Author's Comments, Disclaimers, and Disclosures

This document contains no new or original work and is not presented as being original work of the author.

This document is merely an attempt to gather together in one location a brief summary description of the many dangers encountered by computer users when using email. The work began as an attempt by the author to better understand the possible origins of some of the computer problems encountered by himself and his clients.

I have attempted to always give attribution of the original source with appropriate footnotes. Many of the sources are quoted directly while others may be somewhat modified by this author to better comply with the intent of this document.

If the reader wishes to learn more about any one of the topics, the corresponding footnote, links in that document, and Google searches will reveal more than any sane person should care to learn.

Perhaps a better understanding of some of the malicious email activity will help the reader of this article to better cope with those activities. I am also considering a similar compilation dealing with proper reaction to such malicious activity.

Comments are welcome and should be sent to del@delweg.com. Please make the subject of such email "malicious email".

Basic Email Information and Common Abuses

FUNDAMENTALS

Electronic mail[1]

Electronic mail, most commonly referred to as **e-mail** or **email** since approximately 1993, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. An Internet email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.[2] The first email message was sent by Ray Tomlinson in 1971 between two machines sitting side by side.[3]

Email or email

On March 18, 2011, The AP Stylebook, the de facto style and usage guide for much of the news media, announced on Friday that the abbreviated term for electronic mail is losing a hyphen, and with it, a relic of a simpler time when Internet technology needed to be explained very carefully.[4]

A few editorially conservative publications, most notably the New York Times and The Washington Post still prefer e-mail to email, but most of the English-speaking world has adopted the unhyphenated form.[5]

In 2010, the AP Stylebook changed the preferred spelling from Web site to website.

Mail server

A mail server, or email server is a program, called a Message Transfer Agent (MTA), running on a computer which frequently is also identified as the email server. That computer need not be dedicated to that one purpose, it frequently is running numerous other programs which may or may not be related to email.

Message Transfer Agent[6]

A Message Transfer Agent (MTA) is software that transfers electronic mail messages from one computer to another. An MTA implements both the client (sending) and server (receiving) functions. Extended SMTP (ESMTP) is the protocol in widespread use by most MTAs. SMTP and ESMTP are delivery protocols only. In normal use, mail is "pushed" to a destination mail server (or next-hop mail server) as it arrives. Mail is routed based on the destination server, not the individual user(s) to which it is addressed.

Accepting a message obliges an MTA to deliver it and when a message cannot be delivered, that MTA must send a bounce message back to the sender, indicating the problem.[7]

---

[1] https://en.wikipedia.org/wiki/Email
[2] http://en.wikipedia.org/wiki/Internet_Message_Format#Servers_and_client_applications
[3] http://openmap.bbn.com/~tomlinso/ray/home.html
[4] http://mashable.com/2011/03/18/ap-stylebook-email/
[5] http://grammarist.com/style/email-email/
[6] https://en.wikipedia.org/wiki/Message_transfer_agent
[7] http://en.wikipedia.org/wiki/Internet_Message_Format#Servers_and_client_applications

Simple Mail Transfer Protocol[8]
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission across Internet Protocol (IP) networks.

Post Office Protocol[9] **and Internet Message Access Protocol**[10]
In computing, the Post Office Protocol (POP) is an Internet standard protocol used by local email clients to retrieve email from a remote server.

The Internet Message Access Protocol (IMAP) is an Internet protocol that allows an email client to access email on a remote mail server.

User-level client mail applications typically use SMTP (or ESMTP) only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) to access their mail box accounts on a mail server.

Message header[11]
Each message has exactly one header, which is structured into fields.
The message header must include at least the *From* and *Date* fields.
The message header should include at least the *Message-ID* and *In-Reply-To* fields.
Common header fields for email include: *To, Subject, Bcc, Cc, Content-Type, Precedence, References, Reply-To, Sender, Archived-At*
Trace Information fields are: *Received, Return-Path, Authentication-Results, Received-SPF, Auto-Submitted, VBR-Info.*

Every header field can be forged! In many instances such forgeries are used for malicious and disruptive purposes. One such forgery is called spoofing.

Spoofing[12]
Email spoofing is the creation of email messages with a forged sender address - something which is simple to do. You can manually spoof an email by changing a setting in your mail program. Email spoofing alters the header information of an email to make the message appear to come from a known or trusted source. It is often used as a ruse to collect personal information. Spam and phishing emails typically use spoofing to mislead the recipient about the origin of the message. Not all spoofing is done with malicious intent.

As an example of non-malicious spoofing:

> I choose to use the email service provided by my ISP. They insist that I use the email address dpweg@charter.net. This would confuse my friends, family, and customers who for many years have known me as del@delweg.com. Therefore I spoof my outgoing emails with del@delweg.com in both the From and Reply To fields. This application of spoofing has permitted me to move around the country and switch ISPs without changing email addresses.

[8] http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[9] http://en.wikipedia.org/wiki/Post_Office_Protocol
[10] https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol
[11] http://en.wikipedia.org/wiki/Internet_Message_Format#Servers_and_client_applications
[12] http://en.wikipedia.org/wiki/Email_spoofing

As an example of malicious spoofing consider the following:

> Suppose Tom is sent an email infected with a worm and Tom opens the email, thus triggering the worm.
>
> The worm finds the addresses of Fred and Jane in Tom's address book.
>
> From Tom's computer, the worm sends an email infected with a worm to Fred, but forged to appear to have been sent by Jane. Fred observes the message as being from Jane. Jane is completely unaware that it appears as if she has sent a message to Fred.
>
> Tom is completely unaware that his machine has been infected and unaware of the fact that his computer has sent spoofed infected messages which cannot be traced back to him.

SPAM[13]

An electronic message is spam if

A. The recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients AND
B. The recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent.

A message is Spam if and only if it is both unsolicited and bulk.

- Unsolicited Email is normal email
  (examples: first contact enquiries, job enquiries, sales enquiries)
  Being unsolicited by itself does not make it spam.
- Bulk Email is normal email
  (examples: subscriber newsletters, customer communications, discussion lists)
  Being bulk by itself does not make it spam.

Spam is an issue about consent, not content. Whether the Unsolicited Bulk Email ("UBE") message is an advert, a scam, porn, a begging letter, or an offer of a free lunch, the content is irrelevant - if the message was sent unsolicited and in bulk then the message is spam.

Email scam[14] is an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for business, others invite victims to a website with a detailed pitch.

Scam is about content and intent whereas spam is about consent not content.

Observe that spam messages can, but need not, contain scam content.

The legal status of spam varies from one jurisdiction to another. In the United States, spam was declared to be legal by the CAN-SPAM Act of 2003 provided the message adheres to certain specifications. Because of the minuscule cost of sending email, spammers can send hundreds of millions of email messages each day over an inexpensive Internet connection. A person who creates electronic spam is called a spammer

[13] http://en.wikipedia.org/wiki/Email_spam
[14] http://en.wikipedia.org/wiki/List_of_email_scams

A person who creates electronic spam is called a spammer[15].

Email Harvesting[16]
Email harvesting is the process of obtaining lists of email addresses using various methods for use in bulk email or other purposes.

The simplest method involves spammers purchasing or trading lists of email addresses from other spammers.

Another common method is the use of special software known as "harvesting bots" or "harvesters", which spider Web pages, postings on Usenet, mailing list archives, internet forums and other online sources to obtain email addresses from public data.

Valid email addresses at a specific domain may be found by guessing email addresses using common usernames in email addresses at that domain. For example, trying alan@example.com, alana@example.com, alanb@example.com, etc. Any that are accepted for delivery by the recipient email server, instead of rejected, are added to the list of theoretically valid email addresses for that domain.

Another method of email address harvesting is to offer a product or service free of charge as long as the user provides a valid email address. Common products and services offered are jokes of the day, daily bible quotes, news or stock alerts, free merchandise, or registered sex offender alerts for one's area.

Zombie Computer[17]
A zombie computer is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. As used here a hacker is someone who accesses a computer system by circumventing its security system.

Botnet[18]
A botnet is a collection of internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an IRC channel, or it could be used to send spam email or participate in Distributed Denial of Service (DDoS) attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. The word botnet stems from the two words robot and network. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks. Botnets are used to send about 80% of spam.

DDoS Attack[19]
A distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it

[15] https://en.wikipedia.org/wiki/Spam_%28electronic%29
[16] http://en.wikipedia.org/wiki/Email_address_harvesting
[17] http://en.wikipedia.org/wiki/Zombie_%28computer_science%29
[18] https://en.wikipedia.org/wiki/Botnet
[19] https://en.wikipedia.org/wiki/Denial-of-service_attack

is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

On average spam constitutes 78% of all email sent. Keep in mind that spam is any unsolicited bulk email.

- Spam can simply be annoying inbox clutter.
- Spam is the primary method of email bombing.
- Spam is the primary cause of backscatter.
- Spam is the primary technique for phishing.
- Spam is the primary delivery mechanism for malicious software called malware.

BOMBING[20]

Email bombing is the intentional sending of large volumes of messages to a target address. The overloading of the target email address can render it unusable and can even cause the mail server to crash. Techniques of email bombing are Mass Mailing, List Linking, and Zip Bombing.

Mass mailing (bombing)
Mass mailing consists of sending numerous duplicate mails to the same email address. These types of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters.

Mass mailing is also commonly performed as a DDoS attack by employing the use of "zombie" botnets; networks of computers compromised by malware and under the attacker's control. Similar to their use in spamming, the attacker instructs the botnet to send out millions or even billions of emails, but unlike normal botnet spamming, the emails are all addressed to only one or a few addresses the attacker wishes to flood. This form of email bombing is similar in purpose to other DDoS flooding attacks. As the targets are frequently the dedicated hosts handling website and email accounts of a business, this type of attack can be just as devastating to both services of the host.

The second type of attack using zombies is more difficult to defend against than a simple mass-mailing bomb because of the multiple source addresses and the possibility of each zombie computer sending a different message or employing stealth techniques to defeat spam filters.

List linking (bombing)
List linking means the subject is signed up for large numbers of mailing lists. The use of verification emails for mailing lists is designed to prevent abusive signups, but email bombing can involve workarounds. For example, the bomber can create a new email address for the signup, click the link in the confirmation email, and then set up the account to forward to the target. The target will receive the communications from the mailing list and will not be able to unsubscribe because the mailings are not being sent directly through the organization.

ZIP bomb (bombing)
A zip bomb is a variant of mail-bombing. After most commercial mail servers began checking mail with anti-virus software and filtering certain malicious file types, EXE, RAR, Zip, 7-Zip, mail server software was then configured to unpack archives and check their contents as well. A new idea to combat this solution was composing a "bomb" consisting of an enormous text file,

[20] http://en.wikipedia.org/wiki/Email_bomb

containing, for example, only the letter z repeating millions of times. Such a file compresses into a relatively small archive, but its unpacking (especially by early versions of mail servers) would use a greater amount of processing, which could result in a DoS (Denial of Service).

BACKSCATTER[21]

Backscatter is a message you receive informing you that email you did not send was not delivered to someone you do not know. This type of message is called a Delivery Status Notification or DSN. In most cases DSNs are welcome because the sender usually wants to know when a message cannot be delivered to the recipient or that delivery of the message has been delayed for some reason.[22]

DSNs occur when an email system accepts a message for delivery and then the system determines that the message cannot be delivered. Messages that are accepted must be delivered to the recipient or a DSN must be sent to the sender, or more specifically, the envelope return address, notifying the sender of the delivery problem. There are many possible reasons why a message that has been accepted cannot be delivered but the most common reasons are that the recipient address does not exist or that the recipient's mailbox is full.

Backscatter occurs when a DSN is sent to an email address forged in a spam run or forged by a virus that propagates by email. Accepting a message and then sending a DSN to the possibly forged envelope sender address is just not an acceptable practice today. If the message cannot be delivered it should not be accepted.

Mail servers can handle undeliverable messages in three fundamentally different ways:[23]

- **Reject**. A receiving server can reject the incoming email during the connection stage while the sending server is still connected. If a message is rejected at connect time with a 5xx error code then the sending server can report the problem to the real sender cleanly.
- **Drop**. A receiving server can initially accept the full message, but then determine that it is spam, and quarantine it - delivering to "Junk" or "Spam" folders from where it will eventually be deleted automatically. This is common behavior, even though RFC 5321 says: "...silent dropping of messages should be considered only in those cases where there is very high confidence that the messages are seriously fraudulent or otherwise inappropriate..."
- **Bounce**. A receiving server can initially accept the full message, but then determine that it is spam or to a non-existent recipient, and generate a bounce message back to the supposed sender indicating that message delivery failed.

Backscatter occurs when the "bounce" method is used, and the sender information on the incoming email was that of an unrelated third party.

If you've ever received a “Your mail could not be delivered” bounce notification, a “Your mail contained a virus” notice, or a request to confirm your signup request for a mailing list you've never heard of, you've probably received backscatter. The backscatter problem is inherently

[21] http://en.wikipedia.org/wiki/Backscatter_%28email%29
[22] http://www.tuffmail.com/backscatter.php
[23] http://en.wikipedia.org/wiki/Backscatter_%28email%29

linked to the spam problem, as most backscatter received is due to somebody else on the internet doing something bad and spam-related.[24]

Backscatter arrives in your in-box usually with a subject of "Delivery notification: delivery has failed", "Deliver status notification", "failure notice", etc. The messages typically originate from "Mailer daemon", "postmaster", or "Mail delivery subsystem". Backscatter tells you about problems with messages you did not send.[25]

- Receiving backscatter does not mean your email address has been stolen. Your email address is only being used by a spammer to help get around spam filters.
- Receiving backscatter does not mean you have a virus.
- Receiving backscatter does not mean your computer has been taken over by spammers.

Types of backscatter[26]

- Misdirected bounces from spam runs, from mail servers who "accept then bounce" instead of rejecting mail during the SMTP transaction.
- Misdirected virus/worm "OMG your mail was infected!" email notifications from virus scanners.
- Misdirected "please confirm your subscription" requests from mailing lists that allow email-based signup requests.
- Out of office or vacation autoreplies and autoresponders.
- Challenge requests from "Challenge/Response" anti-spam software. Maybe C/R software works great for you, but it generates significant backscatter to people you don't know.

Stopping backscatter?[27]

If you're an end user, there's not much you can do to prevent the receipt of backscatter.

Whatever you do, don't use a "Challenge/Response" anti-spam application or service. It makes the problem worse for everybody else on the internet – your challenge requests are just another kind of backscatter.

The same goes for those anti-spam applications that promise to send fake bounces on your behalf. Yours will be just another bogus bounce notification bothering some innocent, unrelated third-party.

Don't set an "out of office" reply, either. Besides contributing to the backscatter problem yourself, you're sending random notes that you have a live email address. You're confirming for spammers that your email address is valid!

If you administer a mail server, you can minimize your contribution to the backscatter problem by following the advice given in the article:

http://www.spamresource.com/2007/02/backscatter-what-is-it-how-do-i-stop-it.html

[24] http://www.spamresource.com/2007/02/backscatter-what-is-it-how-do-i-stop-it.html
[25] http://backscattervictims.blogspot.com/2007/10/email-backscatter-victims-unite.html
[26] http://www.spamresource.com/2007/02/backscatter-what-is-it-how-do-i-stop-it.html
[27] http://www.spamresource.com/2007/02/backscatter-what-is-it-how-do-i-stop-it.html

PHISHING[28]

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social web sites, auction sites, online payment processors, or IT administrators are commonly used to lure the 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.

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the yourbank website; actually this URL points to the "yourbank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link suggest a reliable destination, when the link actually goes to the phishers' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phisher.

The techniques used for phishing are many and varied. Several phishing techniques are described here. Notice the really neat names.

Phishing (Generic term)
Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spear phishing
Spear Phishing is phishing directed at specific individuals or companies. To increase their probability of success the attacker may have gathered personal information about their target.

Clone phishing
A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original.

This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

[28] http://en.wikipedia.org/wiki/Phishing
C:\Users\Del\Dropbox\MyWord\Email Articles\malicious email activity.docx

Whaling
Whaling is a phishing attack which is directed specifically at senior executives and other high profile targets inside businesses.

Homograph attack
A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or homograph attack, phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain. Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website.

Filter evasion
To make it harder for anti-phishing filters to detect text commonly used in phishing emails, phishers have used images instead of text.

Website forgery
Once a victim visits the phishing website, the deception is not over. Some phishing methods use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

Cross-site scripting
An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

A Universal Man-in-the-middle (MITM) Phishing Kit, discovered in 2007, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

Phishers have begun to use Flash-based websites to avoid anti-phishing techniques that scan websites for phishing-related text. These look much like the real website, but hide the text in a multimedia object.

Tabnabbing
Tabnabbing silently redirects a user to the affected site by taking advantage of the multiple tabs that users use.

Evil Twins
Evil twins is a phishing technique in which a phisher creates a fake wireless network that looks similar to a legitimate public network that may be found in public places such as airports, hotels, or coffee shops. Whenever someone logs on to the bogus network, fraudsters try to capture their passwords and/or credit card information.

Unnamed
Another (unnamed) attack is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information.

Phishing is not restricted to email. A few non-email phishing techniques are listed here. A Google search will produce more detail about any one of the following.

Vishing (Voice/Phone phishing)
Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of voice and phishing. Voice phishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Voice phishing is very hard for legal authorities to monitor or trace. To protect themselves, consumers are advised to be highly suspicious when receiving messages directing them to call and provide credit card or bank numbers and to NEVER provide such information. When in doubt, calling a company's telephone number listed on billing statements or other official sources is recommended instead of calling numbers from messages of dubious authenticity.

Text-message phishing
Text-message phishing is a phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device. This tactic is also referred to as smishing, which is a combination of SMS and phishing.

Paper mail or fax phishing
Some fraudsters still use low-tech methods to obtain your personal and financial information. Phishing attempts can be made through regular mail or fax machines.

Pop-up windows
Fraudsters may use pop-up windows – small windows or ads – to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer

MALWARE[29]

Malware, short for malicious software, is a general term used to refer to a variety of forms of hostile or intrusive software. Malware is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, or other software.

Malware includes

- viruses
- ransomware

[29] http://en.wikipedia.org/wiki/Malware

- worms
- Trojan horses
- rootkits
- keyloggers
- dialers
- spyware
- adware
- malicious BHOs
- rogue security software, and
- other malicious programs

The majority of active malware threats are usually worms or Trojans rather than viruses.

Worm[30]

A computer worm is a standalone computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth.

Many worms are designed only to spread, and do not attempt to change the systems they pass through. A payload is code in the worm designed to do more than spread the worm–it might delete files on a host system, encrypt files, or send documents via email. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a zombie computer under control of the worm author.

Trojan[31]

A Trojan horse, or Trojan, is a non-self-replicating type of malware which gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload, often including a backdoor allowing unauthorized access to the target's computer. These backdoors tend to be invisible to average users. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems. Trojans may use drive-by downloads or install via online games or internet-driven applications in order to reach target computers.

A Trojan may give a hacker remote access to a targeted computer system. Operations that could be performed by a hacker on a targeted computer system may include:

- Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute denial-of-service attacks)
- Crashing the computer
- Blue screen of death
- Electronic money theft and disabling all internet traffic on the host
- Data theft (e.g. retrieving passwords or credit card information)
- Installation of software, including third-party malware and ransomware
- Downloading or uploading of files on the user's computer

[30] http://en.wikipedia.org/wiki/Computer_worm
[31] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

- Modification or deletion of files
- Keystroke logging
- Watching the user's screen
- Viewing the user's webcam
- Controlling the computer system remotely
- Anonymizing remote third-party internet viewing

Trojan horses in this way may require interaction with a hacker to fulfill their purpose, though the hacker does not have to be the individual responsible for distributing the Trojan horse. It is possible for individual hackers to scan computers on a network using a port scanner in the hope of finding one with a malicious Trojan horse installed, which the hacker can then use to control the target computer.

A recent innovation in Trojan horse code takes advantage of a security flaw in older versions of Internet Explorer and Google Chrome to use the host computer as an anonymizer proxy to effectively hide internet usage. A hacker is able to view internet sites while the tracking cookies, internet history, and any IP logging are maintained on the host computer.

Virus[32]

A computer virus is a computer program that can replicate itself and spread from one computer to another. 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. Viruses almost always corrupt or modify files on a targeted computer.

The term virus is also commonly, but erroneously, used to refer to other types of malware, including but not limited to adware and spyware programs that do not have a reproductive ability. Note that neither adware or spyware are viruses.

The majority of active malware threats are usually Trojans or worms rather than viruses. Malware such as Trojan horses and worms is sometimes confused with viruses, which are technically different: a worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that appears harmless but hides malicious functions. Worms and Trojan horses, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and do nothing to call attention to themselves. Some viruses do nothing beyond reproducing themselves.

Spyware[33]

Spyware is a program that aids in gathering information about a person or organization without their knowledge. Spyware may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

Spyware is mostly used for the purposes such as; tracking and storing internet users' movements on the web; serving up pop-up ads to internet users.

Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

[32] http://en.wikipedia.org/wiki/Computer_virus
[33] http://en.wikipedia.org/wiki/Spyware

While the term spyware suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.

Spyware does not necessarily spread in the same way as a virus or worm because infected systems generally do not attempt to transmit or copy the software to other computers. Instead, spyware installs itself on a system by deceiving the user or by exploiting software vulnerabilities.

Most spyware is installed without users' knowledge, or by using deceptive tactics. Spyware may try to deceive users by bundling itself with desirable software. Another common tactic is to use a Trojan horse.

Some spyware authors infect a system through security holes in the Web browser or in other software. When the user navigates to a Web page controlled by the spyware author, the page contains code which attacks the browser and forces the download and installation of spyware. The installation of spyware frequently involves Internet Explorer. Its popularity and history of security issues have made it a frequent target.

Adware[34]

Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author.

The term adware is frequently used to describe a form of malware which presents unwanted advertisements, in the form of a pop-up, to the user of a computer. When the term is used in this way, the severity of its implication varies. While some sources rate adware only as an irritant, others classify it as an online threat or even rate it as seriously as computer viruses and Trojans.

Dialers[35]

Dialers are necessary to connect to the internet (at least for non-broadband connections), but some dialers are designed to connect to premium-rate numbers. The providers of such dialers often search for security holes in the operating system installed on the user's computer and use them to set the computer up to dial up through their number, so as to make money from the calls.

Keyloggers[36]

Keystroke logging, often referred to as keylogging, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. Keylogging has very legitimate uses in studies of human-computer interaction. There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis.

[34] http://en.wikipedia.org/wiki/Adware
[35] http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialer
[36] http://en.wikipedia.org/wiki/Keystroke_logging

Rootkits[37]

A rootkit is a stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system. Rootkits employ a variety of techniques to gain control of a system; the type of rootkit influences the choice of attack vector. The most common technique leverages security vulnerabilities to achieve surreptitious privilege escalation. Another approach is to use a Trojan horse, deceiving a computer user into trusting the rootkit's installation program as benign.

Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root/Administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it. Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it.

Once installed, a rootkit takes active measures to obscure its presence within the host system through subversion or evasion of standard operating system security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits also take a number of measures to ensure their survival against detection and cleaning by antivirus software.

Modern rootkits do not elevate access, but rather are used to make a software payload undetectable by adding stealth capabilities. Most rootkits are classified as malware, because the payloads they are bundled with are malicious. For example, a payload might covertly steal user passwords, credit card information, computing resources, or conduct other unauthorized activities.

The installation of malicious rootkits is commercially driven, with a pay-per-install (PPI) compensation method typical for distribution.

Ransomware[38]

Ransomware (when carried out correctly is called cryptoviral extortion, and is also called scareware) comprises a class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying. Modern ransomware attacks were initially popular in Russia, but in recent years there have been an increasing number of ransomware attacks in Australia, Germany, and the United States.

Ransomware typically propagates like a conventional computer worm, entering a system through a downloaded file or vulnerability in a network service. The program will then run a payload: such as one that will encrypt personal files on the hard drive. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to effectively restrict interaction with the computer.

[37] http://en.wikipedia.org/wiki/Rootkit
[38] http://en.wikipedia.org/wiki/Ransomware_%28malware%29

Ransomware payloads, especially ones which do not encrypt files, utilize elements of scareware to coax the user into paying for its removal. The payload may, for example, display notices purportedly issued by companies or law enforcement agencies which falsely claim that the user's system had been used for illegal activities, or contains illegal content such as pornography and unlawfully obtained software. In any case, the ransomware will attempt to extort money from the system's user by forcing them to purchase either a program to decrypt the files it had encrypted, or an unlock code which will remove the locks it had applied.

Malicious BHOs

A Browser Helper Object (BHO) is a DLL module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality.

Some forms of malware have also been created as BHOs. For example, the Download.ject malware installs a BHO that would activate upon detecting a secure connection to a financial institution, record the user's keystrokes (intending to capture passwords) and transmit the information to a website used by Russian computer criminals. Other BHOs such as the MyWay Searchbar track users' browsing patterns and pass the information they record to third parties.

Rogue security software is a form of Internet fraud using computer malware that deceives users into paying money for fake or simulated removal of malware. Or it claims to get rid of malware, but instead introduces malware to the computer. Rogue security software has become a growing and serious security threat in desktop computing in recent years.

Rogue Security Software

Rogue security software mainly relies on social engineering (fraud) to defeat the security built into modern operating system and browser software and install itself onto victims' computers. A website may, for example, display a fictitious warning dialog stating that someone's machine is infected with a computer virus, and encourage them through social engineering to install or purchase scareware in the belief that they are purchasing genuine antivirus software.

Most have a Trojan horse component, which users are misled into installing. The Trojan may be disguised as:

- A browser plug-in or extension (typically toolbar)
- An image, screensaver or archive file attached to an email message
- Multimedia codec required to play a certain video clip
- Software shared on peer-to-peer networks
- A free online malware scanning service

Some rogue security software propagate onto users' computers as drive-by downloads which exploit security vulnerabilities in web browsers, pdf viewers, or email clients to install themselves without any manual interaction.

More recently, malware distributors have been utilizing SEO poisoning techniques by pushing infected URLs to the top of search engine results about recent news events. People looking for articles on such events on a search engine may encounter results that, upon being clicked, are instead redirected through a series of sites before arriving at a landing page that says that their machine is infected and pushes a download to a trial of the rogue program.

Cold-calling has also become a vector for distribution of this type of malware, with callers often claiming to be from Microsoft Support or another legitimate organization.

Drive-by Download[39]

Drive-by download means two things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).
2. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.

Drive-by downloads may happen when visiting a website, viewing an email message or by clicking on a deceptive pop-up window. By clicking on a window in the mistaken belief that, for instance, an error report from the computer's operating system itself is being acknowledged, or that an innocuous advertisement pop-up is being dismissed. In such cases, the supplier may claim that the user consented to the download, although actually the user was unaware of having started an unwanted or malicious software download.

A drive-by install is a similar event. It refers to installation rather than download. Sometimes the two terms are used interchangeably.

[39] http://en.wikipedia.org/wiki/Drive-by_download