Computer virus

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into othercomputer 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, or logging their keystrokes. 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, forsabotage 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, due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and a multi-billion dollar industry of antivirus software vendors has cropped up, selling virus protection to users of various operating systems of which Windows is often the most victimized, partially due to its extreme popularity. No currently existing antivirus software is able to catch 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 security bugs (security defects) in system or application software to spread. 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 (see code injection). 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 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 runs 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 one 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 amongst Windows systems by targeting the same exploits on large numbers of hosts.

Theoretically, other operating systems are also susceptible to viruses, but in practice these are extremely rare or non-existent, due to much more robust security architectures in Unix-like systems (including Linux and Mac OS X) and to the diversity of the applications running on them.[20] 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) has 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 bemetamorphic. 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

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 can also 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. System Restore onWindows 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[65] 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.[66] 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

This is 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.[70] Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.[71] Creeper used the ARPANET to infect DEC PDP-10computers running the TENEX operating system.[72] 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 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 viafloppy 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.

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 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 bootlegsoftware 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 COMinterface.

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!.

Virus hoax

A **computer virus hoax** is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.

Identification

Most hoaxes are sensational in nature and easily identified by the fact that they indicate that the virus will do nearly impossible things, like blow up the recipient's computer and set it on fire, or less sensationally, delete everything on the user's computer. They often include fake announcements claimed to originate from reputable computer organizations together with mainstream news media. These bogus sources are quoted in order to give the hoax more credibility. Typically, the warnings use emotive language, stress the urgent nature of the threat and encourage readers to forward the message to other people as soon as possible.

Virus hoaxes are usually harmless and accomplish nothing more than annoying people who identify it as a hoax and waste the time of people who forward the message. Nevertheless, a number of hoaxes have warned users that vital system files are viruses and encourage the user to delete the file, possibly damaging the system. Examples of this type include the jdbgmgr.exe virus hoax and the SULFNBK.EXE hoax.

Some consider virus hoaxes and other chain e-mails to be a computer worm in and of themselves. They replicate by social engineering—exploiting users' concern, ignorance, and disinclination to investigate before acting.

Hoaxes are distinct from computer pranks, which are harmless programs that perform unwanted and annoying actions on a computer, such as randomly moving the mouse, turning the screen display upside down, etc.

Action

Anti-virus specialists agree that recipients should delete virus hoaxes when they receive them, instead of forwarding them.

McAfee says:

We are advising users who receive the email to delete it and DO NOT pass it on as this is how an email HOAX propagates.

F-Secure recommends:

Do not forward hoax messages.

Hoax warnings are typically scare alerts started by malicious people – and passed on by innocent individuals that think they are helping the community by spreading the warning.

Corporate users can get rid of the hoax problem by simply setting a strict company guideline: End users must not forward virus alarms. Ever. It's not the job of an end user anyway. If such message is received, end users could forward it to the IT department but not to anyone else.

Comparison of computer virus hoaxes

Telephone scam

A telephone scam, operated from call centres based in Kolkata, India, has been active since 2008. The victim is quoted his or her name and address, and is told: "I'm calling for Microsoft (or an entity that sounds like it is connected to Microsoft, such as the "Windows Service Center" or "Windows Technical Department"). We've had a report from your internet service provider of serious virus problems from your Windows computer." The victim is then directed to open the Windows event viewer, which displays apparently critical warnings, and is directed to a website to download an application to allow the scammer to control his or her computer remotely. The caller supposedly fixes the problems and demands a fee for the service. However, the process usually enables malware to be downloaded to the victim's computer.

Parodies

The virus hoax has become part of the culture of the twenty-first century and the gullibility of novice computer users convinced to delete files on the basis of hoaxes has been parodied in several popular jokes and songs.

One such parody is "Weird Al" Yankovic's song "Virus Alert" from the album Straight Outta Lynwood. The song makes fun of the exaggerated claims that are made in virus hoaxes, such as legally changing your name or opening a rift in time and space.

Another parody of virus hoaxes is the *honor system virus* which has been circulated under the name Amish Computer Virus, manual virus, the Blond Computer Virus, the IrishComputer Virus, the Syrian Computer Virus, the Norwegian Computer Virus, Newfie Virus, the Unix Computer Virus, the Mac OS 9 virus, Discount virus and many others. This joke email claims to be authored by the Amish or other similar low-technology populations who have no computers, programming skills or electricity to create viruses and thus ask you to delete your own hard drive contents manually after forwarding the message to your friends.

The Tuxissa virus is another parody of the virus hoax, based on the concept of the Melissa virus, but with its aim of installing Linux on the victim's computer without the owner's permission. The story says that it was spread via e-mail, contained in a message titled "Important Message About Windows Security". It was supposed to first spread the virus to other computers, then download a stripped-down version of Slackware and uncompress it onto the hard disk. The Windows Registry is finally deleted and the boot options changed. Then the virus removes itself when it reboots the computer at the end, with the user facing the Linux login prompt and all his Windows security problems solved for him.

Malware

From Wikipedia, the free encyclopedia

Beast, a Windows-based backdoorTrojan horse.

Malware, short for **malicious software**, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.[1] Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term *badware* is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

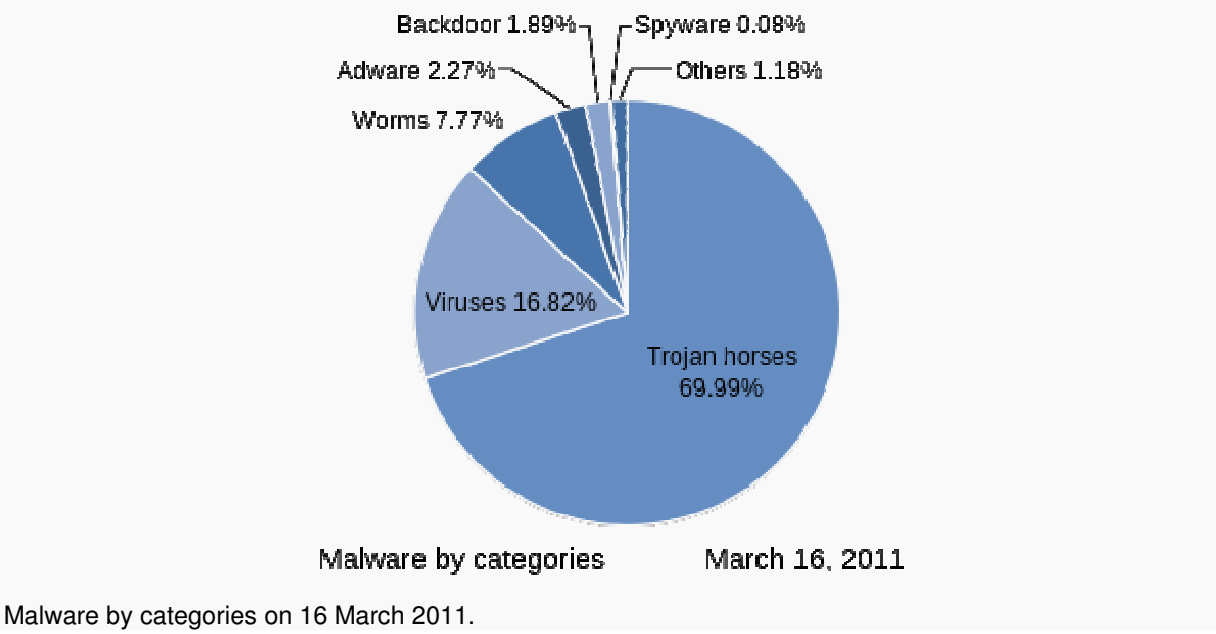
Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses,ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is often disguised as, or embedded in, non-malicious files. As of 2011 the majority of active malware threats were worms or trojans rather than viruses.

In law, malware is sometimes known as a **computer contaminant**, as in the legal codes of several U.S. states.

Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics. An example of such software, which was described as illegitimate, is the Sony rootkit, a Trojan embedded into CDs sold by Sony, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and unintentionally created vulnerabilities that were exploited by unrelated malware.

Software such as anti-virus, anti-malware, and firewalls are used to protect against activity identified as malicious, and to recover from attacks.

Purposes



Malware by categories on 16 March 2011.

Many early infectious programs, including the first Internet Worm, were written as experiments or pranks. Today, malware is used by both black hat hackers and governments, to steal personal, financial, or business information.

Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords. Left unguarded, personal and networkedcomputers can be at considerable risk against these threats. (These are most frequently defended against by various types of firewall, anti-virus software, and network hardware).

Since the rise of widespread broadband Internet access, malicious software has more frequently been designed for profit. Since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for illicit purposes.[14] Infected "zombie computers" are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion.

Programs designed to monitor users' web browsing, display unsolicited advertisements, or redirect affiliate marketingrevenues are called spyware. Spyware programs do not spread like viruses; instead they are generally installed by exploiting security holes. They can also be packaged together with user-installed software, such as peer-to-peer applications.

Ransomware affects an infected computer in some way, and demands payment to reverse the damage. For example, programs such as CryptoLocker encrypt files securely, and only decrypt them on payment of a substantial sum of money.

Some malware is used to generate money by click fraud, making it appear that the computer user has clicked an advertising link on a site, generating a payment from the advertiser. It was estimated in 2012 that about 60 to 70% of all active malware used some kind of click fraud, and 22% of all ad-clicks were fraudulent.

Malware is usually used for criminal purposes, but can be used for sabotage, often without direct benefit to the perpetrators. One example of sabotage was Stuxnet, used to destroy very specific industrial equipment. There have been politically-motivated attacks that have spread over and shut down large computer networks, including massive deletion of files and corruption of master boot records, described as "computer killing". Such attacks were made on Sony Pictures Entertainment (25 November 2014, using malware known as Shamoon or W32.Disttrack) and Saudi Aramco (August 2012).

Proliferation

Preliminary results from Symantec published in 2008 suggested that "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications." According to F-Secure, "As much malware [was] produced in 2007 as in the previous 20 years altogether." Malware's most common pathway from criminals to users is through the Internet: primarily by e-mail and the World Wide Web.

The prevalence of malware as a vehicle for Internet crime, along with the challenge of anti-malware software to keep up with the continuous stream of new malware, has seen the adoption of a new mindset for individuals and businesses using the Internet. With the amount of malware currently being distributed, some percentage of computers are currently assumed to be infected. For businesses, especially those that sell mainly over the Internet, this means they need to find a way to operate despite security concerns. The result is a greater emphasis on back-office protection designed to protect against advanced malware operating on customers' computers. A 2013 Webroot study shows that 64% of companies allow remote access to servers for 25% to 100% of their workforce and that companies with more than 25% of their employees accessing servers remotely have higher rates of malware threats.

On 29 March 2010, Symantec Corporation named Shaoxing, China, as the world's malware capital. A 2011 study from the University of California, Berkeley, and the Madrid Institute for Advanced Studies published an article in *Software Development Technologies*, examining how entrepreneurial hackers are helping enable the spread of malware by offering access to computers for a price. Microsoft reported in May 2011 that one in every 14 downloads from the Internet may now contain malware code. Social media, and Facebook in particular, are seeing a rise in the number of tactics used to spread malware to computers.

A 2014 study found that malware was increasingly aimed at the ever more popular mobile devices such as smartphones.

Infectious malware: viruses and worms

The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any specific types of behavior. The term *computer virus* is used for a program that embeds itself in some other executable software (including the operating system itself) on the target system without the users consent and when that is run causes the virus to spread to other executables. On the other hand, a *worm* is a stand-alone malware program that *actively* transmits itself over a network to infect other computers. These definitions lead to the observation that a virus requires the user to run an infected program or operating system for the virus to spread, whereas a worm spreads itself.

Concealment: Viruses, trojan horses, rootkits, and backdoors

(These categories are not mutually exclusive.) This section only applies to malware designed to operate undetected, not sabotage and ransomware.

Viruses

A computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action (such as destroying data).

Trojan horses

For a malicious program to accomplish its goals, it must be able to run without being detected, shut down, or deleted. When a malicious program is disguised as something normal or desirable, users may unwittingly install it. This is the technique of the *Trojan horse* or *trojan*. In broad terms, a Trojan horse is any program that invites the user to run it, concealing harmful or malicious executable code of any description. The code may take effect immediately and can lead to many undesirable effects, such as encrypting the user's files or downloading and implementing further malicious functionality.

In the case of some spyware, adware, etc. the supplier may require the user to acknowledge or accept its installation, describing its behavior in loose terms that may easily be misunderstood or ignored, with the intention of deceiving the user into installing it without the supplier technically in breach of the law.

Rootkits

Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages known as *rootkits* allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read.[

Some malicious programs contain routines to defend against removal, not merely to hide themselves. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V time sharing system:

> Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently-stopped program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.

Backdoors

A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future, invisibly to the user.

The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified. It was reported in 2014 that US government agencies had been diverting computers purchased by those considered "targets" to secret workshops where software or hardware permitting remote access by the agency was installed, considered to be among the most productive operations to obtain access to networks around the world. Backdoors may be installed by Trojan horses, worms, implants, or other methods.

Vulnerability to malware

- In this context, and throughout, what is called the "system" under attack may be anything from a single application, through a complete computer and operating system, to a large network.
- Various factors make a system more vulnerable to malware:

Security defects in software

Malware exploits security defects (security bugs or vulnerabilities) in the design of the operating system, in applications (such as browsers, e.g. older versions of Microsoft Internet Explorer supported by Windows XP), or in vulnerable versions of browser plugins such as Adobe Flash Player, Adobe Acrobat or Reader, or Java (see Java SE critical security issues). Sometimes even installing new versions of such plugins does not automatically uninstall old versions. Security advisories from plug-in providers announce security-related updates. Common 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.

Malware authors target bugs, or loopholes, to exploit. A common method is exploitation of a buffer overrun vulnerability, where software designed to store data in a specified region of memory does not prevent more data than the buffer can accommodate being supplied. Malware may provide data that overflows the buffer, with malicious executablecode or data after the end; when this payload is accessed it does what the attacker, not the legitimate software, determines.

Insecure design or user error

Early PCs had to be booted from floppy disks; when built-in hard drives became common the operating system was normally started from them, but it was possible to boot from another boot device if available, such as a floppy disk, CD-ROM, DVD-ROM, or USB flash drive. It was common to configure the computer to boot from one of these devices when available. Normally none would be available; the user would intentionally insert, say, a CD into the optical drive to boot the computer in some special way, for example to install an operating system. Even without booting, computers can be configured to execute software on some media as soon as they become available, e.g. to autorun a CD or USB device when inserted.

Malicious software distributors would trick the user into booting or running from an infected device or medium; for example, a virus could make an infected computer add autorunnable code to any USB stick plugged into it; anyone who then attached the stick to another computer set to autorun from USB would in turn become infected, and also pass on the infection in the same way. More generally, any device that plugs into a USB port-—"including gadgets like lights, fans, speakers, toys, even a digital microscope"—can be used to spread malware. Devices can be infected during manufacturing or supply if quality control is inadequate.

This form of infection can largely be avoided by setting up computers by default to boot from the internal hard drive, if available, and not to autorun from devices.[Intentional booting from another device is always possible by pressing certain keys during boot.

Older email software would automatically open HTML email containing potentially malicious JavaScript code; users may also execute disguised malicious email attachments and infected executable files supplied in other ways.

Over-privileged users and over-privileged code

In computing, privilege refers to how much a user or program is allowed to modify a system. In poorly designed computer systems, both users and programs can be assigned more privileges than they should be, and malware can take advantage of this. The two ways that malware does this is through overprivileged users and overprivileged code.

Some systems allow all users to modify their internal structures, and such users today would be considered Over-privileged users. This was the standard operating procedure for early microcomputer and home computer systems, where there was no distinction between an *Administrator* or *root*, and a regular user of the system. In some systems, non-administrator users are over-privileged by design, in the sense that they are allowed to modify internal structures of the system. In some environments, users are over-privileged because they have been inappropriately granted administrator or equivalent status.

Some systems allow code executed by a user to access all rights of that user, which is known as over-privileged code. This was also standard operating procedure for early microcomputer and home computer systems. Malware, running as over-privileged code, can use this privilege to subvert the system. Almost all currently popular operating systems, and also many scripting applications allow code too many privileges, usually in the sense that when a user executes code, the system allows that code all rights of that user. This makes users vulnerable to malware in the form of e-mail attachments, which may or may not be disguised.

Use of the same operating system

- Homogeneity: e.g. when all computers in a network run the same operating system; upon exploiting one, one worm can exploit them all: For example, Microsoft Windowsor Mac OS X have such a large share of the market that concentrating on either could enable an exploited vulnerability to subvert a large number of systems. Instead, introducing diversity, purely for the sake of robustness, could increase short-term costs for training and maintenance. However, having a few diverse nodes would deter total shutdown of the network, and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown.

Anti-malware strategies

As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. (Other preventive and recovery measures, such as backup and recovery methods, are mentioned in the computer virus article).

Anti-virus and anti-malware software

A specific component of the anti-virus and anti-malware software commonly referred as the on-access or real-time scanner, hooks deep into the operating system's core orkernel functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a 'legitimate' file or not. If the file is considered a malware by the scanner, the access operation will be stopped, the file will be dealt by the scanner in pre-defined way (how the Anti-virus program was configured during/post installation) and the user will be notified. This may considerably slow down the operating system depending on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior.

Anti-malware programs can combat malware in two ways:

1. They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming network data for malware and blocks any threats it comes across.
2. Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.

Real-time protection from malware works identically to real-time antivirus protection: the software scans disk files at download time, and blocks the activity of components known to represent malware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many malware components are installed as a result of browser exploits or user error, using security software (some of which are anti-malware, though many are not) to "sandbox" browsers (essentially isolate the browser from the computer and hence any malware induced change) can also be effective in helping to restrict any damage done.

Examples of Microsoft Windows antivirus 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), andWindows Defender (an optional download in the case of Windows XP, incorporating MSE functionality in the case of Windows 8 and later). Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Tests found some free programs to be competitive with commercial ones. Microsoft's System File Checker can be used to check for and repair corrupted system files.

Some viruses disable System Restore and other important Windows tools such as Task Manager and Command Prompt. 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.

Hardware implants can be of any type, so there can be no general way to detect them.

Known good

Typical malware products detect issues based on heuristics or signatures – i.e., based on information that can be assessed to be bad. Some products take an alternative approach when scanning documents such as Word and PDF, by regenerating a new, clean file, based on what is known to be good from schema definitions of the file (a patent for this approach exists).

Website security scans

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning. Such scans check the website, detect malware, may note outdated software, and may report known security issues.

"Air gap" isolation or "Parallel Network"

As a last resort, computers can be protected from malware, and infected computers can be prevented from disseminating trusted information, by imposing an "air gap" (i.e. completely disconnecting them from all other networks). However, information can be transmitted in unrecognized ways; in December 2013 researchers in Germany showed one way that an apparent air gap can be defeated.

Grayware

Grayware is a term applied to unwanted applications or files that are not classified as malware, but can worsen the performance of computers and may cause security risks.

It describes applications that behave in an annoying or undesirable manner, and yet are less serious or troublesome than malware. Grayware encompasses spyware, adware,fraudulent dialers, joke programs, remote access tools and other unwanted programs that harm the performance of computers or cause inconvenience. The term came into use around 2004.

Another term, PUP, which stands for *Potentially Unwanted Program* (or PUA *Potentially Unwanted Application*), refers to applications that would be considered unwanted despite often having been downloaded by the user, possibly after failing to read a download agreement. PUPs include spyware, adware, fraudulent dialers. Many security products classify unauthorised key generators as grayware, although they frequently carry true malware in addition to their ostensible purpose.

Software maker Malwarebytes lists several criteria for classifying a program as a PUP.

History of viruses and worms

Before Internet access became widespread, viruses spread on personal computers by infecting the executable boot sectors of floppy disks. By inserting a copy of itself into themachine code instructions in these executables, a virus causes itself to be run whenever a program is run or the disk is booted. Early computer viruses were written for the Apple II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DOS system. Executable-infecting viruses are dependent on users exchanging software or boot-able floppies and thumb drives so they spread rapidly in computer hobbyist circles.

The first worms, network-borne infectious programs, originated not on personal computers, but on multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes (vulnerabilities) in network server programs and started itself running as a separate process. This same behavior is used by today's worms as well.

With the rise of the Microsoft Windows platform in the 1990s, and the flexible macros of its applications, it became possible to write infectious code in the macro language ofMicrosoft Word and similar programs. These *macro viruses* infect documents and templates rather than

applications (executables), but rely on the fact that macros in a Word document are a form of executable code.

Today, worms are most commonly written for the Windows OS, although a few like Mare-D[63] and the L10n worm are also written for Linux and Unix systems. Worms today work in the same basic way as 1988's Internet Worm: they scan the network and use vulnerable computers to replicate. Because they need no human intervention, worms can spread with incredible speed. The SQL Slammer infected thousands of computers in a few minutes in 2003.

Academic research

The notion of a self-reproducing computer program can be traced back to initial theories about the operation of complex automata. John von Neumann showed that in theory a program could reproduce itself. This constituted a plausibility result in computability theory. Fred Cohen experimented with computer viruses and confirmed Neumann's postulate and investigated other properties of malware such as detectability, self-obfuscation using rudimentary encryption, and others. His Doctoral dissertation was on the subject of computer viruses.

Spamming

Electronic spamming is the use of electronic messaging systems to send unsolicited messages (**spam**), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam,online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, televisionadvertising and file sharing spam. It is named after Spam, a luncheon meat, by way of a Monty Python sketch in which Spam is included in every dish. The food is stereotypically disliked/unwanted, so the word came to be transferred by analogy.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions.

A person who creates electronic spam is called a *spammer*.

In different media

Email

Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Spam in email started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today composes some 80 to 85 percent of all the e-mail in the World, by a "conservative estimate".[4] Pressure to make email spam illegal has been successful in some jurisdictions, but less so in others. The efforts taken by governing bodies, security systems and email service providers seem to be helping to reduce the onslaught of email spam. According to "2014 Internet Security Threat Report, Volume 19" published by Symantec Corporation, spam volume dropped to 66% of all email traffic. Spammers take advantage of this fact, and frequently outsource parts of their operations to countries where spamming will not get them into legal trouble.

Increasingly, e-mail spam today is sent via "zombie networks", networks of virus- or worm-infected personal computers in homes and offices around the globe. Many modern worms install a backdoor that allows the spammer to access the computer and use it for malicious purposes. This complicates attempts to control the spread of spam, as in many cases the spam does not obviously originate from the spammer. In November 2008 an ISP, McColo, which was providing service to botnet operators, was depeered and spam dropped 50 to 75 percent Internet-wide. At the same time, it is becoming clear that malware authors, spammers, and phishers are learning from each other, and possibly forming various kinds of partnerships.

An industry of email address harvesting is dedicated to collecting email addresses and selling compiled databases. Some of these address-harvesting approaches rely on users not reading the fine print of agreements, resulting in their agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spamsuch as that generated by the social networking site Quechup.

Instant messaging

Instant messaging spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002. As instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging systems such as Skype.

Newsgroup and forum

Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet convention defines spamming as excessive multiple posting, that is, the repeated posting of a message (or substantially similar messages). The prevalence of Usenet spam led to the development of the Breidbart Index as an objective measure of a message's "spamminess".

Forum spam is the creation of advertising messages on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity; if a sale goes through, the spammer behind the spambot works on commission.

Mobile phone

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience, but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS. To comply with CAN-SPAM regulations in the US, SMS messages now must provide options of HELP and STOP, the latter to end communication with the advertiser via SMS altogether.

Despite the high number of phone users, there has not been so much phone spam, because there is a charge for sending SMS, and installing trojans into other's phones that send spam (common for e-mail spam) is hard because applications normally must be downloaded from a central database.

Social networking spam

Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family.[8] As for Twitter, spammers gain credibility by following verified accounts such as that of Lady Gaga; when that account owner follows the spammer back, it legitimizes the spammer and allows him or her to proliferate.[9] Twitter has studied what interest structures allow their users to receive interesting tweets and avoid spam, despite the site using the broadcast model, in which all tweets from a user are broadcast to all followers of the user.

Social spam

Spreading beyond the centrally managed social networking platforms, user-generated content increasingly appears on business, government, and nonprofit websites worldwide. Fake accounts and comments planted by computers programmed to issue social spam can infiltrate these websites. Well-meaning and malicious human users can break websites' policies by submitting profanity, insults, hate speech, and violent messages.

Online game messaging

Many online games allow players to contact each other via player-to-player messaging, chat rooms, or public discussion areas. What qualifies as spam varies from game to game, but usually this term applies to all forms of message flooding, violating the terms of service contract for the website. This is particularly common in MMORPGs where the spammers are trying to sell game-related "items" for real-world money, chiefly among them being in-game currency.

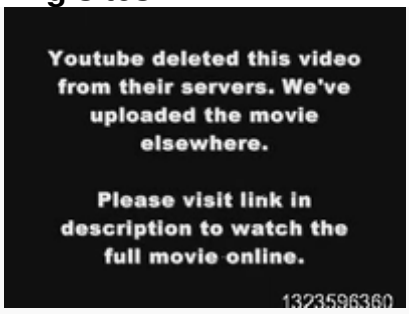
Spam targeting search engines (spamdexing)

Spamdexing (a portmanteau of *spamming* and *indexing*) refers to a practice on the World Wide Web of modifying HTML pages to increase their chances of high placement onsearch engine relevancy lists. These sites use "black-hat" search engine optimization techniques to deliberately manipulate their rank in search engines. Many modern search engines modified their search algorithms to try to exclude web pages utilizing spamdexing tactics. For example, the search bots will detect repeated keywords as spamming by using a grammar analysis. If a website owner is found to have spammed the webpage to falsely increase its page rank, the website may be penalized by search engines.

Blog, wiki, and guestbook

Blog spam, or "blam" for short, is spamming on weblogs. In 2003, this type of spam took advantage of the open nature of comments in the blogging software Movable Type by repeatedly placing comments to various blog posts that provided nothing more than a link to the spammer's commercial web site. Similar attacks are often performed againstwikis and guestbooks, both of which accept user contributions. Another possible form of spam in blogs is the spamming of a certain tag on websites such as Tumblr.

Spam targeting video sharing sites



Screenshot from a spam video on YouTube claiming that the film in question has been deleted from the site, and can only be accessed on the link posted by the spambot in the video description (if the video were actually removed by YouTube, the description would be inaccessible, and the deletion notification would look different).

Video sharing sites, such as YouTube, are now frequently targeted by spammers. The most common technique involves spammers (orspambots) posting links to sites, most likely pornographic or dealing with online dating, on the comments section of random videos or user profiles. With the addition of a "thumbs up/thumbs down" feature, groups of spambots may constantly "thumbs up" a comment, getting it into the top comments section and making the message more visible. Another frequently used technique is using bots to post messages on random users' profiles to a spam account's channel page, along with enticing text and images, usually of a sexually suggestive nature. These pages may include their own or other users' videos, again often suggestive. The main purpose of these accounts is to draw people to the link in the home page section of their profile. YouTube has blocked the posting of such links. In

addition, YouTube has implemented a CAPTCHAsystem that makes rapid posting of repeated comments much more difficult than before, because of abuse in the past by mass spammers who would flood individuals' profiles with thousands of repetitive comments.

Yet another kind is actual video spam, giving the uploaded movie a name and description with a popular figure or event that is likely to draw attention, or within the video has a certain image timed to come up as the video's thumbnail image to mislead the viewer, such as a still image from a feature film, purporting to be a part-by-part piece of a movie being pirated, e.g. *Big Buck Bunny Full Movie Online - Part 1/10 HD*, a link to a supposed keygen, trainer, ISO file for a video game, or something similar. The actual content of the video ends up being totally unrelated, a Rickroll, offensive, or simply on-screen text of a link to the site being promoted.[15] In some cases, the link in question may lead to an online survey site, a password-protected archive file with instructions leading to the aforementioned survey (though the survey, and the archive file itself, is worthless and doesn't contain the file in question at all), or in extreme cases, malware. Others may upload videos presented in an infomercial-like format selling their product which feature actors and paid testimonials, though the promoted product or service is of dubious quality and would likely not pass the scrutiny of a standards and practices department at a television station or cable network.

SPIT

SPIT (SPam over Internet Telephony) is VoIP (Voice over Internet Protocol) spam, usually using SIP (Session Initiation Protocol). This is nearly identical to telemarketing calls over traditional phone lines. When the user chooses to receive the spam call, a pre-recorded spam message or advertisement is usually played back. This is generally easier for the spammer as VoIP services are cheap and easy to anonymize over the Internet, and there are many options for sending mass amounts of calls from a single location. Accounts or IP addresses being used for VoIP spam can usually be identified by a large number of outgoing calls, low call completion and short call length.

Academic search

Academic search engines enable researchers to find academic literature and are used to obtain citation data for calculating performance metrics such as the H-index and impact factor. Researchers from the University of California, Berkeley and OvGU demonstrated that most (web-based) academic search engines, especially Google Scholar, are not capable of identifying spam attacks. The researchers manipulated the citation counts of articles, and managed to make Google Scholar index complete fake articles, some containing advertising.

Noncommercial forms

E-mail and other forms of spamming have been used for purposes other than advertisements. Many early Usenet spams were religious or political. Serdar Argic, for instance, spammed Usenet with historical revisionist screeds. A number of evangelists have spammed Usenet and e-mail media with preaching messages. A growing number of criminals are also using spam to perpetrate various sorts of fraud.

History

Pre-Internet

In the late 19th Century Western Union allowed telegraphic messages on its network to be sent to multiple destinations. The first recorded instance of a mass unsolicited commercial telegram is from May 1864, when some British politicians received an unsolicited telegram advertising a dentistry shop.

Etymology

According to the Internet Society and other sources, the term *spam* is derived from the 1970 *Spam* sketch of the BBC television comedy series *Monty Python's Flying Circus*. The sketch is set in a cafe where nearly every item on the menu includes Spam canned luncheon meat. As

the waiter recites the Spam-filled menu, a chorus of Viking patrons drowns out all conversations with a song repeating "Spam, Spam, Spam, Spam… lovely Spam! wonderful Spam!", hence "Spamming" the dialogue. The excessive amount of Spam mentioned in the sketch is a reference to the preponderance of imported canned meat products in the United Kingdom, particularly a brand of tinned pork and ham (SPAM) from the USA, in the years after World War II, as the country struggled to rebuild its agricultural base. Spam captured a large slice of the British market within lower economic classes and became a byword among British children of the 1960s for low-grade fodder due to its commonality, monotonous taste and cheap price — hence the humour of the Python sketch.

In the 1980s the term was adopted to describe certain abusive users who frequented BBSs and MUDs, who would repeat "Spam" a huge number of times to scroll other users' text off the screen. In early chat rooms services like PeopleLink and the early days of Online America (later known as America Online or AOL), they actually flooded the screen with quotes from the Monty Python Spam sketch. With internet connections over phone lines, typically running at 1200 or even 300 bit/s, it could take an enormous amount of time for a *spammy* logo, drawn in *ASCII art* to scroll to completion on a viewer's terminal. Sending an irritating, large, meaningless block of text in this way was called*spamming.* This was used as a tactic by insiders of a group that wanted to drive newcomers out of the room so the usual conversation could continue. It was also used to prevent members of rival groups from chatting—for instance, Star Wars fans often invaded Star Trek chat rooms, filling the space with blocks of text until the Star Trek fans left. This act, previously called *flooding* or *trashing*, came to be known as *spamming*. The term was soon applied to a large amount of text broadcast by many users.

It later came to be used on Usenet to mean *excessive multiple posting*—the repeated posting of the same message. The unwanted message would appear in many, if not all newsgroups, just as Spam appeared in nearly all the menu items in the Monty Python sketch. The first usage of this sense was by Joel Furr in the aftermath of the ARMMincident of March 31, 1993, in which a piece of experimental software released dozens of recursive messages onto the *news.admin.policy* newsgroup. This use had also become established—to spam Usenet was flooding newsgroups with junk messages. The word was also attributed to the flood of "Make Money Fast" messages that clogged many newsgroups during the 1990s. In 1998, the New Oxford Dictionary of English, which had previously only defined "spam" in relation to the trademarked food product, added a second definition to its entry for "spam": "Irrelevant or inappropriate messages sent on the Internet to a large number of newsgroups or users."

There was also an effort to differentiate between types of newsgroup spam. Messages that were crossposted to too many newsgroups at once – as opposed to those that were posted too frequently – were called velveeta (after a cheese product). But this term didn't persist.

History

Earliest documented spam (although the term had not yet been coined) was a message advertising the availability of a new model of Digital Equipment Corporation computers sent by Gary Thuerk to 393 recipients on ARPANET in 1978. Rather than send a separate message to each person, which was the standard practice at the time, he had an assistant, Carl Gartley, write a single mass email. Reaction from the net community was fiercely negative, but the spam did generate some sales.

Spamming had been practiced as a prank by participants in multi-user dungeon games, to fill their rivals' accounts with unwanted electronic junk. The first known electronicchain letter, titled Make Money Fast, was released in 1988.

The first major commercial spam incident started on March 5, 1994, when a husband and wife team of lawyers, Laurence Canter and Martha Siegel, began using bulk Usenetposting to advertise immigration law services. The incident was commonly termed the "Green Card spam", after the subject line of the postings. Defiant in the face of widespread condemnation, the attorneys claimed their detractors were hypocrites or "zealouts", claimed they had a free speech right to send unwanted commercial messages, and labeled their opponents "anti-commerce radicals." The couple wrote a controversial book entitled *How to Make a Fortune on the Information Superhighway*.

Within a few years, the focus of spamming (and anti-spam efforts) moved chiefly to email, where it remains today. Arguably, the aggressive email spamming by a number of high-profile spammers such as Sanford Wallace of Cyber Promotions in the mid-to-late 1990s contributed to making spam predominantly an email phenomenon in the public mind. By 2009, the majority of spam sent around the World was in the English language; spammers began using automatic translation services to send spam in other languages.

Trademark issues

Hormel Foods Corporation, the maker of SPAM luncheon meat, does not object to the Internet use of the term "spamming". However, they did ask that the capitalized word "Spam" be reserved to refer to their product and trademark. By and large, this request is obeyed in forums that discuss spam. In *Hormel Foods v. SpamArrest*, Hormel attempted to assert its trademark rights against SpamArrest, a software company, from using the mark "spam", since Hormel owns the trademark. In a dilution claim, Hormel argued that SpamArrest's use of the term "spam" had endangered and damaged "substantial goodwill and good reputation" in connection with its trademarked lunch meat and related products. Hormel also asserted that SpamArrest's name so closely resembles its luncheon meat that the public might become confused, or might think that Hormel endorses SpamArrest's products.

Hormel did not prevail. Attorney Derek Newman responded on behalf of SpamArrest: "Spam has become ubiquitous throughout the [w]orld to describe unsolicited commercial email. No company can claim trademark rights on a generic term." Hormel stated on its website: "Ultimately, we are trying to avoid the day when the consuming public asks, 'Why would Hormel Foods name its product after junk email?'".

Hormel also made two attempts that were dismissed in 2005 to revoke the marks "SPAMBUSTER" and Spam Cube. Hormel's corporate attorney Melanie J. Neumann also sent SpamCop's Julian Haight a letter on August 27, 1999 requesting that he delete an objectionable image (a can of Hormel's Spam luncheon meat product in a trash can), change references to UCE spam to all lower case letters, and confirm his agreement to do so.

Cost-benefit analyses

The European Union's Internal Market Commission estimated in 2001 that "junk email" cost Internet users €10 billion per year worldwide. The California legislature found that spam cost United States organizations alone more than $13 billion in 2007, including lost productivity and the additional equipment, software, and manpower needed to combat the problem. Spam's direct effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages. Large companies who are frequent spam targets utilize numerous techniques to detect and prevent spam.

In addition, spam has costs stemming from the *kinds* of spam messages sent, from the *ways* spammers send them, and from the *arms race* between spammers and those who try to stop or control spam. In addition, there are the opportunity cost of those who forgo the use of spam-afflicted systems. There are the direct costs, as well as the indirect costs borne by the victims—both those related to the spamming itself, and to other crimes that usually accompany it, such as financial theft, identity theft, data and intellectual property theft, virus and other malware infection, child pornography, fraud, and deceptive marketing.

The cost to providers of search engines is not insignificant: "The secondary consequence of spamming is that search engine indexes are inundated with useless pages, increasing the cost of each processed query".[3] The methods of spammers are likewise costly. Because spamming contravenes the vast majority of ISPs' acceptable-use policies, most spammers have for many years gone to some trouble to conceal the origins of their spam. Email, Usenet, and instant-message spam are often sent through insecure proxy servers belonging to unwilling third parties. Spammers frequently use false names, addresses, phone numbers, and other contact information to set up "disposable" accounts at various Internet service providers. In some cases, they have used falsified or stolen credit card numbers to pay for these accounts. This allows them

to quickly move from one account to the next as each one is discovered and shut down by the host ISPs.

The costs of spam also include the collateral costs of the struggle between spammers and the administrators and users of the media threatened by spamming. Many users are bothered by spam because it impinges upon the amount of time they spend reading their email. Many also find the content of spam frequently offensive, in that pornographyis one of the most frequently advertised products. Spammers send their spam largely indiscriminately, so pornographic ads may show up in a work place email inbox—or a child's, the latter of which is illegal in many jurisdictions. Recently, there has been a noticeable increase in spam advertising websites that contain child pornography.

Some spammers argue that most of these costs could potentially be alleviated by having spammers reimburse ISPs and persons for their material. There are three problems with this logic: first, the rate of reimbursement they could credibly budget is not nearly high enough to pay the direct costs, second, the human cost (lost mail, lost time, and lost opportunities) is basically unrecoverable, and third, spammers often use stolen bank accounts and credit cards to finance their operations, and would conceivably do so to pay off any fines imposed.

Email spam exemplifies a tragedy of the commons: spammers use resources (both physical and human), without bearing the entire cost of those resources. In fact, spammers commonly do not bear the cost at all. This raises the costs for everyone. In some ways spam is even a potential threat to the entire email system, as operated in the past. Since email is so cheap to send, a tiny number of spammers can saturate the Internet with junk mail. Although only a tiny percentage of their targets are motivated to purchase their products (or fall victim to their scams), the low cost may provide a sufficient conversion rate to keep the spamming alive. Furthermore, even though spam appears not to be economically viable as a way for a reputable company to do business, it suffices for professional spammers to convince a tiny proportion of gullible advertisers that it is viable for those spammers to stay in business. Finally, new spammers go into business every day, and the low costs allow a single spammer to do a lot of harm before finally realizing that the business is not profitable.

Some companies and groups "rank" spammers; spammers who make the news are sometimes referred to by these rankings. The secretive nature of spamming operations makes it difficult to determine how proliferated an individual spammer is, thus making the spammer hard to track, block or avoid. Also, spammers may target different networks to different extents, depending on how successful they are at attacking the target. Thus considerable resources are employed to actually measure the amount of spam generated by a single person or group. For example, victims that use common anti-spam hardware, software or services provide opportunities for such tracking. Nevertheless, such rankings should be taken with a grain of salt.

General costs

In all cases listed above, including both commercial and non-commercial, "spam happens" because of a positive cost-benefit analysis result, if the cost to recipients is excluded as an externality the spammer can avoid paying.

Cost is the combination of

- Overhead: The costs and overhead of electronic spamming include bandwidth, developing or acquiring an email/wiki/blog spam tool, taking over or acquiring a host/zombie, etc.
- Transaction cost: The incremental cost of contacting each additional recipient once a method of spamming is constructed, multiplied by the number of recipients (seeCAPTCHA as a method of increasing transaction costs).
- Risks: Chance and severity of legal and/or public reactions, including damages and punitive damages.
- Damage: Impact on the community and/or communication channels being spammed (see Newsgroup spam).

Benefit is the total expected profit from spam, which may include any combination of the commercial and non-commercial reasons listed above. It is normally linear, based on the

incremental benefit of reaching each additional spam recipient, combined with the conversion rate. The conversion rate for botnet-generated spam has recently been measured to be around one in 12,000,000 for pharmaceutical spam and one in 200,000 for infection sites as used by the Storm botnet. The authors of the study calculating those conversion rates noted, "After 26 days, and almost 350 million e-mail messages, only 28 sales resulted."

In crime

Spam can be used to spread computer viruses, trojan horses or other malicious software. The objective may be identity theft, or worse (e.g., advance fee fraud). Some spam attempts to capitalize on human greed, while some attempts to take advantage of the victims' inexperience with computer technology to trick them (e.g., phishing). On May 31, 2007, one of the world's most prolific spammers, Robert Alan Soloway, was arrested by US authorities. Described as one of the top ten spammers in the world, Soloway was charged with 35 criminal counts, including mail fraud, wire fraud, e-mail fraud, aggravated identity theft, and money laundering. Prosecutors allege that Soloway used millions of "zombie" computers to distribute spam during 2003. This is the first case in which US prosecutors used identity theft laws to prosecute a spammer for taking over someone else's Internet domain name.

In an attempt to assess potential legal and technical strategies for stopping illegal spam, a study from the University of California, San Diego, and the University of California, Berkeley, "Click Trajectories: End-to-End Analysis of the Spam Value Chain", cataloged three months of online spam data and researched website naming and hosting infrastructures. The study concluded that: 1) half of all spam programs have their domains and servers distributed over just eight percent or fewer of the total available hosting registrars and autonomous systems, with 80 percent of spam programs overall being distributed over just 20 percent of all registrars and autonomous systems; 2) of the 76 purchases for which the researchers received transaction information, there were only 13 distinct banks acting as credit card acquirers and only three banks provided the payment servicing for 95 percent of the spam-advertised goods in the study; and, 3) a "financial blacklist" of banking entities that do business with spammers would dramatically reduce monetization of unwanted e-mails. Moreover, this blacklist could be updated far more rapidly than spammers could acquire new banking resources, an asymmetry favoring anti-spam efforts.

Political issues

Spamming remains a hot discussion topic. In 2004, the seized Porsche of an indicted spammer was advertised on the Internet; this revealed the extent of the financial rewards available to those who are willing to commit duplicitous acts online. However, some of the possible means used to stop spamming may lead to other side effects, such as increased government control over the Internet, loss of privacy, barriers to free expression, and the commercialization of e-mail.

One of the chief values favored by many long-time Internet users and experts, as well as by many members of the public, is the free exchange of ideas. Many have valued the relative anarchy of the Internet, and bridle at the idea of restrictions placed upon it. A common refrain from spam-fighters is that spamming itself abridges the historical freedom of the Internet, by attempting to force users to carry the *costs* of material that they would not choose.

An ongoing concern expressed by parties such as the Electronic Frontier Foundation and the American Civil Liberties Union has to do with so-called "stealth blocking", a term for ISPs employing aggressive spam blocking without their users' knowledge. These groups' concern is that ISPs or technicians seeking to reduce spam-related costs may select tools that (either through error or design) also block non-spam e-mail from sites seen as "spam-friendly". Spam Prevention Early Warning System (SPEWS) is a common target of these criticisms. Few object to the existence of these tools; it is their use in filtering the mail of users who are not informed of their use that draws fire.

Some see spam-blocking tools as a threat to free expression—and laws against spamming as an untoward precedent for regulation or taxation of e-mail and the Internet at large. Even though it is possible in some jurisdictions to treat some spam as unlawful merely by applying existing laws

against trespass and conversion, some laws specifically targeting spam have been proposed. In 2004, United States passed the CAN-SPAM Act of 2003 that provided ISPs with tools to combat spam. This act allowed Yahoo! to successfully sue Eric Head, reportedly one of the biggest spammers in the World, who settled the lawsuit for several thousand U.S. dollars in June 2004. But the law is criticized by many for not being effective enough. Indeed, the law was supported by some spammers and organizations that support spamming, and opposed by many in the anti-spam community. Examples of effective anti-abuse laws that respect free speech rights include those in the U.S. against unsolicited faxes and phone calls, and those in Australia and a few U.S. states against spam.

In November 2004, Lycos Europe released a screen saver called make LOVE not SPAM that made Distributed Denial of Service attacks on the spammers themselves. It met with a large amount of controversy and the initiative ended in December 2004.

Anti-spam policies may also be a form of disguised censorship, a way to ban access or reference to questioning alternative forums or blogs by an institution. This form of occult censorship is mainly used by private companies when they can not muzzle criticism by legal ways.

Court cases

United States

Sanford Wallace and Cyber Promotions were the target of a string of lawsuits, many of which were settled out of court, up through a 1998 Earthlink settlement that put Cyber Promotions out of business. Attorney Laurence Canter was disbarred by the Tennessee Supreme Court in 1997 for sending prodigious amounts of spam advertising his immigration law practice. In 2005, Jason Smathers, a former America Online employee, pled guilty to charges of violating the CAN-SPAM Act. In 2003, he sold a list of approximately 93 million AOL subscriber e-mail addresses to Sean Dunaway who, in turn, sold the list to spammers.

In 2007, Robert Soloway lost a case in a federal court against the operator of a small Oklahoma-based Internet service provider who accused him of spamming. U.S. Judge Ralph G. Thompson granted a motion by plaintiff Robert Braver for a default judgment and permanent injunction against him. The judgment includes a statutory damages award of $10,075,000 under Oklahoma law.

In June 2007, two men were convicted of eight counts stemming from sending millions of e-mail spam messages that included hardcore pornographic images. Jeffrey A. Kilbride, 41, of Venice, California was sentenced to six years in prison, and James R. Schaffer, 41, of Paradise Valley, Arizona, was sentenced to 63 months. In addition, the two were fined $100,000, ordered to pay $77,500 in restitution to AOL, and ordered to forfeit more than $1.1 million, the amount of illegal proceeds from their spamming operation. The charges included conspiracy, fraud, money laundering, and transportation of obscene materials. The trial, which began on June 5, was the first to include charges under theCAN-SPAM Act of 2003, according to a release from the Department of Justice. The specific law that prosecutors used under the CAN-Spam Act was designed to crack down on the transmission of pornography in spam.

In 2005, Scott J. Filary and Donald E. Townsend of Tampa, Florida were sued by Florida Attorney General Charlie Crist for violating the Florida Electronic Mail Communications Act. The two spammers were required to pay $50,000 USD to cover the costs of investigation by the state of Florida, and a $1.1 million penalty if spamming were to continue, the $50,000 was not paid, or the financial statements provided were found to be inaccurate. The spamming operation was successfully shut down.

Edna Fiedler, 44, of Olympia, Washington, on June 25, 2008, pleaded guilty in a Tacoma court and was sentenced to 2 years imprisonment and 5 years of supervised release orprobation in an Internet $1 million "Nigerian check scam." She conspired to commit bank, wire and mail fraud, against US citizens, specifically using Internet by having had anaccomplice who shipped counterfeit checks and money orders to her from Lagos, Nigeria, last November. Fiedler shipped out $609,000 fake check and money orders when arrested and prepared to send additional $1.1

million counterfeit materials. Also, the U.S. Postal Service recently intercepted counterfeit checks, lottery tickets and eBay overpayment schemes with a face value of $2.1 billion.

In a 2009 opinion, *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, the Ninth Circuit assessed the standing requirements necessary for a private plaintiff to bring a civil cause of action against spam senders under the CAN-SPAM Act of 2003, as well as the scope of the CAN-SPAM Act's federal preemption clause.

United Kingdom

In the first successful case of its kind, Nigel Roberts from the Channel Islands won £270 against Media Logistics UK who sent junk e-mails to his personal account.

In January 2007, a Sheriff Court in Scotland awarded Mr. Gordon Dick £750 (the then maximum sum that could be awarded in a Small Claim action) plus expenses of £618.66, a total of £1368.66 against Transcom Internet Services Ltd for breaching anti-spam laws. Transcom had been legally represented at earlier hearings, but were not represented at the proof, so Gordon Dick got his decree by default. It is the largest amount awarded in compensation in the United Kingdom since Roberts -v- Media Logistics case in 2005 above, but it is not known, if Mr. Dick ever received anything. (An image of Media Logistics' cheque is shown on Roberts' website) Both Roberts and Dick are well known figures in the British Internet industry for other things. Dick is currently Interim Chairman of Nominet UK (the manager of .UK and .CO.UK) while Roberts is CEO of CHANNELISLES.NET (manager of .GG and .JE).

Despite the statutory tort that is created by the Regulations implementing the EC Directive, few other people have followed their example. As the Courts engage in active case management, such cases would probably now be expected to be settled by mediation and payment of nominal damages.

New Zealand

In October 2008, a vast international internet spam operation run from New Zealand was cited by American authorities as one of the world's largest, and for a time responsible for up to a third of all unwanted e-mails. In a statement the US Federal Trade Commission (FTC) named Christchurch's Lance Atkinson as one of the principals of the operation. New Zealand's Internal Affairs announced it had lodged a $200,000 claim in the High Court against Atkinson and his brother Shane Atkinson and courier Roland Smits, after raids in Christchurch. This marked the first prosecution since the Unsolicited Electronic Messages Act (UEMA) was passed in September 2007. The FTC said it had received more than three million complaints about spam messages connected to this operation, and estimated that it may be responsible for sending billions of illegal spam messages. The US District Court froze the defendants' assets to preserve them for consumer redress pending trial.[69] U.S. co-defendant Jody Smith forfeited more than $800,000 and faces up to five years in prison for charges to which he pled guilty.

Bulgaria

While most countries either outlaw or at least ignore spam, Bulgaria is the first and until now only one to legalize it. According to the Bulgarian E-Commerce act (Чл.5,6) anyone can send spam to mailboxes published as owned by a company or organization, as long as there is a "clear and straight indication that the message is unsolicited commercial e-mail" ("да осигури ясното и недвусмислено разпознаване на търговското съобщение като непоискано") in the message body.

This made lawsuits against Bulgarian ISP's and public e-mail providers with antispam policy possible, as they are obstructing legal commerce activity and thus violate Bulgarian antitrust acts. While there are no such lawsuits until now, several cases of spam obstruction are currently awaiting decision in the Bulgarian Antitrust Commission (Комисия за защита на конкуренцията) and can end with serious fines for the ISP's in question.

The law contains other dubious provisions — for example, the creation of a nationwide public electronic register of e-mail addresses that do not want to receive spam. It is usually abused as

the perfect source for e-mail address harvesting, because publishing invalid or incorrect information in such a register is a criminal offense in Bulgaria.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. The word is aneologism created as a homophone of *fishing* due to the similarity of using fake bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

Phishing is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing is used to portray trust in the user since the user may not be able to tell that the site being visited or program being used is not real, and when this occurs is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

Crack (password software)

Crack is a Unix password cracking program designed to allow system administrators to locate users who may have weak passwordsvulnerable to a dictionary attack. Crack was the first standalone password cracker for Unix systems and (later) the first to introduce programmable dictionary generation.

Crack began in 1990 when Alec Muffett, a Unix system administrator at the University of Wales Aberystwyth was trying to improveDan Farmer's 'pwc' cracker in COPS and found that by re-engineering its memory management he got a noticeable performance increase. This led to a total rewrite which became "Crack v2.0" and further development to improve usability.

Legal issues arising from using Crack

Randal L. Schwartz, a notable Perl programming expert, in 1995 was prosecuted for using Crack on the password file of a system at Intel, a case the verdict of which was eventually expunged.

Crack was also used by Kevin Mitnick when hacking into Sun Microsystems in 1993.

Software cracking

Software cracking (known as "breaking" in the 1980s) is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, especially copy protection features (including protection against the manipulation of software, serial number, hardware key, date checks and disc check) or software annoyances like nag screens and adware.

A **crack** refers to the mean of achieving software cracking, for example a stolen serial number or a tool that performs that act of cracking. Some of these tools are calledkeygen, patch or loader. A keygen is a handmade product license generator that often offers the ability to generate legitimate licenses in your own name. A patch is a small computer program that modifies the machine code of another program. This has the advantage for a cracker to not include a large executable in a release when only a few bytes are changed. A loader modifies the startup flow of a program and does not remove the protection but circumvents it. A well known example of a loader is a trainer used to cheat in games.[6] Fairlight pointed out in one of their .nfo files that these type of cracks are not allowed for warez scene game releases. A nukewar has shown that the protection may not kick in at any point for it to be a valid crack.

The distribution of cracked copies is illegal in most countries. There have been lawsuits over cracking software. It might be legal to use cracked software in certain circumstances.