Source : https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/

Top 10 Vulnerability Assessment Scanning Tools
Comodo HackerProof
OpenVAS
Nexpose Community
Nikto
Tripwire IP360
Wireshark
Aircrack
Nessus Professional
Retina CS Community
Microsoft Baseline Security Analyzer (MBSA)

---.
(source: educba.com)

Botnet

DDoS

Data Breach

Farming

***Fishing**

***Malware**

***Brute Force Algorithm**

What is Botnet?

Botnet is a number of devices connected to the Internet, each running one or more bots. Nowadays, the Internet is bursting with online security threats. Most of these threats are because of technologies that are intended for productive use have been manipulated to be used as a hazard. One such technology is Botnet. Botnets have become a chief threat to security systems these days due to their rising popularity amongst cybercriminals.

A botnet is a string of Internet-connected devices, each of which is performing a task. These devices can be anything from computers to smartphones and the security of these devices gets penetrated with the control being surrendered to a third party.

These penetrated and conceded devices are called “bots”. The supervisor of this botnet is able to manage the actions of these compromised devices.
Botnets gain access to our devices through a malicious piece of code and our devices are hacked, either directly or hacked with the help of a spider, which is a program that crawls through the Internet to look for openings to be exploited in our security. Botnets then try to add our devices to their network of devices, so that they can be controlled by the botnet’s owner. Once the master computer is in control of our device, our computer is used to carry out degenerate tasks.

Let us see how botnets can affect us.

- Botnets use our machine to assist in distributed denial-of-service (DDoS) attacks to shut down websites.
- They send out spam emails to millions of users.
- Botnets are used to generate false Internet traffic on a third-party website for monetary gain.
- Botnets replace ads in our web browser to make them specifically targeted for us.
- They deploy pop-ups ads designed to get us to download a phony anti-spyware package and pay to remove the botnet through it.

Now that it is clear that botnets can be used for malicious uses, the question of protecting our personal information and devices arises. The first step to achieve this is understanding how these bots work and then we can work towards taking preventative actions against them.

To get a better understanding of how botnets work, let us consider the word “botnet” which is a combination of the words “robot” and “network”. This is exactly what a botnet is, a network of robots carrying out malicious tasks.

To create a botnet, botmasters need as many “bots” (compromised devices) under their control as possible. Connecting many bots together will create a bigger botnet, which in turn helps in creating a bigger impact. Imagine the following scenario. You have procured ten of your friends to call the police station at the same time on the same day. Aside from the loud sounds of ringing phones and the scampering of employees from one phone to another, nothing else would happen. Now picture 100 of your friends do the same thing. The instantaneous flow of such a large number of calls and requests would overwork the police station’s phone system, likely shutting it down entirely.

Botnets are used by cybercriminals to create a similar commotion on the internet. They instruct their compromised bots to burden a website to the point that it stops functioning and the access to that website is denied. Such an attack is called a Denial of service (DDoS) attack.

This isn’t usually created to infect just an individual computer. They are designed to compromise millions of devices. This is usually done by injecting the systems with a trojan horse virus. This tactic requires users to infect their own devices by opening bogus email attachments, clicking on random pop up ads and/or downloading unsafe software from a risky website. After infecting the devices, botnets are then free to access and alter personal information and infect other devices.
Complex botnets can find and infect devices on their own. These independent bots perform seek-and-infect tasks, constantly searching the web for vulnerable devices lacking antivirus software or system updates.

Botnets are problematic to detect. They do not disrupt normal computer functions and thus, avoid alerting the user. Some botnets are designed so as to even

prevent detection by cybersecurity software. Botnet designs continue to grow, making newer versions even harder to detect.

Botnet structures are usually designed to give the botmaster as much control as possible.

1. Client-Server Model
In this model, one main server controls the transmission of information from each of the clients.

2. Peer-to-Peer Model
In this model, each bot acts as a client and a server, rather than depending on a central server. These bots have a list of other bots to help them transmit information within themselves.
Now that we've seen how botnets work, we can look at precautionary measures to prevent botnets invasion.

1. Update Operating System
This is the number one tip for keeping botnets or any other malware at bay. Software developers detect threats early on and release updates with security patches. Hence, we should set our OS to update automatically and make sure we're running the latest version.

2. Avoid Opening Email Attachments from Unknown Sources
Along with avoiding opening an attachment from an unknown source, we should also examine emails sent from known sources, as bots use contact lists to send infected emails.

3. Use Firewall
Use a firewall when surfing the Internet. This is easy with Mac computers, as they come with pre-installed Firewall software. For a Windows-based system, install third-party software.

4. Avoid Downloads from File-Sharing Networks
In case there are no other alternatives, then make sure to scan the downloaded file before opening or running it.

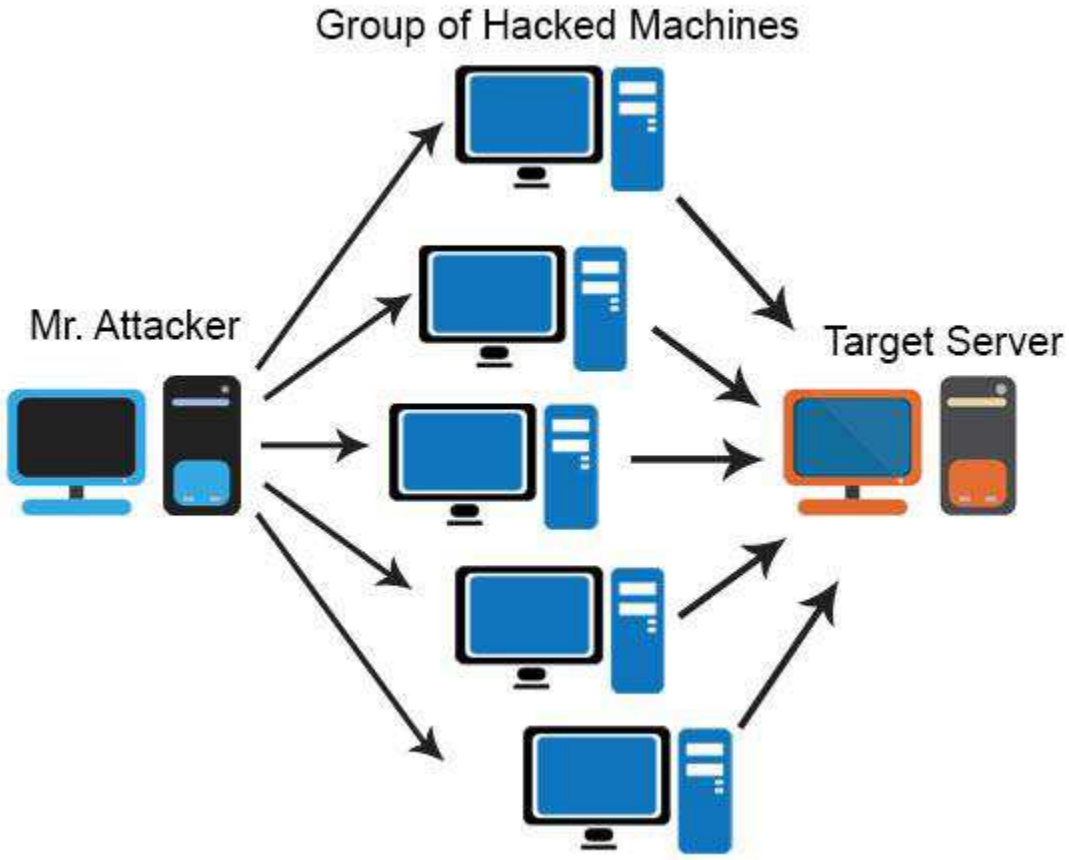
5. Do not Click on Unknown Links
Before clicking on any link, hover your cursor over it, to see where the URL is being directed. Malicious links are often found in YouTube comments, pop up ads, etc.

6. Install Antivirus Software
Try to get antivirus protection designed for all the devices, and not just the computer. With rising technology, the potential for the botnet is also increasing. In the 2016 presidential election, Facebook's fake ad controversy and Twitter bot fiasco were a great worry to many politicians. Studies from MIT have determined that automated accounts and social media bots play a major role in spreading fake news. Aside from this, botnets are dangerous as they steal personal information. Cybercriminals tend to hunt for low-hanging fruit. Taking preventative measures now can protect your devices, data, and identity.

---.

Introduction to DDoS Attack

DDos commonly abbreviated as Distributed Denial of Service which is used to wash out the network resources due to that the end user cannot get access to the essential information and also it makes the performance of application very slow. DDos is an attempt to make a web application or online service busy by congestion with massive floods of traffic which produced from several multiple resources. It is hard to locate where the attack comes from or the origin of attack because it arrives from various sources, usually uses Trojon to infect a system. In this article, we will discuss What is DDoS Attack?
DoS (Denial of Service) attack is different from DDoS attacks because DoS is used to target a single network connection and single computer whereas the DDoS attack used to damage multiple systems and several network connections at the same time, which is referred to as Botnet.



What are Botnets?
Botnets are defined as the attackers construct a network of hacked technology; they spread by a piece of code through social media, websites, and emails. Attackers can control the system remotely, without the end users knowledge once

these systems get infected and frequently they used to commence an attack on the infected computers against any intention.
There are few symptoms to track whether your computer is get infected by DDos,

- Constantly loss of internet connection.
- A website which was available before unexpectedly becomes unavailable.
- Incapable of right to use any website.
- Corrupted network performance.
- Unable to use internet services for a lengthy time period.

Purpose of a DDoS Attack
The purpose of the DDoS attack primarily includes politics, competitions, revenge, war, and criminal activities.

How does it work?

- The DDoS attack has in need of an attacker to get the power of a network of online systems in a process to carry out an attack. Once the systems or other machines get infected with malware each one reflects into a bot, then the attacker can easily get access over the computers through remote controls.
- If the botnet has established, the attacker can able to have complete access to the computers by transferring well-run instructions to each and every bot through the remote controls. Once the IP address of the end user is tracked or targeted by the botnet, each and every bot will start to work on it to respond by transferring request to the targeted machines, and probably origin the server or network resultant in a DoS to normal traffic, and to make overflow capacity.

How can DDoS Attack happen?

- DDos is a form of a cyber attack that has intense critical systems to interrupt network connectivity or service so that it creates a denial of service for users of the specified resource.
- DDoS attacks make use of the power of numerous malware-affected systems to achieve a single system.

The Motive behind a DDoS Attack

- The DDoS attack is used to flood out the network resources so that the end user cannot get access to the necessary information and also it makes the performance of the application very slow.
- The DDoS attacks can control or take down the website of all sizes commencing from large enterprises to small units for more susceptible sites.

- The progress for the attacks differs from pure financial gain to politics.
- The motive behind the DDoS attacks is which can be sold out, so the consumer possibly will ask for an assured website to taken offline and also make payment for its execution. In this case, revenge is often a motive.
- On the other hand, if the attackers require money they might also want to blackmail a website for their required money and also keep their website slow down or suddenly becomes unavailable for long period till their required payment.
- In conclusion, a trendy approach used to control political events and obstruct others a political memo is to thrash and take down websites with unusual views. The activity like this is becoming a progressively more smart way of using DDoS attacks to deal with the media.

What to do after a DDoS Attack

After the DDoS attack process we can find out our system behaviors like slow responses, there will be no access to the website and loss of internet access likewise we will face such cases. If we facing such issues to follow few things,

To make a call to ISP (Internet Service Provider) and let them know that you have attacked by DDoS.

- If you can able to control your website, keep it in safeguarding mode to avoid any loss of data and report to the management team about the concern.
- Call the third –party to inform them about you are under attack which may dependable for security management or service delivery.
- To get as much as information achievable
- To get track of server logs, with the time of events
- To monitor all the occurrence of the system and be attentive that any changes might happen on your system during or after the DDoS attack.
- To showcase the traffic throughputs, traffic statistics.
- To check backend databases and all critical systems and to make a note on any changes that might occur on the system.
- To look out the issues that take place in temporary sites

To employ professional guidance to help ease the issues and execute a flexible solution that will help to reduce any DDoS occurrences. To retain a risk register and renew any tragedy improvement plan to comprise a DDoS endurance plan. To avoid the DDoS attacks, have in contact with DDoS prevention experts.

How to prevent it

The DDoS prevention are followed,

- Attack Prevention and Preemption (before the attack)
- Attack Detection and Filtering (during the attack)
- Traceback and Identification (during and after the attack)

1. In Attack Prevention and Preemption (before the attack) we have to protect the host from agent implants and master by using scanning measures and signatures to identify them. To monitor the network traffic for recognized attack information’s sent between masters and attackers.
2. In Attack Source Trackback and Identification(during and after the attack) to locate the precise source of a packet without relying on source point. The noticed information can be recorded by the routers, and also routers can send the message about the seen packets to their target place.

3. In Attack Detection and Filtering (during the attack) in the Attack Detection, we can identify the attacked DDoS packets and in packet Attack Filtering to categorize those packets and reducing them.

Conclusion
A DDoS (Distributed Denial of Service) attack uses network vulnerability which makes persistently loss of network connection, slow down the system performances, creates more traffic on the internet which results in unable to use internet service for a long period of time. This practice is favorable for the trespasser those who wish for the valid user to cooperate with the safety measures of his essential and sensitive information. Once the system gets attacked by DDoS it might not be found easily and its prevention is also not the easiest one. The only way to get relieved from this is to determine whether any injuries caused by it and to take action to recover it.

---.

Introduction to What is Data Breach?

In this topic, we are going to learn about What is Data Breach. Internet, digital communication, digitization, data sharing are some of the keywords which we come across regularly or rather say on a daily basis. With an increase in demand for data sharing over the network, there is an increase in the rate of the incident against data misuse. Our data is private to us and it has the right to privacy, however, there is an increase in the report of such complaints in which unauthorized person tries to access someone's private data.

All these scenarios, lead to originate a term known as "Data Breach". We will like to discuss in detail about the data breach, its definition, and many more.

Data Breach is an act or process in which some unauthorized person or resource tries to access someone's else data without concerned of the latter.

It is simply a security incident in which data is accessed using unauthorized means. There may be different intuitions for accessing such data without authorization.

Now, we already know a bit about the data breach. Before discussing further, we would like to highlight a bit about its definition.
According to the Wikipedia, It is defined as "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." Data breaches may involve financial information such as credit card or bank details or may be other forms of sensitive data.

To summarize about definition, it is accessing unauthorized data without concern of the data owner or to whom does data originally belongs to directly or indirectly.

Now, let us move to our new topic, which is:
It is now well known to our readers about the data breach. Also, we gave a hint about why it is actually done. The basic intention behind data breach is to get

through applied securities and access intellectual, private data of an organization or a group of people. The intention may vary differently such as for research purpose, for fraud or others also.

Now, it is not a simple concept. It is a complex process which involves lots of phases, these phases may be divided into different sections as per the attack carried out under each phase. These phases may include the research part, analysis part, attacking part, misuse of data and others. This paragraph takes us to the new section. Let us discuss it in brief.

Well to be broadly classified, there can be four different phases of a data breach which are:

1. Research.
2. Attack.
3. Network/Social attack.
4. Ex-filtration.
5.

Let's discuss in details one by one:

- **Research** – This is basically finding the loophole in the system. The intruder tries to find any loophole or weakness into the system using which it can attack a particular set of data. The next phase which follows is Attack
- **Attack** – In this phase, the intruder or cyber attacker tries to make initial contact either through a network or through a social attack. This is one of the most important phases as intruder sometimes also tries to make friendly contact so that the victim does not get any doubt about the possibility of a data breach.
- **Network/Social attack** – This could be further divided into two attacks named as Network attack and the other as a Social attack. Let's discuss each of them one by one. Lets first discuss Network attack.

1. **Network Attack** – A network attack occurs when an intruder tries to enter institution, network, system or organization using some organizational weaknesses. The intruder tries to infiltrate an organization's network.
2. **Social Attack** – Social attack includes tricking people either by getting their trust directly or indirectly for giving access to the organization network. A victim can be duped to pass sensitive information like credentials or other important data.

Now let us discuss Ex-Filtration.

- **Ex-Filtration** – Once the intruder gets access to the organization network, then intruder reaches easily to sensitive data which is highly confidential to misuse it. The intruder can use this sensitive data in any way it wants to access it.

Now our next topic aligned is:
Well, I think it's self-explanatory and there are many reasons to discuss why does data breach actually happen? Well, there could be not one but many reasons why this data breach happens. It could be for research purpose, for data misuse, for online fraud or maybe an endless number of reasons.

A data breach generally follows one common process which is, intruder examining the network, find the loophole in the system, and finally tries to exploit it with either

a network or social attack. Once an intruder is inside the organization he could access sensitive data without any supervision.

Few of the common ways to prevent a data breach is as follows:

1. Keeping only relevant data on the network.
2. Safeguarding data.
3. Dispose of unused data.
4. Review and update the process regularly.
5. Educate users.
6. Keep the password protected.
7. Use licensed software.
8. Use updated software.
9. Avoid using the public network.

& many more…
Next, we will discuss what if data breached has happened.

Well, once it has happened we need to go through following steps to minimize the effect. One should do the following things:

1. Evaluate which data is stolen.
2. Update all passwords with more secure passwords.
3. Inform relevant institutions.
4. Update software's with latest updates.

A common example that most of the people have come across is that an intruder calls the random person and represents himself as a bank employee. The intruder generally tries to win the trust of the victim and then asks for sensitive information like credit card number, CVV number, etc.

With increasing our necessity on the internet, data sharing there is a vulnerability of data breach. An intruder tries to exploit loopholes in the system so as to misuse the data. There could be a different mechanism which could be followed to minimize the chances of the data breach.

---.

Introduction to Pharming

Since the internet was developed it has evolved too much. Evolution has happened not only in terms of usage, speed but also how it is misused. There are always people who are looking for some sort of loopholes using which they could enter the whole system. Once entered they could exploit the resources and could easily misuse it. There are several ways or mechanism using which exploitation is done. Phishing, cyberbullying, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting (XSS) attack are few of them which is commonly used. Once such a common attack is Pharming. So now let us know what it is.

What is Pharming?
If we try to explain in simple words then we can say that Pharming is a simple cyber attack which works on the logic of redirecting the user to different URL or website when a user tries to use access original website. Pharming is a relatively new work. Here initial two characters which are "Ph" keyword Pharming is derived from the term "Phishing". Phishing is another type of cyber attack where intruders try to receive user credentials by making a look-alike fake page of original popular

websites. Normally it is the role of DNS servers to resolve requested domain name to respective website IP addresses. However, an infected DNS server resolves the domain name to fake site IP addresses. Once the user lands on such fake site websites and enters credentials, the user's credentials are captured and are used for wrong uses
Now with that, let us know the definition of Pharming?

Definition
Pharming is one of the various cyber attacks which are practiced by the attackers. Pharming simply redirects the user from accessing the requested site to a different but similar looking fake site. In Pharming simply DNS is infected so that instead of resolving to an actual IP address, it gets resolved to some wrong or fake website IP address.
The infected DNS system is generally referred to as "poisoned".

Understanding
There are several ways by which Pharming is generally practiced. One such common way is to update or infect the user's local system host files. They generally infect personal computer's host files. An attacker generally sends them some malicious code which infects their local system host files. It is the role of host files to convert user requested URLs into a number of manipulated strings which in turn is used by the computer to access web sites.

Another common form of Pharming is infecting DNS directly. Role of DNS is to resolve user requested domain name to a respective website IP address. An injected DNS wrongly resolves incoming request and hence redirecting the user to malicious pages

What is the purpose of Pharming?
By now it is quite clear that for what Pharming is generally used for. Like any other cyber attack, pharming too is practiced with the wrong intention. The basic minds behind Pharming try to get user sensitive information such as username and passwords. These collected sensitive user information are then used for various fraudulent transactions like banking transactions etc.

Another common use or purpose of Pharming is to generate traffic to a webpage. This is done basically to generate revenue by generating traffic on a particular website domain. As more and more traffic is generated by redirecting to the wrong website, more and more revenue is generated.

How do you recognize Pharming?
There are several ways to recognize Pharming. Although there is no full proof mechanism by which we can say that following particular set of operations will keep users safe from Pharming. Let us try to look at a few different ways by which we could detect fake websites at least on a broader scale.

Look for secured websites only – Once you are migrated to a particular website, always check secured websites. Like your website should follow Https:// protocols. For example, the website should start with https://www.WEBSITE.com If the website is following secured Hyper Text Transfer Protocol then only proceed to enter your valuable credentials.

Now let us try to know that apart from https protocol what are the other ways by which we can detect fake websites.

- **Defacements** – Look for any defacement like attackers generally remove original logo with the similar looking logo
- **Suspicious pop-ups** – Check if the website is showing unwanted ads and pop-ups
- **SEO spam** – Comments containing website URL is another way to detect vulnerable website

How do you prevent Pharming?
There are several ways using which Pharming could be totally avoided. Although using malware and anti-virus has no impact on it. There is no point in using such tools against Pharming as in most of the cases attack is done online while navigation of url's in spite of the host system. Now let us look how Pharming could be prevented

- **Do not click on URL directly** – For navigating to a website do not open a URL by clicking on URL directly contained in emails or something. If you wish to visit a website then always open a new tab or browser and then manually enter the link of the desired website which you wish to visit

- **Avoid clicking ads on websites** – Do not click on ads and pop-ups which randomly appear on different websites. These ads could be the potential source for the same

- **Check for https keyword** – As explained earlier also always use websites which has secure protocols. Never try to access those websites which are not following secured protocols

Conclusion
There are several ways by which attackers do cyber attacking. Pharming is one such mechanism. They generally try to find loopholes in the system and then try to get benefit from such loopholes by misusing it. We people generally due to our negligence always visit any website and uses it without providing any attention to the authenticity of the visited website. Some of the other way it is our duty also to detect such malicious websites and avoid using it.

---.

Malware, also generally referred as malicious software could be software-generated using some piece of code which is designed with an intention to effect in the wrong way to a computer or server or may be other peripheral devices. This could be of any form. It could be a script, any executable code, or any other form of software. These pieces of code could be generally termed as a computer virus, worms, ransomware or even simple scripts.
It typically performs its malicious activities after it is implanted into the computer system.

Definition of Malware

Malware could be a piece of code which generally could be in the form of software designed deliberately to affect the computer system. Once it is installed into the computer system, it can access the resources of the computer system, may share data to some remote server without user concern, or may track user details, etc. Now let us know the purpose of doing such malicious activities:

Malicious Activities
There could be many reasons for doing such activities. Let us look the motive for doing such malicious activities.

For Gaining Access to User System – There is much malware which gets installed to the user system either by installing software from unknown sources, etc. Once it is installed, they try to gain access to the user system and tries to gather data at some remote server. This malware monitors user activities, user habits, etc. and once such data is gathered, these malicious software saves it to a server.

Generating Clicks – Another activity which is performed by such malicious software is to generate clicks to advertisements without user concern. These software generated clicks on advertisements which take a user to a different website. Doing such things, they try to generate traffic on a particular website

Showing Advertisement – Many malwares once installed show similar types of advertisements to the user. They generally monitor user activities like the type of website user visits, etc. and based on such things, show advertisements to a user.

Encrypting Files – Few of the malicious software encrypt user files and asks the user to pay a certain amount of money in order to decrypt such files.
Now, these are few of the basic causes for performing such malicious activities.

Types of Malware
Based on how such malware is spread it could be broadly categorized as follows:

Virus – A virus generally spreads when a user installs software and that particular software which is installed is infected with malicious software. A virus is simply a software which gets installed in a user system using some executable files. Once a virus is installed its start infecting other executable files.

Worms – A worm is a malware which generally spreads through the internet. These worms get infected to the user system through the internet.

Rootkits – This is typically a type of malware which remains hidden. Once this malicious software is installed, they try to remain hidden in order to avoid detection. These malicious software tries to modify the operating system so that it remains hidden. Rootkits hide such malicious activities from getting visible to the user.

Anti-Malware Software
Now, with knowing how this software can do malicious activities let us know how this malware could be prevented

Anti – Virus
There are lots of antivirus software which could be installed to prevent any kind of virus. This anti-virus software once installed take care that no virus gets installed. Also, they can scan your system for anti-virus and would repair it. These anti-virus monitors during the installation of new software for viruses.

Anti-Malware software
There is anti-malware software also available which detects for malware installed in the user system. They perform detection of any malware when a user is using the internet over a network. Anti-malware software prevents malware from infecting the user system. Also, it is just like an anti-virus scan for any malware installed.

How to Prevent Malware from Installation?
Now, let us know how we can prevent different types of malware.

Spyware
Adware
Computer virus
Worm
Trojan
Ransomware
Rootkit
Phishing and spear fishing

Installing Legit Software Only – Always install legit software. Software from in-legit manner often contains malware in them.

Installing Software from the Unknown Source – Always install software from known sources. Do not download software from any website apart from getting install it from the known source.

Updating Operating System Updates – Install operating system updates as these updates often contain an updated definition for the detection of malware.

Updating Software Patches – Installed software also gets patches. One needs to install such patches to prevent it.

Installing Anti-Virus – Install anti-virus and anti-malware software to prevent any such malicious activities.

Conclusion
It is used widely to infect the user system. This malware is used to monitor user activities. Based on such activities this malicious software can show advertisements, generate traffic to websites, etc. One must install good anti-malware software to prevent such malicious software

--- end of file ---