COMPUTER MALWARES

We all use systems. We sometimes encounter with some problems which we usually consider it occurred because of virus. Virus! What is a virus? Is it only because of virus is that a computer error occurs? No, Not at all! There is much malicious software's which causes system errors or disturbances. They are called as MALWARE. A malware is nothing but software containing malicious code. It is a combination of malicious code + software. There are many types of malwares with different names causing system disturbances. They are used to cause error in system or to take control of the system or for information gathering. We will illustrate about some of the malwares.

1) Virus: A virus is a program that can replicate itself in a system and can spread from one computer to another by portable mediums or a infected file passed through internet.
2) Worms: A worm is a self-replicating program, which uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
3) Trojan: A Trojan, usually detected as Trojan horse, is malware that is intended to perform desirable effect on a system. It allows remote access to a target computer system. Once a Trojan has been installed on a target computer system, a hacker may have access to the computer remotely and perform various operations, limited by user privileges on the target computer system and the design of the Trojan.
4) Root kit: A root kit is a stealthy type of malware designed to hide the existence of certain processes or programs from normal methods of detection and enables continued access to a computer.
5) Botnet: A botnet is a collection of compromised computers connected to the Internet. The compromised systems are called as bots.
6) Spyware: A spyware is a type of malware that can be installed on systems, and which collects small pieces of information about users without their knowledge. For example, a key logger which captures the key strokes and sends them to the user who has installed it.
7) Adware: A adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer.

A sample virus code which is also called as shutdown virus:

Go to run, type shutdown –a time to shutdown (counted in milli sec)

It will start the shutdown timer. After a given time it will shutdown the system.

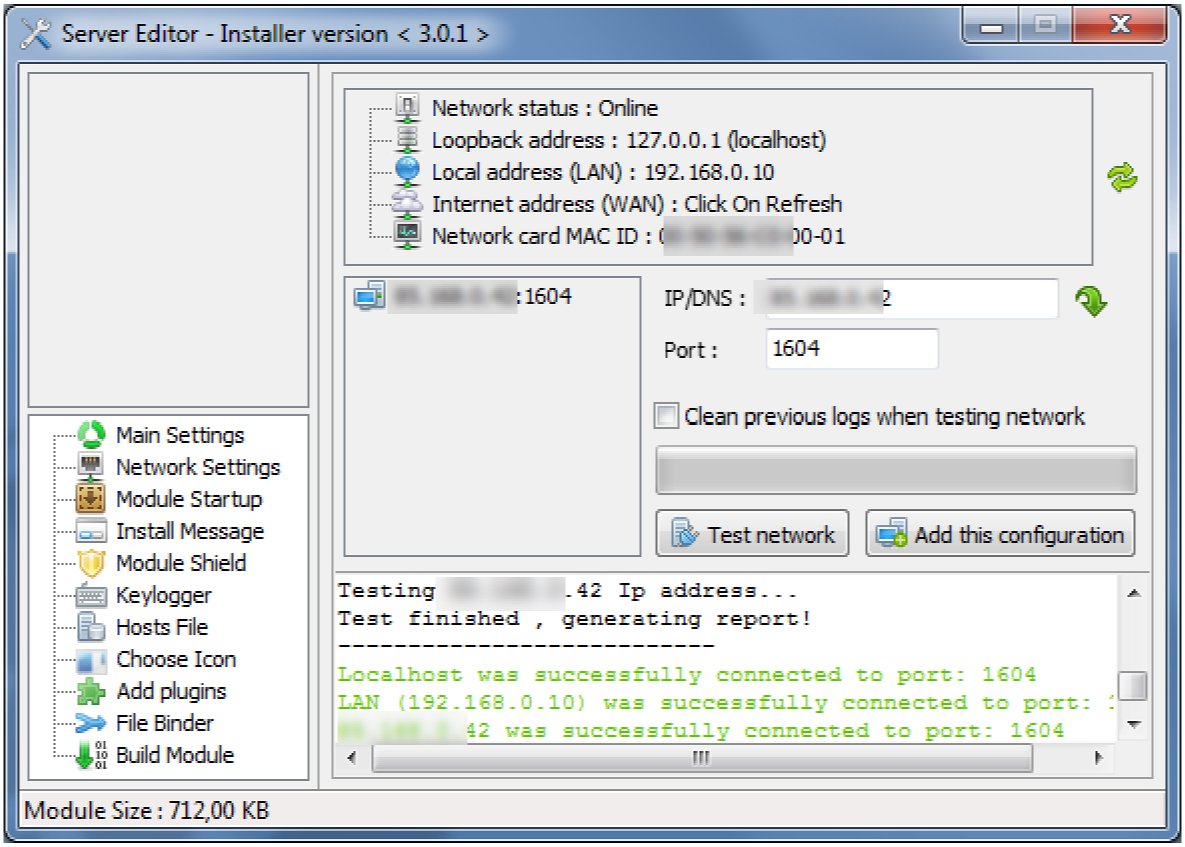
Now, we will move on to creation of a Trojan and learn about its functionality.

There are many Trojan creation software's also known as remote administration tool (RAT). They are used to create Trojans and to maintain access. Some of them are:

1) Beast
2) Turkogen
3) Dark comet
4) Xtreme RAT
5) Poison IVY
6) Back office

We will work on dark comet RAT. The steps to create a Trojan using dark comet are:

1) Go to settings and press server module.
2) A window opens which includes the functionalities which we want include for a Trojan.



Network status : Online
Loopback address : 127.0.0.1 (localhost)
Local address (LAN) : 192.168.0.10
Internet address (WAN) : Click On Refresh
Network card MAC ID : [redacted]00-01

[redacted]:1604

IP/DNS : [redacted]2
Port : 1604

□ Clean previous logs when testing network

```
Testing [redacted].42 Ip address...
Test finished , generating report!
---------------------------
Localhost was successfully connected to port: 1604
LAN (192.168.0.10) was successfully connected to port: 1
[redacted]42 was successfully connected to port: 1604
```

Module Size : 712,00 KB

3) In main settings, give our IP and assign a port number of your wish. Test the network, because, sometimes the port may not be open. Give port number which is available and open.

4) Then go to network settings and module startup and shield. Add the functionalities which we want to include. In install message, we can add a message which appears on the victim's screen when the Trojan is activated that is when the Trojan is clicked.
5) We can also add key logger functionality. We can also add a icon of our wish and plug-ins also.
6) File binder is a privilege in which we can bind the Trojan to a file. No problem, the Trojan will function as described.
7) Then the last step, build the server with any extension the RAT gives us. (usually extensions are same as system file extensions.)

That's it. We now have a Trojan, which can inject in to a system and gives us the access to the system. The Trojan gets activated only if it is opened and clicked. We will get an notification with the victim id at the bottom. We can send it through mail or portable devices. But there is a problem. What is that? ANTI-VIRUS…….

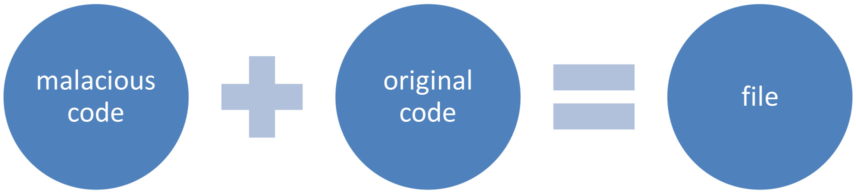
It detects the Trojan by its signature or code. Then archive it and send it. There are some chances of again detection. Then, what to do?

Before explaining how to make a Trojan undetectable, I just want to brief something about anti-virus.

Anti-virus software's are installed on system to protect the system from malwares or some other threat. Whenever a file is trying to add on to system using portable devices or downloaded from internet, it will be scanned and then stored on to the system. The scanning mechanism of antivirus is mainly based on two methods. They are:

1) Code-based
2) Signature-based

In code based scanning mechanism, the antivirus analyzes the code of the file. It separates the original code and malicious code and then deletes the malicious code.



In signature based scanning mechanism, the antivirus allows only defined signatures that are stored in the code of file.

Most of the antivirus use signature scanning mechanism to scan a file. Here, we will change the malicious signature of the Trojan, so that it can be detected by antivirus. There are few tools that are going to be needed to make Trojan undetectable. They are:

1) dsplit.exe: It is a piece of code which divides a file(Trojan) into chunks of files.
2) Hex workshop: it displays the inner code, i.e., in the language the computer interacts with file for functioning. Usually will be in machine level language.
3) Antivirus: we will use Avast antivirus.

Steps involved in making a Trojan undetectable are:

1) Make sure that we keep the Trojan file and dsplit.exe file in a specified folder. Open the command prompt and go to the specified folder where the Trojan is stored that is detected by the antivirus (Avast). Run the command:

dsplit.exe 0 (size of the Trojan) (number of chunks want to divide) (name of the Trojan with extension)

e.g.: dsplit.exe 0 66666 10000 trojan.exe

It will divide the Trojan.exe file into 67 files size in denominations of 10000 bytes. It will divide the files with adding the size at which is divided. E.g.: Trojan_52000.exe

2) Scan the chunks of files (67 files). We will get detected notification. Go to detailed information of that error. There we will get the files where the signature is detected. Check the file name with the size which is at the top. It is the exact location where the groups of signatures are stored. Now again split the file in to chunks of smaller size.

E.g.: dsplit.exe 51000 52000 1000 trojan.exe

Notice here, we got the top file with numbering 52000, but, we are dividing the file from 51000 to 52000. This is because, while binding a code the data is stored from top to bottom, i.e. , the data that is stored in first file will be included in the second file and the data that is stored in second file will be included in third file and so on. That's why we scan from 51000 to 52000 as the signatures will be present in between 51000 to 52000. This concept is as equal as of storing data in stacks and queues (data structures).

3) Again divide the file till the denomination of 1, because we should get the exact location of chunk which has the malicious signatures.

```
dsplit.exe 51500 51600 100 trojan.exe
dsplit.exe 51540 51550 10 trojan.exe
dsplit.exe 51000 52000 1 trojan.exe
```

4) We will get a group of files where signatures are stored. As I have already explained the code is stored in first file is also present in the last file. We will choose last chunk of file which is in the group of files detected by antivirus. That’s why we have scanned till the denomination of 1 so as to get that file.
5) Now open that file in hex workshop. In the data packet column, go to the end of packet and change the data there. Don’t delete it; Just change the case of letters. If it is in capital make it in to small and if it is in small case change it in to capital case. Now save the file hex workshop asks for creation of ‘.bak’ file. It’s not necessary, we can cancel it.
6) Don’t delete the chunk of file as it may hang up your system. Just let be there. Now scan the Trojan file (Trojan.exe). If the antivirus detects again, repeat the same steps till the file gets undetectable. (For Trojan are iterated as per the functionalities added.)

By doing this process the functionality of Trojan doesn’t go. It works as described by us. Use this Trojan to send through mails or portable devices. Sometimes, the mail server doesn’t allow the files with extensions of Trojan. So, zip it or archive it and send to victim and enjoy the show.