In computer security a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Here’s a quick explanation of some of the common security threats you may come across:

1. Malware
2. Computer virus
3. Rogue security software
4. Trojan horse
5. Malicious spyware
6. Computer worm
7. Botnet
8. Spam
9. Phishing
10. Spoofing
11. Rootkit

1. MALWARE:

Malware is short for “malicious software.”

Malware is a term used to mean a “variety of forms of hostile, intrusive, or annoying software or program code.”

Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits

2. COMPUTER VIRUS:

A computer virus is a small piece of software that can spread from one infected computer to another.

The virus could corrupt, steal, or delete data on your computer—even erasing everything on your hard drive.

A virus could also use other programs like your email program to spread itself to other computers.

3. ROGUE SECURITY SOFTWARE:

Have you ever seen a pop-up window that advertises a security update or alert? It appears legitimate and asks you to click on a link to install the “update” or “remove” unwanted malicious software that it has apparently detected. This could be rogue security software designed to lure people into clicking and downloading malicious software. Microsoft has a useful webpage that describes rogue security software and how you can protect yourself.

4. TROJAN HORSE:

Users can infect their computers with Trojan horse software simply by downloading an application they thought was legitimate but was in fact malicious.

Once inside your computer, a Trojan horse can do anything from record your passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record your every move.

5. MALICIOUS SPYWARE:

Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims.

An example would be keylogger software that records a victim’s every keystroke on his or her keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet.

Keylogging software is widely available and is marketed to parents or businesses that want to monitor their kids’ or employees’ Internet usage.

6. COMPUTER WORM:

A computer worm is a software program that can copy itself from one computer to another, without human interaction.

Worms can replicate in great volume and with great speed.

For example, a worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts’ address books.

Because of their speed of infection, worms often gain notoriety overnight infecting computers across the globe as quickly as victims around the world switch them on and open their email. This happened with the Conficker worm (also known as Downadup), which, in just four days, had more than tripled the number of computers it infected to 8.9 million.

7. BOTNET:

A botnet is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse.

An individual computer in the group is known as a “zombie“ computer.

The botnet is under the command of a “bot herder” or a “bot master,” usually to perform nefarious activities. This could include distributing spam to the email contact addresses on each zombie computer.

For example, If the botnet is sufficiently big in number, it could be used to access a targeted website simultaneously in what’s known as a denial-of-service (DoS) attack. The goal of a DoS attack is to bring down a web server by overloading it with access requests. Popular websites such as Google and Twitter have been victims of DoS attacks.

8. SPAM:

Spam in the security context is primarily used to describe email spam —unwanted messages in your email inbox. Spam, or electronic junk mail, is a nuisance as it can clutter your mailbox as well as potentially take up space on your mail server.

Unwanted junk mail advertising items you don’t care for is harmless, relatively speaking. However, spam messages can contain links that when clicked on could go to a website that installs malicious software onto your computer.

9. PHISHING:

Phishing scams are fraudulent attempts by cybercriminals to obtain private information.

Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources.

For example, the message would try to lure you into giving your personal information by pretending that your bank or email service provider is updating its website and that you must click on the link in the email to verify your account information and password details.

10. SPOOFING:

This technique is often used in conjunction with phishing in an attempt to steal your information.

A website or email address that is created to look like it comes from a legitimate source. An email address may even include your own name, or the name of someone you know, making it difficult to discern whether or not the sender is real.

Spends spam using your email address, or a variation of your email address, to your contact list.

Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.

11. ROOTKIT:

According to TechTarget, a rootkit is a collection of tools that are used to obtain administrator-level access to a computer or a network of computers.

A rootkit could be installed on your computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on your PC and may contain spyware that monitors and records keystrokes.

Related posts:

1. Types of Attack
2. Computer and cyber security
3. Introduction to network security
4. Intrusion detection tool
5. Categories of security assessments
6. Security terminologies and principals
7. Intoduction to intrusion
8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions

18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer