In this article we will discuss different types of threats:

**ADWARE**

These are the programs that are powered by some advertising campaign which continuously displays different ads while you are running the application. So, generating revenue for the author of the program. These programs not only display different unwanted ads rather they also collect different sensitive information and communicate it to third party, which is then used for advertisement purpose or some other use without your permission. It usually collects the information about the different application including web browser and internet connection speed etc and their usage. This can also be used to predict the habits of particular user.

Usually downloading of shareware and freeware software from different website may cause Adware to be downloaded from Web sites to your computer. Different email messages and instant messengers can also infect your machine with Adware. A user may naively trigger Adware by accepting an End User License Agreement from a software program linked to the Adware.

**BROWSER HELPER OBJECT**

Browser Helper Object is a type of threat that is usually found as a small program start running automatically every time you launch your Internet browser. Your system usually gets infected by a Browser Helper Object by installing some suspicious programs. It is typically installed by browser toolbar ad-on. These objects can track your activities including internet usage and collect other information (the websites you visit, sometimes very sensitive information including passwords and credit card information as well) that is used on the internet.

**DIALER**

A Dialer is small plug-in that installs automatically when you visit some unauthorized websites or install some suspicious software on your machine. It configures itself to your dialup settings and dials to the number of its choice. Once your system is infected by a Dialer threat; it disconnects the user’s default internet connection, and reconnect to internet using the new dialup connection that is automatically generated by it. The user is billed for the time used sometimes at higher rate. While they may not spy on users, they are malicious in nature and can rack up expensive and unwanted bills.

**DRIVE-BY-DOWNLOADS**

It’s a type of threat that get install itself by displaying a misleading dialogue box on user screen or other stealth installation. So the user may not be aware of what is being installed on his machine. And the installed program could be used for any purpose by the author (it may also include some tracking module that collects user information and communicate to third party).
HIJACKERS

A Hijacker is a small program that always attempting to hijack or take control of the home page of your internet browser. It may then reset it with the site of its own choice; which is almost always loaded with advertisement, popup windows, or may redirect to some unwanted website. Although Hijackers have low security risk; but could be annoying for the users.

These types of threats usually make use of sneaky techniques or misleading dialogue boxes to get them installed on your machine. Hijacker normally put a reference to themselves in the StartUp or Registry, so that it reinstalls itself every time the computer is started. If the user tries to change any of these settings, the hijacker then changes them back upon reboot.

KEYLOGGER

Keyloggers are small programs that record your every detail about your machine i.e. every action you perform on your computer even your keypad activities. So every action you perform is then logged back in a file for example when you typed your password or credit card information all keystrokes will be saved in a file. Keyloggers could be setup on your system by some suspicious software or if you are using a public computer it could be set setup by some other user to track the activated of different people using this computer.

LAYERED SERVICE PROVIDER (LSP)

LSP is a piece of software that is tightly woven into the networking services of a computer. Usually when you are using the protocol of the internet i.e. TCP/IP, the LSP integrate itself with the TCP/IP layer of your network. It has access to all TCP/IP traffic popping into and leaving your machine. So LSP could enhance communication of your system and protect it in many useful ways, if its written by a "good" author. However, spyware authors can also utilize a LSP to spy on the habits and data of the user. As the computer will not see any of the data until the LSP lets it through, it is possible to change information so that the spyware vendor benefits. Worse still, because the LSP is very tightly woven into the TCP/IP layer, trying to remove it without the proper precautions may break the part of the program that handles TCP/IP communications. When the handler is broken, a computer may not be able to connect to the Internet.

PARASITEWARE

Its type of an adware that by default, replace some affiliate tracking links with their own. The behaviour of a Parasiteware is almost same as a parasitic because this type of software credits other sites with commissions and in turn lives off what would have been the affiliate's income. Although Parasiteware is of very low security risk but could be annoying for the end user.

MALWARE

A Malware is a type of program whose basic purpose is to interrupt the normal functioning of a computer. It is specifically designed to disturb the normal routine operation of the computer system. You can classify a Trojan horse or a virus as Malware. Some advertising software can be malicious in that it tries to re-install itself after you remove it.
RATS

RATs abbreviation of Remote Administration Tools, are small but dangerous programs that enables an attacker to gain unrestricted access to your computer whenever you are online. In other words it gives full control of your computer to a remote user; who can then perform different restricted tasks on your machine without any authorization. The attacker can perform activities such as file transfers, adding/deleting files or programs, and controlling the mouse and keyboard. 1188=Rogue Active X are scripts that run on websites and either install software on the PC without the users knowledge or open a gateway onto the users hard drive to access files in an attempt to delete and modify them as they will.

RETOBYES

It's a type of threat whose basic purpose is to prohibit Anti-sypware programs from detecting it. To accomplish it they may also use various other hiding techniques such as using common system file names. Spyware software that actively attacks a detection program or programs in an effort to prevent detection. Retrospies are malicious and usually use different cunning trick to avoid detection.

SCUMWARE

The words Scumware is usually used for any unwanted software/program/plug-in or utility installed on your computer without your permission and prior knowledge.

SEARCHPAGE HIJACKERS

SearchPage Hijackers take control over your default search engine. This doesn't mean you cannot use your favorite search engine, it means that when you mistype something, their search page will pop-up. This generally includes alot of advertisements and generally contains a search engine that will deliver advertising content rather then relevant search results.

SNOOPWARE

Snoopware is another name for Spyware, which refers to the act of intrusive. What it actually does is exactly same as a Spyware software; i.e. it tracks what you do on the internet, collect different information including sensitive information(passwords, credit card numbers) and transfer it to a third party, that may use it for an authorize mean.

SPAM

Spam is unsolicited commercial e-mail or the junk mail you get in your mailbox. While registering at some unauthorized website when you provide your email address along with your other personal information; please make sure to read their privacy policy. Sometimes these websites are partnered with third-party and share your personal information with them. Hence you are automatically enrolled in their advertising programs and received unwanted emails.

SPYWARE

Another type of the threats is stand-alone programs that can secretly observe system activity. Spyware can also detect passwords or other confidential information and communicate them
Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.

SURVEILLANCE SOFTWARE

Surveillance Software is potentially greater and more dangerous in nature than other viruses because they keep on logging your keystrokes, history, passwords, and other confidential and private information (credit card numbers) and then transfer it to a third party without your knowledge. These are often sold as a spouse monitor, child monitor, surveillance tool or a tool to spy on users trying to gain unauthorized access. They stealthily collect user information and monitors activity without the user's knowledge.

It’s not necessary that you will be only spied when you are connected to internet rather these software will save logs to a file for future transmission. Some of them may use email log file feature rather than updating the online database. Several Surveillance Software vendors go as far as using "stealth routines" and "polymorphic" techniques to avoid detection and removal by popular anti-spy software. In conclusion, Surveillance Software is a program that takes your information and then sends that information to another user on the internet.

THIEFWARE

Thiefware is software that pops up on sites and does not pay or even give credit to the web page owner. It can also redirect a search or webpage to the web page of their choosing. This practice is not illegal although many web site owners believe it to be unethical.

TROJANS

You might have heard two different terms Trojans or Trojan Horses both are one and the same thing. These are programs that appear to be safe even beneficial, but in fact, are harmful.

They are named after Trojan Horses that was used in a war by the Greeks to gain access to the city of Troy. That looked like a present of a giant wooden horse, but actually concealed soldiers inside. Similarly these programs appear to beneficial for you but, infect they are very harmful. The harmful contents could be anything from a virus to a RAT (Remote Administrative Tool). Trojans are designed to cause loss or theft of computer data, and to destroy the system. Your computer can get infected by Trojans as email attachments, or bundled with other software programs.