Threatsaurus

The A-Z of computer and data security threats

SOPHOS

The A-Z of computer and data security threats

Whether you're an IT professional, use a computer at work, or just browse the Internet, this book is for you. We explain the facts about threats to your computers and to your data in simple, easy-to-understand language.

Sophos frees IT managers to focus on their businesses. We provide endpoint, encryption, email, web and network security solutions that are simple to deploy, manage and use. Over 100 million users trust us for the best protection against today's complex threats, and analysts endorse us as a leader.

The company has more than two decades of experience and a global network of threat analysis centers that allow us to respond rapidly to emerging threats. As a result, Sophos achieves the highest levels of customer satisfaction in the industry. Our headquarters are located in Boston, Mass., and Oxford, UK.

Contents

Introduction

Everyone knows about computer viruses. Or at least they think they do.

Thirty years ago, the first computer virus appeared, Elk Cloner, displaying a short poem when an infected computer booted up for the 50th time. Since then, cybercriminals have created millions of viruses and other malware—email viruses, Trojans, Internet worms, spyware, keystroke loggers—some spreading worldwide and making headlines.

Many people have heard about viruses that fill your computer screen with garbage or delete your files. In the popular imagination, malware still means pranks or sabotage. The early 1990s saw global panic about the Michelangelo virus. In the 2000s, when millions of computers were infected with the SoBig-F virus and primed to download unknown programs from the web at a set time, antivirus companies scrambled to persuade Internet service providers to shut down servers to avoid a doomsday scenario. Hollywood movies like *Independence Day* reinforced this perception, with virus attacks signaled by flashing screens and alarms.

However, this is far from the truth today. The threats are no less real now, but they are low-profile, well-targeted, and more likely to be about making cash than creating chaos.

Today, malware is unlikely to delete your hard disk, corrupt your spreadsheet, or display a message. Such cyber-vandalism has given way to more lucrative exploits. Today's viruses might encrypt all your files and demand a ransom. Or a hacker might blackmail a large company by threatening to launch a denial-of-service attack, which prevents customers from accessing the company's website.

More commonly, though, viruses don't cause any apparent damage or announce their presence at all. Instead, a virus might silently install a keystroke logger, which waits until the victim visits a banking website and then records the user's account details and password, and forwards them to a hacker via the Internet. The hacker is an identity thief, using these details to clone credit cards or plunder bank accounts. The victim isn't even aware that the computer has been infected. Once the virus has done its job, it may delete itself to avoid detection.

Another trend is for malware to take over your computer, turning it into a remote-controlled zombie. It uses your computer without your knowledge to relay millions of profit-making spam messages. Or, it may launch other malware attacks on unsuspecting computer users.

And as social networks like Facebook and Twitter have grown in popularity, hackers and cybercriminals are exploiting these systems to find new ways of infecting computers and stealing identities.

Hackers may not even target large numbers of victims any more. Such high-visibility attacks bring unwanted attention, and antivirus companies can soon neutralize malware that is widely reported. In addition, large-scale exploits can bring hackers more stolen data than they can handle. Because of this, threats are becoming more carefully focused.

Spearphishing is an example. Originally, phishing involved sending out mass-mail messages that appeared to come from banks, asking customers to re-register confidential details, which could then be stolen. Spearphishing, by contrast, confines itself to a small number of people, usually within an organization. The mail appears to come from colleagues in trusted departments, asking for password information. The principle is the same, but the attack is more likely to succeed because the victim thinks that the message is internal, and his or her guard is down.

Stealthy, small-scale, well-targeted: for now, this seems to be the way that security threats are going.

What of the future, though? Predicting how security threats will develop is almost impossible. Some commentators assumed that there would never be more than a few hundred viruses, and Microsoft's Bill Gates declared that spam would no longer be a problem by 2006. It's not clear where future threats will come from, or how serious they will be. What is clear is that whenever there is an opportunity for financial gain, hackers and criminals will attempt to access and misuse data.


AZ

A-Z of threats


TWO
FOR ON
BUY
ME

Adware

Adware is software that displays advertisements on your computer.

Adware, or advertising-supported software, displays advertising banners or pop-ups on your computer when you use an application. This is not necessarily a bad thing. Such advertising can fund the development of useful software, which is then distributed free (for example, Android apps, many of which are adware funded).

However, adware becomes a problem if it:

- installs itself on your computer without your consent
- installs itself in applications other than the one it came with and displays advertising when you use those applications
- hijacks your web browser in order to display more ads (see **Browser hijacker**)
- gathers data on your web browsing without your consent and sends it to others via the Internet (see **Spyware**)
- is designed to be difficult to uninstall

Adware can slow down your PC. It can also slow down your Internet connection by downloading advertisements. Sometimes programming flaws in the adware can make your computer unstable.

Advertising pop-ups can also distract you and waste your time if they have to be closed before you can continue using your PC.

Some antivirus programs detect adware and report it as potentially unwanted applications. You can then either authorize the adware program or remove it from your computer. There are also dedicated programs for detecting adware.

Anonymizing proxy

Anonymizing proxies allow the user to hide their web browsing activity. They are often used to bypass web security filters—e.g., to access blocked sites from a work computer.

Anonymizing proxies hold significant risks for organizations:

- Security: The anonymizing proxy bypasses web security and allows users to access infected webpages
- Liability: Organizations can be legally liable if their computers are used to view pornography, hate material or to incite illegal behavior. There are also ramifications if users violate third-party licenses through illegal MP3, film and software downloads
- Productivity: Anonymizing proxies can permit users to visit sites that, although safe, are often used for non-work purposes

Advanced persistent threat (APT)

Advanced persistent threats are a type of targeted attack. APTs are characterized by an attacker who has time and resources to plan an infiltration into a network.

These attackers actively manage their attack once they have a foothold in a network and are usually seeking information, proprietary or economic, rather than simple financial data. APTs are persistent in that they may remain on a network for some time before gaining access to the information they seek and stealing it. APTs should not be confused with more common botnets, which are usually opportunistic and indiscriminate attacks seeking any available victim rather than specific information.

Autorun worm

Autorun worms are malicious programs that take advantage of the Windows AutoRun feature. They execute automatically when the device on which they are stored is plugged into a computer.

Autorun worms are commonly distributed on USB drives, automatically infecting computers as soon as the USB is plugged in. AutoPlay is a similar technology to Autorun. It is initiated on removable media prompting users to choose to listen to music with the default media player, or to open the disk in Windows Explorer. Attackers have similarly exploited AutoPlay, most famously via the Conficker worm.

On patched and newer operating systems, Microsoft has set AutoRun to off by default. As a result, autorun worms should pose less of a threat in the future.

Backdoor Trojan

A backdoor Trojan allows someone to take control of a user's computer via the Internet without their permission.

A backdoor Trojan may pose as legitimate software to fool users into running it. Alternatively—as is increasingly common—users may allow Trojans onto their computer by following a link in spam email or visiting a malicious webpage.

Once the Trojan runs, it adds itself to the computer's startup routine. It can then monitor the computer until the user is connected to the Internet. When the computer goes online, the person who sent the Trojan can perform many actions—for example, run programs on the infected computer, access personal files, modify and upload files, track the user's keystrokes, or send out spam email.

Well-known backdoor Trojans include Netbus, OptixPro, Subseven, BackOrifice and, more recently, Zbot or ZeuS.

To avoid backdoor Trojans, you should keep your computers up to date with the latest patches (to close down vulnerabilities in the operating system), and run anti-spam and antivirus software. You should also use a firewall, which can prevent Trojans from accessing the Internet to make contact with the hacker.

Boot sector malware

Boot sector malware spreads by modifying the program that enables your computer to start up.

When you turn on a computer, the hardware looks for the boot sector program, which is usually on the hard disk (but can be on a floppy disk or CD), and runs it. This program then loads the rest of the operating system into memory.

Boot sector malware replaces the original boot sector with its own, modified version (and usually hides the original somewhere else on the hard disk). The next time you start up, the infected boot sector is used and the malware becomes active.

Boot sectors are now used by some malware designed to load before the operating system in order to conceal its presence (e.g., TDL rootkit).

Botnet

A botnet is a collection of infected computers that are remotely controlled by a hacker.

Once a computer is infected with a bot, the hacker can control the computer remotely over the Internet. From then on, the computer is a zombie, doing the bidding of the hacker, although the user is completely unaware. Collectively, such computers are called a botnet.

The hacker can share or sell access to control the botnet, allowing others to use it for malicious purposes.

For example, a spammer can use a botnet to send out spam email. Up to 99% of all spam is distributed this way. This allows the spammers to avoid detection and to get around any blacklisting applied to their own servers. It can also reduce their costs because the computer's owner is paying for the Internet access.

Hackers can also use zombies to launch a distributed denial-of-service attack, also known as a DDoS. They arrange for thousands of computers to attempt to access the same website simultaneously, so that the web server is unable to handle all the requests reaching it. The website thus becomes inaccessible.
(See **Zombie**, **Denial-of-service attack**, **Spam**, **Backdoor Trojan**, **Command and control center**)

Browser hijacker

Browser hijackers change the default homepage and search engine in your Internet browser without your permission.

You may find that you cannot change your browser's homepage once it has been hijacked. Some hijackers edit the Windows registry so that the hijacked settings are restored every time you restart your computer. Others remove options from the browser's tools menu, so that you can't reset the start page.

Browser hijacking is used to boost advertising revenue, as in the use of blackhat SEO, to inflate a site's page ranking in search results.

Browser hijackers can be very tenacious, as well as sneaky. Attackers use clickjacking, also known as a UI redress attack, by inserting multiple transparent, or opaque, layers on a webpage. This technique can trick a user into clicking on a button or link on a page other than the one they were intending to click on. Effectively the attacker is hijacking clicks meant for one page and routing them to other another page, most likely owned by another application, domain, or both.

Although these threats don't reside on your PC, they do affect your browsing experience.

Brute force attack

A brute force attack is one in which hackers try a large number of possible keyword or password combinations to gain unauthorized access to a system or file.

Brute force attacks are often used to defeat a cryptographic scheme, such as those secured by passwords. Hackers use computer programs to try a very large number of passwords to decrypt the message or access the system.

To prevent brute force attacks, it is important to make your passwords as secure as possible. (See **How to choose secure passwords**)


CAUTION
WET
FLOOR

Buffer overflow

A buffer overflow occurs when a program stores excess data by overwriting other parts of the computer's memory, causing errors or crashes.

Buffer overflow attacks take advantage of this weakness by sending more data to a program than it expects. The program may then read in more data than it has reserved space for and overwrite parts of the memory that the operating system is using for other purposes.

Contrary to popular belief, buffer overflows don't just happen in Windows services or core programs. They can occur in any application.

Buffer overflow protection (BOP) looks for code that uses buffer overflow techniques to target security vulnerabilities. (See **Exploit**, **Drive-by download**)

Chain letter

An electronic chain letter is an email that urges you to forward copies to other people.

Chain letters, like virus hoaxes, depend on you, rather than on computer code, to propagate themselves. The main types are:

- Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth
- False claims that companies are offering free flights, free mobile phones or cash rewards if you forward the email
- Messages that claim to be from agencies like the CIA and FBI, warning about dangerous criminals in your area
- Petitions that, even if genuine, continue to circulate long after they expire
- Jokes and pranks (e.g., the claim that the Internet would be closed for maintenance on April 1)
- On social networks like Facebook, posts asking users to share links, such as a photo of a sick infant that needs a heart transplant, or phony scares such as children being targeted with strawberry flavored drugs

Chain letters don't threaten your security, but they can waste time, spread misinformation and distract users from genuine email.

They can also create unnecessary email traffic and slow down mail servers. In some cases, the chain letter encourages people to send email to certain addresses so that they are deluged with unsolicited mail.

The solution to the chain letter problem is simple: Don't forward these messages. (See **Hoax**)

Command and control center

A command and control center (C&C) is a computer that controls a botnet (i.e., a network of compromised or zombie computers). Some botnets use distributed command and control systems, making them more resilient.

From the command and control center, hackers can instruct multiple computers to perform their desired activities.

Command and control centers are often used to launch distributed denial-of-service attacks because they can instruct a vast number of computers to perform the same action at the same time. (See **Botnet**, **Zombie**, **Denial-of-service attack**)


Cookies

Cookie

Cookies are files placed on your computer that allow websites to remember details.

When you visit a website, it can place a file called a cookie on your computer. This allows the website to remember your details and track your visits. Cookies can be a threat to confidentiality, but not to your data.

Cookies were designed to be helpful. For example, if you submit your ID when you visit a website, a cookie can store this data so you don't have to re-enter it the next time. Cookies also have benefits for webmasters, as they show which webpages are most used, providing useful input when planning a redesign of the site.

Cookies are small text files and cannot harm your data. However, they can compromise your confidentiality. Cookies can be stored on your computer without your knowledge or consent, and they contain information about you in a form you can't access easily. And when you revisit the same website, this data is passed back to the web server, again without your consent.

Websites gradually build up a profile of your browsing behavior and interests. This information can be sold or shared with other sites, allowing advertisers to match ads to your interests, display consecutive ads as you visit different sites, and track the number of times you have seen an ad.

If you prefer to remain anonymous, use the security settings on your Internet browser to disable cookies.

Data leakage

Data leakage is the unauthorized movement of information, usually outside an organization. It can be deliberate (data theft) or accidental (data loss).

Data leakage prevention is a top concern for organizations, with data breach scandals frequently popping up in the headlines. Many corporate and government organizations have failed to protect their confidential information, including the identities of their workforce, their customers and the general public.

Users routinely use and share data without giving sufficient thought to confidentiality and regulatory requirements.

A variety of techniques can be used to prevent data leakage. These include antivirus software, encryption, firewalls, access control, written policies and improved employee training. (See **Data loss**, **Data theft**, **How to secure your data**)

Data loss

Data loss is the result of the accidental misplacement of data, rather than its deliberate theft.

Data loss frequently occurs through the loss of a device containing data, such as a laptop, tablet, CD-ROM, mobile phone or USB stick. When these are lost, the data is at risk of falling into the wrong hands unless a strong data security technique is used. (See **Data leakage**, **Data theft**, **How to secure your data**)

Data theft

Data theft is the deliberate theft of information, rather than its accidental loss.

Data theft can take place both inside an organization (e.g., by a disgruntled employee), or by criminals outside the organization.

In 2012 these thefts included hackers breaking into a Belgian credit provider, Dexia, and demanding payment (blackmail) of €150,000 (US$197,000) to prevent the hackers from publishing confidential information.
Another example is India-based call center workers who were selling confidential information on nearly 500,000 British citizens including names, addresses, phone numbers and credit card numbers.

Some other recent data thefts include some of the biggest in history:

- 2007: The TJX Companies discloses theft of 45.6M credit and debit card numbers, costing the retailer $256M
- 2009: Heartland Payment Systems discloses breach of 100M records, costing the credit card processor nearly $140M
- 2011: Email marketing company Epsilon leaks millions of names and email addresses from customer databases of Best Buy, Marks & Spencer and Chase Bank. Initial cost-containment and remediation is estimated at $225M, but could reach as high as $4B
- 2011: Sony Corp suffers breaches that place 100M customer accounts at risk, costing the company up to $2 billion
- 2011: Servers are breached for Global Payments, a payments processor for Visa, exposing information on as many as 7M card holders

Criminals often use malware to access a computer and steal data. A common approach is to use a Trojan to install keylogging software that tracks everything the user types, including usernames and passwords, in order to access the user's bank account.

Data theft also occurs when devices containing data, such as laptops or USB drives, are stolen.
(See **Data leakage**, **Data loss**, **How to secure your data**)

Denial-of-service attack

A denial-of-service (DoS) attack prevents users from accessing a computer or website.

In a DoS attack, a hacker attempts to overload or shut down a service so that legitimate users can no longer access it. Typical DoS attacks target web servers and aim to make websites unavailable. No data is stolen or compromised, but the interruption to the service can be costly for a company.

The most common type of DoS attack involves sending more traffic to a computer than it can handle. There are a variety of methods for DoS attacks, but the simplest and most common is to have a botnet flood a web server with requests. This is called a distributed denial-of-service attack (DDoS). (See **Backdoor Trojan**, **Zombie**)

DNS hijacking

The Domain Name System (DNS) is the phone book of the Internet. It allows computers to translate website names, like www.sophos.com, into IP address numbers so that they can communicate with each other.

A DNS hijacking attack changes a computer's settings to either ignore DNS or use a DNS server that is controlled by malicious hackers. The attackers can then send false IP numbers to the computer and redirect its communication. DNS hijacking is commonly used to redirect users to fake login pages for banks and other online services in order to steal their login credentials. It can also be used to redirect security sites to non-existent servers to prevent affected users from updating their security software.

Document malware

Document malware takes advantage of embedded script or macro content in document files.

Macro viruses infecting Microsoft Office documents first appeared in the mid-1990s and rapidly became the most serious threat of that time. In recent years, malicious content designed to exploit vulnerabilities is now much more common than older macro viruses. By embedding malicious content within documents, hackers can exploit vulnerabilities in the host applications used for opening the documents. (See **Exploit**)

Drive-by download

A drive-by download is the infection of a computer with malware when a user visits a malicious website.

Drive-by downloads occur without the knowledge of the user. Simply visiting an infected website may be sufficient for the malware to be downloaded and run on a computer. Malware exploits vulnerabilities in a user's browser (and browser plugins) in order to infect their computer.

Hackers continually attack legitimate websites in order to compromise them, injecting malicious code into their pages. Then, when a user browses that legitimate (but compromised) site, the injected code is loaded by his/her browser, which initiates the drive-by attack. In this manner, the hacker can infect users without having to trick them into browsing a specific site.

To defend against drive-by downloads, you should have endpoint security software coupled with web security filtering. (See **Exploit**)

Email malware

Email malware refers to malware that is distributed via email.

Historically, some of the most prolific virus families (e.g., Netsky or SoBig) distributed themselves as file attachments in email. These families relied on users double-clicking an attachment, which would run the malicious code, infect their machine and send itself to more email addresses from that computer.

Nowadays, hackers have changed their focus and mainly use the web for malware distribution. They still use email messages, but mostly as a way of distributing links to malicious sites, not for carrying malicious file attachments. However, even today some malware families such as Bredo use email distribution to run malicious code on user machines.

You should use strong anti-spam security in conjunction with endpoint security software to defend against email malware. In addition, user education can raise awareness of email scams and seemingly innocent attachments from strangers. (See **Exploit**, **Botnet**)

Exploit

An exploit takes advantage of a vulnerability in order to access or infect a computer.

Usually an exploit takes advantage of a specific vulnerability in an application and becomes obsolete when that vulnerability is patched. Zero-day exploits are those that are used or shared by hackers before the software vendor knows about the vulnerability (and so before there is any patch available).

To secure against exploits, you should make sure your antivirus or endpoint security software is active and your computers are fully patched. This includes the operating system (OS) as well as applications. (See **Vulnerability**, **Drive-by download**, **Buffer overflow**)

Fake antivirus malware

Fake antivirus malware reports non-existent threats in order to scare the user into paying for unnecessary product registration and cleanup.

Fake antivirus malware is commonly known as scareware. Typically it is installed through malicious websites and takes the form of fake online scans. Cybercriminals attract traffic to these sites by sending out spam messages containing links or by compromising legitimate websites. Frequently they also attempt to poison the results of popular search engines (blackhat SEO) so that users access the malicious distribution sites when conducting a search.

Fake antivirus malware is financially motivated and is a big earner for cybercriminals. The large profits provide significant resources for investment into creation and distribution of fake antivirus. Hacking gangs are very good at rapidly producing professional-looking bogus websites that pose as legitimate security vendors.

Using up-to-date, legitimate antivirus or endpoint security software will protect you against fake antivirus software.

Hacktivism

Hacktivists typically hack for political purposes, attacking corporations, governments, organizations and individuals.

These groups may deface websites, redirect traffic, launch denial-of-service attacks and steal information to make their point.

Hacktivist group LulzSec dominated headlines in 2011 with attacks on Sony, PBS, the U.S. Senate, the CIA, FBI affiliate InfraGard and others, and then disbanded after 50 days.

Anonymous, a loosely-affiliated international hacking group, claims that its tactics initiate civil disobedience. For example, Anonymous has been suspected of taking down sites in El Salvador, Israel and the city of Toronto through distributed denial-of-service attacks. Hackers affiliated with the group also released 90,000 email addresses of U.S. military personnel in an attack on Booz Allen Hamilton.

The variety of targets seems to show that almost any institution could be at risk, although only a tiny minority is affected by hacktivist attacks. Significantly, law enforcement organizations have arrested many members of LulzSec and Anonymous.

Encryption is the best way to protect against hackers and unauthorized access of sensitive data.

Hoax

Hoaxes are reports of non-existent viruses or threats.

Hoaxes are usually in the form of emails that do some or all of the following:

- Warn you that there is an undetectable, highly destructive new piece of malware
- Ask you to avoid reading emails with a particular subject line (e.g., “Justin Bieber”)
- Claim that the warning was issued by a major software company, Internet provider or government agency (e.g., IBM, Microsoft, AOL or the FCC)
- Claim that the new malware can do something improbable (e.g., the “A moment of silence hoax” says that “no program needs to be exchanged for a new computer to be infected”)
- Use techno-babble to describe malware effects (e.g., Sector Zero claims that the malware can “destroy sector zero of the hard drive”)
- Urge you to forward the warning
- Claim that liking a story or individual on Facebook can result in financial windfalls, charitable contributions and free prizes

Many users forwarding such hoax emails can cause a deluge of email, which may overload mail servers. Hoax messages may also distract from efforts to deal with real malware threats.

Since hoaxes aren’t malware, your antivirus and endpoint security software can’t detect or disable them.

Honeypot

A honeypot is a form of trap security specialists use to detect hacking attacks or collect malware samples.

There are many different types of honeypots. Some consist of machines connected to the network that are used to capture network worms. Others provide fake network services (e.g., a web server) in order to log incoming attacks.

Honeypots are frequently used by security specialists or researchers to gather information about current threats and attacks.

Internet worm

Worms are viruses that create copies of themselves across the Internet or local networks.

Worms differ from computer viruses because they can propagate themselves, rather than using a carrier program or file. They simply create exact copies of themselves and use communication between computers to spread.

The Conficker worm is an example of an Internet worm that exploits a system vulnerability to infect machines over the network. Such worms are capable of spreading very rapidly, infecting large numbers of machines.

Some worms open a “back door” on the computer, allowing hackers to take control of it. Such computers can then be used to send spam mail (see **Zombie**).

Operating system vendors regularly issue patches to fix security loopholes in their software. To stay protected, turn on automatic updating to receive regular security updates for Windows or Apple machines.

In-the-cloud detection

In-the-cloud detection uses real-time online checking of data in order to detect threats.

The goal of in-the-cloud detection is to reduce the time taken for a security product to use a new malware signature. By querying data published online (i.e., "in the cloud"), security products avoid having to send out signatures to computers.

In-the-cloud detection offers a very rapid response to new threats as they are discovered, but it has the drawback that it requires an Internet connection in order to do the checking.

Keylogging

Keylogging is when keystrokes are secretly recorded by an unauthorized third party.

This is a common payload in malware because it is an effective way to steal usernames, passwords, credit card details and other sensitive data.

Malware

Malware is a general term for malicious software including viruses, worms, Trojans and spyware. Many people use the terms malware and viruses interchangeably.

Antivirus software usually detects a wider range of threats than just viruses.

Mobile phone malware

Mobile phone malware is malware intended to run on mobile devices, such as smartphones or PDAs.

The first examples of malicious programs for mobile phones showed up in 2004. These programs initially targeted the Symbian operating system, but they marked only the beginning of the threat from mobile malware.

Since then, it's taken a relatively long time for cybercriminals to develop mobile malware in significant numbers. The big wave of mobile phone malware happened when a new generation of smartphones running Android or iOS operating systems became popular. Thousands of mobile malware variants have been discovered since late 2010, when the first malware samples for Android and iOS devices were identified.

Today, malware researchers have discovered many more malicious apps for Android than for iOS, most likely due to Android devices allowing their users to install apps using third-party sources. File sharing sites often host malicious versions of popular applications and games.

With mobile malware, similar to malware for personal computers, the focus for cybercriminals is on making money. Similar to Windows malware, mobile malware spreads fake antivirus applications and steals confidential information.

Other types of mobile malware send SMS messages or place calls to premium rate numbers, if the target device is a part of a mobile phone network.

Even trusted sources host applications that may pose a risk to the user's privacy. Many advertising frameworks may share a user's personally identifiable information, such as location or phone number. These applications may be classified as potentially unwanted applications (PUAs).

You can keep your mobile device free of mobile malware if you keep the mobile operating system current with security updates and by downloading and installing only applications from trusted sources such as Google Play and Apple iTunes. For devices running Android, we recommend installing security software such as Sophos Mobile Security.

Non-compliance

Non-compliance is the failure to comply with government or industry regulations regarding data privacy and security.

Non-compliance can be costly. Organizations may incur fines, suffer a loss of reputation or even face legal action.

A 2012 study by the Ponemon Institute shows that the average cost of a data breach was $6.7 million in the U.S., with an average cost per customer record of $204.

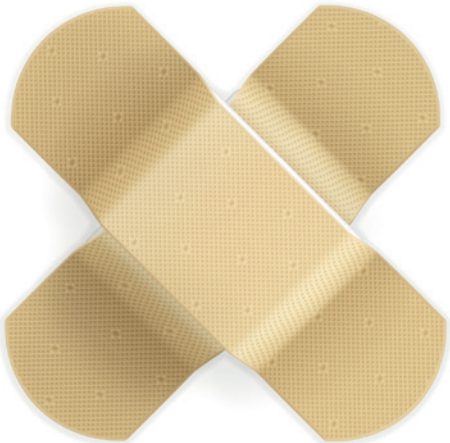
Parasitic virus

Parasitic viruses, also known as file viruses, spread by attaching themselves to programs.

When you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program.

The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory or make changes on your computer.

Parasitic viruses appeared early in virus history and then became quite rare. However, they are now becoming more common again with recent examples including Sality, Virut and Vetor.



Patch

Patches are software add-ons designed to fix software bugs, including security, in operating systems or applications.

Patching against new security vulnerabilities is critical to protect against malware. Many high-profile threats take advantage of security vulnerabilities, such as Conficker. If your patches are not applied or not up to date, you risk leaving your computer open to hackers.

Many software suppliers routinely release new patches, with Microsoft issuing fixes on the second Tuesday of each month ("Patch Tuesday"), and Adobe issuing quarterly updates to Adobe Reader and Acrobat on the second Tuesday after a quarter begins.

To stay abreast of the latest vulnerabilities and patches, subscribe to vulnerability mailing lists. Most reputable vendors offer such a service. For example, Microsoft security information is available at www.microsoft.com/technet/security/bulletin/notify.mspx.

Microsoft Windows home users can use Windows Update (Windows Vista/7) or Security Center (Windows XP) to turn on automatic updating. Apple OS X users can click the Apple logo in the upper-left corner of their desktop and select Software Updates.

Organizations should make sure that all computers connecting to their network abide by a defined security policy that includes having the latest security patches in place, including for operating systems and applications. (See **Exploit**, **Vulnerability**)


What's
your
name?

Phishing

Phishing refers to the process of tricking recipients into sharing sensitive information with an unknown third party.

Typically, you receive an email that appears to come from a reputable organization, such as:

- Banks
- Social media (Facebook, Twitter)
- Online games
- Online services with access to your financial information (e.g., iTunes, student loans, accounting services)
- Departments in your own organization (from your technical support team, system administrator, help desk, etc.)

The email includes what appears to be a link to the organization's website. However, if you follow the link, you are connected to a phony copy of the website. Any details you enter, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site.

Sometimes the link displays the genuine website but superimposes a bogus pop-up window. You can see the address of the real website in the background, but the details you enter in the pop-up window can be stolen.

To better protect against phishing attacks, it's good practice not to click on links in email messages. Instead, you should enter the website address in the address field and then navigate to the correct page, or use a bookmark or a Favorite link.

Phishing attacks via email are beginning to include an offline aspect to convince well-trained users to still leak information. We have seen phishing schemes use phone numbers and fax numbers in addition to websites.

Anti-spam software can block many phishing-related emails, and web security software can block access to phishing-related websites.

Potentially unwanted application (PUA)

Potentially unwanted applications are programs that are not malicious but may be unsuitable for use in a business environment.

Some applications are non-malicious and possibly useful in the right context, but are not suitable for company networks. Examples are adware, dialers, non-malicious spyware, tools for administering PCs remotely and hacking tools.

Certain antivirus and endpoint security programs can detect PUAs on users' computers and report them. The administrator can then either authorize the applications or remove them from the computers.

Ransomware

Ransomware is software that denies you access to your files until you pay a ransom.

In the past, malicious software typically corrupted or deleted data, but now it can hold your data hostage instead. For example, the Archiveus Trojan copies the contents of the My Documents folder into a password-protected file and then deletes the original files. It leaves a message telling you that you require a 30-character password to access the folder, and that you will be sent the password if you make purchases from an online pharmacy.

In that case, as in most ransomware so far, the password or key is concealed inside the Trojan's code and can be retrieved by malware analysts. However, in the future, hackers could use asymmetric or public-key encryption (which uses one key to encrypt the data, but another to decrypt it) so that the password would not be stored on your computer.

For example, in February 2012 the UK Metropolitan Police warned Windows users of a malware attack that poses as a message from computer crime-fighting cops. In this attack ransomware attempts to lock the computer, and posing as an official notice from a law enforcement agency, claims that the victim's PC has visited illegal websites. Only payment of a fine, claims the message, will restore the computer's functionality. However, the threats are a bluff as ransomware is not capable of doing these things.

Ransomware may become a problem as hackers start to use new means to get ransoms paid. Previously the use of premium rate SMS messages limited the usefulness to specific geographic areas.

Rootkit

A rootkit is a piece of software that hides programs or processes running on a computer. It can be used to conceal computer misuse or data theft.

A significant proportion of current malware installs rootkits upon infection to hide its activity. A rootkit can hide keystroke loggers or password sniffers, which capture confidential information and send it to hackers via the Internet. It can also allow hackers to use the computer for illicit purposes (e.g., to launch a denial-of-service attack against other computers, or send out spam email) without the user's knowledge.

Endpoint security products now detect and remove rootkits such as TDL and ZAccess as part of their standard anti-malware routines. However, some rootkits require a standalone removal tool to effectively remove them.

Social engineering

Social engineering refers to the tricks attackers use to fool victims into performing an action. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

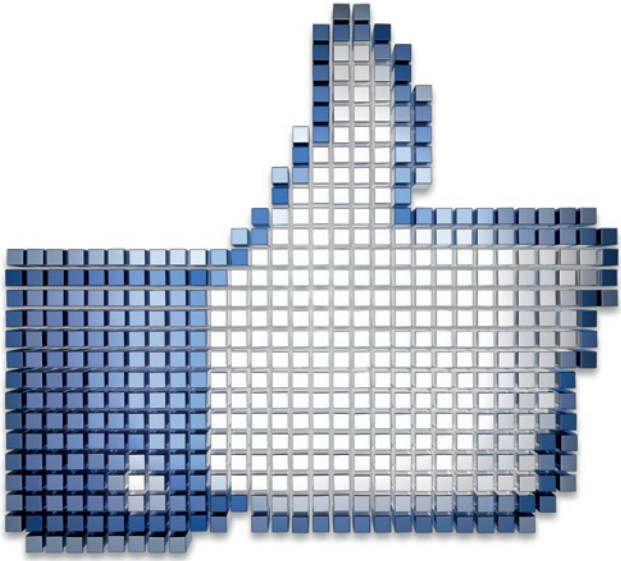
Many social engineering efforts are focused on tricking users into disclosing usernames or passwords, allowing attackers to send messages as an internal user to further their data stealing attempts.

In April 2012, hackers distributed a malware campaign pretending to be an email about a revealing photo of the recipient that was posted online. The email body featured a variety of messages with an attached ZIP file, which contained a Trojan.

Subject lines used in the spammed-out malware campaign included:

> RE: Check the attachment you have to react somehow to this picture
>
> FW: Check the attachment you have to react somehow to this picture
>
> RE: You HAVE to check this photo in attachment man
>
> RE: They killed your privacy man your photo is all over Facebook! NAKED!
>
> RE: Why did you put this photo online?

Keep your wits about you, and your antivirus up to date, and you should have little to fear.



Social networking

Social networking websites allow you to communicate and share information. But they can also be used to spread malware and to steal personal information.

Social networking giant Facebook revealed that 0.06% of the more than one billion logins each day are compromised. Put another way, that's more than 600,000 per day, or one every 140 milliseconds. By comparison, a blink of the eye takes 300-400 milliseconds.

Always take care about what links you click on, and don't enter your personal information until you are confident you have reached a legitimate site. (See **How to be safe on the Internet**)


BLAH
BLAH BLAH
BLAH

Spam

Spam is unsolicited bulk email, the electronic equivalent of junk mail, that comes to your inbox.

Spammers often disguise their email in an attempt to evade anti-spam software. Increasingly spam arrives via legitimate email addresses whose user credentials have been compromised, from services like Yahoo!, Hotmail and AOL. There is also a growing amount of "snowshoe spam" sent from leased static IP space (VPS), or cloud services.

Scammers are also targeting large email service providers (ESPs) with malware in an effort to compromise their mail transfer agents (MTA) in order to send spam.

Spam is often profitable. Spammers can send millions of emails in a single campaign for very little money. If even one recipient out of 10,000 makes a purchase, the spammer can turn a profit.

Does spam matter?

- Spam wastes staff time. Users without anti-spam protection have to check which email is spam and then delete it.
- Users can easily overlook or delete important email, confusing it with spam.
- Spam, like hoaxes or email viruses, uses bandwidth and fills up databases.
- Some spam offends users. Employers may be held responsible, as they are expected to provide a safe working environment.
- Spammers often use other people's computers to send spam (see **Zombie**).
- Spam is frequently used to distribute malware (see **Email malware**).

Spammers are now also exploiting the popularity of instant messaging and social networking sites such as Facebook and Twitter to avoid spam filters and to trick users into revealing sensitive and financial information.

Spearphishing

Spearphishing is targeted phishing using spoof emails to persuade people within a company to reveal sensitive information or credentials.

Unlike phishing, which involves mass-emailing, spearphishing is small-scale and well targeted. The spearphisher emails users in a single business. The emails may appear to come from another staff member at the same company, asking you to confirm a username and password.

Sometimes the emails seem to come from a trusted department that might plausibly need such details, such as IT or human resources. Links in the emails will redirect to a bogus version of the company website or intranet for stealing credentials. (See **Email malware**)

Spoofing

Email spoofing is when the sender address of an email is forged for the purposes of social engineering.

Spoofing can be put to a number of malicious uses.

Phishers (criminals who trick users into revealing confidential information) use spoofed sender addresses to make it appear that their email comes from a trusted source, such as your bank. The email can redirect you to a bogus website (e.g., an imitation of an online banking site), where your account details and password can be stolen.

Phishers can also send email that appears to come from inside your own organization (e.g., from a system administrator), asking you to change your password or confirm your details.

Criminals who use email for scams or frauds can use spoofed addresses to cover their tracks and avoid detection.

Spammers can use a spoofed sender address to make it appear that an innocent individual or company is sending out spam. Another advantage for them is that they are not inundated with non-delivery messages to their own email address.
(See **Email malware**)

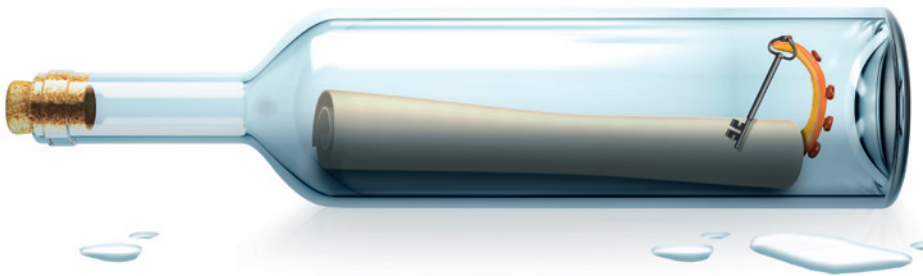
Spyware

Spyware is software that permits advertisers or hackers to gather sensitive information without your permission.

You can get spyware on your computer when you visit certain websites. A pop-up message may prompt you to download a software utility that it says you need, or software may be downloaded automatically without your knowledge.

When spyware runs on the computer, it may track your activity (e.g., visits to websites) and report it to unauthorized third parties, such as advertisers. Spyware consumes memory and processing capacity, which may slow or crash the computer.

Good antivirus and endpoint security solutions can detect and remove spyware programs, which are treated as a type of Trojan.



SQL injection

SQL injection is an exploit that takes advantage of database query software that doesn't thoroughly test for correct queries.

Cyber criminals use SQL injection along with cross-site scripting (XSS) and malware to break into websites and extract data or embed malicious code.

SQL injection sends commands to a web server linked to an SQL database. If the server is not correctly designed and hardened, it might treat data entered in a form field (such as username) as a command to be executed on the database server. For example, an attacker might enter a command string designed to output the entire contents of the database such as customer records and payment information.

Probably the most well-known data breach that employed an SQL injection attack occurred in March 2008, when hackers broke into the systems of payment processor Heartland Payment Systems and compromised 134 million credit card details.

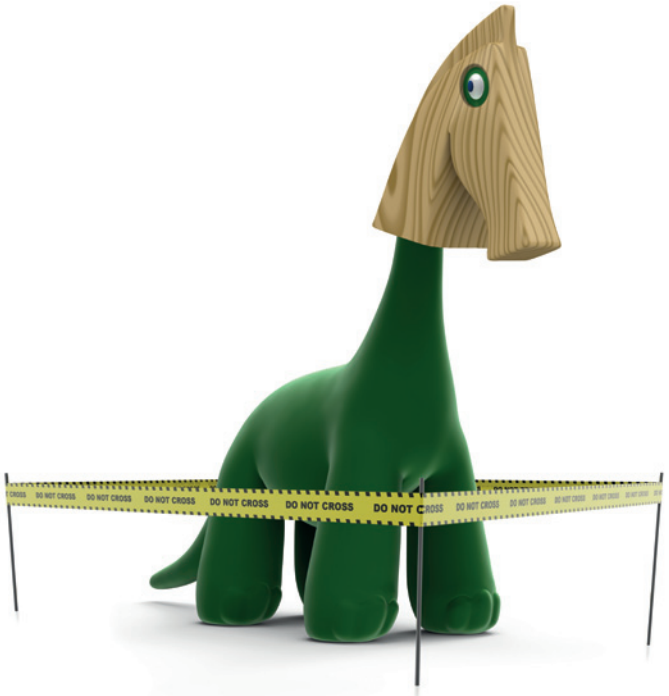
Web application firewalls (WAF) defend against this style of attack with an advanced system of "patterns" designed to detect SQL commands transmitted to the web server. As with any pattern-based system, to offer the best possible protection the patterns must be updated to counter new and creative ways of embedding SQL injection commands.

Suspicious files and behavior

When an endpoint security solution scans files, it labels them as clean or malicious. If a file has a number of questionable characteristics or behavior, it is labeled as suspicious.

Suspicious behavior refers to files doing questionable things when they run on a computer, such as copying themselves to a system folder.

Runtime protection helps protect against suspicious files by analyzing the behavior of all the programs running on your computer and blocking any activity that looks as if it could be malicious. (See **Buffer overflow**)


DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS

Trojan (Trojan horse)

Trojans are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

Trojan is an umbrella term covering many types of malware: bots, backdoor Trojans and downloader Trojans.

A large percentage of today's malware is Trojans.

A Trojan program pretends to do one thing, but actually does something different, usually without your knowledge. Popular examples are video codecs that some sites require to view online videos. When a Trojan codec is installed, it may also install spyware or other malicious software.

Another example is a malicious link that says "Cool Game." When you download and install the game program, it turns out not to be a game at all, but a harmful Trojan that compromises your computer or erases the data on your hard drive.

Trojans are often distributed with pirated software applications and keygens that create illegal license codes for downloadable software.
(See **Backdoor Trojan**)

Virus

Viruses are computer programs that can spread by making copies of themselves.

Computer viruses spread from one computer to another, and from one network to another, by making copies of themselves, usually without your knowledge.

Viruses can have harmful effects such as displaying irritating messages, stealing data, or giving hackers control over your computer.

Viruses can attach themselves to other programs or hide in code that runs automatically when you open certain types of files. Sometimes they can exploit security flaws in your computer's operating system to run and spread automatically.

You might receive an infected file in a variety of ways, including via an email attachment, in a download from the Internet, or on a USB drive. (See **Parasitic virus**, **Email malware**, **Internet worm**, **Malware**)


COMPUTER

Vulnerability

Vulnerabilities are bugs in software programs that hackers exploit to infect computers.

Security vulnerabilities can be found in any software product, leaving users open to attacks. Responsible software vendors, when aware of the problem, create and issue patches to address the problem.

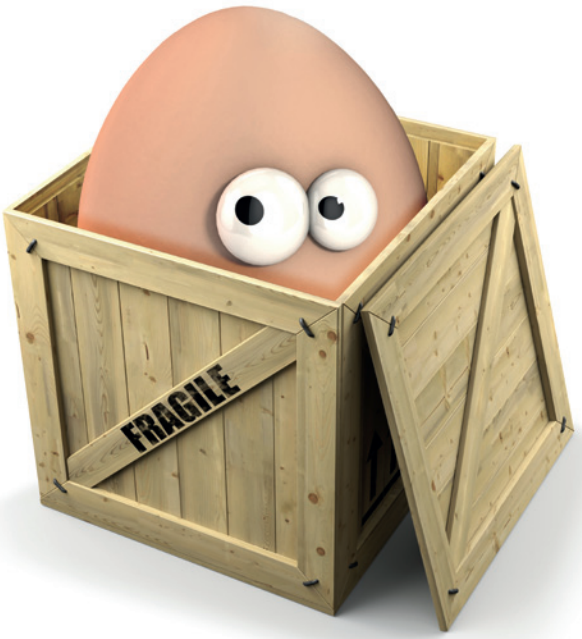
There are companies that pay researchers or ethical hackers for new vulnerabilities. There are also hackers that sell new vulnerabilities on the black market. These zero-day attacks refer to exploiting vulnerabilities before a patch is available.

To reduce vulnerabilities, you should run the latest available patches on your operating system and any installed applications. (See **Exploit**, **Patch**)

Zombie

A zombie is an infected computer that is remotely controlled by a hacker. It is often part of a botnet, which is a network of many zombie, or bot computers.

Once a hacker can control the computer remotely via the Internet, the computer becomes a zombie. (See **Botnet**)


FRAGILE

Security software and hardware


SOPHOS

Anti-malware

Anti-malware software can defend you against viruses and other malware threats including Trojans, worms and, depending on the product, spyware.

Anti-malware software uses a scanner to identify programs that are or may be malicious. Scanners can detect:

- Known malware: The scanner compares files on your computer against a library of identities for known malware. If it finds a match, it issues an alert and blocks access to the file. Detection of known malware relies on frequent updates to a database of the latest virus identities or connection to a cloud-based malware database.
- Previously unknown malware: The scanner analyzes the likely behavior of a program. If it has all the characteristics of a virus, access is blocked, even though the file does not match known viruses.
- Suspicious files: The scanner analyzes the likely behavior of a program. If that behavior is considered undesirable, the scanner warns that it may be malware. Most anti-malware packages offer both on-access and on-demand scanners.

On-access scanners stay active on your computer whenever you are using it. They automatically check files as you try to open or run them, and can prevent you from accessing infected files.

On-demand scanners let you start or schedule a scan of specific files or drives.

Anti-spam

Anti-spam programs can detect unwanted email and prevent it from reaching user inboxes.

These programs use a combination of methods to decide whether an email is likely to be spam. They can:

- Block email that comes from computers on a block list. This can be a commercially available list or a local list of computer addresses that have sent spam to your company before.
- Block email that includes certain web addresses.
- Check whether email comes from a genuine domain name or web address. Spammers often use fake addresses to try to avoid anti-spam programs.
- Look for keywords or phrases that occur in spam (e.g., “credit card,” “lose weight”).
- Look for patterns that suggest the email’s sender is trying to disguise his or her words (e.g., “hardc*re p0rn”).
- Look for unnecessary HTML code (the code used for writing webpages) within email, as spammers often use HTML to try to conceal their messages and confuse anti-spam programs.
- Combine all the information it finds to decide the probability of an email being spam. If the probability is high enough, it can block the email or delete it, depending on the settings you choose.

Anti-spam software needs frequent updating with new rules so it can recognize the latest techniques used by spammers.

Appliance

Appliances are a combination of hardware and software security elements in one solution. This lets you plug appliances in rather than installing the software separately.

The most common types of appliances are email appliances, unified threat management (UTM) appliances and web appliances. They sit at the gateway between an organization's IT systems and the Internet, filtering traffic to block malware, spam and data loss.

Email appliances block spam, phishing, viruses, spyware and other malware, and—depending on the solution—also employ content filtering and encryption to prevent the loss of confidential or sensitive information via email.

Web appliances block malware, spyware, phishing, anonymizing proxies and other unwanted applications at the web gateway. They may also offer tools to enforce Internet use policies.

UTM appliances eliminate the complexity of deploying and managing a variety of point solutions to protect your business against viruses, spam and hackers.

Application control

Application control allows you to control the use of applications that may be inappropriate for use on business computers or networks.

Controlling applications can stop apps from spreading malware and harming network and user productivity. This includes many consumer-based applications such as peer-to-peer file sharing software, games or media players.

You can use application control to restrict users to chosen business applications. For example, you can set a policy to only allow the use of Internet Explorer and block all other Internet browsers.

Categories of applications that businesses may wish to control include voice over Internet Protocol (VoIP), remote management tools and instant messaging clients.

In addition, next generation firewalls can filter network traffic based on type of traffic using specific ports.

Device control

Device control helps you control the use of removable storage, optical media drives and wireless networking protocols.

Device control is a central element of data loss prevention strategies, and also helps prevent malware that spreads through USB drives.

Many organizations use device control to enforce policies relating to the use of removable storage devices. Depending on the solution you have, device control can help you to decide which devices can connect to computers through a central policy.

Encryption

Encryption solutions secure your data by encrypting your desktops, laptops, removable media, CDs, email, network files, cloud storage and other devices. Information can only be accessed with the right keys to decrypt data by entering a password.

Some encryption solutions can be configured so that data is automatically decrypted for authorized users—so they don't need to enter an encryption key or password to access the information.

Depending on the product, encryption solutions often include key management (facilitating the storage, exchange and recovery of encryption keys), encryption policy enforcement, and centralized management and reporting features.

Encrypting any data you have stored by a third party is an important security measure. Additionally, mobile workers can access encrypted data on the go from their mobile devices, including smartphones and tablets.

Encryption solutions allow you to protect your confidential information and comply with regulatory mandates for data security.

Endpoint security

Endpoint security software protects computers or devices against a wide range of security, productivity and compliance threats, and lets you centrally manage the security of multiple endpoints.

Endpoint security products bring together in one solution the individual point products you need to protect against modern threats. They often integrate the protection for multiple features into one agent or central console, easing management and reporting. They can include:

- Antivirus software
- Firewalls
- Device control
- Network access control
- Application control
- Runtime protection
- Encryption technology
- Web security
- Patch management
- Data loss prevention

We recommend using endpoint security software with web content scanning capabilities. Malware is often delivered from websites. You should also consider turning on security filtering features in your web browser.

Firewall

A firewall prevents unauthorized access to a computer or a network.

As its name suggests, a firewall acts as a barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts.

A network firewall is installed on the boundary between two networks. This is usually located between the Internet and a company network. It can be a piece of hardware or software running on a computer that acts as a gateway to the company network.

A client firewall is software that runs on an end user's computer, protecting only that computer.

In either case, the firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it.

Firewalls can filter traffic based on:

- The source and destination addresses and port numbers (address filtering)
- The type of network traffic (e.g., HTTP or FTP protocol filtering)
- The attributes or state of the packets of information sent

A client firewall can also warn the user each time a program attempts to make a connection, and ask whether the connection should be allowed or blocked. It can gradually learn from the user's responses, so that it knows which types of traffic the user allows.

HTTPS scanning

Malware and other threats can hide in the encrypted traffic from trusted websites. HTTPS scanning decrypts, scans and then re-encrypts this data.

HTTPS scanning automatically finds and removes malicious content without human eyes viewing the content, maintaining the privacy of encrypted traffic.

IPS

Intrusion prevention systems (IPS) monitor network and systems for malicious activity.

IPS can log activity information, and also attempt to block activity and report it to network administrators to prevent network infections.

IPsec

IPsec authenticates and encrypts each Internet Protocol (IP) packet of a communication session.

IPsec includes protocols for establishing authentication between agents at the beginning of a session and negotiates cryptographic keys for use during the session.

Mobile device security

The incentive to attack mobile devices is growing along with our increasing reliance on these devices for banking and other transactions.

We've seen mobile malware disguised as fake online banking applications that attempt to steal customer credentials, intercept banking authentication token code via SMS, and drain bank accounts.

According to the Conficker Working Group, smartphone viruses are still fairly rare, but text-messaging attacks are becoming more common. Some malicious apps automatically send text messages to premium phone numbers, racking up unauthorized charges. SMS toll fraud apps have primarily targeted users in Europe.

Mobile device management solutions protect data everywhere and on any device. Your security solution should support a variety of mobile devices and operating systems and manage them from one web-based console. You can protect your data with a solution that can remotely locate, lock and wipe devices if they're lost or stolen.

Network access control (NAC)

A NAC solution protects your network and the information on it from the threats posed by users or devices accessing your network.

There are three main aspects to NAC:

- Authentication of users and devices to check they are who they say they are
- Assessment of computers attempting to access the network to make sure they are virus-free and meet your security criteria
- Enforcement of policies based on the role of the user so each person can access information appropriate to his or her role, while preventing inappropriate access to other information

Reverse proxy

A reverse proxy is a proxy server that retrieves resources on behalf of a client from other servers. These resources are then returned to the client from the reverse proxy.

Runtime protection

Runtime protection blocks attempts to access vulnerable parts of your computer.

Runtime protection analyzes the behavior of all the programs already running on your computer and blocks any activity that looks as if it could be malicious. For example, it checks any changes being made to the Windows registry, which may indicate that malware is installing itself so that it starts automatically whenever you restart the computer.

Runtime protection solutions include:

Host intrusion prevention systems (HIPS) monitor the behavior of code to stop malware before a specific detection update is released. Many HIPS solutions monitor code when it runs and intervene if the code is deemed to be suspicious or malicious.

Buffer overflow prevention systems (BOPS) will catch attacks targeting security vulnerabilities in both operating system software and applications. Attacks are reported when an attempt is made to exploit a running process using buffer overflow techniques.

URL content filtering

URL or web content filtering describes the technology that allows organizations to block categories or specific websites.

With this technology organizations can prevent access to unproductive and illegal sites through the corporate network, and block sites with known malware. This improves productivity while preventing network infections.

Unified threat management (UTM)

UTM integrates endpoint protection and management on the same gateway, simplifying setup and troubleshooting.

By integrating endpoint protection and its management into the gateway, a modern UTM extends the network perimeter to the endpoint and the cloud. So your network and data remain safe from threats no matter where people work, what device they use, or where they connect.

The Sophos UTM gives you the capability to:

- Easily configure and monitor protection with a browser-based interface, but without deep technical knowledge
- Deploy a solution that integrates firewall and intrusion prevention with web control, email security and endpoint protection
- Protect your endpoints against threats and data loss while managing them from within your UTM appliance
- Secure branch offices quickly with integrated VPN technology and our plug-and-protect Sophos RED (Remote Ethernet Device)
- Provide complete UTM security for wireless networks and clients through dedicated wireless access points
- Deploy policies for web protection, firewall or application control. You only have to configure policies once at the gateway and then synchronize with all endpoints, rather than configure separately for each endpoint
- Always keep endpoints connected to the gateway without requiring directory services or VPN connections to headquarters

VPN/SSL VPN

A virtual private network (VPN) is a method of connecting remote offices or PCs to the central network.

This method typically requires remote users to authenticate themselves by entering passwords or keys.

Web application control

Web application control blocks applications that could cause security or legal problems, like P2P or instant messaging.

It accelerates critical applications, such as Salesforce.com, by making sure they have appropriate bandwidth, while blocking or limiting unwanted, unproductive applications (e.g., blocking Facebook games and P2P sites such as Bittorrent or limiting YouTube streaming).

Web application firewall (WAF)

Hackers can use a number of attack methods to silently test your site and applications for security holes. Web application firewalls keep your servers safe by scanning activity and identifying probes and attacks.

A web application firewall is an otherwise traditional firewall appliance that also performs duties traditionally handled by multiple systems, including content filtering, spam filtering, intrusion detection and antivirus.

Organizations that implement an all-in-one web security solution gain distinct advantages over more costly and complex single-function web filtering solutions. A single point of control over web access and usage has a number of benefits:

Malware protection: Mitigate threats from malware, spyware, viruses, worms and other attacks with a robust first line of defense.

Reduced costs: Reduce IT management tasks and simplify routine maintenance and upgrades with a centrally managed appliance for web security.

Legal compliance: Comply with internal policies and legal mandates by blocking access to inappropriate or illegal web content.

Increased productivity: Prevent employees from surfing non-business sites during business hours, lowering the risk of infection from malware on questionable sites. And you can eliminate network-taxing activities such as bit streaming.

Wireless security

Wireless security is the prevention of unauthorized access or damage to computers on a wireless network.

The most common forms of wireless security are wired equivalent privacy (WEP) and Wi-Fi protected access (WPA). WEP is not as secure as WPA.

Safety tips

How to avoid viruses, Trojans, worms and spyware

Use antivirus or endpoint security software

Install antivirus or endpoint security software on all your desktops and servers, and make sure to keep them up to date. New malware can spread extremely quickly, so have an infrastructure in place that can update all the computers in your company seamlessly, frequently and on short notice.

To protect your business from the threats of email-borne viruses, spam and spyware, run email filtering software at your email gateway.

And don't forget to protect your laptop computers and desktop computers used by home workers. Viruses, worms and spyware can easily use these devices to enter your business.

Block file types that often carry malware

Block executable file types; it is unlikely that your organization will ever need to receive these types of files from the outside world.

Subscribe to an email alert service

Consider adding a live malware information feed to your website or intranet so your users know about the very latest computer threats. A great source for up-to-date news is Naked Security at http://nakedsecurity.sophos.com.

Use a firewall on all computers

You should use a firewall to protect computers that are connected to a network. Many worms can enter even a closed network via USB drives, CDs and mobile devices. Laptops and home workers will also need firewall protection.

Stay up to date with software patches

We encourage using automatic (patch) updating, especially in the case of Windows computers. Patches often close loopholes that can make you vulnerable to malware threats.

Back up your data regularly

Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store your backups, perhaps even off-site in case of fire. If your computer is infected with malware, you will be able to restore any lost programs and data. Any sensitive backup information should be encrypted and physically secured.

Implement device control

Prevent unauthorized devices from connecting to your computers. Unauthorized devices such as USB drives, music players and mobile phones can carry malware that will infect a computer when plugged in.

Disable AutoRun functionality

In February 2011 Microsoft automatically disabled AutoRun, preventing malware from copying itself to host computers and shared network drives from devices such as USB drives.

How to avoid hoaxes

Have a company policy on virus warnings

Set up a company policy on virus warnings. For example:

> "Do not forward any virus warnings of any kind to anyone other than the person responsible for antivirus issues. It doesn't matter if the virus warnings come from an antivirus vendor or have been confirmed by a large computer company or your best friend. All virus warnings should be sent to [name of responsible person] only. It is their job to notify everybody of virus warnings. A virus warning that comes from any other source should be ignored."

Stay informed about hoaxes

Stay informed about hoaxes by visiting the Hoaxes pages on our website at www.sophos.com/security/hoaxes/.

Don't forward chain letters

Don't forward a chain letter, even if it offers you rewards for doing so or claims to distribute useful information.

How to secure your data

Encrypt your computers, emails and other devices

By encrypting your data, you can make sure that only authorized users with the appropriate encryption key or password can access the information. With encryption you can keep your data secure at all times, even if it is stored on a laptop, CD or other device that is lost or stolen, or if it's contained in an intercepted email.

Use device and application control

Prevent users from accessing peer-to-peer file sharing and USB drives. These are common paths for data loss.

Only allow compliant computers to access your network.

Only allow computers that comply with your security policy to access your network. This could include requirements for encryption, or device or application control technologies.

Block employee access to cloud based mail services

Put controls in place to monitor or block employee use of cloud storage services such as Dropbox. These controls should include applying web-based URL filtering, application controls and data encryption. You can prohibit access and transfer of confidential information to largely unsecured cloud-based storage services.

Implement outbound content controls

Identify the sensitive data you want to control (e.g., any files containing the term "confidential" or credit card numbers) and then decide how these files can be used. For example, you may wish to present the user with a warning about potential data loss or prevent distribution of the data by email, blogs or forums.

An encryption solution allows users to choose their preferred cloud storage services because the files are always encrypted and the keys are always your own. And because encryption takes place on the client before any data is synchronized, you have full control of the safety of your data. You won't have to worry if the security of your cloud storage provider is breached.

Many endpoint security solutions and email and web appliances offer content filtering as part of their solution.

How to avoid spam

Use email filtering software at your email gateway

You should run email filtering software at the email gateway to protect your business from spam as well as email-borne spyware, viruses and worms.

Never make a purchase from an unsolicited email

By making a purchase, you are funding future spam. Spammers may add your email address to lists to sell to other spammers, so that you receive even more junk email. Worse still, you could be the victim of a fraud.

If you do not know the sender of an unsolicited email, delete it

Most spam is just a nuisance, but sometimes it can contain malware that damages or compromises the computer when the email is opened.

Don't use the preview mode in your email viewer

Many spammers can track when a message is viewed, even if you don't click on the email. The preview setting effectively opens the email and lets spammers know that you receive their messages. When you check your email, try to decide whether a message is spam on the basis of the subject line only.

Don't overexpose your email address

How much online exposure you give your email address is the biggest factor in how much spam you receive. Here are some bad habits that expose your email address to spammers:

- Posting your email address in plain text on websites
- Posting to mailing lists that are archived online
- Submitting your address to online services with questionable privacy practices
- Exposing your address publicly on social networks (Facebook, LinkedIn, etc.)
- Handing your business card out excessively
- Using an easily guessable address based on first name, last name and company
- Not keeping your work and personal email separate

Use the bcc field if you email many people at once

The bcc or blind carbon copy field hides the list of recipients from other users. If you put the addresses in the To field, spammers may harvest them and add them to mailing lists.

Never publish your email address on the Internet

Don't publish your email address on websites, newsgroup lists or other online public forums. Spammers use programs that surf the Internet to find addresses in such places.

Only give your main address to people you trust

Give your main email address only to friends and colleagues.

Use one or two secondary email addresses

If you fill out web registration forms or surveys on sites from which you don't want further information, use a secondary email address. This protects your main address from spam.

Opt out of further information or offers

When you fill out forms on websites, look for the checkbox that lets you choose whether to accept further information or offers. Check or uncheck the box as appropriate.

How to avoid being phished

Never respond to emails that request personal financial information

You should be suspicious of any email that asks for your password or account information, or includes links for that purpose. Banks and ecommerce companies do not usually send such emails.

Look for signs that an email is "phishy"

Phishing emails usually use a generic greeting, such as "Dear valued customer," because the email is spam and the phisher does not have your name. They may also make alarming claims (e.g., that your account numbers have been stolen or lost). The email often includes misspellings or substitute characters (e.g., "1nformatiOn") in an attempt to bypass anti-spam software.

Visit bank websites by typing the address into the address bar

Don't follow links embedded in an unsolicited email. Phishers often use these to direct you to a bogus site. Instead, you should type the full address into the address bar in your browser.

Keep a regular check on your accounts

Regularly log in to your online accounts and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.

Make sure that the website you are visiting is secure

Check the web address in the address bar. If the website you are visiting is on a secure server, it should start with https:// ("s" stands for secure) rather than the usual http://. Also look for a small padlock icon on the browser's status bar. These signs tell you that the website is using encryption.

However, even if a site is secure, there is no guarantee that it is safe because hackers can create websites that use encryption that are designed to steal personal information.

Be cautious with emails and personal data

Always conduct transactions safely. Don't let anyone know your PINs or passwords, do not write them down, and do not use the same password for all your online accounts. Don't open or reply to spam emails as this lets the sender know that your address is valid and can be used for future scams.

Keep your computer secure

Anti-spam software will prevent many phishing emails from reaching you. A firewall also helps to keep your personal information secure and block unauthorized communications. You should also run antivirus software to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails. Keep your Internet browser up to date with the latest security patches.

Always report suspicious activity

If you receive an email you suspect isn't genuine, forward it to the spoofed organization. Many companies have a dedicated email address for reporting such abuse.

How to be safe on the Internet

This section gives general advice on safely using email and the web. You should also see our tips on **How to avoid being phished** and **How to avoid viruses, Trojans, worms and spyware**.

Keep up to date with security patches

Hackers frequently exploit vulnerabilities in operating systems and programs in an attempt to infect computers. Be aware of security updates for your computer's operating system, browser, plugins and other code that could be the target of hackers. If you can, set up your computer to automatically download security patches.

Use firewalls

A network firewall is installed at your company boundary and admits only authorized types of traffic. A client firewall is installed on each computer on your network, and also allows only authorized traffic, blocking hackers and Internet worms. In addition, it prevents the computer from communicating with the Internet via unauthorized programs.

Don't follow links in unexpected emails

Links in unexpected emails can take you to bogus websites, where any confidential information you enter, such as account numbers and passwords, can be stolen and misused.

In addition, hackers often try to direct you to malicious webpages by spamming out links via email.

Use different passwords for every site

You should use a different password for each site where you have a user account. That way, if a password is compromised, only one account will be affected. In addition, make sure that your passwords are hard to guess and never use a dictionary word as your password.

Consider blocking access to certain websites or types of web content

In a company environment, you may want to prevent users from accessing sites that are inappropriate for workplace use, or that may pose a security threat (e.g., by installing spyware on computers) or offend someone. You can do this with web filtering software or a hardware appliance. Even if users are allowed to visit websites, you should make sure that all webpages they visit are scanned for security threats.

Scan email for malware and spam

Anti-spam programs can detect unwanted email and prevent it from reaching users' inboxes, as well as scan for malware contained within the email.

Don't click on pop-up messages

If you see unsolicited pop-ups, such as a message warning that a computer is infected and offering virus removal, don't follow links or click to accept software downloads. Doing so could result in you downloading malicious code such as fake antivirus software.

Use routers

You can use a router to limit connections between the Internet and specific computers. Many routers also incorporate a network firewall.

How to choose secure passwords

Passwords are your protection against fraud and loss of confidential information, but few people choose passwords that are really secure.

Make your password as long as possible

The longer a password is, the harder it is to guess or to find by trying all possible combinations (i.e., a brute force attack). Passwords of 14 characters or more are vastly more difficult to crack.

Use different types of characters

Include numbers, punctuation marks, symbols, and uppercase and lowercase letters. On mobile devices that are not designed for easy special character input, consider using longer passwords with different characters.

Don't use dictionary words

Don't use words, names or place names that are usually found in dictionaries. Hackers can use a dictionary attack (i.e., trying all the words in the dictionary automatically) to crack these passwords.

Don't use personal information

Other people are likely to know information such as your birthday, the name of your partner or child, or your phone number, and they might guess that you have used them as a password.

Don't use your username

Don't use a password that is the same as your username or account number.

Use passwords that are difficult to identify as you type them in

Make sure that you don't use repeated characters or keys close together on the keyboard.

Consider using a passphrase

A passphrase is a string of words, rather than a single word. Unlikely combinations of words can be hard to guess.

Try to memorize your password

Memorize your password rather than writing it down. Use a string of characters that is meaningful to you, or use mnemonic devices to help you recall the password. There are good free programs available that will help you manage your passwords.

Reputed password management programs can help you choose unique passwords, encrypt them and store them securely on your computer. Examples include KeePass, RoboForm and 1Password.

If you write down your password, keep it in a secure place

Don't keep passwords attached to your computer or in any easily accessible place.

Use different passwords for each account

If a hacker cracks one of your passwords, at least only one account has been compromised.

Don't tell anyone else your password

If you receive a request to confirm your password, even if it appears to be from a trustworthy institution or someone within your organization, you should never disclose your password (see **Phishing**).

Don't use your password on a public computer

Don't enter your password on a publicly available computer (e.g., in a hotel or Internet café). Such computers may not be secure and may have keystroke loggers installed.

Change your passwords regularly

The shorter or simpler your password is, the more often you should replace it.

How to use removable media securely

Educate users

Many users are not aware of the potential dangers from removable media such as USBs and CDs that spread malware and cause data loss. Educating users helps reduce the risks significantly.

Identify device types

Computers interact with a growing variety of removable media including USB drives, MP3 players and smartphones. Having visibility of what removable media is attempting to connect to your network can help you set appropriate restrictions or permissions.

Implement device control

Controlling the type of removable media that is permitted and what data is allowed to be exchanged is a vital component of network security. Choose solutions that can set permissions (or restrictions) for individual devices as well as entire classes of devices.

Encrypt your data

Data encryption prevents the loss of data. This is particularly useful for removable media that can be easily misplaced or stolen because the data cannot be viewed or copied by unauthorized third parties.

How to buy online safely

Can you trust your common sense and intuition?

Unfortunately, it isn't practical for users to determine if a website is safe or not with the naked eye.

Although invisible to the visiting online customer, hackers often target improperly secured legitimate websites. Being a large, well-established company is no guarantee that the site is safe.

Purchasing from a secure computer or device running the latest antivirus software, firewalls and security patches will significantly decrease your chances of becoming a victim.

Never follow links from unsolicited online communications, such as email, Twitter or Facebook. Spammers and hackers use social engineering techniques as lures to fraudulent or infected websites.

Only part with sensitive information like your personal or financial details when you are fully satisfied with the legitimacy of the company.

Familiarize yourself with the Terms of Use and the Data Protection Policy

Read the fine print. Terms can sometimes detail hidden and unexpected costs or obligations.

Only purchase through websites using encryption

URLs that start with https:// rather than http:// (the "s" stands for secure) are encrypting information during transfer. Another indicator of a website using encryption is a small padlock icon displayed in the Internet browser.

However, there is no guarantee that these sites are safe, as hackers can create websites that use encryption but are designed to steal personal information.

Provide the minimum amount of personal information

Leave optional fields blank: Middle name, date of birth, mobile phone number, hobbies. Many website operators request optional information alongside required information to process a business transaction. Compulsory fields are often identifiable by an asterisk.

Never share your password

Even if someone else is making the purchase for you, you should enter the password yourself and never share it with others.

To stop subsequent users from accessing your account without authorization, never select the "remember my password" option on a shared computer.

Buy local where possible

When the seller is based in a different country, it can be much more difficult and expensive to resolve any issues and to enforce consumer rights legislation.

Check your bank statements

Check your bank account transactions regularly, particularly after making purchases over the Internet, to be sure that all payments are legitimate. If you discover payments that you cannot identify, inform your bank immediately.

Keep your order confirmations and receipts

Always retain important information relating to a purchase in either printed or electronic format. This information will be very useful in resolving any issues relating to the purchase.

How to stay safe on the move

Educate users

Don't underestimate the risks of data loss from unsecured laptops or removable media. Organizations should develop clear policies concerning the use of mobile devices.

Use secure passwords

Passwords are the very first walls of defense and should always be as strong as possible. (See **How to choose secure passwords**)

Implement additional security checks

Smartcards or tokens require you to enter additional information (e.g., a token code together with your password) in order to access your computer. With fingerprint readers, you need to confirm your identity using your fingerprint when booting up or logging in.

Encrypt all important data

If your data is encrypted, it will remain safe even if your laptop or removable media is lost or stolen. If you don't want to encrypt your entire hard drive, you can create a virtual disk to store confidential information securely.

Restrict Plug and Play

Plug and Play allows USB drives, MP3 players or external hard drives to connect to laptops automatically, making it easy for data to be copied. Instead, lock the computer so only authorized devices are allowed to connect.

How to secure your mobile workforce

PDAs and smartphones are becoming standard business tools storing sensitive business information and enabling email on the move. This makes them vulnerable to attack from malware authors seeking out new ways to defraud users and steal confidential business data.

While mobile viruses and spyware remain a relatively small problem compared with the much larger amount of malware targeting Windows computers, the risks to business reputation, communication and continuity are becoming more serious. Risks include data theft, disruption of mobile phone networks and the hijacking of phones to send unauthorized revenue-generating SMS messages. SophosLabs™ has already identified over 30,000 examples of malicious mobile code.

Mobile devices can be infected in many ways including email, MMS, external memory cards, PC synchronization and even via Bluetooth.

Make sure your security policy includes a strategy for mobile devices, covering:

- Threat management—identification and removal of viruses, spyware and spam
- Device access control and management enforcing a password policy and application management
- Data protection—encryption of sensitive data on devices and remote data deletion
- Network access control—controlling VPN connections across public networks, validation of devices when they connect to the corporate network

Sophos Endpoint Protection protects critical business data while keeping users productive. Crucially, the software gives IT administrators the ability to implement and lock down consistent company-wide security policies for mobile devices.

Malware timeline

When did viruses, Trojans and worms begin to pose a threat?

Most histories of viruses start with the Brain virus, written in 1986. But that was just the first virus for a Microsoft PC. Programs with all the characteristics of viruses date back much farther. Here's a timeline showing key moments in virus history.

1949 Self-reproducing "cellular automata"

John von Neumann, the father of cybernetics, published a paper suggesting that a computer program could reproduce itself.

1959 Core Wars

H Douglas McIlroy, Victor Vysottsky, and Robert P Morris of Bell Labs developed a computer game called Core Wars, in which programs called organisms competed for computer processing time.

1960 "Rabbit" programs

Programmers began to write placeholders for mainframe computers. If no jobs were waiting, these programs added a copy of themselves to the end of the queue. They were nicknamed "rabbits" because they multiplied, using up system resources.

1971 The first worm

Bob Thomas, a developer working on ARPANET, a precursor to the Internet, wrote a program called Creeper that passed from computer to computer, displaying a message.

1975 Replicating code

A K Dewdney wrote Pervade as a sub-routine for a game run on computers using the UNIVAC 1100 system. When any user played the game, it silently copied the latest version of itself into every accessible directory, including shared directories, consequently spreading throughout the network.

1978 The Vampire worm

John Shoch and Jon Hupp at Xerox PARC began experimenting with worms designed to perform helpful tasks. The Vampire worm was idle during the day, but at night it assigned tasks to under-used computers.

1981 Apple virus

Joe Dellinger, a student at Texas A&M University, modified the operating system on Apple II diskettes so that it would behave as a virus. As the virus had unintended side-effects, it was never released, but further versions were written and allowed to spread.

1982 Apple virus with side effects

Rich Skrenta, a 15-year-old, wrote Elk Cloner for the Apple II operating system. Elk Cloner ran whenever a computer was started from an infected floppy disk, and would infect any other floppy put into the disk drive. It displayed a message every 50 times the computer was started.

1985 Mail Trojan

The EGABTR Trojan horse was distributed via mailboxes, posing as a program designed to improve graphics display. However, once run, it deleted all files on the hard disk and displayed a message.

1986 The first virus for PCs

The first virus for IBM PCs, Brain, was allegedly written by two brothers in Pakistan, when they noticed that people were copying their software. The virus put a copy of itself and a copyright message on any floppy disk copies their customers made.

1987 The Christmas tree worm

This was an email Christmas card that included program code. If the user ran it, it drew a Christmas tree as promised, but also forwarded itself to everyone in the user's address book. The traffic paralyzed the IBM worldwide network.

1988 The Internet Worm

Robert Morris, a 23-year-old student, released a worm on the US DARPA Internet. It spread to thousands of computers and, due to an error, kept re-infecting computers many times, causing them to crash.

1989 Trojan demands ransom

The AIDS Trojan horse came on a floppy disk that offered information about AIDS and HIV. The Trojan encrypted the computer's hard disk and demanded payment in exchange for the password.

1991 The first polymorphic virus

Tequila was the first widespread polymorphic virus. Polymorphic viruses make detection difficult for virus scanners by changing their appearance with each new infection.

1992 The Michelangelo panic

The Michelangelo virus was designed to erase computer hard disks each year on March 6 (Michelangelo's birthday). After two companies accidentally distributed infected disks and PCs, there was worldwide panic, but few computers were infected.

1994 The first email virus hoax

The first email hoax warned of a malicious virus that would erase an entire hard drive just by opening an email with the subject line "Good Times."

1995 The first document virus

The first document or "macro" virus, Concept, appeared. It spread by exploiting the macros in Microsoft Word.

1998 The first virus to affect hardware

CIH or Chernobyl became the first virus to paralyze computer hardware. The virus attacked the BIOS, which is needed to boot up the computer.

1999 Email viruses

Melissa, a virus that forwards itself by email, spread worldwide.

Bubbleboy, the first virus to infect a computer when email is viewed, appeared.

2000 Denial-of-service attacks

"Distributed denial-of-service" attacks by hackers put Yahoo!, eBay, Amazon and other high profile websites offline for several hours.

Love Bug became the most successful email virus yet.

2000 Palm virus

The first virus appeared for the Palm operating system, although no users were infected.

2001 Viruses spread via websites or network shares

Malicious programs began to exploit vulnerabilities in software, so that they could spread without user intervention. Nimda infected users who simply browsed a website. Sircam used its own email program to spread, and also spread via network shares.

2003 Zombie, Phishing

The Sobig worm gave control of the PC to hackers, so that it became a "zombie," which could be used to send spam.

The Mimail worm posed as an email from Paypal, asking users to confirm credit card information.

2004 IRC bots

Malicious IRC (Internet Relay Chat) bots were developed. Trojans could place the bot on a computer, where it would connect to an IRC channel without the user's knowledge and give control of the computer to hackers.

2005 Rootkits

Sony's DRM copy protection system, included on music CDs, installed a "rootkit" on users' PCs, hiding files so that they could not be duplicated. Hackers wrote Trojans to exploit this security weakness and installed a hidden "back door."

2006 Share price scams

Spam mail hyping shares in small companies ("pump-and-dump" spam) became common.

2006 Ransomware

The Zippo and Archiveus Trojan horse programs, which encrypted users' files and demanded payment in exchange for the password, were early examples of ransomware.

2006 First advanced persistent threat (APT) identified

First coined by the U.S. Air Force in 2006 and functionally defined by Alexandria, Virginia security firm Mandiant in 2008 as a group of sophisticated, determined and coordinated attackers. APTs are equipped with both the capability and the intent to persistently and effectively target a specific entity. Recognized attack vectors include infected media, supply chain compromise and social engineering.

2008 Fake antivirus software

Scaremongering tactics encourage people to hand over credit card details for fake antivirus products like AntiVirus 2008.

2008 First iPhone malware

The US Computer Emergency Response Team (US-CERT) issues a warning that a fraudulent iPhone upgrade, "iPhone firmware 1.1.3 prep," is making its way around the Internet and users should not be fooled into installing it. When a user installs the Trojan, other application components are altered. If the Trojan is uninstalled, the affected applications may also be removed.

2009 Conficker hits the headlines

Conficker, a worm that initially infects via unpatched machines, creates a media storm across the world.

2009 Polymorphic viruses rise again

Complex viruses return with a vengeance, including Scribble, a virus which mutates its appearance on each infection and used multiple vectors of attack.

2009 First Android malware

Android FakePlayerAndroid/FakePlayer.A is a Trojan that sends SMS messages to premium rate phone numbers. The Trojan penetrates Android-based smartphones disguised as an ordinary application. Users are prompted to install a small file of around 13 KB that has the standard Android extension .APK. But once the "app" is installed on the device, the Trojan bundled with it begins texting premium rate phone numbers (those that charge). The criminals are the ones operating these numbers, so they end up collecting charges to the victims' accounts.

2010 Stuxnet

Discovered in June 2010 the Stuxnet worm initially spreads indiscriminately, but is later found to contain a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems configured to control and monitor specific industrial processes. Stuxnet's most prominent target is widely believed to be uranium enrichment infrastructure in Iran.

2012 First drive-by Android malware

The first Android drive-by malware is discovered, a Trojan called NotCompatible that poses as a system update but acts as a proxy redirect. The site checks the victim's browser's user-agent string to confirm that it is an Android visiting, then automatically installs the Trojan. A device infected with NotCompatible could potentially be used to gain access to normally protected information or systems, such as those maintained by enterprise or government.

Boston, USA | Oxford, UK | **www.sophos.com**

3184.na.07.12

SOPHOS