PC Booster
Believe in better

Adware Glossary

Adware

You can generally find these types of components accompanying freeware applications. They are usually designed to force advertisements onto your PC which are intended to try and make money for the developer that creates them. Popups and banners are the typical methods for displaying the advertisements.

Attack Vectors

This is how malware tries to make it onto your PC through the means of certain protocols such as HTTP, SMTP, FTC, IM, and more. You can try and fight off malicious software by using -anti-malware programs.

Bots

A Bot is a certain type of program and is a shorter expression for the term robot. Bots are usually found to be using internet type programs that will give it access to the root system so it can take over and perform its actions in order to take command of the system. You'll often find that bots attempt to join other machines in order to create a botnet which is a group of machines that have been infected. Bots basically take over the machine in order to perform certain actions. When this occurs, the system really has no control over itself because the bot has taken over. Bots are capable of performing DOS attacks against websites and they can also perform certain activities like spamming.

Browser Helper Object (BHO)

The BHO will often appear to be a tool that can be used in conjunction with Internet Explorer, when in fact it is a malicious program that will compromise the security of your browser, change your default home page, and provide information to third parties about your browsing habits and more.

Browser Hijackers

These types of programs can hijack your browser in an attempt to manipulate your browser settings, in order to gain access to your personal information. Quiet often your firewall does not catch these programs because they appear to be Internet Explorer components. This type of program is generally classified as a Trojan.

Dialers

A malicious program that will dial phone numbers using your modem and perform other types of harmful actions on your PC like calling long distance numbers without you ever knowing it. This can lead to high call charges that you not expect to receive. There are some dialers that are not harmful and are made to assist in connecting to the internet.

Dynamic Testing

A method for testing security solutions in which threads are executed in order to test the ability of that solution. One test may involve opening an email attachment with a virus in it to allow real time protection software programs to analyze the virus and learn how to block the threat in future occurrences.

Drive-by Download

This is one method of downloading a virus to a user's machine, and as a result there are usually attacks against the browser as well as any OS vulnerabilities that exist. Several instances of the download may be placed on the user's machine so that they are sent to many different domains and/or websites. This prevents any detection by anti-malware programs.

Exploits

When vulnerabilities exist in browsers or operating systems, then individuals might create exploits to attack against those types of issues before they have been addressed and fixed. If the user's machine has not been patched, then the programs can successfully make their way onto the system to perform some type of harmful action. These types of programs are designed to perform actions that are otherwise prevented or not allowed. The exploits may be designed in such a way so that multiple harmful activities may be accomplished at the same time.

FTP Threats

Attacks that take place through FTP. Attacks are usually performed by malware programs.

Keyloggers

Programs like this are designed to record the keystrokes that the user makes while typing. This obviously has some serious threats to the user including the fact that they could obtain personal information about the user while they are typing. Keyloggers are capable of storing a lot of information and then sending that information to third parties.

Layered Service Provider (LSP)

This code is used to take over and grab hold of the communication lines between WinSock and your internet browser for the purpose of obtaining your personal information that is being passed back and forth between your PC and internet websites.

Malicious URL

This type of URL will send a user to a specific threat that could lead to an attack.

Malware

This term is basically the catchall term for harmful spyware programs such as adware, Trojans, keyloggers, browser hijackers, and more.

Placebo Files

These types of files can be completely harmless but can also be very malicious at the same time. One example would be opening local ports. These files are completely innocuous and are used in order to create a control group in custom test sets.

Real Time Testing

This is one way of testing for attacks at the very moment that they enter your environment, instead of testing at a scheduled point in time. This approach allows you to identify and eliminate issues as they occur rather than waiting until they have already made their way through to your environment.

Rootkit

This term is used to describe a set or grouping of tools that is used on the host system for the purpose of attacking a user's system or network in the hopes of gaining pertinent information about that particular system or network.

They are often used to camouflage harmful programs from firewalls and system scanners in order to make their way into a system or network. Cloaking utilities is also another way to refer to them. This term has become more widely known following the anti-copy security software on a number of Sony-BMG audio CDs showed tendencies similar to rootkits in the Digital Rights Management Strategy.

SMTP Threats

SMTP threats occur when malware makes use of email to perform attacks on system applications in order to take advantage of vulnerabilities that exist on a system at any given time. This can result in the loss of the user's personal information.

Socially Engineered Attack

Attacks that are attempted in order to gain access to a user's PC based on how susceptible they are to fear and trustworthiness. These types of attacks are very complex and are usually carried out with Trojans or through phishing.

Spyware

This type of attack uses the computer user’s internet connection typically with the user's knowledge or consent for the purpose of gathering personal information and transmitting it to third parties where they may exploit other attacks onto the user. Spyware places packages or applications onto the users system via freeware or shareware applications that are downloaded to the user's PC. Often times the user is not aware that this took place until the programs have made their way onto their systems. Spyware is often used as a generic expression for many types of malware. Users often do not realize that Spyware can be downloaded to their systems simply by visiting a website that contains the malicious software.

Here are some of the different types of Spyware that exist.

1. Backdoor - An unknown or secret way of making an entrance to a computer, program, network, or other type of system. These types of programs are often created to attack systems or programs that have vulnerabilities so that future attacks can also be made. Backdoor’s allow

hackers to gain unauthorized access to steal information and perform other types of harmful activities.

2. Key Loggers - A form or surveillance software that can record the keystrokes that a user makes on his or her keyboard. Key Loggers have the ability to record this information which could lead to the loss of personal information that the user would not otherwise give out.
3. Financials - This type of program has the ability to gain access to financial information such as transaction data and is capable of transmitting that data to an external user.
4. Proxies - Proxies can allow an external user to gain access to a computer so that he or she can use it however they desire. Often at times hackers will use proxies to send out spam or other harmful attacks which are almost entirely untraceable.
5. Password Stealers and Crackers - These programs are designed to steal passwords on computer systems. Stealers and Crackers are capable of decoding any encrypted data in order to gain access to the information within.
6. Downloaders - These programs are used to download other files and programs onto a user's systems without them knowing it is even happening. This is done in order to perform other types of harmful and malicious activities on the user's computer.
7. Hijacker - This type of file can change the default homepage of your browser and can also manipulate browser settings in an attempt to gain access to private information on your PC like browsing history, security settings, bookmarks, and more. They are also capable of setting redirects that takes the user to commercial sites that may not be suitable for the user.
8. RATs - A Remote Access Trojan (RAT) is a type of malware that is created for the purpose of gaining access to a remote computer or

network in order to perform some type of harmful action on that computer or network. This type of access is usually not authorized by the owner of the remote computer or network, and is usually gained through the use of a backdoor program.

Static Testing

This is a method used for testing security programs during which groups of threats a passed to it for analysis. Types of threats included may be malware, vulnerabilities, or URLs.

Tracking Cookies

Cookies are small text files that contain data about the user and these files are created by internet browsers for the purpose of creating a more personalized internet browsing experience. They are used to track information that is collected by web sites and are often very beneficial in the case of repeat visits to those websites because their information is remembered. Cookies can also be used to track your browsing activity in order to provide information about your browsing tendencies and actions.

Trojans

Trojans are quite similar to spyware and can make their way onto your PC before you realize that it happened. They are also referred to as Trojan Horses, and can be used to perform harmful actions on your PC that may cause long term affects to your computing environment. Trojans generally do not replicate themselves, but can deliver other types of malicious software.

Undesirable URL

These types of URLs redirect users to other websites which may have content that is not appropriate for younger viewers. Adult content websites are a popular destination for undesirable URLs as well as sites that have other types of harmful programs within them.

Virus

This is an application that becomes connected to a file in your system or a boot sector in the system diskette. Viruses are downloaded to the user's system and in most cases they do not realize it has happened. These types of programs are created by hackers to perform harmful operations on the users’ files or disks; often they bring those systems down and make them inoperable. Viruses are self-replicating so they can spread throughout the system very rapidly. Many of the common viruses of today are spread through the internet and are built so they can bypass security systems.

Web Threats

These types of threats are typically found in the HTTP protocol and are created to do malicious things to the user's systems. Some of the malicious activities included in web threats are drive-by downloading and phishing.

Worm

This type of malicious program is a self-replicating program that spreads through a computer or network, usually via email, and carries out harmful activities on the user's computer or network. Some of the activities may include wasting system resources, spreading adult related content, system shutdowns and more. Worms typically are stand-alone systems and remain that way when they copy themselves.