

Forum:[Hack Forums](#)

Thread: [Session hijacking to bypass 2FA?](#)

albyaty - December 17, 2020, 12:12 pm

I am currently using a RAT, I am trying to get the cookies or login session for some victims but so far the cookie grabbing plugin that is intergrated in the RAT does not work.

Does anybody have any alternatives that I can use in this case? Will I have to run a kali virtual machine and use evilginx2? are there any other options?

if I already have access to the victim's PC, is it that hard to grab the cookie?

Thanks in advance for the help! ??

Mr zero 0 - December 21, 2020, 12:41 pm

You need to get a new rat friend, seems like your's is outdated, but then after you get it you can just use it in the browser that all the spoofers use I forgot the name atm tho lol xD but it allows user agents, cookies, proxy, and all other all the carders use it

smokey1 - January 11, 2021, 4:57 am

yes, a new rat is what u need. inbox me i might have an idea for u

Jaxsu - January 11, 2021, 9:15 pm

What browser are you trying to session hijack? Different browsers handle secrets differently. IE stores it in a Dat file, Firefox in a sqlite dB, and chrome (and edge) with dpapi encryption. So you need to target a specific browser

Sandikaaa - January 12, 2021, 1:16 pm

just use evilginx2 and patch hosts file its simple ?

Dolla\$ - January 13, 2021, 12:44 am

Just bind an exension on the target navitor, get the cookie throught it.

albyaty - January 16, 2021, 2:51 pm

(Jan 11, 2021 10:15 PM)Jaxsu Wrote: [\[CITE\]](#) What browser are you trying to session hijack? Different browsers handle secrets differently. IE stores it in a Dat file, Firefox in a sqlite dB, and chrome (and edge) with dpapi encryption. So you need to target a specific browser
The victim's browser is chrome

I got the cookie file but it is encrypted and looks useless as far as i can tell.

(Jan 13, 2021 01:44 AM)Jean Valjean Wrote: [\[CITE\]](#) Just bind an exension on the target navitor, get the cookie throught it.
What kind of an extension?

(Dec 21, 2020 01:41 PM)Mr zero 0 Wrote: [\[CITE\]](#) You need to get a new rat friend, seems like your's is outdated, but then after you get it you can just use it in the browser that all the spoofers use I forgot the name atm tho lol xD but it allows user agents, cookies, proxy, and all other

all the carders use it

If you can get me more info I'd really appreciate it, thanks friend.

gucciuser - *January 23, 2021, 4:25 pm*

Just probably use something like hidden RDP and then capture the cookies from the requests?