

Forum:[Hack Forums](#)

Thread: [The making of an actual cmd virus scanner](#)

5chn4pp - July 25, 2015, 9:12 am

I have an idea how to make a cmd virus scanner, but i need help with this.

So, i have a program that can create a md5 hash of a file. here is the line:

Code `fciv -md5 -add ReadMe.txt>output.txt`

As you can see, it makes a output.txt file of the md5 of another .txt file.

Here is how the output looks:

And here is all the files:

My question is, how can i scan all the files on a computer and make them in a single output.txt file?

After we solve that, how can we then scan the output for bad md5 hashes? (all the bad hashes are in the database.txt file)

If you want a download of the files, i can give you them.

.waste - July 25, 2015, 12:14 pm

Search for all drives and scan the the files in each drive for their MD5 hashes, checking them against your database.

5chn4pp - July 25, 2015, 12:16 pm

(Jul 25, 2015 12:14 PM).waste Wrote: [\[CITE\]](#) Search for all drives and scan the the files in each drive for their MD5 hashes, checking them against your database.

drivers are only like 30% of all viruses, and im asking how to actually do the code.

.waste - July 25, 2015, 12:23 pm

(Jul 25, 2015 12:16 PM)FlareMalware Wrote: [\[CITE\]](#) drivers are only like 30% of all viruses, and im asking how to actually do the code.

Reread what I posted, I did not say drivers. You must find all the drive letters. As for what to do when you get the locations, do a recursive search, if its a folder: search the folder, otherwise get the MD5 of the file and check against the database.

If you give me a download to the files I'll see what I can come up with.

5chn4pp - July 25, 2015, 12:27 pm

(Jul 25, 2015 12:23 PM).waste Wrote: [\[CITE\]](#) Reread what I posted, I did not say drivers. You must find all the drive letters. As for what to do when you get the locations, do a recursive search, if its a folder: search the folder, otherwise get the MD5 of the file and check against the database.

If you give me a download to the files I'll see what I can come up with.
well, if i try to scan for example the C: drive, it will not go into the directory and scan there

<https://mega.co.nz/#!nQNwSJDD!D0dc5pUGnvt0SZeZpoF8ObxExFydnoWTQo5L75Jr03g>

.waste - July 25, 2015, 12:34 pm

(Jul 25, 2015 12:27 PM)FlareMalware Wrote: [\[CITE\]](#) well, if i try to scan for example the C: drive, it will not go into the directory and scan there

<https://mega.co.nz/#!nQNwSJDD!D0dc5pUGnvt0SZeZpoF8ObxExFydnoWTQo5L75Jr03g>

Taking a look at fciv, it seems it has a recursive scan feature.

Check out fciv.exe c:\ -r

5chn4pp - July 25, 2015, 12:37 pm

(Jul 25, 2015 12:34 PM).waste Wrote: [\[CITE\]](#) Taking a look at fciv, it seems it has a recursive scan feature.

Check out fciv.exe c:\ -r

I cant believe that worked, well, problem 1 is kinda solved, because it crashes everytime i try to scan my C: drive

EDIT: its taking up all the write speed on the hdd, and thats why its crashing

.waste - July 25, 2015, 12:40 pm

(Jul 25, 2015 12:37 PM)FlareMalware Wrote: [\[CITE\]](#) I cant believe that worked, well, problem 1 is kinda solved, because it crashes everytime i try to scan my C: drive

EDIT: its taking up all the write speed on the hdd, and thats why its crashing

Working for me, no crashes. Read up on some of the switches and uses of fciv [here](#) to get an idea of what you can do with it.

5chn4pp - July 25, 2015, 12:48 pm

(Jul 25, 2015 12:40 PM).waste Wrote: [\[CITE\]](#) Working for me, no crashes. Read up on some of the switches and uses of fciv [here](#) to get an idea of what you can do with it.

Code @echo off

fciv -md5 -add C: -r -type *.exe>outputexe.txt

fciv -md5 -add C: -r -type *.dll>outputdll.txt

I have done this, it will now only list .exe and .dll and now its not crashing anymore. problem 1 solved.

Im also thinking of a "Whitelist" so every normal windows file with a normal md5 hash is not listed, i have no idea how to do that tho.

UPDATE:

I have added bat files to be listed, and improved the code:

Code fciv -md5 -add C: -r -type *.exe -type *.dll -type *.bat>scanned files.txt

New download: posting soon

Hackoo - July 26, 2015, 3:39 pm

(Jul 25, 2015 12:48 PM)FlareMalware Wrote: [\[CITE\]](#) Code @echo off

fciv -md5 -add C: -r -type *.exe>outputexe.txt

```
fciv -md5 -add C: -r -type *.dll>outputdll.txt
```

I have done this, it will now only list .exe and .dll and now its not crashing anymore. problem 1 solved.

Im also thinking of a "Whitelist" so every normal windows file with a normal md5 hash is not listed, i have no idea how to do that tho.

UPDATE:

I have added bat files to be listed, and improved the code:

```
Code fciv -md5 -add C: -r -type *.exe -type *.dll -type *.bat>scanned files.txt
```

New download: posting soon First, i want to thank you for this nice project ?

You forgot to add also VBS and VBE files ?

If i have time, i will join your project

To compare MD5 hash, you need to install this [MD5 Component](#) :

The MD5 component uses the industry-standard MD5 checksum algorithm to get a fingerprint of a file. If you are storing files in a database, this component is a must. To avoid storing duplicate files in the database, store the MD5 checksum along with the file in the database. Every time you save a file, take an MD5 of the file and compare it to the list of MD5s stored in the database to see if this file is already stored. This component can be used in environments that support COM such as Active Server Pages, Windows Scripting Host, Visual Basic, etc.

And this an example that show you how to use it with a vbscript : [Calculate MD5 Checksums.vbs](#)

5chn4pp - July 26, 2015, 3:44 pm

(Jul 26, 2015 03:39 PM)Hackoo Wrote: [CITE](#) First, i want to thank you for this nice project ?

You forgot to add also VBS and VBE files ?

If i have time, i will join your project

To compare MD5 hash, you need to install this [MD5 Component](#)

And this an example that show you how to use it with a vbscript : [Calculate MD5 Checksums.vbs](#)

Thanks for the kind words and links, you can join if you want.

Here is a updated link of what i have done so far

<https://mega.co.nz/#!VpVGSAyI!oJsVGXtzDgDxsZ-oODfOL173-AP5UAcDIw34iY0jP48>

I will give a update on this.

I have a database.txt file with strings of md5 hashes in it. i need to compare that to the scannedfiles.txt then i need it to create a new .txt with all the hashes in the database that were found in the scannedfiles.txt. then it can scan for the md5 hashes we want. after that we need to go to the scannedfiles.txt and get the dir of were the file is so we can create a .bat that will delete the infected file.

Then we just keep updating the database with new infected md5 hashes(also works with sha1 hashes) and then its a anti virus!

Im not sure how to do this, and i dont know .vbs.

Updated the database, I have now found a way for it to detect many files, i will not say it yet.

Added a name, This anti-virus is called Flarus.

Added a interface and a special debug mode, right now its a normal mode but it will be used for finding errors.

Updated files can be found here:

<https://mega.co.nz/#!45E03CKD!XxA5OGkA9vzGiHOuxQcMjxYLB9d5i69xrao7X3lYluw>

Also, this is maybe the smallest anti virus i have ever seen, 69 kb lol. Its also the first open source (If you dont count clam-av) anti virus.

Advertisement - July 27, 2015, 2:08 pm

Is this not whatever language that fciv.exe is programmed in?

5chn4pp - July 27, 2015, 2:11 pm

(Jul 27, 2015 02:08 PM)Rekki Wrote: [\[CITE\]](#) Is this not whatever language that fciv.exe is programmed in?

Its coded in c++, however there is no cmd command for creating a md5 hash, so everything else can be batch.

Advertisement - July 27, 2015, 2:22 pm

(Jul 27, 2015 02:11 PM)FlareMalware Wrote: [\[CITE\]](#) Its coded in c++, however there is no cmd command for creating a md5 hash, so everything else can be batch.

Oh well, what exactly would you need help with for this project?

5chn4pp - July 27, 2015, 2:26 pm

(Jul 27, 2015 02:22 PM)Rekki Wrote: [\[CITE\]](#) Oh well, what exactly would you need help with for this project?

I have a database.txt, with all the bad md5 hashes, i need to compare that database to the scannedfiles.txt that program outputs.

If it finds any matches i need it to create another .txt file with all the matches and then i need it to delete the found files.

It seems like a really cool thing, i have always wanted to see a anti virus in cmd ?

I have a way to update the database often, so it will actually be able to detect files.

Advertisement - July 27, 2015, 2:59 pm

(Jul 27, 2015 02:26 PM)FlareMalware Wrote: [\[CITE\]](#) I have a database.txt, with all the bad md5 hashes, i need to compare that database to the scannedfiles.txt that program outputs.

If it finds any matches i need it to create another .txt file with all the matches and then i need it to delete the found files.

It seems like a really cool thing, i have always wanted to see a anti virus in cmd ?

I have a way to update the database often, so it will actually be able to detect files.

Could you not apply something as simple as, something like this and make a space between hashes like

Code FOR /F "tokens=dependsonsizeofdatabase.txt delims= " %%a in ('database.txt') do (set database=%%a all the way to %% whatever, may have to do several reads)

FOR /F "tokens=* delims= " %%z in ('type hashes.txt ^| findstr %%a')

Or something like that idk on phone but thats my idea for now will clear up if I get a chance on a

PC

5chn4pp - July 27, 2015, 3:07 pm

(Jul 27, 2015 02:59 PM)Rekki Wrote: [\[CITE\]](#) Could you not apply something as simple as, something like this and make a space between hashes like

Code FOR /F "tokens=dependsonsizeofdatabase.txt delims= " %%a in ('database.txt') do (set database=%%a all the way to %% whatever, may have to do several reads)

FOR /F "tokens=* delims= " %%z in ('type hashes.txt ^| findstr %%a')

Or something like that idk on phone but thats my idea for now will clear up if I get a chance on a PC

that might be what i am looking for, but i am not that advanced in batch. If you could help then i wouldbe very thankful.

Update: I have now added a update feature, delete the normal database.txt and select the update tool, if there was no update it will just download the normal file, if there was a update it will download the updated version.

size of zip is now only 40kb

Updated download here:

https://mega.co.nz/#!ws8XHQyT!2NK5c2lgiO9jXM2AYDjkP-wzsi5Ub_kq7k56XIBYeFQ

5chn4pp - July 30, 2015, 1:40 pm

Yes! I got i working! It can now scan and delete files!

I have 1 more thing, The files are needed to be placed on here: C:/antivirus, because if you start the batch in admin mode it cannot find the other files because it starts in system32. How can i make it portable? I know its something like this:

cd %0/antivirus

Advertisement - July 30, 2015, 6:32 pm

Maybe this can be of some use

Code CD %systemdrive%/antivirusSystem drive will find out if it is C: D: E: etc

5chn4pp - July 30, 2015, 6:47 pm

(Jul 30, 2015 06:32 PM)Hiei Wrote: [\[CITE\]](#) Maybe this can be of some use

Code CD %systemdrive%/antivirusSystem drive will find out if it is C: D: E: etc

Yes, that will work better than the one i have right now, editing it now.

For anyone wondering, my anti virus can now detect the following:

Code Careto/Mask

Duqu

Exforel

Flame

Gauss

Hikit

IXESHE

Kimsuky Operation

MiniDuke and CosmicDuke

Regin

Stuxnet
Turla
ACCDFISA
AutoIt Ransomware
CBeplay
CryptoLocker
Dircrypt
FakePolice ransoms common thread
French Ransom
GEMA, GVU, InetAccelerator
Harasom (File encrypting)
Lock Em All
Loktrom (aka WindowsSecurity/Lokomoto)
MBRlock
Pornoblocker
Reveton (Notever)
Tobfy
Urausy (aka "WinLocker")
WinAD
Weelsof
Xorist
Xyeta
Andromeda
Bamital
Betabot
BlackEnergy
BlackShades NET
Carberp
Citadel (Zeus clone, based on 2.x leak)
Conficker
Cridex
DarkComet
Fareit
Gootkit (old variant)
Gootkit (fileless)
Kelihos
Kuluoz
MaxSS TDL4+
MyLoader (Oficla)
NgrBot (Dorkbot)
Poisonivy
Poweliks
PowerLoader
Ramnit
Rustock
Simda
Sinowal
SmokeLoader
SpyEye
TDL2
TDL3
TDL4
Ursnif

WSO PHP web shell
ZeroAccess (KM variant)
ZeroAccess (UM variant)
Zeus
Zeus Gameover
ZeusVM (Zeus clone)and many more

However the database is not ready yet, we are still checking for duplicates and getting access to a virus source.

EDIT: we now have access to a virus source, my scanner will detect over 16 million files once its ready.