Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years.
A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

Different types of firewalls

Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall

Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

See our UTM devices.

Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.
According to Gartner, Inc.'s definition, a next-generation firewall must include:

- Intelligence-based access control with stateful inspection
- Integrated intrusion prevention system (IPS)
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

- URL filtering based on geolocation and reputation

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
- Better detect evasive or suspicious activity with network and endpoint event correlation
- Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
- Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

Learn about our threat-focused firewalls.
See, try or buy a firewall.

Virtual firewall

A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (Amazon Web Services or AWS, Microsoft Azure, Google Cloud Platform or GCP, Oracle Cloud Infrastructure or OCI) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software-defined networks (SDN).

Learn about Cisco virtual firewalls for public cloud and private cloud.

Cloud Native Firewall

Cloud native firewalls are modernizing the way to secure applications and workload infrastructure at scale. With automated scaling features, cloud native firewalls enable networking operations and security operations teams to run at agile speeds.

Advantages of Cloud Native Firewalls

- Agile and elastic security
- Multi-tenant capability
- Smart load balancing

Learn about Cisco cloud-native firewalls.

What is packet filtering?

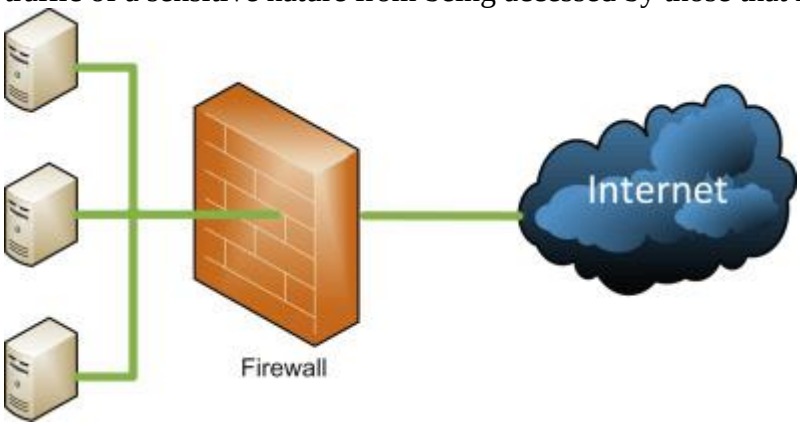
A packet filtering firewall is **a network security feature that controls the flow of incoming and outgoing network data**. The firewall examines each packet, which comprises user data and control information, and tests them according to a set of pre-established rules

Packet filtering can be used to detect malware by analyzing the contents of packets and identifying any malicious files or activities. Packet filtering can be used to detect malware by adding indicating data to packets requiring deep packet inspection and analyzing packet duplicates for malicious traffic

Firewalls

A firewall is a mechanism for maintaining control over the traffic that flows into and out of our network(s). The concept and first implementations of firewall technologies can be traced back to the late 1980s and early 1990s. One of the first papers to discuss the idea of using a firewall is titled "Simple and Flexible Datagram Access Controls," written in 1989 by Jeffrey Mogul [2], then at Digital Equipment Corporation (DEC). We can also see the first commercial firewall from DEC, the DEC SEAL, which shipped in 1992 [3].

A firewall is typically placed in a network where we see the level of trust change. We might see a firewall on the border between our internal network and the Internet, as shown in Figure 10.1. We may also see a firewall put in place on our internal network to prevent network traffic of a sensitive nature from being accessed by those that have no reason to do so.



Sign in to download full-size image

Figure 10.1. Firewall.

Many of the firewalls in use today are based on the concept of examining the packets that are coming in over the network. This examination determines what should be allowed in or out. Whether the traffic is allowed or blocked can be based on a variety of factors and largely depends on the complexity of the firewall. For example, we might allow or disallow traffic based on the protocol being used, allowing Web and e-mail traffic to pass, but blocking everything else.

Packet filtering

Packet filtering is one of the oldest and simplest of firewall technologies. Packet filtering looks at the contents of each packet in the traffic individually and makes a gross determination, based on the source and destination IP addresses, the port number, and the protocol being used, of whether the traffic will be allowed to pass. Since each packet is examined individually and not in concert with the rest of the packets comprising the content of the traffic, it can be possible to slip attacks through this type of firewall.

Stateful packet inspection

Stateful packet inspection firewalls (generally referred to as stateful firewalls) function on the same general principle as packet filtering firewalls, but they are able to keep track of the traffic at a granular level. While a packet filtering firewall only examines an individual packet out of context, a stateful firewall is able to watch the traffic over a given connection, generally defined by the source and destination IP addresses, the ports being used, and the already existing network traffic. A stateful firewall uses what is called a state table to keep track of the connection state and will only allow traffic through that is part of a new or already established connection. Most stateful firewalls can also function as a packet filtering firewall, often combining the two forms of filtering. For example, this type of firewall can identify and track the traffic related to a particular user-initiated connection to a Web site, and knows when the connection has been closed and further traffic should not legitimately be present.

Deep packet inspection

Deep packet inspection firewalls add yet another layer of intelligence to our firewall capabilities. Deep packet inspection firewalls are capable of analyzing the actual content of the traffic that is flowing through them. Although packet filtering firewalls and stateful firewalls can only look at the structure of the network traffic itself in order to filter out attacks and undesirable content, deep packet inspection firewalls can actually reassemble the contents of the traffic to look at what will be delivered to the application for which it is ultimately destined.

To use an analogy, if we ship a package via one of the common parcel carriers, the carrier will look at the size and shape of the package, how much it weighs, how it is wrapped, and the sending and destination addresses. This is generally what packet filter firewalls and stateful firewalls can do. Now, if the parcel carrier were to do all of this as well as open the package and inspect its contents, then make a judgment as to whether the package could be shipped based on its contents, this would be much more in line with deep packet inspection. Although this technology has great promise for blocking a large number of the attacks, we see today it is slower and introduces some delay. Additionally the question of privacy is also raised. In theory, someone in control of a deep packet inspection device could read every one of our e-mail messages, see every Web page exactly as we saw it, and easily listen in on our instant messaging conversations.

Proxy servers

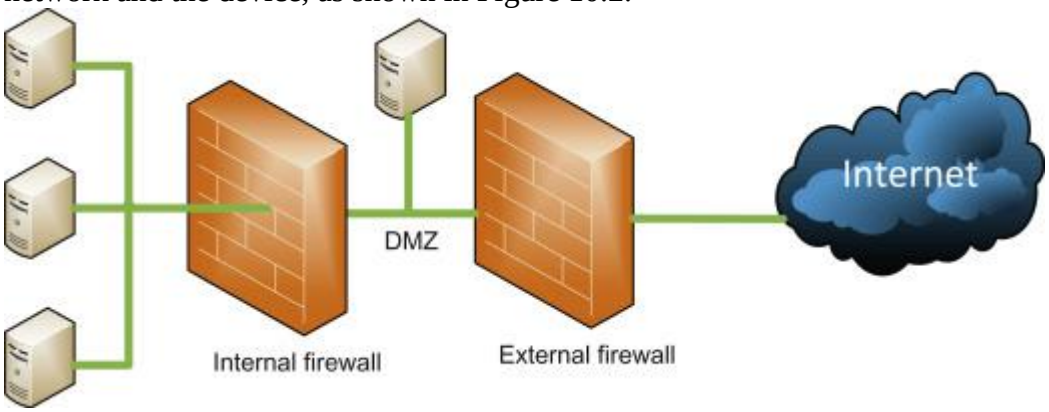
Proxy servers are ultimately a specialized variant of a firewall. These servers provide security and performance features, generally for a particular application, such as mail or Web browsing. Proxy servers can serve as a choke point (discussed earlier in the chapter) in order to allow us to filter traffic for attacks or undesirable content such as malware or traffic to Web sites hosting adult content. They also allow us to log the traffic that goes through them for later inspection, and they serve to provide a layer of security for the devices behind them, by serving as a single source for requests.

Proxy servers are nearly ubiquitous in the business world, largely due to the filtering capability they provide. Many companies rely on them to keep the large amounts of spam that flow over e-mail from reaching their users and lowering productivity. We also see them used to filter Web traffic in such environments in order to keep employees from visiting Web sites that might have objectionable material and to filter out traffic that might indicate the presence of malware. Again the major issue with them is delay introduced with additional step of inspection.

DMZs

A DMZ, or demilitarized zone, is generally a combination of a network design feature and a protective device such as a firewall. As we discussed earlier in the "Security in Network Design" section, we can often increase the level of security on our networks by segmenting

them properly. When we look at systems that need to be exposed to external networks such as the Internet in order to function, such as mail servers, proxy servers, software as a service application, and Web servers, we need to ensure their security and the security of the devices on the network behind them. We can often do this by putting a layer of protection between the device, such as our mail server, and the Internet, and between the rest of our network and the device, as shown in Figure 10.2.



Sign in to download full-size image

Figure 10.2. DMZ.

This allows only the traffic that needs to reach the mail server—for instance, Internet Message Access Protocol (IMAP) and Simple Message Transfer Protocol (SMTP) on ports 143 and 25, respectively—to reach our mail server, and the same ports to pass through on our network. Presuming that no other services are running on the same system, we could restrict the traffic going into and out of the DMZ where our mail server sits to those particular ports.
Read more

Local Area Network Security

Dr.Pramod Pandya, in Network and System Security (Second Edition), 2014

17 Packet Filtering: IP Filtering Routers

An IP packet-filtering router permits or denies the packet to either enter or leave the network through the interface (incoming and outgoing) on the basis of the protocol, IP address, and the port number. The protocol may be TCP, UDP, HTTP, SMTP, or FTP. The IP address under consideration would be both the source and the destination addresses of the nodes. The port numbers would correspond to the well-known port numbers. The packet-filtering firewall has to examine every packet and make a decision on the basis of defined ACL; additionally it will log the following guarded attacks on the network:

- A hacker will attempt to send IP spoofed packets using raw sockets (we will discuss more about usage of raw sockets in the next chapters)
- Log attempted network scanning for open TCP and UDP ports—NIDS will carry out this detective work in more detail
- SYN attacks using TCP connect(), and TCP half open
- Fragment attacks

Network packet capture is essential to any team tasked with keeping IT systems or networks secure, operational and performing at their best.

You may have heard the phrase ‘packets don’t lie’? This refers to the fact that, in the event of a cybersecurity or network performance issue, capturing network packets is often the only way to determine exactly what happened, how it happened, and who or what was impacted.

This is an introduction for those who want to learn about packet capture and associated technologies.

What is a Port?

A port is a point on a computer where information exchange between multiple programs and the internet to devices or other computers takes place. To ensure consistency and simplify programming processes, ports are assigned port numbers. This, in conjunction with an IP address, forms vital information that each internet service provider (ISP) uses to fulfill requests.

Port numbers range from 0 through to 65,536 and are ranked in terms of popularity. Ports numbered 0 to 1,023 are called “well-known" ports, which are typically reserved for internet usage but can also have specialized purposes. These ports, which are assigned by the Internet Assigned Numbers Authority (IANA), are held by leading businesses and Structured Query Language (SQL) services.

Password cracking typically refers to the process of recovering scrambled passwords. It can be used to help a user get back a forgotten password or to help a system administrator check for weak passwords. But more often, password cracking is used by bad actors to gain unauthorized access to systems and resources.

What is password cracking?

Password cracking is the process that involves computational methods to guess or retrieve a password from stored or transmitted data, typically employing algorithms executed by a computer. It is often used by hackers or malicious actors to gain unauthorized access to a target computer system or online account by guessing or cracking the password. It can be accomplished for several reasons, such as gaining access to sensitive information, stealing data or resources, conducting espionage, or carrying out malicious activities. Security professionals also use this method to test the strength of passwords and identify vulnerabilities in a system’s security. However, in most cases, password cracking is done with malicious intent and is considered illegal and unethical.

What techniques are used for password cracking?

There are several password-cracking techniques like brute force, dictionary search, hybrid, rainbow, guessing, phishing, or malware attack that can be used to crack passwords of various accounts like email accounts, social media accounts, and online banking accounts. Password

crackers (hackers or cybercriminals) mainly use brute force, dictionary search, hybrid, rainbow, and social engineering attacks to identify correct passwords.

- **Brute force attack:** In this method, the attacker repeatedly attempts to guess a password by systematically trying every possible character combination until a valid password is found. In this attack, the attacker uses a password-cracking tool that generates a list of possible passwords. The software tool can try different character combinations, including uppercase and lowercase letters, symbols, and numerical digits, and it can also try numerous word and phrase variations that are commonly used as passwords.
    - **Benefits:**
        1. Can eventually crack any password
        2. Effective against simple and short passwords
        3. Can be used against any encryption algorithm
    - **Drawbacks:**
        1. Time-consuming and resource-intensive
        2. Ineffective against complex and longer passwords
        3. Can be easily detected by security systems
- **Dictionary search attack:** In this method, the attacker uses a list of commonly used words or phrases, also known as a dictionary, to guess the password. The attacker uses a software program that automatically tests each word in the dictionary list against the password field of the target account.
    - **Benefits:**
        1. Faster than brute force attacks
        2. Can crack simple passwords
        3. Uses a pre-existing list of common passwords
    - **Drawbacks:**
        1. Limited to common passwords
        2. Ineffective against strong passwords
        3. Cannot crack passwords that are not in the dictionary
- **Hybrid attacks:** This method combines the techniques of dictionary attacks with brute force attacks. In this attack, the attacker starts with commonly used passwords or words from a dictionary and then tries variations of those words by adding every possible combination of characters like numbers, symbols, and lowercase or uppercase letters.
    - **Benefits:**
        1. Faster and more effective than brute force and dictionary attacks
        2. Allows for variations of commonly used passwords
        3. Can crack passwords with some level of complexity
    - **Drawbacks:**
        1. Time-consuming and resource-intensive

2. May not be effective against highly complex or unique passwords
3. Can be detected and blocked by some security systems

- **Rainbow attacks:** In this method, the attacker uses precomputed tables of encrypted passwords to look up the password for a given hash quickly. It is effective against poorly encrypted passwords.
  - **Benefits:**
    1. Can quickly crack weakly encrypted passwords
    2. Precomputed tables allow for quick password lookups
    3. Can be automated and scaled to target large numbers of passwords
  - **Drawbacks:**
    1. Requires a lot of processing power and storage space
    2. Not effective against strong passwords or well-encrypted passwords
    3. Precomputed tables may not include all possible passwords
- **Social engineering attacks:** In this method, attackers manipulate victims into disclosing sensitive information, like passwords, by posing as a legitimate authority figure. This attack can be very effective, as they exploit human psychology and emotions rather than technical vulnerabilities.
  - **Benefits:**
    1. Can be easier and faster than other methods
    2. Exploits human vulnerabilities
    3. Can bypass technical security measures
  - **Drawbacks:**
    1. Requires social skills and knowledge of human behavior
    2. Can be time-consuming to develop and execute
    3. Can be unethical and illegal

How a password hack works

Password cracking can be divided into two categories: online and offline attacks.

In an online password attack, a hacker attempts to enter the correct password on an app's login page, directly on the server. Online password attacks can be challenging to carry out, as they're limited by the speed of the network. They're also relatively easy to detect, due to the web noise generated by constant login requests.

On the other hand, offline password attacks provide hackers with more time and flexibility. In an offline password attack, a hacker intercepts one or more password hashes — algorithms used to encrypt passwords, converting plaintext passwords into unintelligible strings of letters,

numbers, and symbols, so they're harder to read and recognize when stored in a database. The hacker can then take these password hashes offline and unencrypt them using a password cracking tool.

Common password cracking techniques

There are many types of online and offline strategies cybercriminals use to crack user passwords. Ten of the most common include:

1. BRUTE FORCE ATTACK

In a brute-force password attack, a hacker tries to access a secure user account through trial and error. This typically involves systematically entering every possible combination of letters, numbers, and symbols into a password field until one works.

Today, almost all brute force attacks are carried out by bots, or automated software that can be programmed to carry out repetitive, predetermined tasks. Among other actions, bots can randomly generate passwords and quickly enter them into an app or website. This eliminates a lot of the time and hassle required to mount a brute force attack, making it a much more efficient and attractive method for hackers.

Simple cybersecurity measures — like account lockout systems, which block entry to certain IP addresses after a certain number of incorrect login attempts — can thwart a basic brute force attack. That's why, in recent years, hackers have developed the more sophisticated brute force methods outlined below.

2. PASSWORD SPRAYING

A password spray attack is a type of brute force attack in which, rather than trying many random passwords against a single account, a hacker tries the same password against many user accounts at once. This allows them to get around rudimentary security measures like account lockouts.

To maximize the impact of password spraying, hackers often employ weak or commonly used passwords (such as "password" or "123456") in their attacks, which they can source from public reports like NordPass's annual list of the 200 most common passwords.

3. CREDENTIAL STUFFING

Credential stuffing is another brute-force technique. In a credential stuffing attack, hackers use compromised credentials (which they've purchased from the dark web or obtained from a data breach) to log in to other, unrelated user accounts.

Unlike a traditional brute force attack, credential stuffing attacks aren't entirely random, as they rely on known username and password pairs. Since users tend to recycle the same credentials across multiple accounts, it's likely that one breached password will appear again on one of the other apps or websites that they use.

4. DICTIONARY ATTACK

In a dictionary attack, a hacker systematically enters common words and word variations from a specific, preselected list — kind of like a hacker "dictionary."

A dictionary attack can be tailored to a specific group or region that a hacker is targeting. For example, a hacker might use terms and phrases related to local businesses, landmarks, and sports teams when mounting a dictionary attack against a particular company or city.

While custom dictionary attacks can be dangerously effective, they tend to only work when users employ ordinary, everyday terms as passwords. That means enforcing strict password rules — like requiring users to create strong passwords with unique, randomized strings of characters — can be enough to prevent a dictionary attack.

5. MASK ATTACK

A mask attack is similar to a dictionary attack, but it's a far more targeted brute-force technique.

In a mask attack, a hacker analyzes recognizable password creation patterns and/or password hashes they've picked from known data breaches and uses them to apply a filter (or "mask") to their dictionary list of possible passwords. This dramatically reduces the total number of password guesses they must make for a given account, resulting in a much more efficient attack.

6. SPIDERING

Spidering is also intended to support a dictionary attack and similarly requires some dedicated effort on the part of the hacker.

In a spidering attack, a hacker gets to know their intended victim — generally, a larger, more established company — by studying their internal and external communications. This can include social media posts, web content, employee handbooks, product manuals, and even marketing style guides.

From there, the hacker can compile a list of identifying information and common keywords and business/product terms that are unique to the company. They can use these terms to generate a shortlist of possible credentials, which makes guessing passwords on key corporate accounts that much easier.

7. MAN-IN-THE-MIDDLE (MitM) ATTACK

Man-in-the-middle (MitM) attacks involve eavesdropping on or otherwise intercepting sensitive communications between the app or website a user is connected to and another, separate platform.

MitM attacks can take active or passive form. Active MitM attacks often manifest as session hijacking, where a hacker spies on web traffic over a given network, identifies active session IDs, and then uses the attached session tokens to breach a user's account.

In a passive MitM attack, a hacker might create a free, public wifi hotspot, like the kind offered at airports, cafes, and public parks. They then get a full view of all of the online activities and data exchanges carried out by unsuspecting users who join their fraudulent network.

8. RAINBOW TABLES

Rainbow tables are comprehensive directories that use a password hash algorithm to list out every possible plaintext version of an encrypted password. Think of it like a hacker "cheat sheet" that allows cybercriminals to skip the work of actually having to hack passwords or a password hash themselves.

In a rainbow table attack, a hacker consults this directory and matches the list of solved password hashes to encrypted passwords they find in a breached database, allowing them to successfully sign in to a user's account.

9. PHISHING

A phishing attack is less about cracking passwords and more about getting users to share them voluntarily, albeit through deceitful means.

Essentially, phishing is a form of social engineering. In a typical phishing attack, a hacker sends their intended victim a persuasive message via email or text, hoping to trick them into sharing their credentials or other sensitive information.

This can happen by way of a fraudulent link that, when clicked, downloads malicious software on a user's device, or via a spoofed website that gets the user to type their credentials into a fake login screen.

Phishing attacks can be random, or they can target specific individuals or organizations.

A common example of a random phishing attack involves an email scam, in which the author pretends to be the executor of a will, which they claim comes from a recipient's (fictional) long-lost relative. This fake executor promises to transfer a large sum of inheritance money to the recipient, but claims they need the recipient's bank account credentials in order to wire the funds. Of course, if the recipient provides these credentials, the hacker behind the scheme will simply breach their account and quickly drain their balance.

A more targeted phishing attack, on the other hand, might mimic the messages a certain company sends to help users reset passwords. By clicking an embedded reset-password link and/or entering their credentials, a user is actually giving a hacker access to their account or allowing them to install dangerous programs on their device.

10. MALWARE

Malware, short for "malicious software," refers to programs that are designed specifically for stealing passwords and other private information from a device where they have been (often unknowingly) installed.

Malware can piggyback on a link embedded within a phishing text or email, or it can hide within attachments, files, or websites that a user is tricked into opening or downloading.

Malware can take many different forms and work in a number of ways. Two categories of malware that can be used to crack passwords are:

- **Spyware:** Spyware hides on a user's system and secretly gathers information about their internet activity and behaviors, including any passwords, pins, and payment information they enter on an app or website.
- **Keyloggers:** Keyloggers are a specific type of spyware that monitors and records a user's keystrokes, or everything a user types into their device. That makes it easy for hackers to track and recognize common typing patterns, like a user's password for a given app or website.

- **Password cracking tools**
- Password cracking tools help hackers, well, crack passwords. They're especially useful in offline password attacks, where there might be thousands or even millions of possible plaintext combinations for each of the password hashes uncovered in a database breach. In this case, the right cracking tool can do all the computational work, applying strategic algorithms and machine learning to unencrypt each hash.
- Some of the most popular password cracking tools include:
- *JOHN THE RIPPER*
- John the Ripper (JTR) is one of the oldest and most well-known password crackers on the market. It's a command-based app that works in Linux and Mac OS environments, and it can automatically detect and support a wide range of hash types and ciphers.
- While John the Ripper's basic platform comes as free, open-source software, there is also a "pro" version of the app that includes a more extensive wordlist, as well as support for specific operating systems.
- *CAIN AND ABEL*
- Another leading password cracker is Cain and Abel (frequently shortened to just Cain). It's available for Windows only, and it uses a graphical user interface (GUI) format, which makes it particularly attractive to amateur or beginner hackers.

- Much like John the Ripper, Cain and Abel can recover passwords using a variety of password cracking and decrypting methods, including through brute-force and dictionary attacks.

- *OTHER PASSWORD CRACKING TOOLS*
- While JTR and Cain are the two most common password cracking tools, they are far from the only available options.

- There are many other password crackers on the market, including platforms like Ophcrack, Hashcat, and THC Hydra, all of which can pose a significant threat to your app and your users.

What is a keylogger?

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data. Some uses of keyloggers could be considered ethical or appropriate in varying degrees. Keylogger recorders may also be used by:

- employers to observe employees' computer activities;
- parents to supervise their children's internet usage;
- device owners to track possible unauthorized activity on their devices; or
- law enforcement agencies to analyze incidents involving computer use.

Types of keyloggers

A **hardware-based keylogger** is a small device that serves as a connector between the keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide the device.

A **keylogging software program** does not require physical access to the user's computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT). The

rootkit can launch and operate stealthily to evade manual detection or antivirus scans.

How do keyloggers work?

How a keylogger works depends on its type. Hardware and software keyloggers work differently due to their medium.Most workstation keyboards plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware keylogger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the keylogger collects each keystroke and saves it as text in its own hard drive, which may have a memory capacity up to several gigabytes. The person who installed the keylogger must later return and physically remove the device to access the gathered information. There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver.

A common software keylogger typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does the recording and an executable file that installs the DLL file and triggers it. The keylogger program records each keystroke the user types and periodically uploads the information over the internet to whomever installed the program. Hackers can design keylogging software to use keyboard application program interfaces (APIs) to another application, malicious script injection or memory injection.

There are two main types of software keyloggers: **user mode keyloggers** and **kernel mode keyloggers**.A user mode keylogger uses a Windows API to intercept keyboard and mouse movements. GetAsyncKeyState or GetKeyState API functions might also be captured depending on the keylogger. These keyloggers require the attacker to actively monitor each keypress.

A kernel mode keylogger is a more powerful and complex software keylogging method. It works with higher privileges and can be harder to locate in a system. Kernel mode keyloggers use filter drivers that can intercept keystrokes. They can also modify the internal Windows system through the kernel.

Some keylogging programs may also include functionality to record user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

Keylogger detection and removal

Due to the variety of keyloggers that use different techniques, no single detection or removal method is considered the most effective. Since keyloggers can manipulate an operating system kernel, examining a computer's Task Manager isn't necessarily enough to detect a keylogger.

Security software, such as an anti-keylogger software program, is designed specifically to scan for software-based keyloggers by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes. Using an anti-keylogger can be more effective than an antivirus or antispyware program. The latter may accidentally identify a keylogger as a legitimate program instead of spyware.

Depending on the technique an antispyware application uses, it may be able to locate and disable keylogger software with lower privileges than it has. Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.

Protection against keyloggers

While visual inspection can identify hardware keyloggers, it is impractical and time-consuming to implement on a large scale. Instead, individuals can use a firewall to help protect against a keylogger. Since keyloggers transmit data back and forth from the victim to the attacker, the firewall could discover and prevent that data transfer.

Password managers that automatically fill in username and password fields may also help protect against keyloggers. Monitoring software and antivirus software can also keep track of a system's health and prevent keyloggers.

System cages that prevent access to or tampering with USB and PS/2 ports can be added to the user's desktop setup. Extra precautions include using a security token as part of two-factor authentication (2FA) to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an onscreen keyboard and voice-to-text software to circumvent using a physical keyboard.

Application allow listing can also be used to allow only documented, authorized programs to run on a system. It is also always a good idea to keep any system up to date.

Hardware vs. software keyloggers

Keyloggers come in at least two broad flavors—hardware devices and the more familiar software variety. Hardware devices can be embedded in the internal PC hardware itself, or be an inconspicuous plugin that's secretly inserted into the keyboard port between the CPU box and the keyboard cable so that it intercepts all the signals as you type. But that means that the cybercriminal has to have physical access to the PC while you're not present in order to plant the hardware keyloggers.

Software keyloggers are much easier to introduce to and install on victims' devices, which is why that variety is much more common. Unlike other kinds of malware, software keyloggers are not a threat to the systems they infect themselves. In fact, the whole point of keyloggers is to work behind the scenes, sniffing out the keystrokes while the computer continues to operate normally. But even if they don't harm the hardware, keyloggers are definitely a threat to users, especially when they steal sensitive data.

Keystroke Logging Definition

The concept of a keylogger breaks down into two definitions:

1. **Keystroke logging**: Record-keeping for every key pressed on your keyboard.

2. **Keylogger tools:** Devices or programs used to log your keystrokes.

You'll find use of keyloggers in everything from Microsoft products to your own employer's computers and servers. In some cases, your spouse may have put a keylogger on your phone or laptop to confirm their suspicions of infidelity. Worse cases have shown criminals to implant legitimate websites, apps, and even USB drives with keylogger malware.

Whether for malicious intent or for legitimate uses, you should be aware how keyloggers are affecting you. First, we'll further define keystroke logging before diving into how keyloggers work. Then you'll be able to better understand how to secure yourself from unwanted eyes.

Types of Keyloggers

Keylogger tools are mostly constructed for the same purpose. But they've got important distinctions in terms of the methods they use and their form factor.

Here are the two forms of keyloggers

1. **Software keyloggers**
2. **Hardware keyloggers**

Software Keyloggers

Software keyloggers are computer programs that install onto your device's hard drive. Common keylogger software types may include:

API-based keyloggers directly eavesdrop between the signals sent from each keypress to the program you're typing into. Application programming interfaces (APIs) allow software developers and hardware manufacturers to speak the same "language" and integrate with each other. API keyloggers quietly intercept keyboard APIs, logging each keystroke in a system file.
"Form grabbing"-based keyloggers eavesdrop all text entered into website forms once you send it to the server. Data is recorded locally before it is transmitted online to the web server.
Kernel-based keyloggers work their way into the system's core for admin-level permissions. These loggers can bypass and get unrestricted access to everything entered in your system.

Hardware Keyloggers

Hardware keyloggers are physical components built-in or connected to your device. Some hardware methods may be able to track keystrokes without even being connected to your device. For brevity, we'll include the keyloggers you are most likely to fend against:

Keyboard hardware keyloggers can be placed in line with your keyboard's connection cable or built into the keyboard itself. This is the most direct form of interception of your typing signals.
Hidden camera keyloggers may be placed in public spaces like libraries to visually track keystrokes.
USB disk-loaded keyloggers can be a physical Trojan horse that delivers the keystroke logger malware once connected to your device.

keylogger or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a command-and-control (C&C) server. The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.

Types of Keyloggers

A software keylogger is a form of malware that infects your device and, if programmed to do so, can spread to other devices the computer comes in contact with. While a hardware keylogger cannot spread from one device to another, like a software keylogger, it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access.

Software Keyloggers

Software keyloggers consist of applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user's keystrokes.

A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.

After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger. This is done using a remote server that both the keylogger software and the hacker are connected to. The hacker retrieves the data gathered by the keylogger and then uses it to figure out the unsuspecting user's passwords.

The passwords stolen using the key logger may include email accounts, bank or investment accounts, or those that the target uses to access websites where their personal information can be seen. Therefore, the hacker's end goal may not be to get into the account for which the password is used. Rather, gaining access to one or more accounts may pave the way for the theft of other data.

Hardware Keyloggers

A hardware keylogger works much like its software counterpart. The biggest difference is hardware keyloggers have to be physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.

If an unauthorized individual is allowed to use a device on the network, they could install a hardware keylogger that may run undetected until it has already collected sensitive information. After hardware keystroke loggers have finished keylogging, they store the data, which the hacker has to download from the device.

The downloading has to be performed only after the keylogger has finished logging keystrokes. This is because it is not possible for the hacker to get the data while the key logger is working. In some cases, the hacker may make the keylogging device accessible via Wi-Fi. This way, they do not have to physically walk up to the hacked computer to get the device and retrieve the data.

Spyware Definition

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit. Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.
Spyware is one of the most commonly used cyberattack methods that can be difficult for users and businesses to identify and can do serious harm to networks. It also leaves businesses vulnerable to data breaches and data misuse, often affects device and network performance, and slows down user activity. The term "spyware" first emerged in online discussions in the 1990s, but only in the early 2000s did cybersecurity firms use it to describe unwanted software that spied on their user and computer activity. The first anti-spyware software was released in June 2000, then four years later, scans showed that around 80% of internet users had their systems affected by spyware, according to research by America Online and the National Cyber Security Alliance. However, 89% of users were unaware of the spyware's existence and 95% had not granted permission for it to be installed.

Types of Spyware

Attackers use various types of spyware to infect users' computers and devices. Each spyware variety gathers data for the attacker, with the lesser types monitoring and sending data to a third party. But more advanced and dangerous spyware types will also make modifications to a user's system that results in them being exposed to further threats.

Some of the most commonly used types of spyware include:

1. Adware: This sits on a device and monitors users' activity then sells their data to advertisers and malicious actors or serves up malicious ads.
2. Infostealer: This is a type of spyware that collects information from devices. It scans them for specific data and instant messaging conversations.
3. Keyloggers: Also known as keystroke loggers, keyloggers are a type of infostealer spyware. They record the keystrokes that a user makes on their infected device, then save the data into an encrypted log file. This spyware method collects all of the information that the user types into their devices, such as email data, passwords, text messages, and usernames.
4. Rootkits: These enable attackers to deeply infiltrate devices by exploiting security vulnerabilities or logging into machines as an administrator. Rootkits are often difficult and even impossible to detect.
5. Red Shell: This spyware installs itself onto a device while a user is installing specific PC games, then tracks their online activity. It is generally used by developers to enhance their games and improve their marketing campaigns.
6. System monitors: These also track user activity on their computer, capturing information like emails sent, social media and other sites visited, and keystrokes.
7. Tracking cookies: Tracking cookies are dropped onto a device by a website and then used to follow the user's online activity.
8. Trojan Horse Virus: This brand of spyware enters a device through Trojan malware, which is responsible for delivering the spyware program.

Most spyware targets Windows computers and laptops, but attackers are increasingly targeting other forms of devices.

1. Apple device spyware: Malware targeting Apple devices, particularly its Mac computers, has increased rapidly in the last few years. Mac spyware is similar in behavior to those targeting Windows operating systems but are typically password-stealing or backdoor types of spyware. They frequently see the attacker attempt attacks such as keylogging, password phishing, remote code execution, and screen captures.
2. Mobile spyware: Spyware targeting mobile devices steals data such as call logs, browser history, contact lists, photos, and short message service (SMS) messages. Certain types will log user keystrokes, record using the device's microphone, take photos, and track location using Global Positioning System (GPS) trackers. Others take control of devices through commands sent from SMS messages, data transfers, and remote servers. Hackers can also use mobile spyware to breach an organization through mobile device vulnerabilities, which may not be detected by the security team.

What Does Spyware Do?

All types of spyware sit on a user's device and spy on their activity, the sites they visit, and the data they amass or share. They do this with the objective of monitoring user activity, tracking login and password details, and detecting sensitive data.

Other spyware strands are also capable of installing further software on the user's device, which enables the attacker to make changes to the device. But spyware typically follows a three-step process from being installed on a device to sending or selling the information it has stolen.

1. Step 1—Infiltrate: Spyware is installed onto a device through the use of an application installation package, a malicious website, or as a file attachment.
2. Step 2—Monitor and capture: Once installed, the spyware gets to work following the user around the internet, capturing the data they use, and stealing their credentials, login information, and passwords. It does this through screen captures, keystroke technology, and tracking codes.
3. Step 3—Send or sell: With data and information captured, the attacker will either use the data amassed or sell it to a third party. If they use the data, they could take the user credentials to spoof their identity or use them as part of a larger cyberattack on a business. If they sell, they could use the data for a profit with data organizations, other hackers, or put it on the dark web.

Through this process, the attacker can collect and sell highly sensitive information, such as the user's email addresses and passwords, internet usage information and browsing habits, financial details, and account personal identification number (PIN) codes.

How Spyware Attacks Your System

Attackers carefully disguise spyware to infiltrate and infect devices without being discovered. They do this by obscuring the malicious files within regular downloads and websites, which encourages users to open them, often without realizing it. The malware will sit alongside trusted programs and websites through code vulnerabilities or in custom-made fraudulent applications and websites.

One common method for delivering spyware is bundleware. This is a bundle of software packages that attaches itself to other programs that a user downloaded or installed. As a result, it will install without the user knowing about it. Other bundleware packages force the user to agree to download a full software bundle, with no idea that they have voluntarily infected their device. Spyware can also infiltrate a computer through the same routes as other forms of malware, such as compromised or spoofed websites and malicious email attachments.
Mobile spyware typically attacks mobile devices through three methods:

1. Flaws in operating systems: Attackers can exploit flaws in mobile operating systems that are typically opened up by holes in updates.
2. Malicious applications: These typically lurk within legitimate applications that users download from websites rather than app stores.
3. Unsecured free Wi-Fi networks: Wi-Fi networks in public places like airports and cafes are often free and simple to sign in to, which makes them a serious security risk. Attackers can use these networks to spy on what connected users are doing.

Problems Caused by Spyware

The effects of spyware are wide-ranging. Some could go unseen, with users not knowing they have been affected for months or even years. Others might just cause an inconvenience that users may not realize is the result of being hacked. Some forms of spyware are capable of causing reputational and financial damage.
Common problems that spyware can result in include:

1. Data theft: One of the most common problems caused by spyware is data theft. Spyware is used to steal users' personal data, which can then be sold to third-party organizations, malicious actors, or hacking groups.
2. Identity fraud: If spyware harvests enough data, then it can be used for identity fraud. This sees the attacker amass data like browsing history, login credentials for email accounts, online banking, social networks, and other websites to spoof or imitate the user's identity.
3. Device damage: Some spyware will be poorly designed, which ends up having a negative effect on the computer it attaches itself to. This can end up draining system performance and eating up huge amounts of internet bandwidth, memory, and processing power. Even worse, spyware can cause operating systems to crash, disable internet security software, and make computers overheat, which can cause permanent damage to the computer.
4. Browsing disruption: Some spyware can take control of the user's search engine to serve up harmful, fraudulent, or unwanted websites. They can also change homepages and alter computer settings, as well as repeatedly push pop-up ads.

How do I Get Spyware?

Spyware can increasingly affect any device, from computers and laptops to mobile phones and tablets. Devices that run Windows operating systems are typically the most susceptible to an attack, but cyber criminals are increasingly devising methods that afflict Apple and mobile devices.
Some of the most prominent causes of spyware infiltrating a device or system include:

1. Misleading marketing: Spyware authors will often disguise their malicious software as a legitimate tool, such as a hard disk cleaner, download manager, or new web browser.
2. Phishing or spoofing: Phishing occurs when an attacker encourages a recipient to click on a malicious link or attachment in an email, then steals their credentials. They often use spoofed websites that appear to be a legitimate site that steal users' passwords and personal information.
3. Security vulnerabilities: Attackers often target code and hardware vulnerabilities to gain unauthorized access to devices and systems and plant their spyware.
4. Software bundles: Bundleware sees users unknowingly install spyware within a bundle of software they believe to be legitimate.
5. Trojans: A Trojan is a type of malware that pretends to be another piece of software. Cyber criminals use Trojans as a method for delivering malware strains, such as spyware, cryptojackers, and viruses, onto devices.

A device can also become infected with spyware as a result of a user's actions, such as:

- Accepting cookie consent requests from insecure websites
- Accepting pop-ups from untrusted sites
- Clicking on malicious links
- Opening malicious attachments
- Downloading games, movies, or music from pirated or spoofed websites
- Downloading malicious mobile apps

How to Tell if You Have Spyware

Despite spyware being designed to go undetected, there are several telltale signs that could be indicators of a device being infiltrated. These include:

1. Negative hardware performance, such as:

- A device running slower than usual
- Devices suffering frequent crashes and freezes

1. A drop in application or browser performance, such as:

- Pop-up ads repeatedly appearing in browsers
- Unusual error messages
- Unexpected browser changes
- New icons appearing in the taskbar
- Browser searches redirecting to new search engines

Note that these symptoms are also indicative of the presence of other malware, not just spyware, so it is important to dig deeper into issues and scan devices to discover the root of the problem.

Spyware Removal

The first step in removing spyware is to ensure the system is cleared of infection. This will prevent new password changes and future logins from also being stolen. It is also

important to purchase robust cybersecurity software that offers comprehensive spyware removal, deep cleans devices affected by spyware, and repairs any files or systems that may have been infected.With the system cleaned up, financial services need to be advised that potentially fraudulent activity has occurred that could affect bank accounts and credit cards. If the spyware has affected an organization, then legal and regulatory violations need to be reported to the appropriate law enforcement agency.

Spyware Protection

Spyware and other malicious attack methods are a constant threat to any device connected to the internet. Therefore, the first line of defense against spyware is to deploy an internet security solution that includes proactive anti-malware and antivirus detection. In addition, tools like antispam filters, cloud-based detection, and virtual encrypted keyboards are useful to eliminate potentially malicious risks.

Some spyware types are also able to install software and modify the settings on a user's device. This means it is also vital for users to use secure passwords, not recycle their credentials on multiple applications and websites, and use processes like multi-factor authentication (MFA) to keep their identity secure and their devices updated.

In addition to software, there are several steps that can be taken to protect devices and systems:
Cookie consent: It can be easy for users to simply click "accept" on the cookie consent pop-ups that appear on nearly every website they visit. However, they need to be careful about issuing their consent every time and only accept cookies from websites they trust.

1. Browser extensions: Users can also install anti-tracking extensions that prevent the relentless online tracking of their activity on web browsers. These extensions can block activity tracking by both reputable sources and malicious actors, keeping users' data private when they access the internet.
2. Security updates: Updating software with the latest versions is vital to preventing spyware and other types of malware. Spyware typically makes its way onto devices through gaps in code or vulnerabilities in operating systems. So it is important to constantly patch potential issues and fix vulnerabilities immediately.
3. Avoid free software: It can be appealing to download free software, but doing so can have costly ramifications for users and their organizations. The free software may be insecure and the creator can make a profit from users' data.
4. Use secure networks: Unsecured Wi-Fi networks are an easy resource for hackers to breach devices. Avoid using free Wi-Fi networks, and only connect to trusted, secure networks.
5. Best practice and behavior: Practicing good cybersecurity behavior is crucial to avoiding spyware. All users need to be aware of the security risks they face, avoid opening emails or downloading files from people they do not know, and make it a habit to hover over links to check if they are reputable before clicking on them.

Computer and laptop users can follow steps to keep their devices secure. These include enabling and downloading pop-up blockers on their desktops and limiting allowed applications and permissions. All users should also avoid clicking links or opening attachments in all emails, even those purporting to be from trusted senders, as this is a prime delivery method for spyware and other malicious attacks.
There are also steps that can be taken to specifically protect mobile devices from spyware. These include:

Only download apps from the official store of the operating system, such as the Google Play Store, Apple's App Store, and official publishers.

1. Be careful about giving permission to apps that track data or location and take control of cameras or microphones.
2. Avoid clicking links in emails and SMS messages. Instead, only enter trusted Uniform Resource Locators (URLs) directly into the browser address bar.

What is computer virus?

A computer virus is a type of malware that attaches to another program (like a document), which can replicate and spread after a person first runs it on their system. For instance, you could receive an email with a malicious attachment, open the file unknowingly, and then the computer virus runs on your computer. Viruses are harmful and can destroy data, slow down system resources, and log keystrokes.

Cybercriminals aren't creating new viruses all the time, instead they focus their efforts on more sophisticated and lucrative threats. When people talk about "getting a virus" on their computer, they usually mean some form of malware—it could be a virus, computer worm, Trojan, ransomware or some other harmful thing. Viruses and malware continue to evolve, and often cybercriminals use the type that gives them the best return at that particular time.

The types of computer virus,

1. Boot Sector Virus

From a user perspective, boot sector viruses are some of the most dangerous. Because they infect the master boot record, they are notoriously difficult to remove, often requiring a full system format. This is especially true if the virus has encrypted the boot sector or excessively damaged the code.

They typically spread via removable media. They reached a peak in the 1990s when floppy disks were the norm, but you can still find them on USB drives and in email attachments. Luckily, improvements in BIOS architecture have reduced their prevalence in the last few years.

2. Direct Action Virus

A direct action virus is one of the two main types of file infector viruses (the other being a resident virus). The virus is considered "non-resident"; it doesn't install itself or remain hidden in your computer's memory.

It works by attaching itself to a particular type of file (typically EXE or COM files). When someone executes the file, it springs into life, looking for other similar files in the directory for it to spread to.On a positive note, the virus does not typically delete files nor hinder your system's performance. Aside from some files becoming inaccessible, it has a minimal impact on a user and can be easily removed with an anti-virus program.

3. Resident Virus

Resident viruses are the other primary type of file infectors. Unlike direct action viruses, they install themselves on a computer. It allows them to work even when the original source of the infection has been eradicated. As such, experts consider them to be more dangerous than their direct action cousin.

Depending on the programming of the virus, they can be tricky to spot and even trickier to remove. You can split resident viruses into two areas; fast infectors and slow infectors. Fast infectors cause as much damage as quickly as possible and are thus easier to spot; slow infectors are harder to recognize because their symptoms develop slowly.

In a worst-case scenario, they can even attach themselves to your anti-virus software, infecting every file the software scans. You often need a unique tool---such as an operating system patch---for their total removal. An anti-malware app will not be enough to protect you.

4. Multipartite Virus

While some viruses are happy to spread via one method or deliver a single payload, multipartite viruses want it all. A virus of this type may spread in multiple ways, and it may take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files.

They can simultaneously infect both the boot sector and executable files, allowing them to act quickly and spread rapidly.

The two-pronged attack makes them tough to remove. Even if you clean a machine's program files, if the virus remains in the boot sector, it will immediately reproduce once you turn on the computer again.

5 Polymorphic Virus

According to Symantec, polymorphic viruses are one of the most difficult to detect/remove for an anti-virus program. It claims anti-virus firms need to "spend days or months creating the detection routines needed to catch a single polymorphic".

But why are they so hard to protect against? The clue is in the name. Anti-virus software can only blacklist one variant of a virus---but a polymorphic virus changes its signature (binary pattern) every time it replicates. To an anti-virus program, it looks like an entirely different piece of software, and can, therefore, elude the blacklist.

6. Overwrite Virus

To an end-user, an overwrite virus is one of the most frustrating, even if it's not particularly dangerous for your system as a whole.

That's because it will delete the contents of any file which it infects; the only way to remove the virus is to delete the file, and consequently, lose its contents. It can infect both standalone files and entire pieces of software.

Overwrite viruses typically have low visibility and are spread via email, making them hard to identify for an average PC user. They enjoyed a heyday in the early 2000s with Windows 2000 and Windows NT, but you can still find them in the wild.

7.Spacefiller Virus

Also known as "Cavity Viruses", spacefiller viruses are more intelligent than most of their counterparts. A typical modus operandi for a virus is to simply attach itself to a file, but spacefillers try to get into the empty space which can sometimes be found within the file itself. This method allows it to infect a program without damaging the code or increasing its size, thus enabling it to bypass the need for the stealthy anti-detection techniques other viruses rely on. Luckily, this type of virus is relatively rare, though the growth of Windows Portable Executable files is giving them a new lease of life.

What is incident response? Plans, teams and tools

Incident response is an organized, strategic approach to detecting and managing cyber attacks in ways that minimize damage, recovery time and total costs.Strictly speaking, incident response is a subset of incident management. *Incident management* is an umbrella term for an enterprise's broad handling of cyber attacks, involving diverse stakeholders from the executive, legal, HR, communications and IT teams. Incident response is the part of incident management that handles technical cybersecurity tasks and considerations.

Many experts use the terms *incident response* and *incident management* interchangeably, however, because both incident management and incident response strategies work to ensure business continuity in the face of a security crisis, such as a data breach.

Why is incident response important?

Today, Benjamin Franklin might say the only certainties are death, taxes and cyber attacks.Research suggests critical security incidents are all but inevitable, thanks to both criminal ingenuity on the attacker's side and human error on the user's side. A reactive, disorganized response to an attack gives bad actors the upper hand and puts the business at greater risk. At worst, the financial, operational and reputational damage from a major security incident could force an organization to go out of business.On the other hand, a cohesive, well-vetted incident response strategy that follows incident response best practices limits fallout and positions the business to recover as quickly as possible.

Types of security incidents

In developing incident response strategies, it's important to first understand how security vulnerabilities, threats and incidents relate.

A *vulnerability* is a weakness in the IT or business environment. A *threat* is an entity -- whether a malicious hacker or a company insider -- that aims to exploit a vulnerability in an attack. To qualify as an *incident*, an attack must succeed in accessing enterprise resources or in otherwise putting them at risk. Finally, a *data breach* is an incident in which attackers successfully compromise sensitive information, such as personally identifiable information or intellectual property.

When it comes to cybersecurity, an ounce of prevention is worth a pound of cure. Experts say organizations should fix known vulnerabilities and proactively develop response strategies for dealing with common security incidents. These include the following:

- Unauthorized attempts to access systems or data.
- Privilege escalation attacks.
- Insider threats.
- Phishing attacks.
- Malware attacks.
- Denial-of-service (DoS) attacks.

- Man-in-the-middle attacks.
- Password attacks.
- Web application attacks.
- Advanced persistent threats.

But since all security events are not equally serious -- and enterprises simply do not have the resources to aggressively address each and every one -- incident response requires prioritization. Weigh an incident's urgency and importance to determine if it warrants a full-fledged response. For example, an active ransomware attack is both urgent (i.e., time-sensitive) and important (i.e., it puts critical IT assets and business continuity at risk). Such an attack logically warrants a major, expedited response.

Learn more about the top cybersecurity threats enterprises face today.

What is an incident response plan?

An incident response plan is an organization's go-to set of documentation that details the following:

- **What.** Which threats, exploits and situations qualify as actionable security incidents, and what to do when they occur.
- **Who.** In the event of a security incident, who is responsible for which tasks and how others can contact them.
- **When.** Under what circumstances team members should perform certain tasks.
- **How.** Specifically how team members should complete those tasks.

An incident response plan acts as a detailed, authoritative map, guiding responders from initial detection, assessment and triage of an incident to its containment and resolution.

How to create an incident response plan

Successful incident response requires proactively drafting, vetting and testing plans *before* crisis strikes. Best practices include the following:

1. **Establish a policy.** An incident remediation and response policy should be an evergreen document describing general, high-level incident-handling priorities. A good policy empowers incident responders and guides them in making sound decisions when the proverbial excrement hits the fan.
2. **Build an incident response team.** An incident response plan is only as strong as the people involved. Establish who will handle which tasks, and ensure everyone has adequate training to fulfill their roles and responsibilities.
3. **Create playbooks.** Playbooks are the lifeblood of incident response. While an incident response policy offers a high-level view, playbooks get into the weeds, outlining standardized, step-by-step actions responders should take in specific scenarios. Playbook benefits include greater consistency, efficiency and effectiveness -- in both incident response and incident responder training. Learn how to create playbooks.
4. **Create a communication plan.** An incident response plan can't succeed without a solid communication plan among diverse stakeholders. These may include the incident response, executive, communications, legal and HR teams, as well as customers, third-party partners, law enforcement and the general public.

In general, an incident response plan should include the following components:

- A plan overview.
- A list of roles and responsibilities.
- A list of incidents requiring action.
- The current state of network infrastructure and security controls.
- Detection, investigation and containment procedures.
- Eradication procedures.
- Recovery procedures.
- The breach notification process.
- A list of post-incident follow-up tasks.
- A contact list.
- Incident response plan testing.

- Ongoing revisions.

How to manage an incident response plan

The worst time to find out if an incident response plan has holes is during a real security crisis, which makes ongoing testing critical. Experts advise organizations to hold regular simulations featuring diverse attack vectors, such as ransomware, malicious insiders and brute-force attacks.

Many enterprises conduct incident response tabletop exercises to vet their plans. A discussion-based tabletop exercise involves talking through the specifics of an attack and the team's response. An operational tabletop exercise includes hands-on tasks, with enactment of relevant processes to see how they unfold. Templates such as this one can help plan effective simulations.

After both simulated and real security incidents, response teams should study what happened and review lessons learned. Note any security gaps that emerged, recommend appropriate additional controls, brainstorm ways to improve processes and update the incident response plan accordingly.

Remember, an incident response plan is not a set-it-and-forget-it proposition. It should continually evolve to reflect changes in the threat landscape, IT infrastructure and business environment. Experts recommend formal, comprehensive reassessments and revisions annually, at the very least.

Incident response frameworks: Phases of incident response

Rather than trying to recreate the wheel, an organization looking to build an incident response plan can refer to established incident response frameworks for high-level guidance and direction.

Well-known frameworks from NIST, SANS Institute, ISO and ISACA all differ slightly in their approaches, yet they each describe similar phases of incident response:

1. **Preparation/planning.** Build an incident response team and create policies, processes and playbooks; deploy tools and services to support incident response.
2. **Detection/identification.** Use IT monitoring to detect, evaluate, validate and triage security incidents.
3. **Containment.** Take steps to stop an incident from worsening and regain control of IT resources.
4. **Eradication.** Eliminate threat activity, including malware and malicious user accounts; identify any vulnerabilities the attackers exploited.
5. **Recovery.** Restore normal operations and mitigate relevant vulnerabilities.
6. **Lessons learned.** Review the incident to establish what happened, when it happened and how it happened. Flag security controls, policies and procedures that functioned sub-optimally and identify ways to improve them. Update the incident response plan accordingly.

Who is responsible for incident response?

Behind every great incident response program is a coordinated, efficient and effective incident response team. After all, without the right people to support them and put them into practice, security policies, processes and tools mean very little. This cross-functional group consists of people from diverse parts of the organization who are responsible for completing the steps and processes involved in incident response.

Types of incident response teams

The three most common types of incident response teams are as follows:

- Computer security incident response team (CSIRT).
- Computer incident response team (CIRT).
- Computer emergency response team (CERT).

These acronyms are often used interchangeably in the field, and the teams generally have the same goals and responsibilities. One important note is that the name *CERT* is a registered trademark of Carnegie Mellon University, so companies must apply for authorization to use it.

Another term commonly heard during an incident response team conversation is *security operations center* (SOC). A SOC encompasses the people, tools and processes that manage an organization's security program. While SOC teams may be responsible for incident response, it is not their sole task within an organization. SOC teams' other duties can include conducting asset discovery and management, keeping activity logs and ensuring regulatory compliance, among others.

Incident response team members

The size of an incident response team and the members included will vary based on the individual organization's needs. Some members may even fill multiple roles and responsibilities.

In general, an incident response team consists of the following members:

- **Technical team.** This is the core incident response team of IT and security members who have technical expertise across company systems. It often includes an incident response manager, incident response coordinator, team lead, security analysts, incident responders, threat researchers and forensics analysts.
- **Executive sponsor.** This is an executive or board member, often the CSO or CISO.
- **Communications team.** This includes PR representatives and others who manage internal and external communications.
- **External stakeholders.** Members include other employees or departments within the organization, such as IT, legal or general counsel, HR, PR, business continuity and disaster recovery, physical security and facilities teams.
- **Third parties.** These external members might include security or incident response consultants, external legal representation, MSPs, managed security service providers, cloud service providers (CSPs), vendors and partners.

What does an incident response team do?

The chief goals of an incident response team are to detect and respond to security events and minimize their business impact. As such, team responsibilities largely align with the phases outlined in an incident response framework and plan. Team tasks include the following:

- Prepare for and prevent security incidents.
- Create the incident response plan.
- Test, update and manage the incident response plan before use.
- Perform incident response tabletop exercises.
- Develop metrics to analyze program initiatives.
- Identify security events.
- Contain security events, quarantine threats and isolate systems.
- Eradicate threats, discover root causes and remove affected systems from production environments.
- Recover from threats and get affected systems back online.
- Conduct follow-up activities, including documentation, incident analysis and identifying how to prevent similar events and improve future response efforts.
- Review and update the incident response plan regularly.

Digital forensics

Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation. It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices. The process's goal of digital forensics is to collect, analyze, and preserve evidence.

Objectives of Digital Forensics

Knowing the primary objectives of using digital forensics is essential for a complete understanding of what is digital forensics:

- It aids in the recovery, analysis, and preservation of computers and related materials for the investigating agency to present them as evidence in a court of law
- It aids in determining the motive for the crime and the identity of the primary perpetrator
- Creating procedures at a suspected crime scene to help ensure that the digital evidence obtained is not tainted
- Data acquisition and duplication: The process of recovering deleted files and partitions from digital media in order to extract and validate evidence
- Assists you in quickly identifying evidence and estimating the potential impact of malicious activity on the victim
- Creating a computer forensic report that provides comprehensive information on the investigation process
- Keeping the evidence safe by adhering to the chain of custody

Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below:

Computer Forensics

It analyzes digital evidence obtained from laptops, computers, and storage media to support ongoing investigations and legal proceedings.

- Mobile Device Forensics

It entails obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

- Network Forensics

Network or cyber forensics depends on the data obtained from monitoring and analyzing cyber network activities such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

- Digital Image Forensics

This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

- Digital Video/Audio Forensics

This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

- Memory Forensics

It refers to the recovery of information from a running computer's RAM and is also known as live acquisition.

2Scripting languages

Scripting languages are high-level programming languages that are interpreted rather than compiled, meaning they are executed line by line at runtime. They are often used for automating tasks, manipulating text and files, and interacting with other programs or systems. Some of the popular scripting languages for digital forensics are Python, Perl, Ruby, and PowerShell. Scripting languages are useful for digital forensics, as they allow you to quickly write and run scripts for data extraction, analysis, and reporting, without having to deal with low-level details or complex syntax. You should be able to write and read scripts in at least one scripting language, and understand how to use libraries and modules for common digital forensics tasks.

Python is widely used for automation, scripting, and developing tools. Python has a rich ecosystem of libraries and frameworks that can be leveraged in digital forensics tasks.

3Object-oriented programming

Object-oriented programming (OOP) is a programming paradigm that organizes data and behavior into reusable units called objects, which have attributes and methods. Objects can be grouped into classes, which define the common characteristics and behaviors of the objects. OOP also supports concepts such as inheritance, polymorphism, abstraction, and encapsulation, which help to create modular and maintainable code. OOP is important for digital forensics, as it allows you to create and use custom objects and classes for representing and manipulating data from different devices and sources, such as disk images, memory dumps, network packets, etc. You should be able to apply the principles and concepts of OOP in your programming language of choice, and use existing OOP frameworks and libraries for digital forensics.

Object-oriented programming (OOP) is like building with Lego blocks. You create "objects" that have their own data and actions. These objects can be reused and combined, making it

easier to design and manage complex programs. It's like putting together pieces to make something bigger and more organized.

Object-oriented programming arrange your code according to its behaviour, this give better understanding that what your code does. OOPs help to reduce lines of code while you are working in a large project in which objects need same method and functions multiple times for different parts of code. For example if you have class Dog and functions like color , bark , run , name etc. You can make objects of class Dog and same functions can be reused multiple times for different objects.

4Low-level programming

Low-level programming refers to programming that is closer to the hardware or machine level, such as assembly language or C. Low-level programming gives you more control and flexibility over the memory, registers, instructions, and system calls of the computer, but also requires more attention to detail and error handling. Low-level programming is relevant for digital forensics, as it allows you to access and manipulate the raw data and structures of the digital devices, such as boot sectors, file systems, partitions, etc. You should be able to understand and write low-level code, and use tools such as debuggers, disassemblers, and hex editors for low-level analysis.

5Web development

Web development is the process of creating and maintaining websites and web applications, using languages such as HTML, CSS, JavaScript, PHP, etc. Web development is related to digital forensics, as it allows you to create and use web-based tools and interfaces for data visualization, presentation, and collaboration. For example, you can use web development to create dashboards, reports, or interactive graphs for displaying and exploring the results of your digital forensics analysis. You can also use web development to create and use web-based platforms and services for digital forensics, such as cloud computing, online databases, or web APIs. You should be able to use and integrate web development languages and technologies, and understand how they work and communicate with each other.

You need to learn web development but try to learn latest frameworks because they have lots of new feature which can help you to create report easily and by doing this you can also be relevant in industry.

6Programming best practices

Programming best practices are the guidelines and standards that help you to write high-quality, readable, and secure code. Programming best practices include things such as naming conventions, coding style, documentation, testing, debugging, error handling, version control, etc. Programming best practices are essential for digital forensics, as they help you to avoid errors, bugs, and vulnerabilities in your code, which could compromise the integrity, reliability, and validity of your digital forensics analysis. You should be able to follow and apply programming best practices in your code, and use tools and resources that support them.

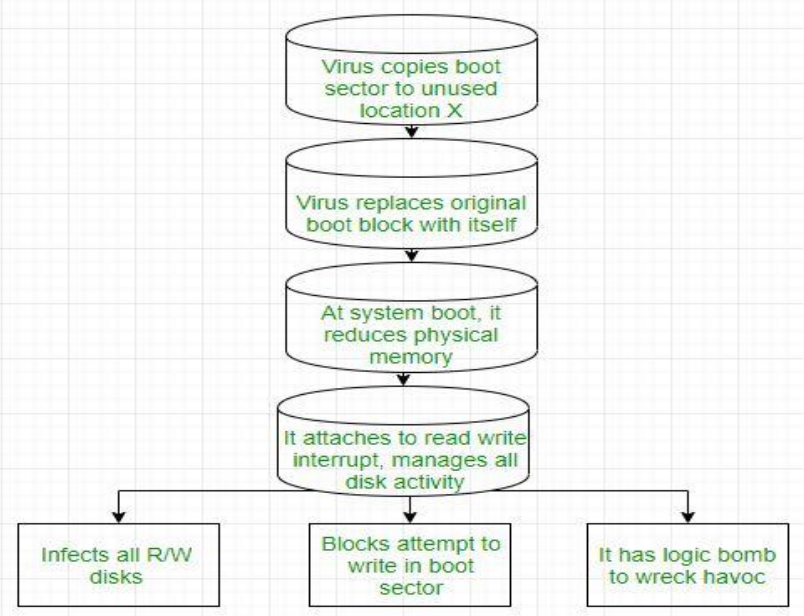
Virus

A computer virus is a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy

Various types of viruses:

- **File Virus:**
  This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a **Parasitic virus** because it leaves no file intact but also leaves the host functional.

- **Boot sector Virus:**
  It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory viruses** as they do not infect the file systems.



- **Macro Virus:**
  Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

- **Source code Virus:**
  It looks for source code and modifies it to include virus and to help spread it.

- **Polymorphic Virus:**
  A **virus signature** is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

- **Encrypted Virus:**
  In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

- **Stealth Virus:**
  It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

- **Tunneling Virus:**
  This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

- **Multipartite Virus:**
  This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

- **Armored Virus:**
  An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

- **Browser Hijacker:**
  As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.
- **Memory Resident Virus:**

Resident viruses installation store for your RAM and meddle together along with your device operations. They behave in a very secret and dishonest way that they can even connect themselves for the anti-virus software program files.

- **Direct Action Virus:**

The main perspective of this virus is to replicate and take action when it is executed. When a particular condition is met the virus will get into action and infect files in the directory that are specified in the AUTOEXEC.BAT file path.

> **A computer worm** is a type of malware that can automatically propagate or self-replicate without human interaction, enabling its spread to other computers across a network. A worm often uses the victim organization's internet or a local area network (LAN) connection to spread itself.

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, cybercriminals can use worms to perform a range of malicious actions, such as:

- Launching distributed denial of service (DDoS) attacks
- Conducting ransomware attacks
- Stealing sensitive data
- Dropping other malware
- Consuming bandwidth
- Deleting files
- Overloading networks

Why are worms dangerous?

- A **computer worm** is harmful because it may perform a broad range of attacks, including crashing systems through self-replication, downloading malicious applications, and providing hackers with backdoor access to equipment.
- Worms can also be hard to remediate. Because they spread automatically and quickly, it can take a lot of time and effort to eradicate a worm outbreak from the environment and fully recover. When a worm spreads inside a data storage environment, for example, it can take months to completely clean it up. Even when a worm doesn't have a malicious payload that does damage, it poses a serious nuisance for IT managers who have to dedicate valuable resources to navigate the incident response process.

What Is a Trojan Horse Virus?

A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

How a Trojan horse works

Before a Trojan horse can infect a machine, the user must download the server side of the malicious application. The Trojan horse cannot manifest by itself. The executable file (.exe file) must be implemented and the program must be installed in order for the attack to be unleashed on the system. Social engineering tactics are often used to convince end users to download the malicious application. The download trap may be found in banner ads, website links or pop-up advertisements.

However, the most popular tactic for spreading Trojan horses is through seemingly unthreatening emails and email attachments. Trojan horse developers frequently use spamming techniques to send their emails to hundreds or thousands of people. As soon as the email has been opened and the attachment has been downloaded, the Trojan server will be installed and will run automatically each time the computer turns on.

How to protect against a Trojan horse

The easiest way to protect a system from a Trojan horse is by never opening or downloading emails or attachments from unknown sources. Deleting these messages before opening will prevent the Trojan horse threat.

However, computer security begins with and depends on the installation and implementation of an internet security suite. Because the user is often unaware that a Trojan horse has been installed, antimalware software must be used to recognize malicious code, isolate it and remove it. To avoid being infected by a Trojan horse, users should keep their antivirus and antimalware software up to date and practice running periodic diagnostic scans.

Other tips for protecting a system include:

- Updating the operating system (OS) software as soon as the software company releases an update.
- Protecting personal accounts with complicated and unique passwords that contain numbers, letters and symbols.
- Using discretion with all email attachments, even those from recognized senders, since a Trojan horse could have infected their computer and is using it to spread malware.
- Backing up files on a regular basis so they can be easily recovered if a Trojan horse attack occurs.
- Protecting all personal information with firewalls.
- Avoiding suspicious and unsafe websites; Internet security software can sometimes be used to indicate which sites are safe and which should be avoided.
- Only installing or downloading programs from verified, trustworthy publishers.
- Refusing pop-up ads that attempt to entice users to click through for tempting offers and promotions.
- Never opening an email if the topic, content or sender is unknown or if there is any suspicion or question about the email in general.

How to remove a Trojan horse

If a Trojan horse is identified on a computer, the system should immediately be disconnected from the Internet and the questionable files should be removed using an antivirus or antimalware program or by reinstalling the operating system.

The hardest part of the removal process is recognizing which files are infected. Once the Trojan has been identified, the rest of the process becomes simpler. Users can sometimes find the infected files using the dynamic link library (DLL) error which is frequently presented by the computer to signify the presence of a Trojan horse. This error can be copied and searched online to find information about the affected .exe file.Once the files are identified, the System Restore function must be disabled. If this function is not disabled, then all the malicious files that are deleted will be restored and will infect the computer once again.

Next, users must restart their computer. While restarting, users should press the F8 key and select safe mode. Once the computer has successfully started up, users should access Add or Remove programs in the Control Panel. From here, the infected programs can be removed and deleted. In order to ensure all extensions associated with the Trojan application are removed, all of the program files should be deleted from the system. Once this is complete, the system should be restarted once again, but this time in the normal start-up mode. This should complete the Trojan horse removal process.

Backdoor

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

Backdoor installation is achieved by taking advantage of vulnerable components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated.

Webserver backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)
- Advanced persistent threat (APT) assaults

Backdoor malware is generally classified as a Trojan. A Trojan is a malicious computer program pretending to be something it's not for the purposes of delivering

malware, stealing data, or opening up a backdoor on your system. Much like the Trojan horse of ancient Greek literature, computer Trojans always contain a nasty surprise.

- Trojans are an incredibly versatile instrument within the cybercriminal toolkit. They come under many guises, like an email attachment or file download, and deliver any number of malware threats.

- To compound the problem, Trojans sometimes exhibit a worm-like ability to replicate themselves and spread to other systems without any additional commands from the cybercriminals that created them. Take, for example, the Emotet banking Trojan. Emotet got its start in 2014 as an information stealer, spreading across devices and stealing sensitive financial data. Since then Emotet has evolved into a delivery vehicle for other forms of malware. Emotet helped make the Trojan the top threat detection for 2018, according to the State of Malware report.

What is steganography?

Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.

Content concealed through steganography is sometimes encrypted before being hidden within another file format. If it isn't encrypted, then it may be processed in some way to make it harder to detect.
As a form of covert communication, steganography is sometimes compared to cryptography. However, the two are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt.

The term 'steganography' comes from the Greek words 'steganos' (which means hidden or covered) and 'graphein' (which means writing). Steganography has been practiced in various forms for thousands of years to keep communications private. For example, in ancient Greece, people would carve messages on wood and then use wax to conceal them. Romans used various forms of invisible inks, which could be deciphered when heat or light were applied.

Steganography is relevant to cybersecurity because ransomware gangs and other threat actors often hide information when attacking a target. For example, they might hide data, conceal a malicious tool, or send instructions for command-and-control servers. They could place all this information within innocuous-seeming image, video, sound, or text files.
How steganography works

Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called 'least significant bit' (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file. For example:

- In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or ‘alpha’.
- LSB steganography alters the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you would need an eight-megabyte image file.
- Modifying the last bit of the pixel value doesn’t result in a visually perceptible change to the picture, which means that anyone viewing the original and the steganographically-modified images won’t be able to tell the difference.

The same method can be applied to other digital media, such as audio and video, where data is hidden in parts of the file that result in the least change to the audible or visual output.

Another steganography technique is the use of word or letter substitution. This is where the sender of a secret message conceals the text by distributing it inside a much larger text, placing the words at specific intervals. While this substitution method is easy to use, it may also make the text look strange and out of place since the secret words might not fit logically within their target sentences.

Other steganography methods include hiding an entire partition on a hard drive or embedding data in the header section of files and network packets. The effectiveness of these methods depends on how much data they can hide and how easy they are to detect.

. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Steganography Examples Include

- Writing with invisible ink
- Embedding text in a picture (like an artist hiding their initials in a painting they've done)
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing information in either metadata or within a file header
- Hiding an image in a video, viewable only if the video is played at a particular frame rate
- Embedding a secret message in either the green, blue, or red channels of an RRB image

Steganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.

What Is the Difference Between DoS Attacks and DDoS Attacks?

A **denial-of-service (DoS) attack** floods a server with traffic, making a website or resource unavailable. A **distributed denial-of-service (DDoS) attack** is a DoS attack that uses multiple computers or machines to flood a targeted resource. Both types of attacks overload a server or web application with the goal of interrupting services.

As the server is flooded with more Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packets than it can process, it may crash, the data may become corrupted, and resources may be misdirected or even exhausted to the point of paralyzing the system.
The principal difference between a DoS attack and a DDoS attack is that the former is a system-on-system attack, while the latter involves several systems attacking a single system. There are other differences, however, involving either their nature or detection, including:

1. Ease of detection/mitigation: Since a DoS comes from a single location, it is easier to detect its origin and sever the connection. In fact, a proficient firewall can do this. On the other hand, a DDoS attack comes from multiple remote locations, disguising its origin.
2. Speed of attack: Because a DDoS attack comes from multiple locations, it can be deployed much faster than a DoS attack that originates from a single location. The increased speed of attack makes detecting it more difficult, meaning increased damage or even a catastrophic outcome.
3. Traffic volume: A DDoS attack employs multiple remote machines (zombies or bots), which means that it can send much larger amounts of traffic from various locations simultaneously, overloading a server rapidly in a manner that eludes detection.
4. Manner of execution: A DDoS attack coordinates multiple hosts infected with malware (bots), creating a botnet managed by a command-and-control (C&C) server. In contrast, a DoS attack typically uses a script or a tool to carry out the attack from a single machine.
5. Tracing of source(s): The use of a botnet in a DDoS attack means that tracing the actual origin is much more complicated than tracing the origin of a DoS attack.

Types of DoS Attacks and DDoS Attacks

DoS and DDoS attacks can take many forms and be used for various means. It can be to make a company lose business, to cripple a competitor, to distract from other attacks, or simply to cause trouble or make a statement. The following are some common forms taken by such attacks.

Teardrop Attack

A teardrop attack is a DoS attack that sends countless Internet Protocol (IP) data fragments to a network. When the network tries to recompile the fragments into their original packets, it is unable to. For example, the attacker may take very large data packets and break them down into multiple fragments for the targeted system to reassemble. However, the attacker changes how the packet is disassembled to confuse the targeted system, which is then unable to reassemble the fragments into the original packets.

Flooding Attack

A flooding attack is a DoS attack that sends multiple connection requests to a server but then does not respond to complete the handshake.

For example, the attacker may send various requests to connect as a client, but when the server tries to communicate back to verify the connection, the attacker refuses to respond. After repeating the process countless times, the server becomes so inundated with pending requests that real clients cannot connect, and the server becomes “busy” or even crashes.

IP Fragmentation Attack

An IP fragmentation attack is a type of DoS attack that delivers altered network packets that the receiving network cannot reassemble. The network becomes bogged down with bulky unassembled packets, using up all its resources.

Volumetric Attack

A volumetric attack is a type of DDoS attack used to target bandwidth resources. For example, the attacker uses a botnet to send a high volume of request packets to a network,

overwhelming its bandwidth with Internet Control Message Protocol (ICMP) echo requests. This causes services to slow down or even cease entirely.

Protocol Attack

A protocol attack is a type of DDoS attack that exploits weaknesses in Layers 3 and 4 of the OSI model. For example, the attacker may exploit the TCP connection sequence, sending requests but either not answering as expected or responding with another request using a spoofed source IP address. Unanswered requests use up the resources of the network until it becomes unavailable.

Application-based Attack

An application-based attack is a type of DDoS attack that targets Layer 7 of the OSI model. An example is a Slowloris attack, in which the attacker sends partial Hypertext Transfer Protocol (HTTP) requests but does not complete them. HTTP headers are periodically sent for each request, resulting in the network resources becoming tied up.

The attacker continues the onslaught until no new connections can be made by the server. This type of attack is very difficult to detect because rather than sending corrupted packets, it sends partial ones, and it uses little to no bandwidth.

SQL Injection

- **SQL injection** is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server.

1. SQL injection is a code injection technique that can compromise your database.
2. SQL injection is one of the most common web hacking techniques.
3. SQL injection is the injection of malicious code into SQL statements via web page input.
4. The Exploitation of SQL Injection in Web Applications
5. Web servers communicate with database servers anytime they need to retrieve or store user data. SQL statements by the attacker are designed so that they can be executed while the web server is fetching content from the application server. It compromises the security of a web application.
6. Example of SQL Injection
7. Suppose we have an application based on student records. Any student can view only his or her own records by entering a unique and private student ID.
8. Suppose we have a field like the one below:
9. **Student id:** The student enters the following in the input field: **12222345 or 1=1**.
   Query:

```
10. SELECT * from STUDENT where
11. STUDENT-ID == 12222345 or 1 = 1
```

12. Now, this **1=1** will return all records for which this holds true. So basically, all the student data is compromised. Now the malicious user can also delete the student records in a similar fashion. Consider the following SQL query.

Query:

```
SELECT * from USER where
USERNAME = “” and PASSWORD=””
```

Now the malicious can use the ‘=’ operator in a clever manner to retrieve private and secure user information. So instead of the above-mentioned query the following query when executed retrieves protected data, not intended to be shown to users.

Query:

```
Select * from User where
(Username = “” or 1=1) AND
(Password=”” or 1=1).
```

Since **1=1** always holds true, user data is compromised.

Impact of SQL Injection

The hacker can retrieve all the user data present in the database such as user details, credit card information, and social security numbers, and can also gain access to protected areas like the administrator portal. It is also possible to delete user data from the tables.

Nowadays, all online shopping applications and bank transactions use back-end database servers. So in case the hacker is able to exploit SQL injection, the entire server is compromised.

Preventing SQL Injection

- User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.
- Restricting access privileges of users and defining how much amount of data any outsider can access from the database. Basically, users should not be granted permission to access everything in the database.
- Do not use system administrator accounts

What Is Buffer Overflow?

Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems. It is one of the best-known software security vulnerabilities yet remains fairly common. This is partly because buffer overflows can occur in various ways and the techniques used to prevent them are often error-prone.

The software error focuses on buffers, which are sequential sections of computing memory that hold data temporarily as it is transferred between locations. Also known as a buffer overrun, buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

What Is a Buffer Overflow Attack?

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application’s execution path and overwrites elements of its memory, which amends the program’s execution path to damage existing files or expose data.

A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on. Most buffer overflows are caused by the combination of manipulating memory and mistaken assumptions around the composition or size of data.
A buffer overflow vulnerability will typically occur when code:

1. Is reliant on external data to control its behavior
2. Is dependent on data properties that are enforced beyond its immediate scope
3. Is so complex that programmers are not able to predict its behavior accurately

Types of Buffer Overflow Attacks

There are several types of buffer overflow attacks that attackers use to exploit organizations' systems. The most common are:

1. Stack-based buffer overflows: This is the most common form of buffer overflow attack. The stack-based approach occurs when an attacker sends data containing malicious code to an application, which stores the data in a stack buffer. This overwrites the data on the stack, including its return pointer, which hands control of transfers to the attacker.
2. Heap-based buffer overflows: A heap-based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a program's memory space beyond the memory it uses for current runtime operations.
3. Format string attack: A format string exploit takes place when an application processes input data as a command or does not validate input data effectively. This enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application. This could trigger new actions that threaten the security and stability of the system.

Wireless network security.

The temptation is real. Most of us have at least considered using an open wireless network when we're traveling or at a local store or restaurant, despite knowing that "open wireless network" means "not secured." We know the risks, but we consider connecting -- or connect -- nonetheless. The risks of being attacked may seem hypothetical, but they're real.

Network, IT and security admins involved in managing wireless networks have to secure those networks to protect the users, devices and services using them. One of the best ways to do this is to make users aware of the different types of wireless network attacks they may encounter, as well as putting the appropriate safeguards in place.

Let's take a look at the most common forms of wireless network attacks and specific types within each category, and then talk about how to prevent them.

3 categories of wireless network attacks

Wireless network attacks can be bucketed into three categories: passive attacks, active attacks and attacks against wireless network components:

- **Passive attacks** take place when an attacker is within range of a wireless network and can monitor wireless communications. The most common passive attack is

packet sniffing. Passive attacks generally can't be detected because attackers are only listening and not transmitting.

- **Active attacks** often involve attackers deploying rogue wireless access points -- for example, setting up an open network named "Free Wi-Fi" -- in hopes that people connect to it. Active attacks are often used to perform man-in-the-middle (MitM) attacks because they can intercept, monitor and alter communications passing through them.
- **Attacks against wireless network components** involve attackers targeting individual components of a network, such as exploiting an access point's unpatched firmware or using an access point's default password to gain unauthorized administrative access to it.

12 common types of wireless network attacks

Each category can be broken down into more specific attacks. The most common types of wireless network attacks are the following:

1. packet sniffing 2 rogue access points
2. Wi-Fi phishing and evil twins 3 spoofing attacks
3. encryption cracking 4 MitM attacks
4. DoS attacks 8 Wi-Fi jamming
5. war driving attacks 11 war shipping attacks
6. theft and tampering 12 default passwords and service set identifiers (SSIDs)

1. Packet sniffing

Packet sniffing is the act of gaining access to raw network traffic. Packet sniffers, such as Wireshark, detect, monitor and gather network packets. While packet sniffing is a legitimate activity, packet sniffers can also be used by attackers to spy on network traffic.

2. Rogue access points

A rogue access point is any unauthorized access point connected to a network. If an attacker successfully places a rogue access point, the attacker can then access the network it connects to.

3. Wi-Fi phishing and evil twins

Wi-Fi phishing is when malicious actors create access points that imitate legitimate Wi-Fi access points.An evil twin is a type of rogue access point used for Wi-Fi phishing. It advertises itself as an existing, authorized access point. It uses the SSID of an authorized access point to

trick users into connecting to it. Sometimes, attackers disable the authorized access point to subvert the entire network. Even if the authorized access point isn't disabled, the evil twin still often gets access to some network traffic.

4. Spoofing attacks

Spoofing attacks involve malicious actors pretending to be legitimate users or services. Types of spoofing attacks include the following:

- **MAC address spoofing** happens when attackers detect network adapter MAC addresses on authorized devices and attempt to start new connections impersonating the authorized devices.
- **Frame spoofing**, also known as *frame injection*, occurs when attackers send malicious frames that appear to be from legitimate senders.
- **IP spoofing** takes place when attackers use modified IP packets to hide where the packets originate.
- **Data replay** occurs when attackers capture wireless data transmission, modify the transmission and resend the modified transmission to a target system.
- **Authentication replay** happens when attackers capture authentication exchanges between users and reuse those exchange in attacks.

5. Encryption cracking -- WEP/WPA attacks

- Many older, outdated security protocols, including Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), are vulnerable to attack. WEP, introduced in the 1990s, encrypts data transmitted over a LAN. It is flawed, however, and should never be used in enterprise networks.
- WPA, introduced in 2003, was created to be more effective than WEP. It uses stronger encryption and better authentication than WEP. WPA is also vulnerable to attacks, however, and should also never be used. WPA2 was introduced in 2004 to formally replace WEP. It includes AES encryption. WPA3, introduced in 2018, offers even stronger encryption than WPA2.

6. MitM attacks

- MitM attacks occur when cybercriminals eavesdrop on communications between two parties -- for example, two users communicating with each other or a user communicating with an application or service. Attackers can intercept sensitive information and relay information by pretending to be one of the legitimate parties.

7. DoS attacks

- DoS attacks occur when malicious actors flood a network with traffic, thus overwhelming the network and making it impossible for legitimate users to access it.

8. Wi-Fi jamming

- Like DoS attacks, Wi-Fi jamming attacks overwhelm a network and prevent legitimate users from connecting to it. An example of a Wi-Fi jamming attack is flooding access points to "jam" the connection.

9. War driving attacks

- War driving occurs when attackers search for open or vulnerable wireless networks to exploit. Also known as *access point mapping*, attacks involve nefarious actors driving around with wireless devices -- usually, computers or mobile devices -- searching for open networks to connect to.

10. War shipping attacks

- War shipping attacks involve attackers sending physical spying devices to companies, which, once within the company's building, connect to the target network to exfiltrate data. An example of this attack could be an attacker sending a wireless-enabled device to a mailroom. Once it arrives, the device scans for networks to connect to and attack.

11. Theft and tampering

- Attackers can conduct physical attacks on wireless networks by stealing or damaging wireless access points and routers. These attacks not only prevent users from accessing networks and cause network downtime -- and, therefore, business disruption and potential revenue loss -- but also can be costly for the companies replacing the stolen or damaged devices.

12. Default passwords and SSIDs

- Corporate networks should never use default passwords and SSIDs. Employees who work from home should also be advised to change default passwords and SSIDs. Default SSIDs enable attackers to find out which router an employee is using and, in turn, find potential vulnerabilities specific to that router. Default and manufacturer-provided passwords, which are often printed on the side of consumer routers, should be changed to prevent unauthorized users from seeing and using them. Password security best practices -- such as not using easy-to-guess passwords -- should be followed.