Spyware and Trojan Horses

Sonali Jadha
Department of Computer Engineering
Rajashri Shahu College of Engineering, India

Abstract— This seminar covers a contemporary issue in Computer Security; Spyware and Trojan Horses. These are separate security threats to networked systems, both of which are realized using differing software development techniques. We introduce the concepts of Spyware and Trojan Horses, followed by detailing how each is constructed and installed. We go into depth on their operation, which is revealed with the aid of demonstration software. Following our examples, we present a range of preventions, solutions and cures to each threat posed. We discuss the issues surrounding the user's interaction with such software and conclude by specifying an optimal solution for the avoidance of the threats posed. This seminar is aimed at everyday computer users, Software Engineers and Computer Security professionals. The differing levels of information conveyed will be of use to each of the aforementioned groups. We are confident that each group will receive sufficient information to minimize the risks posed to them by Spyware, Trojan Horses and other affiliated network-based software. Smart phones are increasingly being equipped with operating systems that compare in complexity with those on desktop computers. This trend makes smart phone operating systems vulnerable to many of the same threats as desktop operating systems. In this paper, we focus on the threat posed by smart phone rootkits. Rootkits are malware that stealthily modify operating system code and data to achieve malicious goals, and have long been a problem for desktops. However, the ubiquity of smart phones and the unique interfaces that they expose, such as voice, GPS of rootkits particularly devastating. We conclude the paper by identifying the challenges that need to be addressed to effectively detect rootkits on smart phones.

Key words: Spyware Horses, Trojan Horses

I. INTRODUCTION

A. Malware

Many PC users consider malware, viruses, spyware, adware, worms, Trojans, etc. as the same thing. While all these infections harm our computers, they are not the same. They are all types of malicious software that each behave differently.

The word malware is a combination of two words "malicious" and "software". It is a generic term used to describe all of the hostile and intrusive program codes including viruses, spyware, worms, Trojans, or anything that is designed to perform malicious operations on a computer.

The meanings of many of these words have changed over time. Some refer to how the malware infects your system while other words are used to describe what the malware does once it's active in your machine.

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. For a malicious program to accomplish its goals, it must be able to run without being detected, shut down, or deleted. When a malicious program is disguised as something normal or desirable, users may unwittingly install it. This is the technique of the *Trojan horse* or *Trojan*. In broad terms, a Trojan horse is any program that invites the user to run it, concealing harmful or malicious executable code of any description. The code may take effect immediately and can lead to many undesirable effects, such as encrypting the user's files or downloading and implementing further malicious functionality.

B. Symptoms

1) My computer is running extremely slowly

This could be a symptom of many things, including infection by a virus. If it has been infected by a virus, worm or Trojan, among other things, which are running on the computer, they could be running tasks that consume a lot of resources, making the system run more slowly than usual.

2) Applications won't start

How many times have you tried to run an application from the start menu or desktop and nothing happens? Sometimes another program might even run. As in the previous case, this could be another type of problem, but at the very least it's a symptom that tells you that something is wrong.

3) I cannot connect to the Internet or it runs very slowly

Loss of Internet communication is another common symptom of infection, although it could also be due to a problem with your service provider or router. You might also have a connection that runs much more slowly than usual. If you have been infected, the malware could be connecting to a URL or opening separate connection sessions, thereby reducing your available bandwidth or making it practically impossible to use the Internet.

4) When I connect to the Internet, all types of windows open or the browser displays pages I have not requested

This is another certain sign of infection. Many threats are designed to redirect traffic to certain websites against the user's will, and can even spoof Web pages, making you think you are on a legitimate site when really you have been taken to a malicious imitation.

Library files for running games, programs, etc. have disappeared from my computer. Once again, this could be a sign of infection, although it could also be down to incomplete or incorrect installation of programs.

II. SPYWARE

A. What is spyware?

Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

"Spyware" is mostly classified into four types: system monitors, Trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users.

Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

While the term spyware suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.

Sometimes, spyware is included along with genuine software, and may come from a malicious website. In response to the emergence of spyware, a small industry has sprung up dealing in anti-spyware software. Running anti-spyware software has become a widely recognized element of computer security practices, especially for computers running Microsoft Windows. A number of jurisdictions have passed anti-spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.

Spyware does not necessarily spread in the same way as a virus or worm because infected systems generally do not attempt to transmit or copy the software to other computers. Instead, spyware installs itself on a system by deceiving the user or by exploiting software vulnerabilities. Most spyware is installed without users' knowledge, or by using deceptive tactics. Spyware may try to deceive users by bundling itself with desirable software. Other common tactics are using a Trojan horse. Some spyware authors infect a system through security holes in the Web browser or in other software. When the user navigates to a Web page controlled by the spyware author, the page contains code which attacks the browser and forces the download and installation of spyware.

One way to distinguish a virus from spyware is by its behavior. A virus seeks to infect a computer; to replicate; and ultimately, to infect as many computers as possible, as quickly as possible. When you accidentally install a virus onto your computer, the malicious code that is "the virus" tries to find ways to use your computer to infect other computers. For example, an email-delivered virus (a worm) may search your computer's file system for your Outlook address book, and send infected email messages to contacts it finds in the address book. Before you dismiss your own address book as a modest success, consider what a jackpot email addresses like all_users@company.com or winelovers@makewinenotwar.biz is for a virus. A Spyware application is often content to hide on your system. Spyware disguises itself as a legitimate application or secretly resides as one more data link library or registry setting Joe Average User knows nothing about, so that it can collect information about you, your messaging and browsing behavior, your online preferences. Spyware may have a heavier "footprint" on your computer than a virus: spyware will embed itself deeply into critical components of your operating system and bloat your memory with its monitoring and collection processing executables. So where virus activities are overt and sufficiently extensive in their impact to attract attention quickly, spyware activities are typically covert and their infestations are often long lasting.

1) Network Technology

The network infrastructure which is used for Spyware implementation is relatively complex. Due to the commercial nature of Spyware, very few details are given pertaining to its construction. The diagram shown in Figure and our technical analysis should not be deemed to be entirely accurate.

The Spyware entity exists on the client machine. The client machine is connected to a network appliance, which may be a router, network switch or modem (any device providing internet access). The internet connection is used by the client to make various session contacts with Spyware affiliated servers. The Spyware will locate an available port on the client machine, and forward its network traffic through this port. Data pertaining to the user's habitual use is concatenated and routed through the internet to the Spyware Server. This is added to the User Data database, which may be connected to the server using a suitable database connection technology. Banner adverts are subsequently accessed using the same access technology on a different database, and routed back through the internet to the end user. These targeted adverts will appear on the user's desktop.

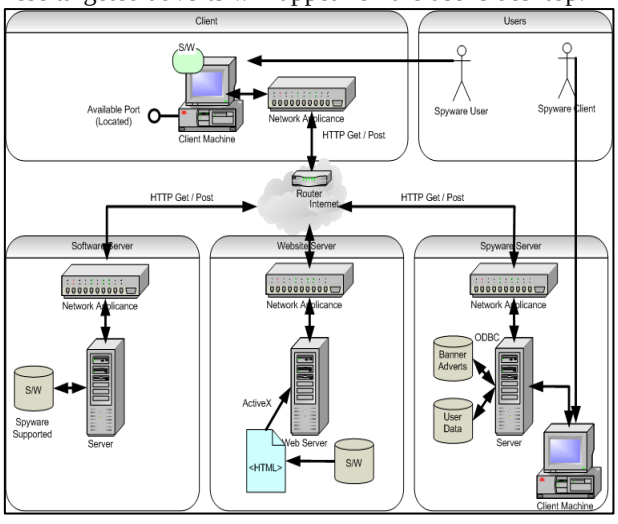

Fig. 1: A typical spyware network.

The user contracts Spyware in the initial circumstance from one of two sources.

– Spyware may be installed by the download of a Spyware supported program from an FTP site or other software server. CNET Download.com is one such example. The FTP / HTTP Get request will initiate the download of the software onto the client machine. Installation will be

performed by the user and during this installation they will be asked permission to install the Spyware as well as the software.

– Spyware may be installed through accessing a website, whose prime aim is to post Spyware onto the client. The Spyware installation will be embedded within the web page. ActiveX (a Microsoft technology) is then utilised to install the Spyware (generally as a browser plug-in), on the client. ActiveX is a mechanism which allows applications to be run within other applications. This installation will allow the Spyware to operate every time the browser is opened.

2) Client Technology

Spyware operation on the Client machine is again, an unknown process. However, when one reads further into the Spyware domain, it becomes more transparent as to how this software achieves its goals. Once the Spyware has been installed, its operation is composed of two processes. One, a memory resident application which is created at boot-up, the other a plug-in which operates when the Browser software is run. Strings of URLs visited by the user are passed from the Browser interface to the Spyware plug-in. The URLs visited are forwarded from the plug-in to the memory-resident process started at boot. This can perform a series of actions. Personal data collected by the plug-in is sent from the main process through the internet to the Spyware server. Banner adverts and pop-ups pulled from this database are sent back to the user. These advertisements are pushed to the desktop by the memory resident process. In addition to this, various alterations are made by the memory-resident process to the keys in the client registry, ensuring that the Spyware entity starts at boot. Furthermore, file locks are implemented by the process on the operating system kernel, ensuring that the Spyware is very difficult for the user to completely remove. In some cases, complete removal will simply result in re-installation.

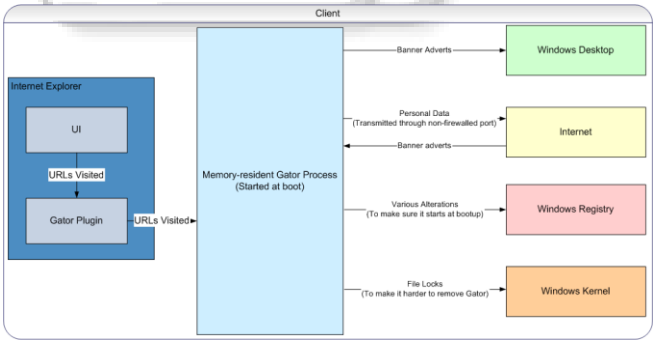

Fig. 2: Client side spyware operation.

3) Classes of Spyware

a) Tracking Cookies

A piece of information sent by a web server to a user's browser. (A web server is the computer that "hosts" a web site and responds to requests from a user's browser.) Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, etc. The browser saves the information and sends it back to the web server whenever the browser returns to the web site. It may keep track of the different pages within the site that the user accesses. Browsers may be configured to alert the user when a cookie is being sent, or to refuse to accept cookies. Some sites, however, cannot be accessed unless the browser accepts cookies.

b) Browser Hijacking

Browser hijacking is a form of unwanted software that modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser. A browser hijacker may replace the existing home page, error page, or search page with its own. These are generally used to force hits to a particular website, increasing its advertising revenue.

c) Keylogger

A Keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file, usually encrypted. A Keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. The log file created by the Keylogger can then be sent to a specified receiver. Some Keylogger programs will also record any e-mail addresses you use and Web site URLs you visit.

d) Spybots

Spybots are the prototypical example of "spyware." A spybot monitors a user's behavior, collecting logs of activity and transmitting them to third parties. A spybot may be installed as a browser helper object, it may exist as a DLL on the host computer, or it may run as a separate process launched whenever the host OS boots.

e) Adware

Software that displays advertisements tuned to the user's current activity, potentially reporting aggregate or anonymized browsing behavior to a third party.

III. TROJANS HORSES

A. What is Trojan horse?

A Trojan is a program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility. Malware is designed to run undetected in the background.

Although there are other reasons why your system might slow down or frequently crash, if you're noticing these obvious indications of malware, your system may have been compromised. In the IT environment, the Trojan horse acts as a means of entering the victim's computer undetected and then allowing a remote user unrestricted access to any data stored on the user's hard disk drive whenever he or she goes online. Their primary objective is to allow a remote user a means gaining access to a victim's machine without their knowledge. Once that has been achieved, the intruder can do anything with the machine that the user can do.

Passwords offer no protection at all because today's Trojans are capable of recording the victim's keystrokes and then transmitting the information back to the intruder. Those passwords can subsequently be deciphered by the Trojan and even changed in order to prevent the user getting access to their own files!

Practically every Trojan virus has two functional parts called the server and the client. The server part is the part of the program that infects a victim's computer. The client part is can monitor, administer and perform any action

on your machine just as if they were sitting right in front of it. A Trojan horse works a bit like the backdoor to your house. If you leave it unlocked, anybody can come in and take whatever they want while you're not looking.

Once infected, the computer becomes accessible to any remote user, usually referred to as a "cracker" or "intruder" that has the client part of the Trojan. That person can perform any action that the user can. For example, if the user keeps his credit card details on the computer, the intruder can steal that information. The intruder can also steal passwords in order to gain access to restricted information or to password protected web sites as well.

1) Trojan Horse Examples (Back Orifice)-

– The attacker may infect the victim with a Trojan horse using a number of mechanisms. Peer-to-peer networks, e-mail and file downloads are the most common forms of infection. Following this, the Trojan is installed and once installed, it becomes a memory resident process which is started at system boot-up. The executed Trojan will locate an available port and IP Address on the victim's machine, prior to sending a 'phone-home' message to the attacker, using the IRC or ICQ protocol. The attacker is then able to directly connect to the Trojan horse.

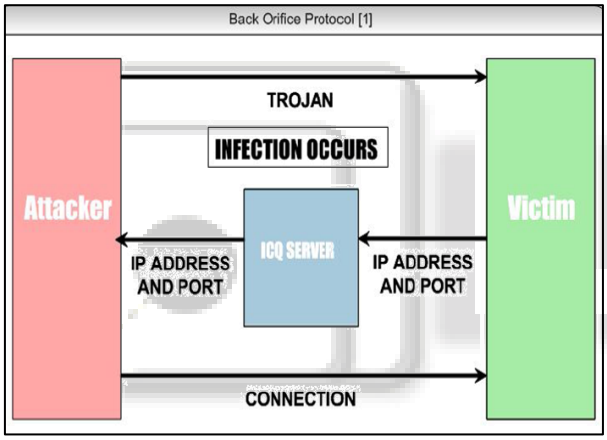

Fig. 3: The Back Orifice Protocol [1]-Infection Stage.

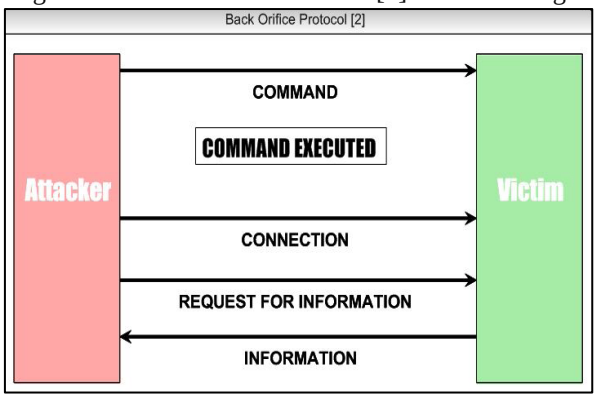

Fig. 4: The Back Orifice Protocol[2]-Execution Stage.

– Once a connection is established to the client machine by the attacker, the attacker is able to execute a command. This may be any type of command, from changing the color of the desktop background, to formatting the hard drive of the victim's client. We show the connection being requested and allowed, prior to the information request being sent and information being returned. The protocol would behave in this manner, were the attacker to request a file from the victim's machine.

– Finally, once the attacker has performed all the actions they wish to, a cleanup command is sent to the victim's client. This will remove all traces of the Trojan horse from the victim's machine; including all files and registry keys. It is not possible to detect that an attack has taken place after the cleanup command is executed.

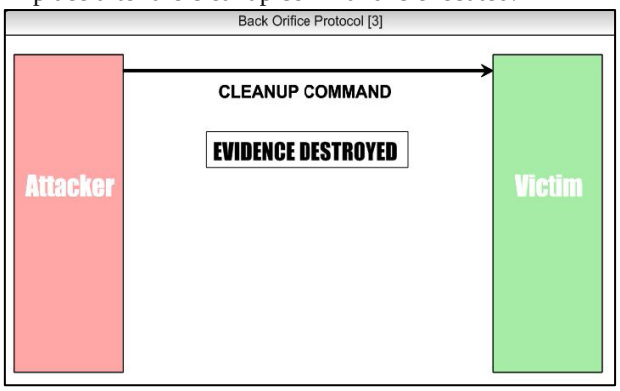

Fig. 5: The Back Orifice Protocol [3]-Removal Stage.

IV. MALWARE ON SMART PHONES

A. Background

The increasing complexity of smart phones has also increased their vulnerability to attacks. Recent years have witnessed the emergence of mobile malware, which are viruses and worms that infect smart phone. For instance-Secure reported an almost 400% increase in mobile malware within a two year period from 2005-2007. Mobile malware typically use many of same type of attack as do malware for traditional computing infrastructures, but often spread via Bluetooth, SMS and MMS. Smart phone are most vulnerable to rootkits. Rootkits are malware that achieve its goal by infecting operating system.

B. Rootkits

Rootkits typically infect the system by installing themselves as kernel modules, which are loaded each time the operating system Malware on Smart Phones is booted. However, this approach leaves a disk footprint, i.e., the Smart phones are an attractive target for attackers, both in the kinds kernel module containing the rootkit, thereby exposing the rootkit of attacks that are possible and in the social implications of these to antivirus tools. Sophisticated rootkits avoid this problem by di- attacks. As a consequence, Although such rootkits only persist until the system is has the unique advantage of being able to affect the cell phone in- rebooted, they are effective on desktop computers, which are often infrastructure as well as other phones on the cellular network. These not rebooted for several days or months at a time. Abilities have driven malware authors to focus on smart phones, once infected, a rootkit can serve as the stepping stone for several with a recent report from MacAfee stating that nearly 14% of future attacks. For example, rootkits are commonly used to mobile users worldwide have been directly infected or have known conceal keylogger, which steal sensitive user data, such as pass- someone infected by mobile malware. Nearly 72% of the users words and credit card numbers, by silently logging keystrokes. They surveyed in the MacAfee study expressed concerns regarding the might also install backdoor programs on the system, which allow a safety of using emerging mobile services and more than 86% were remote attacker to gain

entry into the system in the future. Rootkits concerned about receiving inappropriate or unsolicited content, fraud- can also perform other stealthy activities, such as disabling the fire-ulent bill increases, or information loss and theft.

1) Spying on conversations via GSM

The goal of this attack is to allow a remote attacker to stealthily listen into or record confidential conversation using a victim's rootkit infected smart phone.

The Freerunner phone is equipped with GSM radio, which is connected via the serial bus. During normal operation of phone, user-space application issues a system call to the kernel requesting services from the GSM device. GSM device are controlled through a series id command called as AT command. For example, GSM device support AT commands to dial a number, fetch SMS messages and so on. To maliciously operate the GSM device, e.g., to place a phone call to a remote attacker, the rootkit must issue AT commands from kernel.

Most smart phones today contain a calendar program, which notify user when schedule occur. Rootkit operate by intercepting these notification set by user. Notification is displayed by user space program to notify the user if impending meeting. The rootkit intercepts this notification and active it's malicious functionality. The attack code stealthily dials a phone number belonging to a remote attacker, who record confidential conversations of the victim.

When an alarm is signaled, a specific message is delivered via the write system call. Rootkits hooks the system call with the malicious write function implemented in the rootkit.

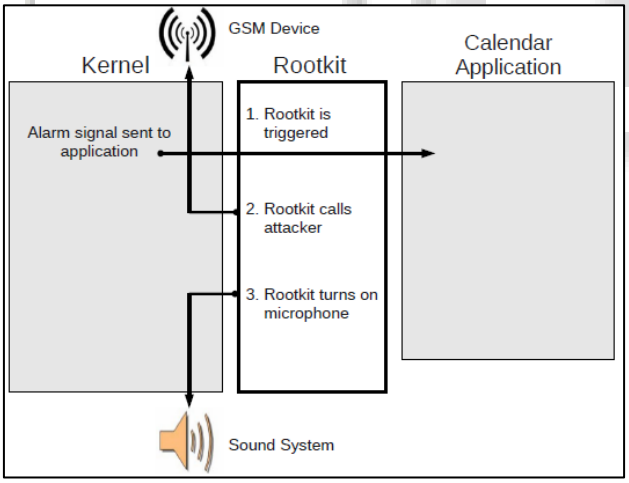

Fig. 6: The GSM rootkits intercepts an alarm signal.

The goal of malicious write function in our prototype rootkit is to check for the alarm notification in write calls.

When rootkit is triggered, our rootkit places a phone call by emulating the functionality of user space telephony applications. Typically, user space applications make calls by issuing a sequence of system calls to issue AT commands to the GSM device. The number to be dialed is located in the AT commands. Rootkit calls the attacker by issuing the same sequence of AT command from within the kernel. The AT commands issued by the rootkit activate the telephony subsystem and successfully established a connection to the attackers phone. The prototype rootkit must also activate the sound system by turning on the microphone.

V. SOLUTION: FIREWALL

A. Firewall Technology

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

1) Packet Firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped (i.e., not forwarded to their destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23, the port where a Telnet server application would be listening.

2) Stateful Firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection.

This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

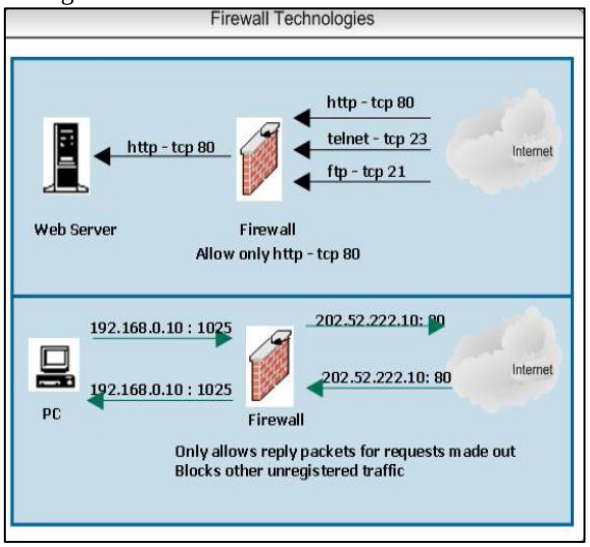

Fig. 7: Packet filtering (top) Vs Stateful Inspection (bottom).

VI. CONCLUSION

We need to be careful when download something. We also need an anti-virus to protect our computer from be infected by virus.

We need to be a smart user because this can help us from be tricked with nice thing but behind the scenes it infects our computer with a Trojan or Spyware.

Preventing spyware and adware from getting onto your computer is your first step!

- Do not download unnecessary software from the internet, especially free ones because they most likely have adware or spyware inside them.
- If a download screen appears, asking you to confirm your download, click no if you not trying to install anything.
- Avoid clicking advertised popups especially ones that mention "free" stuff if possible.

REFERENCES

[1] A.baliga, L.Iftode and X.Chen"Automatic containment of rookit attack", 10 jan 2010.
[2] Andrew Brown, Tim Cocks, Kumutha Swampillai, "Spyware and Trojan horses[ss1]"School of computer science, The University of Birmingham,12 feb 2004.
[3] A Typical Spyware Network - Derived and produced by Andrew Brown, Tim Cocks and Kumutha Swampillai
[4] The Back Orifice Protocol - Derived and produced by Andrew Brown, Tim Cocks and Kumutha Swampillai
[5] Client-Side Spyware Operation - Derived and produced by Andrew Brown, Tim Cocks and Kumutha Swampillai.

