

Forum:[Hack Forums](#)

Thread: [Decrypt Cookies and Passwords from Chrome](#)

SIM-4329724 - August 17, 2020, 9:09 am

Hello, I need help please, I have access to a remote machine, I recovered the folder where firefox and chrome store their cookies and password, by default the firefox data is not not encrypted, so I easily recovered them by the DBrowser tool, but unfortunately I cannot recover the data on chrome because they are protected by the DPAPI (it is possible to crack the DPAPI by launching the tool Mimikatz on the machine but it will attract the attention of sysadmin because mimikatz is detectable by windows defender) so I need a solution to crack in offline mode (the recovered folder is in C: \ Users \ [Username] \ AppData \ Local \ Google \ Chrome \ User Data \ Default \))

Note: In the case of a linux machine, I also got the chrome folder under ~ / .config / google-chrome / Default but I can't crack the data either [whether it's under windows (DPAPI) or under linux), chrome pissed me off ...

Fire_Star - August 20, 2020, 7:04 am

which rat r u using?? I might be able to help u out with this.

Instead of retrieving the folder and file from the remote machine. Try using and keylogger or stealer that can recover Password and cookies from Popular Browsers.

Elijah - August 20, 2020, 9:06 am

(Aug 20, 2020 07:04 AM)Fire_Star Wrote: [\[CITE\]](#) which rat r u using?? I might be able to help u out with this.

Instead of retrieving the folder and file from the remote machine. Try using and keylogger or stealer that can recover Password and cookies from Popular Browsers.

you know any stealer which steals cookies?

Fire_Star - August 20, 2020, 9:18 am

(Aug 20, 2020 09:06 AM)Elijah Wrote: [\[CITE\]](#) you know any stealer which steals cookies?
Not aware of any stealer that's being sold on HF. There are some on Github though.

<https://github.com/LimerBoy/Adamantium-Thief>

https://github.com/0xPh0enix/Adamantium-Thief/releases/tag/cookie_fix

Hope This Helps.

Elijah - August 20, 2020, 11:07 am

(Aug 20, 2020 09:18 AM)Fire_Star Wrote: [\[CITE\]](#) Not aware of any stealer that's being sold on HF.
There are some on Github though.

<https://github.com/LimerBoy/Adamantium-Thief>

https://github.com/0xPh0enix/Adamantium-Thief/releases/tag/cookie_fix

Hope This Helps.

am not a coder, dont know how to compile it,

By any chance can you compile silent executable of it?

Fire_Star - August 20, 2020, 11:17 am

(Aug 20, 2020 11:07 AM)Elijah Wrote: [\[CITE\]](#) am not a coder, dont know how to compile it,
By any chance can you compile silent executable of it?

Am not a coder either my Friend. Even I don't know how to compile it or make a silent FUD executable out of it.

Elijah - August 20, 2020, 11:26 am

(Aug 20, 2020 11:17 AM)Fire_Star Wrote: [\[CITE\]](#) Am not a coder either my Friend. Even I don't know how to compile it or make a silent FUD executable out of it.

ahh thanks mate.

Fire_Star - August 20, 2020, 11:28 am

(Aug 20, 2020 11:26 AM)Elijah Wrote: [\[CITE\]](#) ahh thanks mate.

You are welcome Friend.

SIM-4329724 - August 20, 2020, 1:54 pm

I'm not using any RAT , I don't have access anymore to the server , I'm just trying to retrieve passwords in an OFFLINE mode from the folders , keyloggers and passwords grabber won't help me..

LightIsDark - August 20, 2020, 6:39 pm

(Aug 20, 2020 01:54 PM)lordOfSadi Wrote: [\[CITE\]](#) I'm not using any RAT , I don't have access anymore to the server , I'm just trying to retrieve passwords in an OFFLINE mode from the folders , keyloggers and passwords grabber won't help me..

Pretty Sure you are scewed, chrome stores cryptographic keys inside of "Local State" and you need to do certain things to decrypt them, in addition to this, google chrome has cookies saved for runtime or something, pretty sure the only way to get cookies from google chrome is Javascript injection, and form grabbing.

SIM-4329724 - August 21, 2020, 8:09 pm

{ "Chrome stores cryptographic keys in" Local State " } is the answer I was looking for.

Do u know how can I grab the master key ?