

Introduction of Cybercrime

Definition of Cybercrime

Cybercrime can be defined as “The illegal usage of any communication device to commit or facilitate in committing any illegal act.”

(or)

Cybercrime may be defined as “Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime”.

In simple words, Any criminal activity carried out over the internet is referred to as cybercrime.

A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.

Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user’s personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Cybercriminal

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams.

Cybercriminals are widely available in what is called the “**Dark Web**” where they mostly provide their illegal services or products.

Not every hacker is a cybercriminal because hacking itself is not considered a crime as it can be used to reveal vulnerabilities to report and patch them which is called a “**white hat hacker**.”

However, hacking is considered a cybercrime when it has a malicious purpose of conducting any harmful activities and we call this one “**black hat hacker**” or a cyber-criminal.

It is not necessary for cybercriminals to have any hacking skills as not all cyber-crimes include hacking.

Types of Cybercrimes

Cybercrimes can generally be divided into two types:

- Crimes that target networks or computer devices
Examples: Malware, DoS Attacks
- Crimes using devices to participate in criminal activities
Examples: Phishing Emails, Cyberstalking, Identity Theft

Classifications of Cybercrimes

Cybercrimes in general can be classified into four categories:

1. Individual:

In this type the main target is individuals. It includes phishing, spoofing, spam, cyberstalking, and more.

2. Organization:

In this type the main target is organizations. Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.

3. Property:

In this type the main target is property, It includes obtaining access to individuals' bank or credit card information, accessing their funds, making online transactions and more.

4. Society/Government:

In this type the main target is Government/Society And this is the most dangerous form of cybercrime as it includes cyber-terrorism. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

Most Common Cyber Crimes

The following are some common cybercrimes.

1.Malware:

Malware can simply be described as code written to steal data or destroy things on a computer. Malware is a broad phrase that encompasses a wide range of cyberattacks such as Trojans, viruses, and worms.

Viruses: Viruses, like their biological namesakes, attach themselves to clean files and infect other clean files. Viruses can spread uncontrollably, causing damage to the core functionality as well as deleting and corrupting files. Viruses usually appear as executable files downloaded from the internet.

Trojan: This type of malware covers up as genuine software that can be hacked. It prefers to function invisibly and creates security backdoors that allow other viruses to enter the system.

Worms: Worms use the network's interface to infect a whole network of devices, either locally or via the internet. Worms infect more machines with each successive infected machine.

2. Phishing:

Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.

In recent years, phishing emails have become much more complex, making it impossible for some users to distinguish between a real request for information and a fraudulent one. Phishing emails are sometimes lumped in with spam, but they are far more dangerous than a simple advertisement.

Phishing is a type of social engineering attack that targets the user and tricks them by sending fake messages and emails to get sensitive information about the user or trying to download malicious software and exploit it on the target system.

3.DDoS Attack:

As the name suggests, a distributing denial-of-service (DDoS) attack focuses on network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working.

A DoS attack can be carried out in a variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines, that will overload the system.

DDoS attacks are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources.

4. Identity Theft:

Identity theft occurs when a cybercriminal uses another person's personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

5. Internet Fraud:

Internet fraud is a type of cybercrimes that makes use of the internet and it can be considered a general term that groups all the crimes that happen over the internet like spam, banking frauds, theft of service, etc.

6. Website Spoofing:

The word spoof means to hoax, trick, or deceive. Website spoofing is when a website is designed to look like a real one and deceive you into believing it is a legitimate site. This is done to gain your confidence, get access to your systems, steal data, steal money, or spread malware.

Website spoofing works by replicating a legitimate website with a big company's style, branding, user interface, and even domain name in an attempt to trick users into entering their usernames and passwords. This is how the bad guys capture your data or drop malware onto your computer.

7. Cyber Bullying:

Cyberbullying is harassment with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted.

Examples include:

- spreading lies about or posting embarrassing photos or videos of someone on social media
- sending hurtful, abusive or threatening messages, images or videos via messaging platforms
- impersonating someone and sending mean messages to others on their behalf or through fake accounts.

8. Cyberstalking:

Cyberstalking is a crime committed when someone uses the internet and other technologies to harass or stalk another person online. Even though cyberstalking is a broad term for online harassment, it can include offence, false allegations, teasing, and even extreme threats.

This kind of cybercrime involves online harassment where the user is subjected to a excess of online messages and emails. Typically cyberstalkers use social media, websites and search engines to threaten a user and impart fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

The Internet spawns crime

Cybercrime also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Worms versus Viruses

Malware can be defined as a special kind of code or application specifically developed to harm electronic devices or the people using those devices. Viruses and worms are both types of malware; however, there are significant differences between them.

Virus:

According to the definition, a Virus is a program developed using malicious codes with a nature that links itself to the executable files and propagates device to device. Viruses are often transferred through the downloaded files and the shared files. They can also be attached with a scripting program and non-executable files like images, documents, etc. After the user executes the infected program, the virus gets activated and starts replicating further on its own.

Viruses can harm the system by the following means:

- Filling up the disk space unnecessarily
- Formatting the hard disk drive automatically
- Making the system slow
- Modify, or delete personal data or system files
- Stealing sensitive data

How does a virus spread?

The virus does not have the capability of spreading itself. It requires the host and human support to spread. The virus is developed in such a way that it attaches itself to the executable files. It further spreads when the infected executable file or software is transferred from one device to another. As soon as human launches the infected file or a program, the virus starts replicating itself.

Worm:

Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread. They are standalone computer malware that doesn't even require human support to execute. Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

Worms can harm the system by the following means:

- Worms stay within the memory of an infected computer, making a computer think they are part of the system files, this helps worms to avoid any suspicious detection.
- Unlike a typical virus, worms don't harm the system data.
- Consume system resources like CPU, memory, or network bandwidth.
- Make the entire system or network crash. Because of self-replicating nature.

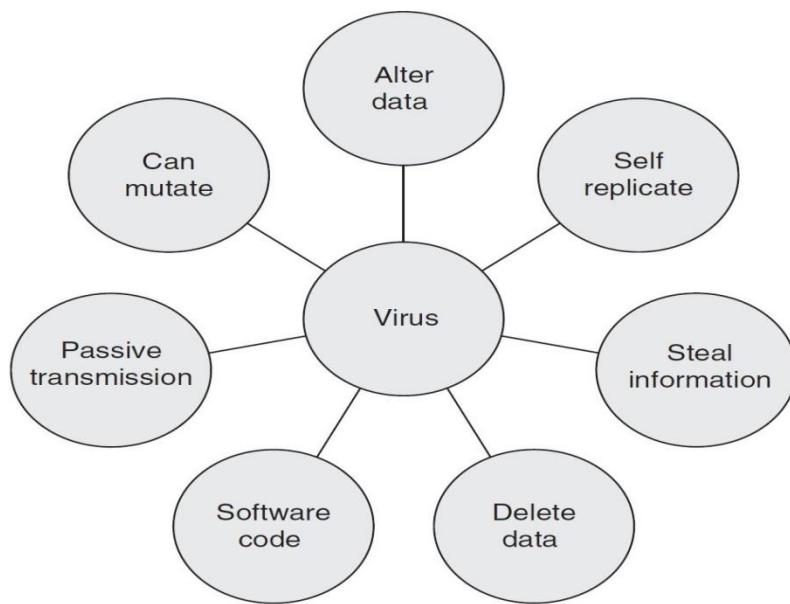
How does a worm spread?

Unlike viruses, worms don't require host files to spread. This means that worms do not attach themselves with executable files or programs. Instead, worms find a weak spot in the system and enter through vulnerability (weak spot) in the network.

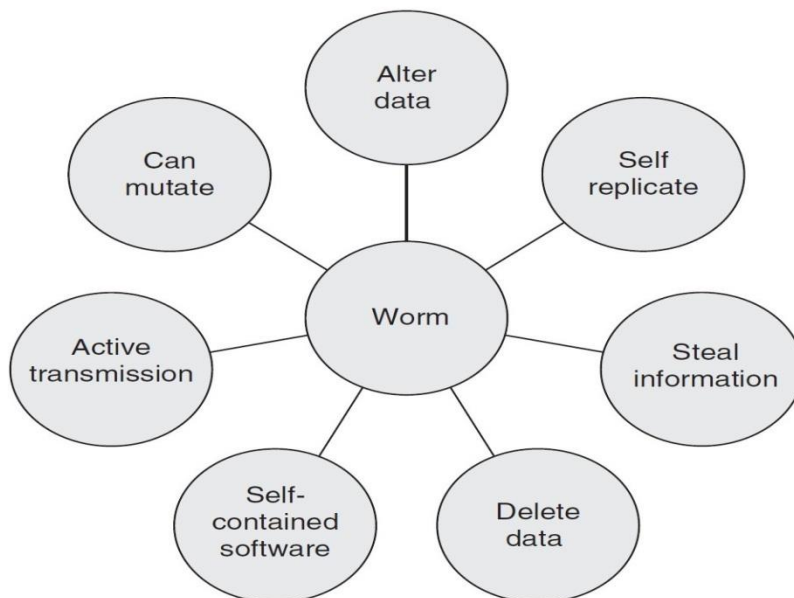
Before we detect and remove worms from our system, they replicate and spread automatically and consume all the network bandwidth. This can result in the failure of the entire network and web servers. Because worms can spread automatically, their spreading speed is comparatively faster than other malware.

Virus	Worm
The virus is a malicious program attached to the executable files so that it can spread from one system to another.	A worm is a program made up of malicious code that replicates itself and propagates itself from device to device using a network.
Human action is required for viruses. Without human help, they cannot execute and spread.	Human action is not required for the worms. They are designed and developed in such a way that they can automatically execute and spread.
The virus spreads at a relatively slower speed than a Worm.	Worms spreading speed is fast, and they can infect multiple devices or networks quickly.
The host is required to spread viruses. Viruses connect themselves to the host and travel with the host. They spread into devices where the host reaches.	The host is not necessary for the worms to replicate from one device to another. Worms exploit the vulnerability of a network to spread.

Virus:



Worm:



Computers' roles in crimes

Computers serve a major role in crime which is usually referred to as “Cybercrime”. This cybercrime is performed by a knowledgeable computer user who is usually referred to as a “hacker”, who illegally browses or steals a company’s information or a piece of individual private information and uses this information for malevolent uses.

In some cases, this person or group of individuals may become evil and they destroy and corrupt data files. This cyber or computer-based crime is also known as hi-tech crime or electronic crime. As the computer is the main source of communication across the world, thus this can be used as a source of stealing information and this information can be used for their own benefits.

The role of a computer in the crime may vary depending upon the activity that a person does, for instance, a person may steal the details and misuse them on one hand, and on the other hand, a terrorist may use the information to do violent activities and some persons may steal financial information for trading purposes and so on, but these all activities can be done by the means of a computer only.

There are several examples of crime that use computers they are as follows:

- Spying:

This is a process of spying on a person or business.

- Malware creation:

The process of creating malware like viruses etc.

- Cybersquatting:

It is a process of gaining personal information and trying to resell them.

- Harvesting:

Here, hackers usually steal a person’s private information from an account and use it for illegal activities.

- Wiretapping:

Here, the hacker connects a device to a phone line and tries to listen to the conversations.

Introduction to digital forensics

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.

Digital Forensics helps the forensic team to analyze, inspect, identify, and preserve the digital evidence residing on various types of electronic devices.

The essential objective of using Computer forensics is that it helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.

Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

Types of Digital Forensics

The types of digital forensics are:

Disk Forensics:

It deals with extracting data from storage media by searching active, modified, or deleted files.

Network Forensics:

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

Wireless Forensics:

It is a division of network forensics. The main aim of wireless forensics is to offer the tools needed to collect and analyze the data from wireless network traffic.

Database Forensics:

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

Malware Forensics:

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Email Forensics

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

Memory Forensics:

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from raw dump.

Mobile Phone Forensics:

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters

Introduction to Incident

Incident

Computer security incidents are some real or suspected offensive events related to cybercrime. In other words, an occurrence or an incident (attack) is an event wherever a system/service fails to produce a feature or service that it had been designed to deliver.

Incidents are categorized into three types:

Low-level incidents: where the impact of cybercrime is low.

Mid-level incidents: The impact of cybercrime is comparatively high and needs security professionals to handle the situations.

High-level incidents: where the impact of cybercrime is the most serious and needs security professionals, and forensic investigators to handle the situations and analyze the scenario, respectively.

Incident Response Methodology

Incident response is the process of dealing with a data breach or cyber attack, including how an organization attempts to control the consequences of such an incident. The goal is to effectively manage incidents to minimize damage to systems and data, reduce recovery time and cost, and control damage to brand reputation.

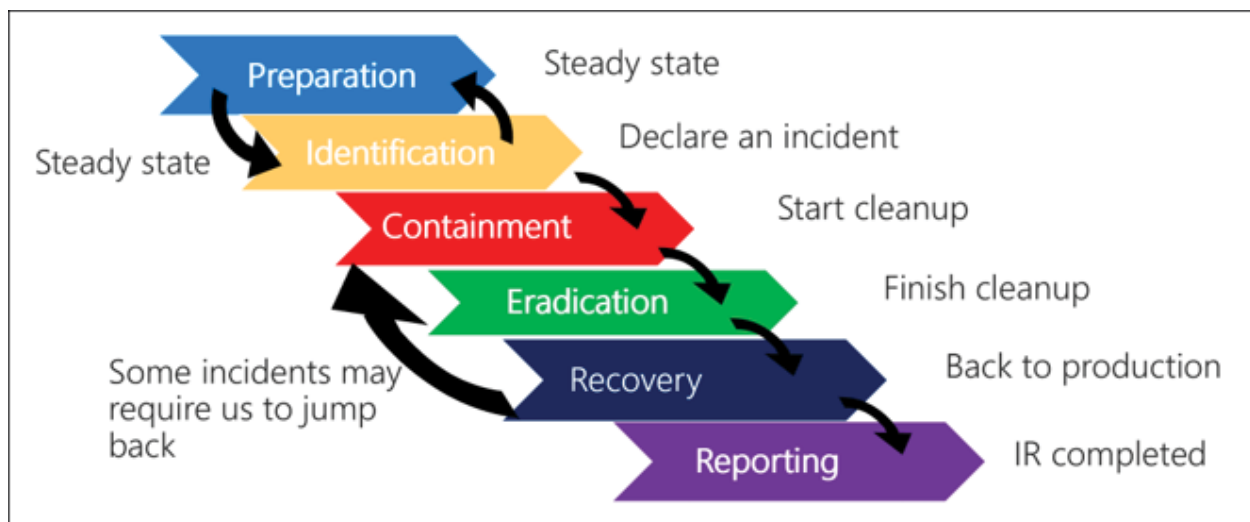
Organizations must implement a clear incident response plan. This plan should state what constitutes a security incident and describe a straightforward process teams can follow when an incident occurs.

It is also important that organizations designate a team, employee, or leader responsible for managing the overall incident response initiative and executing on the plan. In a larger organization, this team is called the Computer Security Incident Response Team (CSIRT).

Steps:

A standard incident response methodology that may be implemented by an organization includes the following steps:

1. Preparation
2. Identification (Detection)
3. Containment (Response)
4. Eradication (Mitigation)
5. Recovery
6. Lessons learned (post incident activity, postmortem, or reporting)



1. Preparation:

The preparation phase includes steps taken before an incident occurs. These include training, writing incident response policies and procedures, and providing tools such as laptops with sniffing software, crossover cables, original OS media, removable drives, etc. Preparation should include anything that may be required to handle an incident or that will make incident response faster and more effective.

2. Identification (Detection):

One of the most important steps in the incident response process is the detection phase. Detection, also called identification, is the phase in which events are analyzed in order to determine whether these events might comprise a security incident. I.e. determining whether an event qualifies as a security incident.

3. Containment (Response):

The response phase, or containment, of incident response is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident. Responses might include taking a system off the network, isolating traffic, powering off the system, or other items to control both the scope and severity of the incident.

In this phase, limiting the damage of the incident and isolating affected systems to prevent further damage.

4. Eradication (Mitigation):

In this phase, finding the root cause of the incident and removing affected systems from the production environment.

The mitigation phase, or eradication, involves the process of understanding the cause of the incident so that the system can be reliably cleaned and ultimately restored to operational status later in the recovery phase.

5. Recovery:

In this phase, ensuring no threat remains and permitting affected systems back into the production environment. The recovery phase involves carefully restoring the system or systems to operational status.

6. Lessons learned (post incident activity, postmortem, or reporting):

Prepare complete documentation of the incident, investigate the incident further, and understand what was done to contain it and whether anything in the incident response process could be improved.

Important considerations for this phase should include how the response could have been quicker or more effective, which organizational shortcomings might have contributed to the incident, and what other elements might have room for improvement. Feedback from this phase feeds directly into continued preparation, where the lessons learned are applied to improving preparation for the handling of future incidents.

Activities in Initial Response

1. Obtaining Preliminary Information:

One of the primary steps of any study is to gain enough information to determine an appropriate response this is the goal of the initial response phase.

It is necessary for your organization's initial response to include the following activities:

- a.** An incident receiving the initial notification.
- b.** After the initial notification, record the details, including an incident declaration, if appropriate.
- c.** Assembling the CSIRT (Computer Security Incident Response Team).
- d.** Perform the traditional investigative steps.
- e.** Interviews to be conducted.
- f.** Determine whether the incident is escalated or not.

Again, to develop an appropriate response strategy, the idea is to gather enough information.

2. Documenting Steps to Take:

The other reason of the initial response phase is to document steps that must be taken. When an incident is detected, organization and discipline prevent "knee-jerk" reactions and panic.

Phases after Detection of Incident

1. Recording the Details after Initial Detection:

- a. Initial response checklists:** To record the circumstances surrounding a reported incident, use an initial response checklist as the mechanism.
- b. Second section of the initial response checklist :** The second part of the initial response checklist could be used by the members of the CSIRT to address the technical details surrounding the incident.

2. Incident Declaration : In most of the cases, it will be immediately obvious whether or not the activity is actually a computer security incident in which suspicious activity is reported.

3. Assembling the Computer Security Incident Response Team : Responding to incidents, many organizations have a CSIRT that is formed in response to a particular situation or incident rather than an established and dedicated centralized team.

4. Performing Traditional Investigation Steps :

- a. Host-based evidence
- b. Network-based evidence
- c. Other evidence

5. Conducting Interviews: The first step is to start asking the “who, what, when, where, and how” questions, when your CSIRT learns of a suspected incident.

6. Formulating a Response Strategy: The most important aspect of incident response is arguably your response strategy. In this phase, you consider what remedial steps to take to recover from the incident.

