10908662

1. Malicious software known as spyware is created to stealthily gather data from a user's computer or device without that user's knowledge or consent.
2. 1.Objectives

* Investment Offer Fraud: Often referred to as Ponzi schemes or investment scams, investment offer fraud primarily tries to trick people or organizations into parting with money under the false pretense of offering investments or high returns that seem too good to be true. Investment offer scammers aim to take money straight from their victims.
* The goal of data piracy, on the other hand, is to steal and take advantage of confidential or valuable information. Trade secrets, financial information, intellectual property, and personal information are a few examples of this. The goal of data pirates is to make money off of the stolen information directly or to utilize it for other nefarious activities like business espionage, identity theft, or data sales on the black market.

2.Methods

* Investment Offer Fraud: Those who commit investment offer fraud usually fabricate investment possibilities that seem risk-free and guarantee large profits. To draw in new investors and give returns to previous ones, they can employ complex plans and pyramid schemes, all the while taking money for themselves. False information and convincing sales pitches are common tools used in these scams to entice victims.
* Data theft: Theft of confidential information from computer systems or networks through unauthorized access is known as data piracy. To obtain data, hackers may employ malware, phishing, social engineering, or hacking techniques. After that, they might sell the stolen information, use it to commit extortion, or carry out other illegal actions.

3.Victims

* Investment Offer Fraud: People or organizations that invest funds or other resources in the fraudulent scheme are usually the victims of investment offer fraud. They are tricked into thinking they are investing wisely and have the potential to make large gains.
* Data theft: The people who fall prey to data theft include private citizens, commercial enterprises, and even governmental organizations. Data pirates can exploit the stolen information for a number of crimes, including fraud, espionage, and harming people's and companies' finances and reputations.

1. 1. Physical layer

* Eavesdropping/Tapping: To intercept data being transmitted, attackers can physically tap into wireless signals or communication connections. This is commonly known as wiretapping.

2. Data link layer

* MAC spoofing: By altering their Media Access Control (MAC) address, attackers can pose as a trustworthy device on the network and obtain unapproved access.
* Attackers can use Address Resolution Protocol (ARP) spoofing or poisoning to link their MAC address to a valid IP address, diverting network traffic to their device.
* VLAN Hopping: In situations with switched networks, attackers might take advantage of security flaws to move between virtual LANs (VLANs) and access private network segments without authorization.

3.Network layer

* IP spoofing is the technique by which attackers can seem to be a reliable source by altering the source IP address of their packets, hence evading network security measures.
* Routing Attacks: These comprise attacks on routing protocols that have the ability to reroute traffic to nefarious locations, such as BGP hijacking.

4.Transport layer

* Man-in-the-Middle (MitM) attacks: These include the unintentional interception and manipulation of data between two communication parties. Session hijacking and SSL/TLS interception are examples of such attacks.
* Attackers have the ability to overwhelm a target server with a huge volume of SYN requests, resulting in a denial of service by overloading its resources.

5.Session layer

* Session hijacking: Through the theft of cookies or session tokens, an attacker can gain control of an established session between two parties and pretend to be a genuine user.
* Attacks known as denial of service (DoS) can interfere with session layer protocols, preventing communication and rendering services unusable.

6. Presentation layer

* Malware Payloads: When processing data, attackers have the ability to insert malicious code that takes advantage of holes in the application layer.

7. Application layer

* SQL Injection: Via the manipulation of input into web applications, attackers can run unauthorized SQL queries against the database and perhaps obtain sensitive data.
* Cross-Site Scripting (XSS): When malicious scripts are injected into websites that other users visit, there is a chance that their accounts may be compromised and their data will be stolen.
* Phishing: Social engineering assaults that deceive people into divulging private data, like passwords and usernames.