus solutions developed at IBM were intended for staff use only.
- October: The Jerusalem virus, part of the (at that time unknown) Suriv family, is detected in the city of Jerusalem. The virus destroys all executable files on infected machines upon every occurrence of Friday the 13th (except Friday 13 November 1987 making its first trigger date May 13, 1988). Jerusalem caused a worldwide epidemic in 1988.
- November: The SCA virus, a boot sector virus for Amigas appears, immediately creating a pandemic virus-writer storm. A short time later, SCA releases another, considerably more destructive virus, the Byte Bandit.
- December: Christmas Tree EXEC was the first widely disruptive replicating network program, which paralyzed several international computer networks in December 1987. It was written in Rexx on the VM/CMS operating system and originated in what was then West Germany. It re-emerged in 1990.

1988

- March 1: The Ping-Pong virus (also called Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A or VeraCruz), an MS-DOS boot sector virus, is discovered at University of Turin in Italy.
- June: The CyberAIDS and Festering Hate Apple ProDOS viruses spreads from underground pirate BBS systems and starts infecting mainstream networks. Festering Hate was the last iteration of the CyberAIDS series extending back to 1985 and 1986. Unlike the few Apple viruses that had come before which were essentially annoying, but did no damage, the Festering Hate series of viruses was extremely destructive, spreading to all system files it could find on the host computer (hard drive, floppy, and system memory) and then destroying everything when it could no longer find any uninfected files.
- November 2: The Morris worm, created by Robert Tappan Morris, infects DEC VAX and Sun machines running BSD UNIX that are connected to the Internet, and becomes the first worm to spread extensively "in the wild", and one of the first well-known programs exploiting buffer overrun vulnerabilities.

1989

- October: Ghostball, the first multipartite virus, is discovered by Friðrik Skúlason. It infects both executable .COM-files and boot sectors on MS-DOS systems. It captures certain information entered or saved by the user, with the corresponding threat to privacy, causes the loss of information stored on the computer, either specific files or data in general, affects the productivity of the computer, the network to which it's connected or other remote sites, decrease the security level of the computer, but does not automatically spread itself.
- December: Several thousand floppy disks containing the AIDS Trojan, the first known ransomware, are mailed to subscribers of PC Business World magazine and a WHO AIDS conference mailing list. This DOS Trojan lies dormant for 90 boot cycles, then encrypts all filenames on the system, displaying a notice asking for $189 to be sent to a post office box in Panama in order to receive a decryption program.

1990–1999

1990

- Mark Washburn, working on an analysis of the Vienna and Cascade viruses with Ralf Burger, develops the first family of polymorphic viruses, the Chameleon family. Chameleon series debuted with the release of 1260.
- June: The Form computer virus is isolated in Switzerland. It would remain in the wild for almost 20 years and reappear afterwards; during the 1990s it tended to be the most common virus in the wild with 20 to more than 50 per cent of reported infections.

1992

- March: The Michelangelo virus was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped, according to mass media hysteria surrounding the virus. Later assessments of the damage showed the aftermath to be minimal. John McAfee had been quoted by the media as saying that 5 million computers would be affected. He later said that, pressed by the interviewer to come up with a number, he had estimated a range from 5 thousand to 5 million, but the media naturally went with just the higher number.

1993

- "Leandro" or "Leandro & Kelly" and "Freddy Krueger" spread quickly due to popularity of BBS and shareware distribution.

1994

- April: OneHalf is a DOS-based polymorphic computer virus.

1995

- The first Macro virus, called "Concept", is created. It attacked Microsoft Word documents.

1996

- "Ply" — DOS 16-bit based complicated polymorphic virus appeared with built-in permutation engine.
- Boza, the first virus designed specifically for Windows 95 files arrives.
- Laroux, the first Excel macro virus appears.
- Staog, the first Linux virus attacks Linux machines

1998

- June 2: The first version of the CIH virus appears. It is the first known virus able to erase flash ROM BIOS content.

1999

- January 20: The Happy99 worm first appeared. It invisibly attaches itself to emails, displays fireworks to hide the changes being made, and wishes the user a happy New Year. It modifies system files related to Outlook Express and Internet Explorer (IE) on Windows 95 and Windows 98.
- March 26: The Melissa worm was released, targeting Microsoft Word and Outlook-based systems, and creating considerable network traffic.
- June 6: The ExploreZip worm, which destroys Microsoft Office documents, was first detected.
- December 30: The Kak worm is a Javascript computer worm that spread itself by exploiting a bug in Outlook Express.

2000-2009

2000

- May 5: The ILOVEYOU worm, also known as Love Letter, or VBS, or Love Bug worm, is a computer worm purportedly created by a Filipino computer science student. Written in VBScript, it infected millions of Windows computers worldwide within a few hours of its release. Using social engineering techniques, it is considered to be one of the most damaging worms ever.
- June 28: The Pikachu virus is believed to be the first computer virus geared at children. It contains the character "Pikachu" from the Pokémon series, and is in the form of an e-mail titled "Pikachu Pokemon" with the message: "Pikachu is your friend." The attachment to the email has "an image of a pensive Pikachu", along with a message stating, "Between millions of people around the world I found you. Don't forget to remember this day every time MY FRIEND." Along with the image, there is a program, written in Visual Basic 6, called "pikachupokemon.exe" that modifies the AUTOEXEC.BAT file and adds a command for removing the contents of directories C:\Windows and C:\Windows\System at computer's restart. But, a message would pop up during startup, asking the user if they would like to delete the contents. The affected operating systems are Windows 95, Windows 98 and Windows Me.

2001

- February 11: The Anna Kournikova virus hits e-mail servers hard by sending e-mail to contacts in the Microsoft Outlook addressbook. Its creator, Dutchman Jan de Wit, was sentenced to 150 hours of community service.
- May 8: The Sadmind worm spreads by exploiting holes in both Sun Solaris and Microsoft IIS.
- July: The Sircam worm is released, spreading through Microsoft systems via e-mail and unprotected network shares.
- July 13: The Code Red worm attacking the Index Server ISAPI Extension in Microsoft Internet Information Services is released.
- August 4: A complete re-write of the Code Red worm, Code Red II begins aggressively spreading onto Microsoft systems, primarily in China.
- September 18: The Nimda worm is discovered and spreads through a variety of means including vulnerabilities in Microsoft Windows and backdoors left by Code Red II and Sadmind worm.
- October 26: The Klez worm is first identified. It exploits a vulnerability in Microsoft Internet Explorer and Microsoft Outlook and Outlook Express.

2002

- February 11: The Simile virus is a metamorphic computer virus written in assembly.
- Beast is a Windows-based backdoor Trojan horse, more commonly known as a RAT (Remote Administration Tool). It is capable of infecting almost all versions of Windows. Written in Delphi and released first by its author Tataye in 2002, its most current version was released October 3, 2004
- March 7: Mylife is a computer worm that spread itself by sending malicious emails to all the contacts in Microsoft Outlook.
- August 30: Optix Pro is a configurable remote access tool or trojan, similar to SubSeven or BO2K.

2003

- January 24: The SQL Slammer worm, aka *Sapphire worm*, *Helkern* and other names, attacks vulnerabilities in Microsoft SQL Server and MSDE becomes the fastest spreading worm of all time (measured by doubling time at the peak rate of growth), crashing the Internet within 15 minutes of release.
- April 2: Graybird is a trojan horse also known as Backdoor.Graybird.
- June 13: ProRat is a Turkish-made Microsoft Windows based backdoor trojan horse, more commonly known as a RAT (Remote Administration Tool).
- August 12: The Blaster worm, aka the *Lovesan* worm, rapidly spreads by exploiting a vulnerability in system services present on Windows computers.
- August 18: The Welchia (Nachi) worm is discovered. The worm tries to remove the blaster worm and patch Windows.
- August 19: The Sobig worm (technically the Sobig.F worm) spreads rapidly through Microsoft systems via mail and network shares.
- September 18: Swen is a computer worm written in C++.
- October 24: The Sober worm is first seen on Microsoft systems and maintains its presence until 2005 with many new variants. The simultaneous attacks on network weakpoints by the Blaster and Sobig worms cause massive damage.
- November 10: Agobot is a computer worm that can spread itself by exploiting vulnerabilities on Microsoft Windows. Some of the vulnerabilities are MS03-026 and MS05-039.
- November 20: Bolgimo is a computer worm that spread itself by exploiting a buffer overflow vulnerability at Microsoft Windows DCOM RPC Interface.

2004

- January 18: Bagle is a mass-mailing worm affecting all versions of Microsoft Windows. There were 2 variants of Bagle worm, Bagle.A and Bagle.B. Bagle.B was discovered on February 17, 2004.
- January 23: The L10n worm (usually pronounced "lion") was a Linux worm that spread by exploiting a buffer overflow in the BIND DNS server. It was based on an earlier worm known as the Ramen worm (commonly, albeit incorrectly referred to as the Ramen Virus) which was written to target systems running versions 6.2 and 7.0 of the Red Hat Linux distribution.
- Late January: The MyDoom worm emerges, and currently holds the record for the fastest-spreading mass mailer worm.
- February 16: The Netsky worm is discovered. The worm spreads by email and by copying itself to folders on the local hard drive as well as on mapped network drives if available. Many variants of the Netsky worm appeared.
- March 19: The Witty worm is a record-breaking worm in many regards. It exploited holes in several Internet Security Systems (ISS) products. It was the fastest disclosure to worm, it was the first internet worm to carry a destructive payload and it spread rapidly using a pre-populated list of ground-zero hosts.
- May 1: The Sasser worm emerges by exploiting a vulnerability in the Microsoft Windows LSASS service and causes problems in networks, while removing MyDoom and Bagle variants, even interrupting business.
- June 15: Caribe or Cabir is a computer worm that is designed to infect mobile phones that run Symbian OS. It is the first computer worm that can infect mobile phones. It spread itself through Bluetooth. More information can be found on F-Secure and Symantec.
- August 16: Nuclear RAT (short for Nuclear Remote Administration Tool) is a backdoor trojan that infects Windows NT family systems (Windows 2000, Windows XP, Windows 2003).
- August 20: Vundo, or the Vundo Trojan (also known as Virtumonde or Virtumondo and sometimes referred to as MS Juan) is a trojan known to cause popups and advertising for rogue antispyware programs, and sporadically other misbehaviour including performance degradation and denial of service with some websites including Google and Facebook.
- October 12: Bifrost, also known as Bifrose, is a backdoor trojan which can infect Windows 95 through Vista. Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attack.
- December: Santy, the first known "webworm" is launched. It exploited a vulnerability in phpBB and used Google in order to find new targets. It infected around 40000 sites before Google filtered the search query used by the worm, preventing it from spreading.

2005

- August 2005: Zotob
- October 2005: The copy protection rootkit deliberately and surreptitiously included on music CDs sold by Sony BMG is exposed. The rootkit creates vulnerabilities on affected computers, making them susceptible to infection by worms and viruses.
- Late 2005: The Zlob Trojan, is a Trojan horse program that masquerades as a required video codec in the form of the Microsoft Windows ActiveX component. It was first detected in late 2005.
- Bandook or Bandook Rat (Bandook Remote Administration Tool) is a backdoor Trojan horse that infects the Windows family. It uses a server creator, a client and a server to take control over the remote computer. It uses process hijacking / kernel patching to bypass the firewall, and let the server component hijack processes and gain rights for accessing the Internet.

2006

- January 20: The Nyxem worm was discovered. It spread by mass-mailing. Its payload, which activates on the third of every month, starting on February 3, attempts to disable security-related and file sharing software, and destroy files of certain types, such as Microsoft Office files.
- February 16: discovery of the first-ever malware for Mac OS X, a low-threat trojan-horse known as OSX/Leap-A or OSX/Oompa-A, is announced.
- Late March: Brontok variant N was found in late March. Brontok was a mass-email worm and the origin for the worm was from Indonesia.
- Late September: Stration or Warezov worm first discovered.

2007

- January 17: Storm Worm identified as a fast spreading email spamming threat to Microsoft systems. It begins gathering infected computers into the Storm botnet. By around June 30 it had infected 1.7 million computers, and it had compromised between 1 and 10 million computers by September. Thought to have originated from Russia, it disguises itself as a news email containing a film about bogus news stories asking you to download the attachment which it claims is a film.
- July: Zeus is a trojan that targets Microsoft Windows to steal banking information by keystroke logging.

2008

- February 17: Mocmex is a trojan, which was found in a digital photo frame in February 2008. It was the first serious computer virus on a digital photo frame. The virus was traced back to a group in China.
- March 3: Torpig, also known as Sinowal and Mebroot, is a Trojan horse that affects Windows, turning off anti-virus applications. It allows others to access the computer, modifies data, steals confidential information (such as user passwords and other sensitive data) and installs more malware on the victim's computer.
- May 6: Rustock.C, a hitherto-rumoured spambot-type malware with advanced rootkit capabilities, was announced to have been detected on Microsoft systems and analyzed, having been in the wild and undetected since October 2007 at the very least.
- July 6: Bohmini.A is a configurable remote access tool or trojan that exploits security flaws in Adobe Flash 9.0.115 with Internet Explorer 7.0 and Firefox 2.0 under Windows XP SP2.
- July 31: The Koobface computer worm targets users of Facebook and Myspace. New variants constantly appear.
- November 21: Computer worm Conficker infects anywhere from 9 to 15 million Microsoft server systems running everything from Windows 2000 to the Windows 7 Beta. The French Navy, UK Ministry of Defence (including Royal Navy warships and submarines), Sheffield Hospital network, German Bundeswehr and Norwegian Police were all affected. Microsoft sets a bounty of US$250,000 for information leading to the capture of the worm's author(s). Five main variants of the Conficker worm are known and have been dubbed Conficker A, B, C, D and E. They were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively. On December 16, 2008, Microsoft releases KB958644 patching the server service vulnerability responsible for the spread of Conficker.

2009

- July 4: The July 2009 cyber attacks occur and the emergence of the W32.Dozer attack the United States and South Korea.
- July 15: Symantec discovered Daprosy Worm. Said trojan worm is intended to steal online-game passwords in internet cafes. It could, in fact, intercept all keystrokes and send them to its author which makes it potentially a very dangerous worm to infect B2B (business-to-business) systems.

2010 and later

2010

- January: The Waledac botnet sent spam emails. In February 2010, an international group of security researchers and Microsoft took Waledac down.
- February 18: Microsoft announced that a BSoD problem on some Windows machines which was triggered by a batch of Patch Tuesday updates was caused by the Alureon Trojan.
- June 17: Stuxnet, a Windows Trojan, was detected. It is the first worm to attack SCADA systems. There are suggestions that it was designed to target Iranian nuclear facilities. It uses a valid certificate from Realtek.
- September 9: The virus, called "here you have" or "VBMania", is a simple Trojan horse that arrives in the inbox with the odd-but-suggestive subject line "here you have". The body reads "This is The Document I told you about, you can find it Here" or "This is The Free Download Sex Movies, you can find it Here".
- September 15: The virus called Kenzero is a virus that spreads online from Peer to peer (P2P) sites taking browsing history.

2011

- SpyEye and Zeus merged code is seen. New variants attack mobile phone banking information.
- Anti-Spyware 2011, a Trojan horse that attacks Windows 9x, 2000, XP, Vista, and Windows 7, posing as an anti-spyware program. It actually disables security-related process of anti-virus programs, while also blocking access to the Internet, which prevents updates.
- Summer 2011: The Morto worm attempts to propagate itself to additional computers via the Microsoft Windows Remote Desktop Protocol (RDP). Morto spreads by forcing infected systems to scan for Windows servers allowing RDP login. Once Morto finds an RDP-accessible system, it attempts to log into a domain or local system account named 'Administrator' using a number of common passwords. A detailed overview of how the worm works—along with the password dictionary Morto uses—was done by Imperva.
- July 13: the ZeroAccess rootkit (also known as Sirefef or max++) was discovered.
- September 1: Duqu is a worm thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu. Duqu gets its name from the prefix "~DQ" it gives to the names of files it creates.

2012

- May: Flame - also known as Flamer, sKyWIper, and Skywiper - a modular computer malware that attacks computers running Microsoft Windows. Used for targeted cyber espionage in Middle Eastern countries. Its discovery was announced on 28 May 2012 by MAHER Center of Iranian National Computer Emergency Response Team (CERT), Kaspersky Lab and

CrySyS Lab of the Budapest University of Technology and Economics. CrySyS stated in their report that "sKyWIper is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found".

- August 16: Shamoon is a computer virus designed to target computers running Microsoft Windows in the energy sector. Symantec, Kaspersky Lab, and Seculert announced its discovery on August 16, 2012.
- September 20: NGRBot is a worm that uses the IRC network for file transfer, sending and receiving commands between zombie network machines and the attacker's IRC server, and monitoring and controlling network connectivity and intercept. It employs a user-mode rootkit technique to hide and steal its victim's information. This family of bot is also designed to infect HTML pages with inline frames ([HTML element#Frames|[iframes]]), causing redirections, blocking victims from getting updates from security/antimalware products, and killing those services. The bot is designed to connect via a predefined IRC channel and communicate with a remote botnet.

2013

- September: The CryptoLocker Trojan horse is discovered. Cryptolocker encrypts the files on a user's hard drive, then prompts them to pay a ransom to the developer in order to receive the decryption key. In the following months, a number of copycat ransomware Trojans are also discovered.
- December: The Gameover ZeuS Trojan is discovered. This type of virus steals one's login details on popular Web sites that involve monetary transactions. It works by detecting a login page, then proceeds to inject a malicious code into the page, keystroke logging the computer user's details.

2014

- November: The Regin Trojan horse is discovered. Regin is a dropper that is primarily spread via spoofed Web pages. Once downloaded, Regin quietly downloads extensions of itself, making it difficult to be detected via anti-virus signatures. It is suspected to have been created by the United States and United Kingdom over a period of months or years, as a tool for espionage and mass surveillance.

Virus

1260

1260, or V2PX, was a demonstration computer virus written in 1989 by Mark Washburn that used a form of polymorphic encryption. Derived from Ralph Burger's publication of the disassembled Vienna virus source code, the 1260 added a cipher and varied its signature by randomizing its

decryption algorithm. Both the 1260 and Vienna infect .COM files in the current or PATH directories upon execution. Changing an authenticated executable file is detected by most modern computer operating systems.

4K

4k is a computer virus which infects COM files and EXE files. The virus was one of the first to employ stealth tactics. Infected systems will hang, after September 22 every year, which is also the date of birth Bilbo Baggins, a character from *The Lord of the Rings*. The code was intended to display the message *Frodo Lives*, but hangs in all known variants.

This virus was spread without the aid of the Internet. It was ported between systems by floppy disks.

History

It first appeared in October 1989. The first U.S. specimen was contracted in Dallas, TX, and quarantined with verification given by antivirus professionals. Reporters and TV crews recorded this in the local area news in August 1990. Its trail led from Dallas back to New York via a professional at a software firm creating software for lawyers. Virus firms had been tracking it previously in London a month or two before getting calls from New York. No specimens were quarantined or properly recorded in New York.

Raymond Glath of Phoenix, AZ, was the developer and owner of the Vi-Spy product which continued production until mid-release of Windows 95. Reports to McAfee antivirus and Vi-Spy antivirus firms resulted in only one product properly detecting the virus, Vi-Spy.

Operation

The virus added itself to the system in a way which defied normal infection processes. Because of this, it was able to infect a system without using system subroutines, which is what most antivirus products were watching. This is why the virus received the additional name 'stealth'. The infection process used a mathematical algorithm to determine the letters E-X-E & C-O-M. When a file was opened by the OS, the virus checked the extension of the file, and sometimes, other extension letters would be identified as a program file causing the virus to infect a data file and obviously corrupting its contents.

Because the virus appended itself to a file, while hiding the increase in file length, the system could cross-link files and diagnostics on the disks would report allocation errors. This would damage programs and data alike. The description of the problems found while trying correct the 'stupid-looking errors' would cause most computer professionals to erase the system and start over. A few days later the problems would arise again. Diagnostic disks and writable installation disks used to fix the computer would commonly be infected with the virus and this would aid in the spread.

5lo

5lo is a computer virus that increases file size and does little more than replicate. Size: 1,032 bytes.

Infection

5lo infects resident .EXE files only. When it infects a file, it increases the file size by about 1000-1100 bytes (though a typical value is 1032 bytes.) At the file's direct end, this message can be found (resulting in the virus's name):

92.05.24.5lo.2.23MZ

Other strings can be found in the virus's code:

????????.EXE and *.EXE

5lo stays resident. Whenever a .EXE file is run, 5lo will infect it (and another .EXE file). The virus also changes the file's timestamp to the date and time of infection. After these infections, a counter within the virus starts. However, this counter is never checked, so the virus doesn't activate. 5lo appends its code into infected files. It also changes the field 0Ch in the .EXE file's header to FFAAh. The virus identifies itself from memory by using the interrupt INT 21, AX=3521h which it has hooked. All the checks work correctly and the virus won't infect files multiple times and it installs itself to memory only once.

When 5lo is running in memory, it isn't discoverable by typing in MEM /C. This is because when the virus installs, it ties itself to the operating system. Free memory decreases by about 2 KB.

A and A

A & A is a computer virus which infects COM files. It changes an infected program's time and date stamp to the date and time of infection. When activated, the virus clears and reprints blocks of the screen. The infection code contains the string {A&A}

Abraxas

Abraxas, also known as Abraxas5, discovered in April 1993, is an encrypted, overwriting, file infecting computer virus which infects .COM and .EXE files, although it does not infect command.com. It does not become memory resident. Each time an infected file is executed, Abraxas infects the copy of dosshell.com located in the C:\DOS directory (creating the file if it does not exist), as well as one EXE file in the current directory. Due to a bug in the virus, only the first EXE file in any directory is infected.

Abraxas-infected files will become 1,171 bytes in length and contain Abraxas' viral code. The file's date and time in the DOS disk directory listing will be set to the system date and time when infection occurred. The following text strings can be found within the viral code in all Abraxas infected programs:

"*.exe c:\dos\dosshell.com .. MS-DOS (c)1992"

"->>ABRAXAS-5<<--"

"...For he is not of this day"

"...Nor he of this mind"

Execution of infected programs will also result in the display of a graphic "ABRAXAS" on the system display, accompanied by an ascending scale being played on the system speaker.

Abraxas was created with the PS-MPC virus creation tool, which can be used to create similar, easily detected viruses, which are usually encrypted as well.

Acid

Acid is a computer virus which infects .COM and .EXE files including command.com. Each time an infected file is executed, Acid infects all of the .EXE files in the current directory. Later, if an infected file is executed, it infects the .COM files in the current directory. Programs infected with Acid will have had the first 792 bytes of the host program overwritten with Acid's own code. There will be no file length increase unless the original host program was smaller than 792 bytes, in which case it will become 792 bytes in length. The program's date and time in the DOS disk directory listing will not be altered.

The following text strings are found in infected files:

- "*.EXE *.COM .."
- "Program too big to fit in memory"
- "Acid Virus"
- "Legalize ACiD and Pot"
- "By: Copyfright Corp-$MZU"

Acme

Acme is a computer virus which infects EXE files. Each time an infected file is executed, Acme may infect an EXE in the current directory by creating a hidden 247 byte long read-only COM file with the same base name. (In DOS, if the file extension is not specified, and two files with the same base name exist, one with .COM and one with .EXE, the .COM file will always be executed first.) Acme is a variant of Clonewar, a spawning virus. Acme is also perhaps a descendant of the small single-step infector Zeno, which is not to be confused with the Zeno programming language.

ABC

ABC, discovered in October 1992, is a memory-resident, file-infecting computer virus which infects EXE files and may alter both COM and EXE files. ABC activates on the 13th day of every month.

Upon infection, ABC becomes memory-resident at the top of system memory but below the 640K DOS boundary and hooks interrupts 16 and 1C. The copy of command.com pointed to by the COMSPEC environment variable may also be altered. ABC infects/alters COM and EXE files as they are executed.

After infection, total system memory, as measured by the DOS CHKDSK program, will not be altered, but available free memory will have decreased by approximately 8,960 bytes. Altered, but not infected, COM or EXE files will have 4 to 30 bytes added to their length. Infected EXE files (COM files are never infected) have a file length increase of 2,952 to 2,972 bytes, and ABC is located at the end of the infected EXE. An altered/infected file's date and time in the DOS disk directory listing may have been updated to the current system date and time when the file was altered/infected.

No text strings are visible within the viral code in infected EXE files, but the following text strings are encrypted within the initial copy of the ABC virus:

ABC_FFEA

Minsk 8.01.92

ABC

ABC causes keystrokes on the compromised machine to be repeated. It seems double-letter combinations trigger this behavior, e.g. "book" becomes "boook [*sic*]". System hangs may also occur when some programs are executed, a likely side effect of ABC-induced corruption.

The ABC virus is not to be confused with the ABC keylogger trojan, written in 2004 by Jan ten Hove.

Actifed

Actifed is a G2-generated encrypted computer virus which infects .COM and .EXE files but *not* command.com. The virus is loaded into memory by executing an infected program and then affects the computer's run-time operation and corrupts program files.

It is interesting that G2 is a computer virus creation tool written by Dark Angel of the Phalcon/Skism organization. This organization also wrote the "Phalcon-Skism Mass Produced Code Generator" [PS-MPC] which was used in the creation of Abraxas and numerous other viruses.

G2 generates compact, easily modified, fully commented, source code of .COM and .EXE infectors. It also supports the creation of resident and non-resident encrypted and non-encrypted viruses. The PS-MPC has similar use.

Ada

Ada is a computer virus that can affect any of the DOS operating systems.[1] Ada was first discovered in 1991.

History

Ada virus was first discovered in Argentina in October, 1991.

Virus Characteristics

Ada is a memory resident (stays in the memory of the computer it infects after the program it infect executes) virus that infects files. The Ada virus mainly targets .COM files, specifically COMMAND.COM.

Infected programs will have 2,600 bytes additional data inserted at the beginning of the file, and the file itself will contain the text strings:

- COMMAND.COM
- PCCILLIN.COM
- PCCILLIN.IMG
- HATI-HATI !! ADA VIRUS DISINI !!Delete

Computers infected with the Ada virus will often have a slow clicking sound emitting from their speakers; this clicking may sometimes change in pitch. Computers infected also may show a "Disk Full" error even if the disk still has space on it.

While infected with the Ada virus, system memory measured by the DOS CHKDSK decreases by 21,296 bytes to 21,312 bytes. The virus will reside in the memory after an infected file is run and will infect any other .COM files executed on the computer. It will also hijack interrupts 08, 13 and 21.

Infection Route

There is only one way to infect a computer with the Ada virus; by executing an infected file. The infected file may come from a variety of sources: floppy disks, files downloaded from the Internet, and infected networks.

Agena

Agena is a computer virus first discovered in Spain in September 1992. It is a memory resident, file infecting computer virus which infects .COM and .EXE files, including command.com. Agena becomes memory resident at the top of system memory but below the 640K DOS boundary. Once it is memory resident, Agena infects .COM and .EXE files as they are executed. Infected programs will have a file length increase of 723 to 738 bytes with the virus being located at the end of the file. An infected file's date and time in the DOS disk directory listing are not altered. Total system and available free memory, as indicated by the DOS CHKDSK program, will have decreased by 1,296 bytes. Interrupts 20 and 21 are hooked by the virus. It is unknown what Agena may do besides replicate. No text strings are visible within the viral code in infected programs.

AGI-Plan

AGI-Plan was a memory resident DOS file infector first isolated at the Agiplan software company in Germany. Because of CARO standards that dictate that viruses should not be named after companies, AGI-Plan's technical name is Month 4-6. This name also violates CARO standards, but a more minor

rule involving syntax. AGI-Plan is related to the Zero Bug virus, as both it and AGI-Plan prepend 1,536 bytes to files they infect.

AGI-Plan is not initially damaging until several months after the initial infection, hence its name. After activation, AGI-Plan will begin to corrupt write operations, which results in slow, difficult-to-notice damage overtime.

AGI-Plan is notable for reappearing in South Africa in what appeared to be an intentional re-release several years after. AGI-Plan never succeeded in spreading significantly beyond the isolated incidents in Germany and South Africa.

AI

AI is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's run time operation and corrupts program or overlay files. It does not appear to work with all .EXE files but does infect standard DOS files easily. AI adds meaningless garbage bytes to the end of the host file.

AIDS

AIDS is a computer virus written in Turbo Pascal 3.01a which overwrites ComFiles. AIDS is the first virus known to exploit the MS-DOS "corresponding file" vulnerability. In MS-DOS, if both foo.com and foo.exe exist, then foo.com will always be executed first. Thus, by creating infected com files, AIDS code will always be executed before the intended exe code.

When the AIDS virus activates, it displays the following screen.

ATTENTION I have been elected to inform you that throughout your process of collecting and executing files, you have accdientally [(sic)] ¶HÜ¢KΣ► [PHUCKED] yourself over: again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a √ìτûs [virus] has infected your system. Now what do you have to say about that? HAHAHAHAHA. Have ¶HÜÑ [PHUN] with this one and remember, there is NO cure for AIDS

In the message above, the word "AIDS" covers about half of the screen. The system is then halted, and must be powered down and rebooted to restart it.

The AIDS virus overwrites the first 13,952 bytes of an infected com file. Overwritten files must be deleted and replaced with clean copies in order to remove the virus. It is not possible to recover the overwritten portion of the program.

The AIDS II virus appears a more elegant revision of AIDS. AIDS II also employs the corresponding file technique to execute infected code.

AIDS II

AIDS II is a companion computer virus, which infects COM files. It was first discovered in April 1990, and is a variant of AIDS. Unlike other generic file infectors, AIDS II was the second known virus to employ what could be called a "corresponding file technique" of infection so that the original target EXE file is never changed.(The original AIDS was the first.) The virus takes advantage of the DOS feature where if a file exists in both COM and EXE form, the COM file is executed. When an "infected" file is executed, since a corresponding COM file exists, the COM file containing the viral code is executed. The virus first locates an uninfected EXE file in the current directory and creates a corresponding (or companion) COM file with the viral code. These COM files will always be 8,064 bytes in length with a file date/time of the date/time of infection. After creating the new COM file, the virus then plays a loud chiptune note, and displays the following message:

"Your computer is infected with ...

❤Aids Virus II❤

- Signed WOP & PGT of DutchCrack -"

AIDS II then spawns to the EXE file that was attempting to be executed in the first place, and the program runs without problem. After completion of the program, control returns to the virus. The loud note is played again with the following message displayed

"Getting used to me?

Next time, use a Condom ....."

Since the original EXE file remains unaltered, CRC programs cannot detect this virus having infected a system. One way to manually remove AIDS II is to check the disk for programs which have both a .EXE and .COM file, with the COM file having a length of 8,064 bytes. The COM files thus identified should be erased.

According to Symantec, AIDS II may play a melody and display the following string

"Your computer is infected with AIDS VIRUS II"

The displayed text strings do not appear in the viral code.

The AIDS II virus is not to be confused with the AIDS trojan. It also should not be mistaken for the original AIDS computer virus, for which AIDS II is a companion/successor.

Alabama

Alabama is a computer virus, discovered October 1989 on the campus of Hebrew University in Jerusalem.

Infection

Alabama is a fairly standard file infector outside its odd behaviour of deciding what files to infect. When an infected file is executed, Alabama goes memory resident. Whenever a .EXE file is executed from this point on, Alabama will search out for another file to infect. This is probably intended to place blame on the file that is being executed instead of the virus itself. Files infected by Alabama increase in size by 1,560 bytes.

Symptoms

A number of symptoms are associated with Alabama:

- EXE files will increase by 1,560 bytes in size upon infection.
- On Fridays, Alabama will begin to modify the File Allocation Table. As a result, when a file is executed, another may appear in its place. This is potentially dangerous. For more information, see the payload section.
- One hour after an infected program is run, Alabama will bring up a flashing box with the text "SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW.....Box 1055 Tuscambia ALABAMA USA."

The third symptom is by far the clearest indication of an Alabama infection. It is unknown what the PO Box address in the virus refers to. However, the implication of the message is that Alabama was released in an attempt to curb software piracy. Similar motivations led to the creation of the first known PC virus, Brain. This message also suggests that the PO Box may very well not belong to the author: the author clearly meant Tuscumbia, Alabama, as Tuscambia is not a city. This supports the theory that the virus originated in Israel.

Payload

On Fridays, Alabama will begin to modify the File Allocation Table in an odd way. Instead of searching for a file to infect, Alabama searches for a file to cross-reference. The virus modifies the FAT entry so that when the user executes one file, another will appear. For instance, on a machine where Alabama is resident, executing PROGRAM1.EXE on a Friday may cause the virus to search for another program and find PROGRAM2.EXE. Alabama will then modify the FAT so that whenever PROGRAM1.EXE is executed, PROGRAM2.EXE displays instead. This certainly can result in confusion, and may result in programs being lost or incorrectly deleted.

Prevalence

The WildList, an organisation tracking computer viruses, never reported Alabama as being in the field. It was isolated spreading in Israel, but this may have been a limited local outbreak.

Since the advent of Windows, even successful DOS viruses have become increasingly rare. As such, Alabama can be considered obsolete.

Variants

There is one known variant of Alabama. Alabama.B was distributed as a modified SDIR.COM. SDIR.COM was a program created to replace the DOS DIR command. Like the original Alabama, the "B" variant does not infect .COM files. The modified SDIR.COM is simply used as a dropper.

Alcon

Alcon, or RSY (which is more or less as commonly used of a name as Alcon), is a computer virus that was discovered to be spreading in Europe in 1997. It is a boot virus.

Infection

Alcon is a standard boot sector virus that spreads via floppies. Instead of the MBR, it infects the DBR, making some antivirus programs miss it.

Symptoms

Alcon contains no notable symptoms beyond one extremely damaging one, which is overwriting random information. Assuming that the overwrites are subtle, this may result in significant compounding data overtime, as Alcon is a slow damager.

Alcon contains the text "R.SY".

Prevalence

Alcon was listed as being spreading by the WildList from April 1998 to July 1999. F-Secure lists it as having been common in Europe throughout 1997. Like most boot viruses, it is near extinct, although it was certainly in the last wave of boot viruses, so cases involving Alcon may be false positives, but may also be due to older, unused infected disks resurfacing.

Aliases and variants

Alcon's most common alias is RSY, based on inclusions in the virus code. Other aliases include Kendesm, Ken&Desmond, and Ether. It is unknown where these names are derived from.

This virus is unrelated to W32/Alcon.

Ambulance

Ambulance or Ambulance Car is a computer virus that infected computers running a DOS operating system in June 1990. It was discovered in Germany.

Description

Ambulance does not become memory resident. It infects only one .COM file in any given directory, but not the first one. Thus, there must be at least two .COM files in a directory for it to spread.

When an infected file is executed, an ASCII art ambulance can be seen moving across the screen, a siren starts to sound, and it displays an alert message such as: BOOM! It is not a deliberately destructive virus; it simply spreads itself around and shows off its payload once in a while.

Variants

- Ambulance Car-B
- RedX-Any
- Ambulance.793
- Ambulance.793.A

- Ambulance.795
- Ambulance.796A

These are just some of many variants detected.

Anna Kournikova

The Anna Kournikova computer worm was a computer worm written by a Dutch programmer named Jan de Wit on February 11, 2001. It was designed to trick email users into opening a mail message purportedly containing a picture of the tennis player Anna Kournikova, while actually hiding a malicious program. If set off, the program plunders the address book of the Microsoft Outlook e-mail program and attempts to send itself to all the people listed there. The Kournikova worm tempts users with the message: "Hi: Check This!", with what appears to be a picture file labelled "AnnaKournikova.jpg.vbs". The worm arrives in an email with the subject line "Here you have, ;0)" and an attached file called AnnaKournikova.jpg.vbs. When launched under Microsoft Windows the file does not display a picture of Anna Kournikova but launches a viral Visual Basic Script that forwards itself to everybody in the Microsoft Outlook address book of the victim.

The worm was created using a simple and widely available Visual Basic Worm Generator program developed by an Argentinian programmer called “[K]Alamar”.[2] While similar to the ILOVEYOU worm that struck a year earlier, in 2000, the Anna Kournikova worm did not corrupt data on the infected computer.

Apparently, the author created the worm in a matter of hours. "The young man had downloaded a program on Sunday, February 11, from the Internet and later the same day, around 3:00 p.m., set the worm loose in a newsgroup." De Wit turned himself in to authorities in the town of Sneek located in the northern province of Friesland in the Netherlands. "By the time he understood what the worm did, he had conferred with his parents and decided to turn himself in to the police,"

It has been reported that the efforts of another virus writer working undercover for the FBI, David L. Smith, led to the identification of Jan de Wit and that the FBI passed the information to authorities in the Netherlands. De Wit turned himself in to the police in his hometown Sneek on February 14, 2001, a few days after the worm was released.

Reportedly, and resembling the cases of other computer virus writers, only a few days later the mayor of Sneek, Mayor Sieboldt Hartkamp, made a tentative job offer to De Wit, quoting his programming skills.

De Wit was tried in Leeuwarden and was charged with spreading data into a computer network with the intention of causing damage, a crime that carried a maximum sentence of four years in prison and a fine of 100,000 guilders (US$41,300).

The lawyers for Jan de Wit called for the dismissal of charges against him, arguing that the worm caused minimal damage. The FBI submitted evidence to the Dutch court and suggested that US$166,000 in damages was caused by the worm. De Wit admitted he created the worm using a worm creation toolkit but told the court when he posted the virus to a newsgroup he did it "without thinking and without overseeing the consequences". He denied any intent to cause damage. De Wit was sentenced to 150 hours community service or 75 days in jail.

AntiCMOS

AntiCMOS is a boot virus. Its first discovery was at Lenart, Slovenia, which led to its alias of Lenart. It was isolated in Hong Kong several times at the beginning of 1994, but did not become common until it spread to North America in the Spring of 1995. AntiCMOS is a fairly standard boot virus, and is primarily notable for being one of the few DOS viruses to remain in the wild as of 2005.

AntiCMOS is so named because it has the intended effect of erasing all CMOS information. This does not occur because of a bug in the virus code. This is true of all AntiCMOS variants that have appeared in the wild. The payload date of December 1993 and the obsolete nature of these variants makes it very unlikely that AntiCMOS's payload will ever be a threat.

AntiCMOS.B

AntiCMOS.B is a boot virus. It was isolated in mid-1995. Like AntiCMOS.A, AntiCMOS.B became common worldwide. However, this variant never reached the success level of the original, and is now considered obsolete. Infected floppy disks contain the following text:

I am Li Xibin

Additionally, AntiCMOS.B attempts to play a tune, but this fails due to coding errors. AntiCMOS.B is otherwise a typical boot virus, much like its predecessor.

AntiCMOS.C

AntiCMOS.C is a boot virus and very minor variant of the AntiCMOS family. Unlike AntiCMOS and AntiCMOS.B, AntiCMOS.C remained in the field for a very short period of time, and is now considered entirely obsolete.

Bomber

Bomber (also known as Commander Bomber) is a DOS polymorphic memory resident computer virus, known for its technique of "patchy infection". This method of infection is very similar to that which is utilised by the OneHalf computer virus.

Contrary to the usual method of infecting executables (which is to append virus body to the executable and to change the entry point), it inserts several fragments ("patches") of its code in random places inside the file. These fragments transfer control to each other using various mechanisms.

The method of infection makes the detection of the virus difficult by anti-virus programs, and it means that they would have to scan the file in its entirety in order to detect the virus.

The size of the Bomber executable is approximately 4096 bytes and contains the following text:

COMMANDER BOMBER WAS HERE

[DAME] [DAME]

Brain

Brain is the industry standard name for a computer virus that was released in its first form in January 1986, and is considered to be the first computer virus for MS-DOS. It infects the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system. Brain was written by two brothers, Basit Farooq Alvi and Amjad Farooq Alvi, from Lahore, Punjab, Pakistan.

Description

Brain affects the IBM PC computer by replacing the boot sector of a floppy disk with a copy of the virus. The real boot sector is moved to another sector and marked as bad. Infected disks usually have five kilobytes of bad sectors. The disk label is changed to ©Brain, and the following text can be seen in infected boot sectors:

Welcome to the Dungeon (c) 1986 Basie & Amends (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!

There are many minor and major variations to that version of the text. The virus slows down the floppy disk drive and makes seven kilobytes of memory unavailable to DOS. Brain was written by Amjad Farooq Alvi, who at the time lived in Chairman, near Lahore Railway Station, in Lahore, Pakistan. The brothers told *TIME* magazine they had written it to protect their medical software from piracy, and it was supposed to target copyright infringement only. The cryptic message "Welcome to the Dungeon", a safeguard and reference to an early programming forum on Dungeon BBS, appeared after a year because the brothers licensed a beta version of the code. The brothers could not be contacted to receive the final release of this version of the program.

Brain lacks code for dealing with hard disk partitioning, and avoids infecting hard disks by checking the most significant bit of the BIOS drive number being accessed. Brain does not infect the disk if the bit is clear, unlike other viruses at the time, which paid no attention to disk partitioning and

consequently destroyed data stored on hard disks by treating them in the same way as floppy disks. Brain often went undetected, partially due to this deliberate non-destructiveness, especially when the user paid little to no attention to the slow speed of floppy disk access.

The virus came complete with the brothers' address and three phone numbers, and a message that told the user that their machine was infected and to call them for inoculation:

Welcome to the Dungeon © 1986 Brain & Amjads (pvt). BRAIN COMPUTER SERVICES 730 IZANAMI

BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination…

This program was originally used to track a heart monitoring program for the IBM PC, and pirates were distributing illicit copies of the disks. This tracking program was supposed to stop and track illegal copies of the disk, however program also sometimes used the last 5k on an Apple floppy, making additional saves to the disk by other programs impossible.

Author response

When the brothers began to receive a large number of phone calls from people in United Kingdom, United States and elsewhere, demanding that they disinfect their machines, they were stunned and tried to explain to the outraged callers that their motivation had not been malicious. Their phone lines were overloaded. The brothers with another brother Shahid Farooq Alvi are still in business in Pakistan as Brain NET Internet service providers with a company called Brain Telecommunication Limited.

In 2011, 25 years after Brain was released, Mikko Hyppönen of F-Secure travelled to Pakistan to interview Amjad for a documentary. Being inspired by this documentary and its wide spread, a group of Pakistani bloggers interviewed Amjad, under the banner of Bloggerine.

Variants

Ashar is an older version of Brain. There are six variants, each with a different message.

Byte Bandit

Byte Bandit is a boot sector computer virus created for the Commodore Amiga. It first appeared in January 1988, and was created by SCA.

It was one of the most feared Amiga viruses until the infamous Lamer Exterminator because not only did it spread from system to system automatically, it was also destructive.

Byte Bandit made no attempt to disguise itself as modern viruses, trojans, and worms do. While it naturally over-wrote the bootblock, it also hooked into the system, remaining reset-resident and causing system data corruption and system failures. The virus increments a copy counter every time it writes itself to a disk, which is in the text string "Virus by Byte Bandit in 9.87. Number of copys:" which also gives a date of September 1987 for the creation, as well as the assumed name of the programmer.

Christmas Tree EXEC

Christmas Tree EXEC was the first widely disruptive computer worm, which paralyzed several international computer networks in December 1987.

Written by a student at the Clausthal University of Technology in the REXX scripting language, it drew a crude Christmas tree as text graphics, then sent itself to each entry in the target's email contacts file. In this way it spread onto the European Academic Research Network (EARN), the BITNET, and IBM's worldwide VNET. On all of these systems it caused massive disruption.

Its core mechanism was essentially the same as the ILOVEYOU worm of 2000 - although running on mainframes rather than PCs, spreading over a different network, and scripted using REXX rather than VBScript.

The name was actually "CHRISTMA EXEC" because the IBM VM systems originally required file names to be formatted as 8+space+8 characters. Additionally, IBM required REXX script files to have a file type of "EXEC". The name is sometimes written as "CHRISTMAS EXEC" (adding a 9th character) to make the name more readable. The user was prompted to: "...just type CHRISTMAS..." - and this in fact launched the "worm".

It displays this message as ASCII once the program is run and forwards itself to mailbox addresses contained in the users address file.


A
VERY
HAPPY
CHRISTMAS
AND MY
BEST WISHES
FOR THE NEXT
YEAR

CIH

CIH, also known as Chernobyl or Spacefiller, is a Microsoft Windows 9x computer virus which first emerged in 1998. It is one of the most damaging viruses, overwriting critical information on infected system drives, and more importantly, in most cases destroying the system BIOS. The virus was created by Chen Ing-hau (陳盈豪, pinyin: *Chén Yínghán*) who was a student at Tatung University in Taiwan. 60 million computers were believed to be infected by the virus internationally, resulting in an estimated $1 billion US dollars in commercial damages.

Chen claimed to have written the virus as a challenge against bold claims of antiviral efficiency by antivirus software developers. Chen stated that after the virus was spread across Tatung University by classmates, he apologized to the school and made an antivirus program available for public download; the antivirus program was co-authored with Weng Shi-hao (翁世豪), a student at Tamkang University. Prosecutors in Taiwan could not charge Chen at the time because no victims came forward with a lawsuit. These events led to new computer crime legislation in Taiwan.

The name "Chernobyl Virus" was coined some time after the virus was already well known as CIH, and refers to the complete coincidence of the payload trigger date in some variants of the virus (actually the virus creation date in 1998, to trigger exactly a year later) and the Chernobyl accident, which happened in the Ukrainian SSR on April 26, 1986.

The name "Spacefiller" was introduced because most viruses write their code to the end of the infected file, however CIH looks for gaps in the existing program code where it writes its own code. This does not increase the file size and in that way helps the virus avoid detection.

History

In December 31 1999, Yamaha shipped a Software update to their CD-R400 drives that was infected with the virus. In October 2000, a demo version of the first-person shooter game *SiN* was infected by one of its mirror sites. In March 1999, several thousand IBM Aptivas shipped with the CIH virus, just one month before the virus would trigger.

CIH's dual payload was delivered for the first time on April 26, 1999, with most of the damage occurring in Asia. CIH filled the first 1024 KB of the host's boot drive with zeros and then attacked certain types of BIOS. Both of these payloads served to render the host computer inoperable, and for most ordinary users the virus essentially destroyed the PC. Technically, however, it was possible to replace the BIOS chip, and methods for recovering hard disk data emerged later.

Today, CIH is not as widespread as it once was, due to awareness of the threat and the fact it only affects older Windows 9x (95, 98, Me) operating systems.

The virus made another comeback in 2001 when a variant of the LoveLetter Worm in a VBS file that contained a dropper routine for the CIH virus was circulated around the internet, under the guise of a nude picture of Jennifer Lopez.

A modified version of the virus called CIH.1106 was discovered in December 2002, but it is not considered a serious threat.

Virus specifics

CIH spreads under the Portable Executable file format under Windows 95, 98, and ME. CIH does not spread under Windows NT-based operating systems, such as Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10.

CIH infects Portable Executable files by splitting the bulk of its code into small slivers inserted into the inter-section gaps commonly seen in PE files, and writing a small re-assembly routine and table of its own code segments' locations into unused space in the tail of the PE header. This earned CIH another name, "Spacefiller". The size of the virus is around 1 kilobyte, but due to its novel multiple-cavity infection method, infected files do not grow at all. It uses methods of jumping from processor ring 3 to 0 to hook system calls.

The payload, which is considered extremely dangerous, first involves the virus overwriting the first megabyte (1024KB) of the hard drive with zeroes, beginning at sector 0. This deletes the contents of the partition table, and may cause the machine to hang or cue the blue screen of death.

The second payload tries to write to the Flash BIOS. Due to what may be an unintended feature of this code, BIOSes that can be successfully written to by the virus have critical boot-time code replaced with junk. This routine only works on some machines. Much emphasis has been put on machines with motherboards based on the Intel 430TX chipset, but by far the most important variable in CIH's success in writing to a machine's BIOS is the type of Flash ROM chip in the machine. Different Flash ROM chips (or chip families) have different write-enable routines specific to those chips. CIH makes no attempt to test for the Flash ROM type in its victim machines, and has only one write-enable sequence.

For the first payload, any information that the virus has overwritten with zeros is lost. If the first partition is FAT32, and over about one gigabyte, all that will get overwritten is the MBR, the partition table, the boot sector of the first partition and the first copy of the FAT of the first partition. The MBR and boot sector can simply be replaced with copies of the standard versions, the partition table can be rebuilt by scanning over the entire drive and the first copy of the FAT can be restored from the second copy. This means a complete recovery with no loss of user data can be performed automatically by a tool like Fix CIH.

If the first partition is not FAT32 or is smaller than 1GB the bulk of user data on that partition will still be intact but without the root directory and FAT it will be difficult to find it especially if there is significant fragmentation.

If the second payload executes successfully, the computer will not start at all. A technician is required to reprogram or replace the Flash BIOS chip, as most systems that CIH can affect predate BIOS restoration features.

CIH v1.2/CIH.1103

This variant is the most common one and activates on April 26.

It contains the string: *CIH v1.2 TTIT*

CIH v1.3/CIH.1010A and CIH1010.B

This variant also activates on April 26. It contains the string: *CIH v1.3 TTIT*

CIH v1.4/CIH.1019

This variant activates on the 26th of any month. It is still in the wild, although it is not that common. It contains the string *CIH v1.4 TATUNG*.

CIH.1049

This variant activates on August 2 instead of April 26

Commwarrior

Commwarrior is a Symbian Bluetooth worm that was the first to spread via Multimedia Messaging Service (MMS) and Bluetooth. The worm affects only the Nokia Series 60 software platform.

Infection

Commwarrior was particularly effective via the MMS vector it used to infect other phones. It appeared as though it had been sent from a source that was known to the victim, leading even security-conscious users to open the infected message. Actually, the message was sent at random to a contact in the sender's address book.

Once the message is opened, the virus attempts to install itself on the phone via a SIS file. As it runs, the worm is executed every time the phone is switched on.

A secondary method of infection is to create a malicious .SIS file on a compromised phone. Once per minute thereafter, the worm attempts to send this file to any phone that has Bluetooth enabled.

Symptoms

According to Sophos, during installation the program has a one in six chance of displaying the following text: *"CommWarrior v1.0 (c) 2005 by e10d0r"*

Creeper

Creeper was an experimental computer program written by Bob Thomas at BBN in 1971. Its original iteration was designed to move between DEC PDP-10 mainframe computers running the TENEX operating system using the ARPANET, with a later version by Ray Tomlinson designed to copy itself between computers rather than simply move. This self-replicating version of Creeper is generally accepted to be the first computer worm.

The program was not actively malicious software as it caused no damage to data, the only effect being a message outputted to the screen reading "I'm the creeper: catch me if you can"

Reaper

Reaper was a similar program created by Ray Tomlinson to move across the ARPANET and delete copies of the self-replicating Creeper.

Eliza

Eliza is a computer virus discovered in December,1991. Infects COM files including Command.com. It has been reported that it is defective, yet destroys the .EXE files it creates. The .COM files do not get deleted. The date of the file will not be altered by the infection to avoid detection, infected files increase in length by 1,193 or 1,194 bytes. Eliza is also found in later versions of Windows.

DOS Strain

One of the forms of Eliza attacks the MS-DOS operating system by reproducing itself into COM and .EXE files. However, the virus has a bug in it which does not allow it to behave properly. It only attacks .EXE files. Because it is defective and easy to track, Eliza has been considered a minimal threat.

Windows NT/2000/XP/Vista/7 Strain

It is not known whether the Windows strain was developed by the same person, but the particular strain targeting Windows is much more damaging and is considered a legitimate threat. One site reports that it does the following:

- Remotely controls your computer
- Wastes system resources and clogs CPU usage
- Tracks internet and keystrokes, allowing the hacker to record/steal passwords, credit card numbers, etc.

You can remove the virus from your computer with an antivirus program or by going into safe mode to remove the infected files manually.

Elk Cloner

Elk Cloner is one of the first known microcomputer viruses that spread "in the wild", *i.e.*, outside the computer system or laboratory in which it was written. It attached itself to the Apple II operating system and spread by floppy disk. It was written around 1982 by a 15-year-old high school student, Rich Skrenta. It was originally a joke, created and put onto a game disk.

Infection and symptoms

Elk Cloner spread by infecting the Apple DOS 3.3 operating system using a technique now known as a "boot sector" virus. It was attached to a game, the game was then set to play. The 50th time the game was started, the virus was released, but instead of playing the game, it would change to a blank screen that displayed a poem about the virus named Elk Cloner. If a computer booted from an infected floppy disk, a copy of the virus was placed in the computer's memory. When an uninfected disk was inserted into the computer, the entire DOS (including Elk Cloner) would be copied to the disk, allowing it to spread from disk to disk. To prevent the DOS from being continually re-written each time the disk was accessed, Elk Cloner also wrote a signature byte to the disk's directory, indicating that it had already been infected.

The poem that Elk Cloner would display was as follows:

Elk Cloner: The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes, it's Cloner!

It will stick to you like glue

It will modify RAM too

Send in the Cloner!

Elk Cloner did not cause deliberate harm, but Apple DOS disks without a standard image had their reserved tracks overwritten.

Development

Elk Cloner was created as a prank in 1981 by Rich Skrenta, a 15-year-old high school student. Skrenta already had a notoriety among his friends because, in sharing computer games and software, he would often alter the floppy disks to shut down or display taunting on-screen messages. Due to this reputation for pranks, many of his friends simply stopped accepting floppy disks from him. Skrenta thought of methods to alter floppy disks without physically touching them. During a winter break from Mt. Lebanon High School in Mt. Lebanon, Pennsylvania, Skrenta discovered how to launch the messages automatically on his Apple II computer. He developed what is now known as a boot sector virus, and began circulating it in early 1982 among high school friends and a local computer club. Twenty-five years later in 2007, Skrenta called it "some dumb little practical joke."

Distribution

According to contemporary reports, the virus was rather contagious, successfully infecting the floppies of most people Skrenta knew, and upsetting many of them.

Part of the "success", of course, was that people were not at all wary of the potential problem, nor were virus scanners or cleaners available. The virus could be removed using Apple's MASTER CREATE utility or other utilities to re-write a fresh copy of DOS to the infected disk. Furthermore, once Elk Cloner was removed, the previously-infected disk would not be re-infected since it already contained the Elk Cloner "signature" in its directory. It was also possible to "inoculate" uninfected disks against Elk Cloner by writing the "signature" to the disk; the virus would then think the disk was already infected and refrain from writing itself.

Form

Form was a boot sector virus isolated in Switzerland in the summer of 1990 which became very common worldwide. The origin of Form is widely listed as Switzerland, but this may be an assumption based on its isolation locale. The only notable characteristics of Form are that it infects the boot sector instead of the Master Boot Record (MBR) and the clicking noises associated with some infections. Infections under Form can result in severe data damage if operating system characteristics are not identical to those Form assumes.

It is notable for arguably being the most common virus in the world for a period during the early 1990s.

Infection

Form infects the boot sector. When a computer is booted from an infected sector, Form goes resident, hooks the interrupt vector table, and runs the original boot sector which it's hidden in an area it flags as defective. It will subsequently infect any media inserted into the machine.

Symptoms

Form has a range of symptoms, most of which will not be evident in all infections.

- Form's most famous side effect is a clicking noise produced by typing on the keyboard on the 18th of every month. However, this payload very rarely appears on modern computers, as it will not execute if a keyboard driver is installed.
- Form consumes 2KB of memory, and the DOS MEM command will report that this memory is unavailable. This appears on all infections.
- On floppy disks, 1 KB (2 bad sectors) will be reported. This appears in all infections.
- The Form data sector contains the text "The FORM-Virus sends greetings to everyone who's reading this text. FORM doesn't destroy data! Don't panic! Fuckings go to Corinne." Additionally, some versions of Form have had this text removed.

- Form makes the assumption that the active partition is a DOS FAT partition. If this is not true, such as under Windows NT, Form will overwrite in a way that may result in irreversible data loss.

Prevalence

Form was listed as spreading by the WildList from the first ever version of the WildList in July 1993 until January 2006.

As with most boot viruses, a Form infection is a rare find in modern times. Since the advent of Windows, boot viruses have become increasingly uncommon, including Form. Generally, Form infections are due to the use of floppy disks infected during the original pandemic that have since been taken out of storage.

Variants

Form has a number of variants. The widely documented versions are as follows.

- Form.A is a common variant of the original, where the clicking payload occurs every day, as opposed to just the 18th.
- Form.B is a minor variant of the original, with the clicking payload set for the 18th of each month instead of the 24th. It was a rare find in the field during the mid1990s, but has since become obsolete.
- Form.C is a virtually undocumented, trivial variant of the original. It is suggested that Form.C is another minor variant of Form, except only activates in May. Like Form.B, it was documented as being discovered rarely in the wild during the mid-1990s.
- Form.D is the most common version of Form besides the original. Some reports indicate that it affects the partition table in some way. It was a somewhat common virus in 1997 and 1998.
- FormII is an undocumented variant.
- Form-Canada is an undocumented variant.

Graybird

Graybird is a Trojan horse that hides its presence on the compromised computer and downloads files from remote Web sites. There are many variations of this virus such as Backdoor.Graybird.P (the most recently discovered variation). It was discovered in September 3, 2003. It affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP, and Windows Vista

Hare

The Hare Virus is a destructive computer virus which infected DOS and Windows 95 machines in August 1996. It was also known as *Hare.7610*, *Krsna* and *HD Euthanasia*.

Description

The virus was capable of infecting .COM and .EXE executable files, as well as the Master boot record of hard disks and the boot sector on floppy disks. The virus was set to read the system date of the computer and activate on August 22 and September 22, at which time it would erase the hard disk in the computer and display the following message:

- HDEuthanasia by Demon Emperor: Hare Krsna, hare, hare

.

ILOVEYOU

ILOVEYOU, sometimes referred to as Love Letter, was a computer worm that attacked tens of millions of Windows personal computers on and after 4 May 2000 local time in the Philippines when it started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". The latter file extension (in this case, 'VBS' - a type of interpreted file) was most often hidden by default on Windows computers of the time, leading unwitting users to think it was a normal text file. Opening the attachment activated the Visual Basic script. The worm did damage on the local machine, overwriting random types of files (including Office files, image files, and audio files; however after overwriting MP3 files the virus would hide the file), and sent a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. In contrast, the Melissa virus only sent copies to the first 50 contacts.

Key to success

On the machine system level, ILOVEYOU relied on the scripting engine system setting (which runs scripting language files such as .vbs files) being enabled, and took advantage of a feature in Windows that hid file extensions by default, to which malware authors would use as an exploit; to do this, it parsed file names from right to left, stopping at the first period character. The attachment, which had two periods, could thus display the inner fake "txt" file extension. Text files are considered to be innocuous, as they are normally incapable of running executable code. The worm also used social engineering to entice users to open the attachment (out of actual desire to connect or simple curiosity) to ensure continued propagation. Systemic weaknesses in the design of Microsoft Outlook and Microsoft Windows were exploited that allowed malicious code capable of complete access to the operating system, secondary storage, and system and user data simply by unwitting users clicking on an icon.

Spread

Messages generated in the Philippines began to spread westwards through corporate email systems. Because the worm used mailing lists as its source of targets, the messages often appeared to come from acquaintances and were therefore often regarded as "safe" by their victims, providing further incentive to open them. Only a few users at each site had to access the attachment to generate millions more messages that crippled mail systems and overwrote millions of files on computers in each successive network.

Impact

The malware originated in the Pandacan neighborhood of Manila in the Philippines on May 5, 2000, thereafter following daybreak westward across the world, moving first to Hong Kong, then to Europe, and finally the United States, as employees began their workday that Friday morning. The outbreak was later estimated to have caused US$5.5-8.7 billion in damages worldwide, and estimated to cost US$15 billion to remove the worm. Within ten days, over fifty million infections had been reported, and it is estimated that 10% of internet-connected computers in the world had been affected. Damage cited was mostly the time and effort spent getting rid of the infection and recovering files from backups. To protect themselves, The Pentagon, CIA, the British Parliament and most large corporations decided to completely shut down their mail systems. This virus affected over 45 million computers and was one of the world's most dangerous computer related disasters.

Architecture

The ILOVEYOU Script (the attachment) was written in Microsoft Visual Basic Scripting (VBS) which runs in Microsoft Outlook and was enabled by default. The script added Windows Registry data for automatic startup on system boot.

The worm then searched connected drives and replaced files with extensions JPG, JPEG, VBS, VBE, JS, JSE, CSS, WSH, SCT, DOC, HTA, MP2, and MP3 with copies of itself, while appending the additional file extension VBS, making the user's computer unbootable. However, the MP3 and sound related files are hidden and not overwritten.

The worm propagated itself by sending out one copy of the payload to each entry in the Microsoft Outlook address book (Windows Address Book). It also downloaded the Barok trojan renamed for the occasion as "WIN-BUGSFIX.EXE".

The fact that the virus was written in VBS provided users a way to modify the virus. A user could easily modify the virus to replace important files in the system, and destroy it. This allowed many variations of ILOVEYOU to spread across the internet, each one doing different kinds of damage.

Some mail messages sent by ILOVEYOU:

- VIRUS ALERT!!
- Important! Read Carefully!!

Developments

On 5 May 2000, two young Filipino computer programmers named Reonel Ramones and Onel de Guzman became targets of a criminal investigation by agents of the Philippines' National Bureau of Investigation (NBI). Local Internet service provider Sky Internet had reported receiving numerous contacts from European computer users alleging that malware (in the form of the "ILOVEYOU" worm) had been sent via the ISP's servers.

After surveillance and investigation by Darwin Bawasanta of Sky Internet, the NBI traced a frequently appearing telephone number to Ramones' apartment in Manila. His residence was searched and Ramones was arrested and placed on inquest investigation before the Department of Justice (DOJ). Onel de Guzman was likewise charged *in absentia*.

At that point, the NBI were unsure what felony or crime would apply. It was suggested they be charged with violating Republic Act 8484 (the Access Device Regulation Act), a law designed mainly to penalise credit card fraud, since both used pre-paid (if not stolen) Internet cards to purchase access to ISPs. Another idea was that they be charged with malicious mischief, a felony (under the Philippines Revised Penal Code of 1932) involving damage to property. The drawback here was that one of its elements, aside from damage to property, was intent to damage, and de Guzman had claimed during custodial investigations that he may have unwittingly released the worm.

To show intent, the NBI investigated AMA Computer College, where de Guzman had dropped out at the very end of his final year. They found that, for his undergraduate thesis, de Guzman had proposed the implementation of a trojan to steal Internet login passwords. This way, he proposed, users would finally be able to afford an Internet connection. The proposal was rejected by the College of Computer Studies board, prompting de Guzman to cancel his studies the day before graduation.

Legislative aftermath

Since there were no laws in the Philippines against writing malware at the time, both Ramones and de Guzman were released with all charges dropped by state prosecutors. To address this legislative deficiency, the Philippine Congress enacted Republic Act No. 8792, otherwise known as the E-Commerce Law, in July 2000, just two months after the worm outbreak. In 2002, the ILOVEYOU virus obtained a world record for being the most virulent computer virus at the time.

INIT 1984

INIT 1984 is a computer virus that was set up to trigger on Macintosh computers running the classic Mac OS on any given Friday the 13th. The virus was first discovered and isolated in March, 1992. It functions by infecting startup (INIT) files, then modifying or deleting those files upon startup on Friday the 13th. The virus has a low threat assessment.

Jerusalem

Jerusalem is a DOS virus first detected in Jerusalem, in October 1987. On infection, the Jerusalem virus becomes memory resident (using 2kb of memory), and then infects every executable file run, except forCOMMAND.COM. COM files grow by 1,813 bytes when infected by Jerusalem and are not re-infected. .EXE files grow by 1,808 to 1,823 bytes each time they are infected. The virus re-infects .EXE files each time the files are loaded until they are too large to load into memory. Some .EXE files are infected but do not grow because several overlays follow the genuine .EXE file in the same file. Sometimes .EXE files are incorrectly infected, causing the program to fail to run as soon as it is executed.

The virus code itself hooks into interrupt processing and other low level DOS services. For example, code in the virus suppresses the printing of console messages if, for example, the virus is not able to

infect a file on a read-only device such as a floppy disk. One of the clues that a computer is infected is the mis-capitalization of the well-known message "Bad command or file name" as "Bad Command or file name".

The program contains one destructive payload that is set to go off on Friday the 13th, all years but 1987. On that date, the virus deletes every program file that was executed. Jerusalem is also known as BlackBox because of a black box it displays during the payload sequence. If the system is in text mode, Jerusalem creates a small black rectangle from row 5, column 5 to row 16, column 16. The rectangle is scrolled up by two lines.

As a result of the virus hooking into the low-level timer interrupt, PC-XT systems slow down to one fifth of their normal speeds 30 minutes after the virus has installed itself. The slowdown is less noticeable on faster machines. The virus contains code that enters a processing loop each time the processor's timer tick is activated.

Symptoms also include spontaneous disconnection of workstations from networks and creation of large printer spooling files. Disconnections occur since Jerusalem uses the 'interrupt 21h' low-level DOS functions that Novell Netware and other networking implementations required to hook into the file system.

Jerusalem was initially very common (for a virus of the day) and spawned a large number of variants. However, since the advent of Windows, these DOS interrupts are no longer used, so Jerusalem and its variants have become obsolete.

Aliases

- 1808(EXE)
- 1813(COM)
- ArabStar
- BlackBox
- BlackWindow
- Friday13th (Note: The name can also refer to two viruses that are unrelated to Jerusalem: Friday-13th-440/Omega and Virus-B)
- HebrewUniversity
- Israeli
- PLO
- Russian

Get Password 1 (GP1)

Discovered in 1991 this Novell NetWare-specific virus attempts to gather passwords from the NetWare DOS shell in memory upon user login, which it then broadcasts to a specific socket number on the network where a companion program can recover them.

Suriv viruses

The Suriv viruses are earlier, more primitive versions of Jerusalem. Suriv 1 and 2 triggers on April 1 while Suriv 3 triggers on Friday 13, switching off the computer on the 13th.

Sunday (Jeru-Sunday)

Files infected by Sunday grow by 1,636 bytes.

On each Sunday the virus displays one of the following messages during 30 minute intervals.

- Today is SunDay! Why do you work so hard?
- All work and no play make you a dull boy!
- Come on ! Let's go out and have some fun!

The variant is intended to delete every program as it is run. Software bugs prevent this from happening.

Sunday has several variants.

- Sunday.a - The version described above.
- Sunday.b - A version of Sunday which has a working program-deleting function.
- Sunday.1.b - Like Sunday.b, except that a bug regarding the Critical Error Handler, which causes problems on write-protected disks, has been fixed.
- Sunday.1.d - Like Sunday.1.a, except the same bug is fixed in a different way.
- Sunday.1.Tenseconds - Like Sunday.a, except the delay for the messages is now 10 seconds. In addition, the test for Sunday is correctly set for day 0 (zero) instead of 7 (seven).
- Sunday.2 - Like Sunday.1.a, except files grow by 1,733 bytes.

Anarkia

Anarkia is almost identical to the original Jerusalem. It uses the self-recognition code "Anarkia".

PQSR

PQSR causes infected files to grow by 1,720 bytes. On the 13th of any month, the virus deletes any program run on the PC. Garbage is written to the master boot record and the nine sectors after the MBR. The virus uses "PQSR" as its self-recognition code.

Jeruspain (Jeru-Spanish)

If the virus is memory-resident, Jeruspain will delete any program run on the 26th of any month.

Frère

Frère plays Frère Jacques if the day is Friday or the 13th of any month.

Westwood (Jerusalem-Westwood)

Westwood causes files to grow by 1,829 bytes. If the virus is memory-resident, Westwood deletes any file run during Friday the 13th.

Jerusalem-113

Programs will not run during Saturdays. The virus avoids PHENOME.COM instead of COMMAND.COM, and therefore infects COMMAND.COM.

Jerusalem-Apocalypse

Jerusalem-Apocalypse contains the text "Apocalypse!!". If the virus is memory-resident, it will delete any file on Friday the 13th.

Jerusalem-T1

If the virus is memory-resident, it will delete any file run on Tuesday the 1st.

Jerusalem-T13

The virus causes .COM and .EXE files to grow by 1,812 bytes. If the virus is memory-resident, it will delete any program run on Tuesday the 13th.

Jerusalem-Sat13

If the virus is memory-resident, it will delete any program run on Saturday the 13th.

Jerusalem-Czech

If the virus is memory-resident, it will delete any program run on Friday the 13th. Jerusalem-Czech has a self-recognition code and a code placement that differ from the original Jerusalem.

Jerusalem-Frère.2

Jerusalem-Frère plays Frère Jacques once per minute. A variant called Two Tigers plays the same tune.

Jerusalem-Nemesis

The virus avoids NEMESIS.COM instead of COMMAND.COM, and therefore infects COMMAND.COM. Jerusalem-Nemesis contains the string "NEMESIS.COM".

Jerusalem-Captain Trip

Jerusalem-Captain Trip contains the strings "Captain Trips" and "SPITFIRE". Captain Trips is the name of the apocalyptic plague described in Stephen King's novel The Stand.

If the year is any year other than 1990 and the day is a Friday on or after the 15th, if a program is run, Jerusalem-Captain Trip creates an empty file with the same name as the program. On several other dates it installs a routine in the timer tick that activates when 15 minutes pass. On the 16th Jerusalem-Captain Trip re-programs the video controller. Jerusalem-Captain Trip has several errors.

Jerusalem-J

The variant causes .COM files to grow by 1,237 bytes. .EXE files grow by about 1,232 bytes. The virus has no "Jerusalem effects."

Jerusalem-Yellow

Jerusalem-Yellow does not infect .EXE files. All files infected grow by 1,363 bytes apiece.

After the virus is loaded into memory, when 45 minutes pass or when 4,096 keystrokes are entered, Jerusalem-Yellow creates a large yellow box with a shadow in the middle of the screen and the computer hangs.

Jerusalem-Jan25

If the virus is memory-resident, it will delete any program run on January the 25th.

Friday-15th (Skism)

Friday-15th causes infected files to grow by 1,813 bytes. If the virus is memory-resident and a program is run on Friday the 15th, the virus will create a new file with the same name as the program. it is needed to format your computer

Carfield (Jeru-Carfield)

The virus causes infected files to grow by 1,508 bytes.

If the virus is memory-resident and the day is Monday, the computer will display the string "Carfield!" every 42 seconds.

Mendoza (Jerusalem Mendoza)

The virus does nothing if the year is 1980 or 1989.

For all other years a flag is set if the virus is memory resident and if the floppy disk motor count is 25. The flag will be set if a program is run from a floppy disk.

If the flag is set, every program which runs is deleted.

If the flag is not set and 30 minutes passes, the cursor is changed to a block. After one hour, Caps Lock, Nums Lock, and Scroll Lock are switched to "Off".

Other variants

- Jerusalem.1244
- Jerusalem.1808.Standard
- Jerusalem.Mummy.1364.a
- Standard.SuMsdos
- Standard.Var
- Standard.AA33CCDDEE
- Standard.UMsDos
- Standard.null
- Standard.Nocommand
- Jan25
- a
- Anarkia.2
- Puerto
- Spanish
- Messina
- ffd
- 1af
- Critical
- Flag_ee,
- *a204*
- Frère2
- Frère3
- 2e7
- Not13
- b0f
- Phenomen
- 52f

- 7c01
- 6d46
- JVT1
- J
- Friday15
- 3503
- Feb-7th
- Nov30
- sUMFDos
- SKISM
- 5a4
- 65d6
- BSA
- Dragon.
- Lee Morton's Lover
- Slow

Kama Sutra

The Kama Sutra worm, also known as Blackworm, Nyxem, and Blackmal, is a type of malware (malicious software) that infects PCs using Microsoft Windows.

Discovered January 16, 2006, Kama Sutra was designed to destroy common files such as Microsoft Word, Excel, and PowerPoint documents when each computer's calendar hit February 3 and on the 3rd of each following month.

The worm arrived via e-mail, enticing computer users with promises of sexy pictures. The subject lines included "School girl fantasies gone bad", "Hot Movie", "Crazy illegal Sex!" and "Kama Sutra pics". When users clicked on the attachment, the machine became infected. Once executed, the worm can corrupt and overwrite the most common Windows file types, .doc, .pdf, .zip, and .xls, among others; the data are changed and become unrecoverable. The worm also tries to disable antivirus software.

Lamer Exterminator

Lamer Exterminator is a computer virus created for the Commodore Amiga. It was first detected in Germany in October 1989. It is a boot block virus contained in the first 1024 bytes of the disk.

It is notable as the first virus known to be defensive. It hooks into the system in such a way that examining a bootblock will return a normal result and upon replicating will also encrypt itself.

Variants of the virus are known to use one of three different decrypt routines defined by The Amiga Virus Encyclopedia. A detection program can look for any of the known decrypt routines on the boot block area of the disk, or alternatively try to blindly brute force decrypt them. The first decrypt routine is a simple XOR of every byte which only takes a maximum of 256 attempts to decrypt. The next includes an add byte in its decrypt routine, and takes a maximum of 256x256 attempts. The third uses 16 bit words in its decrypt routine, and takes a maximum of 65535x65535 attempts which makes it an impractical approach with modern computers. The first two versions (and variants that use the same decrypt routines), can also be identified as containing an identification word 0xABCD, as the last data on the boot block containing anything but zero values.

Symptoms

- Over-writes the bootblock
- Remains RAM resident (allocating 1024 bytes and identifying itself: 'The LAMER Exterminator !!!')
- Hooks into the system (remaining reset-resident)
- Destroys media blocks by overwriting them 84 times with the string 'LAMER!', causing read/write errors on affected storage media. This causes filesystem corruption and data loss, which is unrecoverable.

MacMag

The MacMag virus, also known by various other names, was a computer virus introduced in 1988 by Richard Brandow, who at the time was editor and publisher of MacMag computer magazine in Montréal.

Operation of the virus

The virus infected Macintosh computers, and the intention was that on 2 March 1988 all infected computers would show the message "RICHARD BRANDOW, publisher of MacMag, and its entire staff would like to take this opportunity to convey their UNIVERSAL MESSAGE OF PEACE to all Macintosh users around the world", and the virus would then delete itself. According to the virus itself, it was written by Drew Davidson. The virus was a boot sector virus, which was spread in the form of a HyperCard stack called "New Apple Products," which contained very poor pictures of the then-new Apple scanner. It copied a resource into the System folder on a Mac, as an "initial" program, which would run automatically every time the system started up. The program then copied itself onto any bootable disk which was opened.

Damage caused

Brandow intended the virus to be benign, giving a friendly message and causing no harm. However a bug in the virus caused infected Mac II computers to undergo system crashes before this date. Another bug, which affected very few users, caused files other than the original virus to be deleted during the termination stage. It also caused a great deal of anxiety among users who found that their computers were infected with an unwanted program the nature of which was unknown. The virus infected Aldus software's FreeHand, and Aldus had to recall thousands of copies of FreeHand, leading them to threaten legal action.

MDEF

MDEF was a computer virus affecting Macintosh machines. There are four known strains. The first, MDEF A (aka Garfield), was discovered in May 1990. Strains B (aka Top Cat), C, and D were discovered in August 1990, October 1990, and January 1991, respectively.

MDEF A, B, and C can infect application files and system files, and sometimes document files as well. The D strain will infect only applications. None of the viruses were designed to do damage, but they often do. MDEF D can sometimes damage applications beyond repair.

Quick action by computer security personnel and the New York State Police resulted in identification of the author, a juvenile. This was the same person responsible for writing the CDEF virus.

Melissa

The Melissa virus, also known as "Mailissa", "Kwyjibo", or "Kwejeebo", is a mass-mailing macro virus. As it is not a standalone program, it is not a worm.

The virus is said to have infected up to 20% of computers worldwide.

David L. Smith

Around March 26, 1999 Melissa was put in the wild by David L. Smith of Aberdeen Township, New Jersey. (The virus itself was credited to *Kwyjibo*, who was shown to be macrovirus writers *VicodinES* and *ALT-F11* by comparing MS Word documents with the same globally unique identifier — this

method was also used to trace the virus back to Smith.) On December 10, 1999 Smith pleaded guilty and was sentenced to 10 years, serving 20 months, and was fined US $5,000. The arrest was the result of a collaborative effort involving (amongst others) the FBI, the New Jersey State Police, Monmouth Internet and a Swedish computer scientist.

Michelangelo

The Michelangelo virus is a computer virus first discovered on 4 February 1991 in Australia. The virus was designed to infect DOS systems, but did not engage the operating system or make any OS calls. Michelangelo, like all boot sector viruses, basically operated at the BIOS level. Each year, the virus remained dormant until March 6, the birthday of Renaissance artist Michelangelo. There is no reference to the artist in the virus, but due to the name and date of activation it is very likely that the virus writer intended Michelangelo to be referenced to the virus. Michelangelo is a variant of the already endemic Stoned virus.

On March 6, if the PC is an AT or a PS/2, the virus overwrites the first one hundred sectors of the hard disk with nulls. The virus assumes a geometry of 256 cylinders, 4 heads, 17 sectors per track. Although all the user's data would still be on the hard disk, it would be irretrievable for the average user.

On hard disks, the virus moves the original master boot record to cylinder 0, head 0, sector 7.

On floppy disks, if the disk is 360 KB, the virus moves the original boot sector to cylinder 0, head 1, sector 3.

On other disks, the virus moves the original boot sector to cylinder 0, head 1, sector 14.

- This is the last directory of the 1.2 MB disks.
- This is the second-to-last directory of the 1.44 MB disks.
- The directory does not exist on 720 KB disks.

Although designed to infect DOS systems, the virus can easily disrupt other operating systems installed on the system since, like many viruses, the Michelangelo infects the master boot record of a hard drive. Once a system became infected, any floppy disk inserted into the system (and written to; in 1992 a PC system could not detect that a floppy had been inserted, so the virus could not infect the floppy until some access to the disk is made) becomes immediately infected as well. And because the virus spends most of its time dormant, activating only on March 6, it is conceivable that an infected computer could go for years without detection — as long as it wasn't booted on that date, while infected.

The virus first came to widespread international attention in January 1992, when it was revealed that a few computer and software manufacturers had accidentally shipped products, for example Intel's LANSpool print server, infected with the virus. Although the infected machines numbered only in the hundreds, the resulting publicity spiraled into "expert" claims, partially led by anti-virus company founder John McAfee, of thousands or even millions of computers infected by Michelangelo. However, on March 6, 1992, only 10,000 to 20,000 cases of data loss were reported.

In subsequent years, users were advised not to run PCs on March 6, waiting until March 7, or else reset the PC date to March 7 at some time on March 5 (to skip March 6). Eventually, the news media lost interest, and the virus was quickly forgotten. Despite the scenario given above, in which an infected computer could evade detection for years, by 1997 no cases were being reported in the wild.

Navidad virus

W32.Navidad is a mass-mailing worm program or virus, discovered in December of 2000, designed to spread through email clients such as Microsoft Outlook while masquerading as an electronic Christmas card. Infected computers can be identified by the mysterious blue eye icons which appear in the Windows system tray.

Users who move their mouse cursor over the eyes will be presented with a variety of different messages, including one which states: "Emmanuel-God is with us!May god bless u.And Ash, Lk, and LJ!!"

Natas

Natas (Satan spelled backwards) is a computer virus written by James Gentile, a then-18-year-old hacker from San Diego, California who went by the alias of "Little Loc" and later "Priest". The virus was made for a Mexican politician who wanted to win the Mexican elections by affecting all the Mexican Federal Electoral Institute (IFE) computers with a floppy disk.

Description

Natas is a memory-resident stealth virus and is highly polymorphic, that affects master boot records, boot sectors of diskettes, files .COM and also .exe programs.

History

The virus first appeared in Mexico City in May 1992, spread by a consultant using infected floppy disks. The virus became widespread in Mexico and the southwest United States. The virus also made its way to the other side of the USA, infecting computers at the United States Secret Service knocking their network offline for approximately three days. This led to an investigation of Priest and incorrect suspicion that the virus specifically targeted government computers.

Natas also infected computers in Canada, England, Russian Federation and Brazil.

nVIR

nVIR is an obsolete computer virus which can replicate on Macintosh computers running any System version from 4.1 to OS 8. The source code to the original nVIR has been made widely available, and so numerous variants have arisen. Each variant causes somewhat different symptoms, such as: application crashes, printing errors on laser printers, slow system response time, or unpredictable system crashes. nVIR spreads through any nVIR-infected program, but due to the long period of time nVIR lies basically dormant in a host system, nVIR generally finds its way into system backups and is not detected until the first overt symptoms appear. For example, if a disk used in an infected Macintosh is removed and inserted in a second Macintosh, the other machine will become infected if any application on that disk is executed in the second machine. Further, any method used to transfer programs between Macintoshes will spread nVIR, including file transfer over a network. However, nVIR cannot spread via a print network's hardware.

nVIR carries an additional code resource, CODE 256 (though some variants carry CODE 255), and patches the jump table to point to it. The original application's entry point is saved in the nVIR 2 resource. nVIR introduces to the System file the INIT 32 resource which is executed at startup, at which time nVIR patches the TEInit trap. Any application subsequently calling this trap will be infected. The nVIR 3 (or nVIR 5) resource is a copy of INIT 32. An nVIR 10 resource in the System file will prevent nVIR infection. If an application calls OpenResFile prior to TEInit, that application will be damaged.

nVIR 0 resource holds a counter that is set to 1000 on the first infection of the system. Each reboot decrements the counter by 1. Each application launch decrements it by 2. When the counter reaches 0, nVIR will beep 1 out of 8 reboots and 1 of 4 infected application launches. If MacinTalk is installed in the machine's System folder, the machine may occasionally say "Don't Panic". Otherwise, it may beep unexpectedly.

nVIR has been known to 'hybridize' with different variants of nVIR on the same machine.

OneHalf

OneHalf is a DOS-based polymorphic computer virus (hybrid boot and file infector) discovered in October 1994. It is also known as Slovak Bomber, Freelove or Explosion-II. It infects the master boot record (MBR) of the hard disk, and any files with extensions .COM, .SCR and .EXE. However, it will not infect files that have SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV or CHKDSK in the name.

It is also known as one of the first viruses to implement a technique of "patchy infection", introduced in Bomber.

OneHalf has about 20 different variants, all with functionally similar behaviour.

Payload

OneHalf is known for its peculiar payload: at every boot, it encrypts two unencrypted cylinders of the user's Hard disk, but then temporarily decrypts them when they are accessed. This makes sure the user does not notice that their hard disk is being encrypted like this, and lets the encryption continue further. It also hides the real MBR from programs on the computer, to make detection harder. The

encryption is done by bitwise XORing by a randomly generated key, which can be decrypted simply by XORing with the same bit stream again. Once the virus has encrypted half of the disk, and/or on the 4th, 8th, 10th, 14th, 18th, 20th, 24th, 28th and 30th of any month and under some other conditions, the virus will display the message:

Dis is one half.

Press any key to continue ...

Removal

OneHalf's unique payload makes removal harder: simply removing the virus and cleaning the MBR will leave the data encrypted, requiring backups to restore it. As such, special tools are needed to decrypt the hard disk before removing the virus. One such tool was developed for SAC (Slovak Antivirus Center) to do this job.

Ontario

Ontario.512 is a computer virus, discovered in July 1990. It is named after its point of isolation, the Canadian province of Ontario. This family of Computer virus consists of Ontario.1024,Ontario.512 and Ontario.2048. Because Ontario.1024 was also discovered in Ontario, it is likely that both viruses originate from within the province. By the Ontario.2048 variant, the author had adopted "Ontario" as the family's name and even included the name "Ontario-3" in the virus code.

Ontario.512

Infection

Ontario.512 is an encrypting DOS file infector. Upon the execution of an infected .COM, .EXE or .OVL file, Ontario.512 goes memory resident and infects files of these times upon being opened. COMMAND.COM is infected using a special routine. Infected files will increase either 512 bytes (COM files) or between 512 and 1,023 bytes (EXE and OVL files). Some systems with larger file sectors may display increases of greater than 1,023 bytes for infected files of these types.

Symptoms

Ontario.512 primarily only infects files, so there is no one significant symptom. The two main symptoms are:

- An increase in size of infected COM files of 512 bytes.
- An increase in size of infected EXE and OVL files of between 512 and 1,023 bytes, and even greater on some systems.
- Systems thoroughly infected by Ontario.512 may suffer from increasing file corruption and other hard drive problems over time.
- Unspecified printer problems have been observed with the Ontario family, although most of these observations have related to Ontario.1024, not Ontario.512. It is unknown what specific problems these are, and if they affect Ontario.512.

The increase in COM file size in conjunction with EXE and OVL file increases is a very good guideline when determining Ontario.512 infection, although file length changes are common among virtually every file infector.

Prevalence

The WildList, an organisation tracking computer viruses, never reported Ontario.512 as being in the field. However, Ontario.1024 was included on the list for a period of time. It is unclear whether Ontario.512 was discovered in the field, or off a BBS out of Toronto, where Ontario.2048 was posted.

Ontario.1024

Ontario.1024 is a computer virus, discovered in October 1991, over a year after the isolation of the first Ontario virus, Ontario.512. Relative to Ontario.512, most additions involve making the virus harder to detect.

Infection

Ontario.1024 is an encrypting, stealth DOS file infector. Upon the execution of an infected .COM or .EXE file, Ontario.1024 goes memory resident and infects files of these types upon being opened. COMMAND.COM is infected using a special routine. Infected files will increase in size by 1,024 bytes. However, when Ontario.1024 is in memory, no increase in file size will be observed due to the virus' stealthing. Unlike Ontario.512, it will not infect .OVL files.

Symptoms

Ontario.1024 is the least readily identified version of the Ontario family. The following symptoms can be observed:

- An increase in size of infected COM and EXE files of 1,024 bytes.
- A decrease in available system memory of 3,072 bytes.
- File size being changed after executables (infected ones) are executed, to display original file size.
- Occasional printer-related problems.

The first three symptoms are good indications that a virus is present, but are not necessarily specific to Ontario.1024.

Prevalence

The WildList, an organisation tracking computer viruses, listed Ontario.1024 as being in the field from July 1993 to December 1998, when it was removed due to lack of a submitted sample. These reports indicated that Ontario.1024 had spread as widely as Australia and Israel at its peak in 1994-1995.

Like all DOS file infectors, the advent of Windows significantly hindered the spread of Ontario.1024. Trend Micro reports 301 infections since 6 November 2000, with rates having fallen to about once every month or two by 2005.

Ontario.2048

Ontario.2048 is a computer virus, discovered in September 1992. It is the third and final known variant of the Ontario family, both chronologically and in complexity. Because of its rather extreme differences from the original virus, some vendors identify it as a member of a separate family - hence the alias Bootache.2048.

Infection

Ontario.2048 is an encrypting, polymorphic, stealth DOS file infector. Upon the execution of an infected .COM, .EXE, .OVL, or .SYS file, Ontario.2048 goes memory resident and infects files of these times upon being opened. COMMAND.COM is infected using a special routine, and will not increase in file size. Infected files will increase in size by 2,048 bytes. However, when Ontario.2048 is in memory, no increase in file size will be observed due to the virus' stealthing.

When the DOS DEBUG program is in memory, Ontario.2048 will detect it and disinfect programs in memory to avoid being analysed. Ontario.2048 also features an extremely complex encryption system; a given sample of Ontario.2048 may only share two bytes in common with another.

Symptoms

Ontario.2048 can result in the following symptoms:

- An increase in size of infected files by 2,048 bytes.
- A decrease in available system memory of 5,120 bytes.
- File size being changed after executables (infected ones) are executed, to display original file size.

- Occasional printer-related problems have been observed in the Ontario.1024 variant of this family; it is unknown whether this carries over to Ontario.2048.

The first three symptoms are good indications that a virus is present, but are not necessarily specific to Ontario.1024.

Ontario.2048 also contains text, which is invisible because Ontario.2048 is encrypted. The following text strings are present:

COMSPEC=\COMMAND.COM COMEXEOVLSYS

MSDOS5.0

YAM

Your PC has a bootache! - Get some medicine!

Ontario-3 by Death Angel

The first line is a reference to the method used to find COMMAND.COM to infect, as well as file types that the virus infects. The second line refers to the version of MS-DOS that Ontario.2048 was written on. The third is a reference to the Youngsters Against McAfee virus group, which the author had joined by this point.

A number of descriptions note multipartite function in Ontario.2048. This is incorrect. Ontario.2048 does contain a boot sector within it with a boot virus. If inserted into the boot sector, it would be a functioning boot virus (although it would not spread the file infection portion of Ontario.2048). However, Ontario.2048 never performs the injection; the code is functionally useless. Based on the virus author's documentation for the virus, this appears to be intentional (reasons unknown).

Prevalence

The WildList, an organisation tracking computer viruses, has never listed Ontario.2048 as being in the field. However, Ontario.1024 was included for a period of time.

Like all DOS file infectors, the advent of Windows significantly hindered the spread of Ontario.2048. Trend Micro statistics report only two infections since November 6, 2006, which indicates that the virus is now obsolete.

Pikachu virus

The Pikachu virus, sometimes referred to as Pokey Virus, was a computer virus believed to be the first computer virus geared at children due to its incorporation of Pikachu from the Pokémon series. It arrived in the form of an e-mail titled "Pikachu Pokemon [*sic*]" with the email saying that "Pikachu is your friend." Opening the attached executable met users with an image of Pikachu, along with a message stating, "Between millions of people around the world I found you. Don't forget to remember this day every time MY FRIEND." The virus itself appeared in the attachment to the email as a file named "PikachuPokemon.exe". It was often compared to the Love Bug, though the Pikachu virus was noted to be far less dangerous and slower in its dissemination.

Spread

The virus was mainly spread through Microsoft Outlook email attachments. The email containing the attached virus propagated through infected users by sending itself to all contacts in the user's Outlook address book.

Execution

When the user clicked on the attachment, PikachuPokemon.exe added the lines "del C:\WINDOWS" and "del C:\WINDOWS\system32" to the file "autoexec.bat" These commands would be executed at the next boot, attempting to delete two critical directories of the Windows operating system. However, users would be given a prompt asking whether or not they wanted to delete those folders. It is believed that this defect may be the reason that the Pikachu virus did not become more widespread and cause more damage to computer systems.

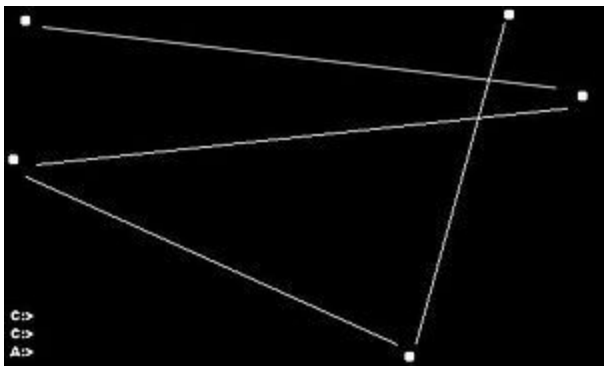
Ping-Pong virus

The Ping-Pong virus (also called Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A or VeraCruz) is a boot sector virus discovered on March 1, 1988 at the University of Turin in Italy. It was likely the most common and best known boot sector virus until outnumbered by the Stoned virus.

Replication method

Computers could be contaminated by an infected diskette, showing up as a 1 KB bad cluster (the last one on the disk, used by the virus to store the original boot sector) to most disk checking programs. Due to being labelled as bad cluster, MS-DOS will avoid overwriting it. It infects disks on every active drive and will even infect non-bootable partitions on the hard disk. Upon infection, the virus becomes memory resident.

Effect



The virus would become active if a disk access is made exactly on the half-hour and start to show a small "ball" bouncing around the screen in both text mode (the ASCII bullet character "•") and graphical mode. No serious damage is incurred by the virus except on '286 machines (and also V20, '386 and '486), which would sometimes crash during the ball's appearance on the screen. The cause of this crash is the "MOV CS,AX" instruction, which only exists on '88 and '86 processors. For this reason, users of machines at risk were advised to save their work and reboot, since this is the only way to temporarily get rid of the virus.

The original Ping Pong virus (Ping-Pong.A) only infects floppy disks. Later variants of this virus such as Ping-Pong.B and Ping-Pong.C also infect the hard disk boot sector as well. While the virus is active, one cannot replace the boot sector—it either prevents writing to it or it immediately re-infects it.

Ping-Pong.A is extinct but the hard-disk variants can still appear.

RavMonE.exe

RavMonE, known more correctly as RJump, is a Trojan that opens a backdoor on computers running Microsoft Windows. Once a computer is infected, the virus allows unauthorized users to gain access to the computer's contents. This poses a security risk for the infected machine's user, as the attacker can steal personal information, and use the computer as an access point into an internal network.

RavMonE was made famous in September 2006 when a number of iPod videos were shipped with the virus already installed. Because the virus only infects Windows computers, it can be inferred that Apple's contracted manufacturer was not using Macintosh computers. Apple came under some public criticism for releasing the virus with their product.

Description

RavMonE is a worm written in the Python scripting language and was converted into a Windows executable file using the Py2Exe tool. It attempts to spread by copying itself to mapped and removable storage drives. It can be transmitted by opening infected email attachments and downloading infected files from the Internet. It can also be spread through removable media, such as CD-ROMs, flash memory, digital cameras and multimedia players.

Action

Once the virus is executed, it performs the following tasks.

1. It copies itself to %WINDIR% as RavMonE.exe.
2. It adds the value "RavAV" = "%WINDIR%\RavMonE.exe" to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
3. It opens a random port and accepts remote commands.
4. It creates a log file RavMonLog to store the port number.
5. It posts a HTTP request to advise the attacker of the infected computer's IP address and the number of the port opened.

When a removable storage device is connected to the infected computer it copies the following files to that device:

- autorun.inf - a script to execute the worm the next time the device is connected to a computer
- msvcr71.dll - a Microsoft C Runtime Library module containing standard functions such as to copy memory and print to the console

Aliases

- Backdoor.Rajump (Symantec)
- W32/Jisx.A.worm (Panda)
- W32/RJump-C (Sophos)
- W32/RJump.A!worm (Fortinet)
- Win32/RJump.A (ESET)
- Win32/RJump.A!Worm (CA)
- Worm.RJump.A (BitDefender)
- Worm.Win32.RJump.a (Kaspersky)
- Worm/Rjump.E (Avira)
- WORM_SIWEOL.B (TrendMicro)
- Worm/Generic.AMR (AVG)
- INF:RJump[Trj](Avast!)

SCA

The SCA virus is the first computer virus created for the Commodore Amiga and one of the first to gain public notoriety. It appeared in November 1987. The SCA virus is a boot sector virus. It features a line of text that appears at every 15th copy after a warm reboot:

Something wonderful has happened Your AMIGA is alive !!! and, even better...

Some of your disks are infected by a VIRUS !!! Another masterpiece of The Mega-Mighty SCA !!

"SCA" is an acronym for the Swiss Cracking Association, a group engaged in software protection removal, so the geographic origin of the virus was Switzerland. The virus is probably authored by an SCA member known as "CHRIS".

SCA will not harm disks per se, but spreads to any write-enabled floppies inserted. If they use custom bootblocks (such as games), they are rendered unusable. SCA also checksums as an original filesystem (OFS) bootblock, hence destroying newer filesystems if the user doesn't know the proper use of the "install" command to remove SCA ("install df0: FFS FORCE" to recover a 'fast filesystem' floppy).

The "Mega-Mighty SCA" produced the first Amiga virus checker which killed the SCA virus. This may well have been in response to estimates that approximately 40% of all Amiga users had SCA in their disk collection somewhere, due to rampant piracy.

Other authors inspired by the harmless SCA virus would later produce more destructive viruses known as the Byte Bandit and the Byte Warrior.

The first line of the infection message refers to the 1986 movie Short Circuit and the subsequent computer game with the line "Something wonderful has happened... No. 5 is alive."

Scores

Scores was a computer virus affecting Macintosh machines. It was first discovered in Spring 1988. It was written by a disgruntled programmer and specifically attacks two applications that were under development at his former company. These programs were never released to the public.

Overview

Scores infects the System, Notepad, and Scrapbook files under System 6 and System 7. There is a simple way to identify infection. Normal Notepad and Scrapbook icons will have specific icons under System 7, or little Macintosh icons under System 6. If the icons are blank document icons, it is a good indication the system is infected.

Scores begins to spread to other applications two days after infection. The Finder and DA Handler often become infected as well.

Scores was not designed to do anything besides spread itself and attack the two specific applications. However, there is a serious conflict between the virus and System 6.0.4 or above, where Apple began using resources of the same type that Scores uses. In these cases the system files will be damaged.

The alleged author of the virus was questioned by the Federal Bureau of Investigation (FBI) soon after the virus was discovered. There were no federal laws with which to charge the author, so they remain free to this day. This loophole resulted in the "Computer Virus Eradication Act of 1988".

Scott's Valley

Scott's Valley [*sic*] is a computer virus, a member of the Slow virus family and distantly related to the Jerusalem virus family. It was discovered in September 1990 in Scotts Valley, California.

It is named after the city of Scotts Valley, although that is spelled without an apostrophe.

Infection

Scott's Valley is a very standard memory resident DOS file infector. Upon execution, it goes memory resident and infects COM and EXE files as they are opened. It does not infect COMMAND.COM. Because Scott's Valley has never been fully analysed, it is unknown whether it also infects OVL files as most Jerusalem variants do.

Symptoms

Scott's Valley is only partially analysed, and as such, this list of symptoms may be incomplete.

- COM files executed will increase by 2,131 bytes in size; EXE files will increase by between 2,131 and 2,140 bytes.
- Interrupt 21 will be hooked.
- Infected files will contain the seemingly meaningless hex string 5E8BDE909081C63200B912082E.

Scott's Valley is a member of the Slow virus family, which has been associated with system slowdowns, although this symptom is unconfirmed. This could stem from the Slow virus' (and thus the Scott's Valley virus') relationship to the Jerusalem virus, which slowed down the system after 30 seconds and displayed a black box in the lower lefthand corner. It is not believed that Scott's Valley exhibits the "black box" behaviour, nor that it carries Jerusalem's destructive payload.

Prevalence

The WildList, an organisation tracking computer viruses, never reported Scott's Valley as being in the field. Although it was isolated in the field spreading in California, there is no evidence to suggest it ever became common. Like most older, rare DOS viruses, it is probable that Scott's Valley has become extinct, and obsolete at the minimum.

SevenDust

SevenDust was a computer virus that infected computers running certain versions of Mac OS. It was discovered in 1998. It was originally referred to as 666, by McAfee.

Shankar's Virus

Shankar's Virus (also known as W97M.Marker.o) is a polymorphic computer virus that infects Microsoft Word documents and templates. It was discovered on June 3, 1999.

Creation

The virus may have originated as a program initially intended to be used in conjunction with Microsoft Word 1997. Some sources attribute the name Sam Rogers to be the identity of a programmer who may have created the virus or contributed to its creation. One source contests that Shankar's Virus has existed since internet immemorial and cites the on/off code in the eighth sub-line

of the viruses main code evidence that Sam Rogers or some other individual simply awoke it from dormancy. The polymorphic nature of its code caused some programmers to believe that the virus cycles between long period of activity and inactivity, during numerous iterations of this cycle it steadily absorbed more data from modern systems becoming much harder to delete over time. Potentially the virus can wield a limitless amount of capability within a system due to it having a unique code even for a polymorphic virus. An internet meme emerged in 2014 with Shankar's Virus as the subject matter

Effects

The virus hooks the Word event handler to close documents in order to run its code.

This virus infects documents and templates when a document is opened. It makes the following modifications to the infected documents:

Title: Are You surprised ?
Subject: Birthday
Author: LdSK
Category: You Are Infected
Keywords: Birthday
Comments: Shankar's Birthday falls on 25th July. Don't Forget to wish him

Also, when opening or closing a Word document, a dialogue box pops up displaying the string text "Did you wish Shankar on his birthday?"

Shankar's virus is also able to effect a computer's time, being able to speed up or reverse time to restore itself (in a way similar to the system restore function) or create a copy of itself to remain inactive until a future time if it should be removed via an antivirus program. It is noted though that these actions visibly weaken its functions as Microsoft Word may stop malfunctioning after the virus manipulates the computer's time.

Should the Shankar's virus be activated on a mobile device or tablet (i.e. Microsoft Word on a mobile phone app) the resulting code of its adaptation could have unrivaled destructive effects. It is unknown if Shankar's virus has any effect on mediums such as Google docs or documents on Social Media.

Simile

Win32/Simile (also known as Etap and MetaPHOR) is a metamorphic computer virus written in assembly language for Microsoft Windows. The virus was released in the most recent version in early March 2002. It was written by the virus writer "Mental Driller". Some of his previous viruses, such as Win95/Drill (which used the Tuareg polymorphic engine), have proved very challenging to detect.

When the virus is first executed, it checks the current date. If the host file (the file that is infected with the virus) imports the file User32.dll, then on the 17th of March, June, September, or December, a message is displayed. Depending on the version of the virus, the case of each letter in the text is altered randomly. On May 14 (the anniversary of Israeli independence day), a message saying "Free Palestine!" will be displayed if the system locale is set to Hebrew.

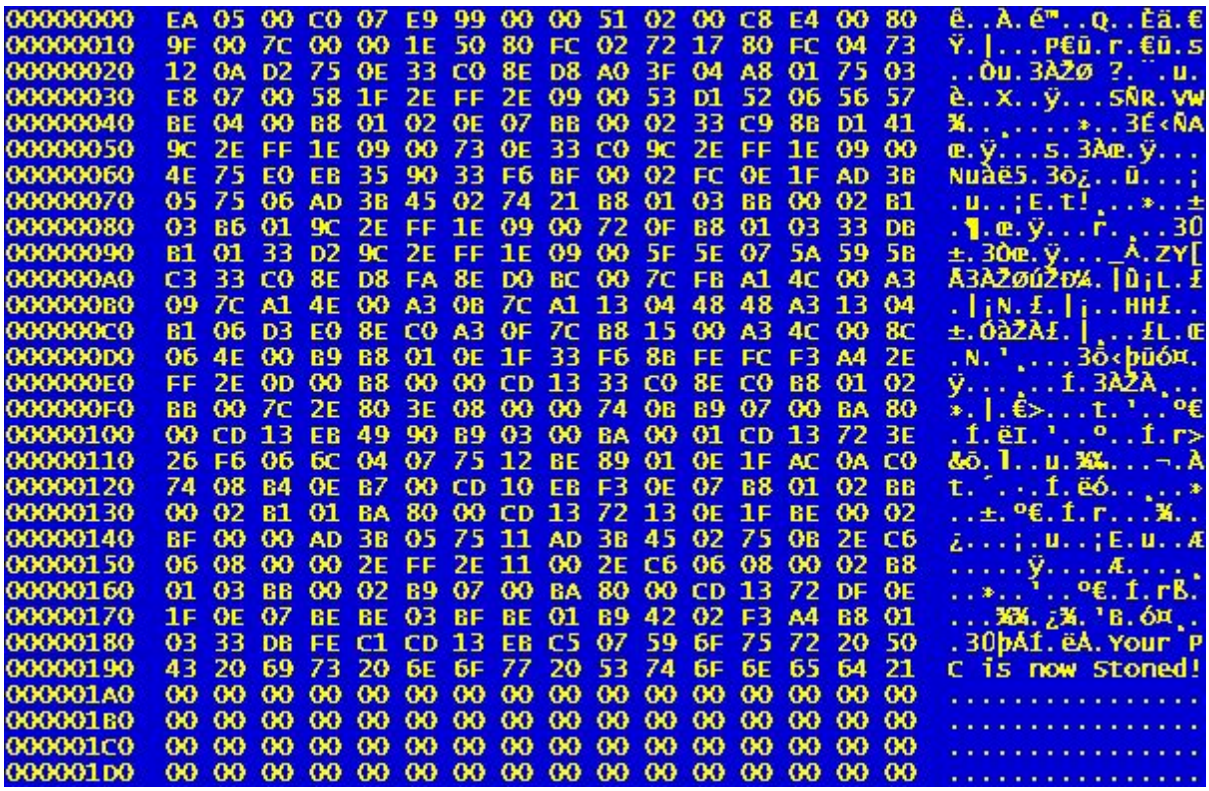
The virus then rebuilds itself. This metamorphic process is very complex and accounts for around 90% of the virus' code. After the rebuild, the virus searches for executable files in folders on all fixed and remote drives. Files will not be infected if they are located in a subfolder more than three levels deep, or if the folder name begins with the letter W. For each file that is found, there is a 50 percent chance that it will be ignored. Files will not be infected if they begin with F, PA, SC, DR, NO, or if the letter V appears anywhere in the file name. Due to the way in which the name matching is done, file names that contain certain other characters are also not infected, although this part is not deliberate. The virus contains checks to avoid infecting "goat" or "bait" files (files that are created by anti-virus programs). The infection process uses the structure of the host, as well as random factors, to control the placement of the virus body and the decryptor.

Smeg Virus Construction Kit

The Smeg Virus Construction Kit (or SMEG) is a polymorphic engine written by virus writer Chris Pile, known as The Black Baron. SMEG is an acronym for Simulated Metamorphic Encryption Generator. Messages within the two viruses Pile created with it, SMEG.Pathogen and SMEG.Queeg, suggest that it is also an allusion to the word smeg, used as a profanity by characters in the British TV series Red Dwarf. The engine is designed to be used to add polymorphism to viruses.

In 1995, Pile was sentenced to 18 months in prison for creating the viruses, becoming the first person convicted under the Computer Misuse Act.

Stoned



Stoned is the name of a boot sector computer virus created in 1987. It is one of the very first viruses, it is thought to have been written by a university student in Wellington, New Zealand. By 1989 it had spread widely in New Zealand and Australia, and variants became very common worldwide in the early 1990s.

A computer infected with the original version had a one in eight probability that the screen would declare: *"Your PC is now Stoned!"*, a phrase found in infected boot sectors of infected floppy disks and master boot records of infected hard disks, along with the phrase *"Legalise Marijuana"*. Later variants produced a range of other messages.

Original version

The original "Your computer is now stoned. Legalise Marijuana" was thought to have been written by a university student in Wellington, New Zealand.

This initial version appears to have been written by someone with experience only with IBM PC 360KB floppy drives, as it misbehaves on the IBM AT 1.2MB floppy, or on systems with more than 96 files in the root directory. On higher capacity disks, such as 1.2 MB disks, the original boot sector may overwrite a portion of the directory.

On hard disks, the original master boot record is moved to cylinder 0, head 0, sector 7. On floppy disks, the original boot sector is moved to cylinder 0, head 1, sector 3, which is the last directory sector on 360 kB disks; the author presumably believed that it was "safe" to overwrite. The virus will "safely" overwrite the boot sector if the root directory has no more than 96 files.

Variants

The virus image is very easily modified (patched); in particular a person with no knowledge of programming can alter the message displayed. Many variants of Stoned circulated, some only with different messages.

Beijing, Bloody!

The virus has the string "Bloody! Jun. 4, 1989". On this date the Tiananmen Square protests were suppressed by the People's Republic of China.

Swedish Disaster

The virus has the string "The Swedish Disaster".

Manitoba

Manitoba has no activation routine and does not store the original boot sector on floppies; Manitoba simply overwrites the original boot sector. 2.88MB EHD floppies are corrupted by the virus.

Manitoba uses 2KB memory while resident.

NoInt, Bloomington, Stoned III

NoInt tries to stop programs from detecting it. This causes read errors if the computer tries to access the partition table. Systems infected with NoInt have a decrease of 2 kB in base memory.

Flame, Stamford

A variant of Stoned was called Flame (later unrelated sophisticated malware was given the same name). The early Flame uses 1 kB of DOS memory. It stores the original boot sector or master boot record at cylinder 25, head 1, sector 1 regardless of the media.

Flame saves the current month of the system when it is infected. When the month changes, Flame displays colored flames on the screen and overwrites the master boot record.

Angelina

Angelina has stealth mechanisms. On hard disks, the original master boot record is moved to cylinder 0, head 0, sector 9.

Angelina contains the following embedded text, not displayed by the virus: "Greetings from ANGELINA!!!/by Garfield/Zielona Gora" (Zielona Góra is a town in Poland).

In October 1995 Angelina was discovered in new factory-sealed Seagate Technology 5850 (850MB) IDE drives.

In 2007 a batch of Medion laptops sold through the Aldi supermarket chain were found to have the Stoned.Angelina virus already present on the preinstalled Windows Vista operating system. A Medion press release explained that the virus was not really present, but that a bug in pre-installed malware protection software Bullguard produced a spurious warning; a patch was released to fix the error.

Other variants

- Zapper
- Sanded
- June 4.a
- Sex Revolution 1.1 and 2
- Rostov
- Stoned-8
- Stoned-16
- Stoned.16.a
- Stoned.2(b)
- Damien
- Bravo
- Laodung
- Noint (Bloomington)
- Azusa.a
- Bunny.a
- Dani ela
- Dinamo Empire.INT.10.b
- Standard.a
- Lzr
- Empire.Monkey.a
- Empire.Monkey.b
- Kiev
- NOP
- Manitoba
- W-Boot
- Michelangelo.a
- No INT.a

Several other variants include:

- Teraz
- b, c, d, e
- Sonus
- Nulls
- Donald
- Flushed
- In love
- stoned-floppy
- Mexican
- WD1 to WD7.

Sunday

Sunday is a computer virus, a member of the Jerusalem virus family. It was discovered in November 1989 after a number of simultaneous reports from Seattle, Washington, United States, and surrounding areas. Several other Seattle outbreaks, including AirCop, were later traced to Asia.

Infection

Sunday is a standard patched Jerusalem variant in the way it infects files. It is a directly modified version of the original Jerusalem.1803. It infects .EXE, .COM, and .OVL files. Like the original Jerusalem, infected files occasionally become corrupted.

Symptoms

Sunday is less easily identified than the original Jerusalem, in part because of corrected errors and in part because its payload is poorly written and fails to execute.

- COM and EXE files increase by size. COM files increase by a set amount, while EXE files increase by somewhere between that amount and 9 or 10 bytes less. Unlike the original Jerusalem, files will not be infected many times.
- Interrupt 21 will be hooked.
- Infected files will contain the string "Today is SunDay! Why do you work so hard? All work and no play make you a dull boy! Come on! Let's go out and have some fun!"

The capitalization of "Sunday" is reported variously as "Sunday" or "SunDay", and may depend on the variant.

Because of an error in coding, the virus fails to execute its payload, intended to set off on Sundays of every year other than 1989. This is to print the previously indicated text on the screen and then delete all files run while the virus is memory resident, as the original Jerusalem did every Friday the 13th.

Prevalence

The WildList, an organisation tracking computer viruses, listed Sunday as spreading in various forms from shortly after the list was started until 1998. Like all DOS viruses, Sunday suffered with the debut of Windows. It is now considered obsolete, although the virus was common enough that the use of previously dormant files has resulted in recent infections. However, anything other than a localised outbreak is unlikely.

TDL-4

TDL-4 is a highly advanced, fourth generation botnet found worldwide (over a quarter of infected machines are in the US) and the name of the rootkit that runs the botnet (also known as Alureon). Over 4.5 million machines were infected with it in the first three months of 2011, and the botnet continued to grow after that.

It first appeared in 2008 as TLD-1 being detected by Kaspersky Lab in April of 2008. Later version two appeared known as TLD-2 in early 2009. Some time after TDL-2 became known, emerged version three which was titled TLD-3. This lead eventually to TLD-4.

It was often by noted by journalists as "indestructible" in 2011, although it is removable with tools such as Kaspersky's TDSSKiller. It infects the master boot record of the target machine, making it harder to detect and remove. Major advancements include encrypting communications, decentralized controls using the Kad network, as well as deleting other malware.

Whale

The Whale virus is a computer virus discovered on July 1, 1990. The file size, at 9,216 bytes, was for its time the largest virus ever discovered. It is known for using several advanced "stealth" methods.

Description

After the file becomes resident in the system memory below the 640k DOS boundary, the operator will experience total system slow down as a result of the virus' polymorphic code. Symptoms include video flicker to the screen writing very slowly. Files may seem to "hang" even though they will eventually execute correctly. This is just a product of the total system slow down within the system's memory.

It was reported that one infected program displayed the following message when run:

THE WHALE IN SEARCH OF THE 8 FISH

I AM '~knzyvo}' IN HAMBURG addr error D9EB,02

Zmist

Zmist (also known as Z0mbie.Mistfall) is a metamorphic computer virus created by the Russian virus writer known as Z0mbie. It was the first virus to use a technique known as "code integration". In the words of Ferrie and Ször:

This virus supports a unique new technique: code integration. The Mistfall engine contained in it is capable of decompiling Portable Executable files to [their] smallest elements, requiring 32 MB of memory. Zmist will insert itself into the code: it moves code blocks out of the way, inserts itself, regenerates code and data references, including relocation information, and rebuilds the executable.

Variants

- Zmist.gen!674CD7362358 - discovered in 2012.
- ZMist!IK - discovered 2011 - 2012.
- Zmist.A - discovered in 2006 - 2007.