

Forum:[Hack Forums](#)

Thread: [Decrypting Chrome Passwords](#)

DramaKing - August 3, 2023, 9:30 am

I'm trying to exfiltrate saved browser passwords from a compromised computer. Don't want to have to pay a premium for a FUD crypter, so I copied the Chrome AppData and Protect folders to my main computer and ran mimikatz. I've tried getting some of the DPAPI masterkeys, but none that I have tried have worked (there are 46 masterkey files). Supposedly, the decryption key is in the Local State file but I'm lost after that. Anyone know how to do this?

Error message is "ERROR kull_m_dpapi_unprotect_blob ; CryptDecrypt."

osn64698 - August 3, 2023, 10:54 am

Last time I fucked with mimikatz I remember that it does not support certain chrome versions.

DramaKing - August 3, 2023, 12:10 pm

(Aug 3, 2023 10:54 AM)osn64698 Wrote: [\[CITE\]](#) Last time I fucked with mimikatz I remember that it does not support certain chrome versions.

Thought of that, but I did see that Mimikatz was updated for Chrome 80+. Plus, Nirsoft software still works. That just has to be run on the user's machine.

DramaKing - October 7, 2023, 10:10 am

I seem to have figured it out. I need to use dpapi::chrome /in:"Login Data" /masterkey:3f7a17dd6658319fcd4b832afc20ac7dacbb9d7cd668527c71f98e90464624634c614a7923a3beb23c4e24dd718f2a8e838ce72935fb29f11507affb543a53c3 /state:"Local State"

If I wanted to decrypt credman and Windows Vault creds, then I could simply run dpapi::cred /in:file, check the guidMasterKey, find the matching file in the user's Protect file, decrypt the masterkey, and then the file. However, after chatting with Bing and looking through forums, I found that Chrome doesn't use the user's masterkeys. It uses DPAPI in the SYSTEM context with the masterkeys located in C:\Windows\System32\Microsoft\Protect\S-1-5-18\. And even though File Explorer cannot view hidden files in that directory, as long as Remote UAC is off, they can be accessed over SMB.

TheDeadPool - November 5, 2023, 9:49 am

Try this Repository available on Github

github
[dot]com/ohyicong/decrypt-chrome-passwords

DramaKing - November 5, 2023, 11:46 am

(Nov 5, 2023 10:49 AM)TheDeadPool Wrote: [\[CITE\]](#) Try this Repository available on Github

github
[dot]com/ohyicong/decrypt-chrome-passwords

I'm using Nirsoft's ChromePass now. Weirdly, it doesn't use the system masterkeys, but it works.

TheDeadPool - November 5, 2023, 8:22 pm

(Nov 5, 2023 12:46 PM)DramaKing Wrote: [\[CITE\]](#) I'm using Nirsoft's ChromePass now. Weirdly, it doesn't use the system masterkeys, but it works.

But for me this code works smooth and faster

DramaKing - November 10, 2023, 12:12 pm

(Nov 10, 2023 12:49 PM)43pic Wrote: [\[CITE\]](#) can someone tell me whos behind this phone number and tell me their location? 669-324-0588 is their number

Hijacking threads is frowned on here. You need to make your own thread. Anyway, it's probably a mobile number, and that data is private. It would require a background check or going through a data broker.

gangushbo - December 14, 2023, 2:49 pm

learn some new things from this thread

Silkroad - December 14, 2023, 3:21 pm

(Nov 5, 2023 12:46 PM)DramaKing Wrote: [\[CITE\]](#) I'm using Nirsoft's ChromePass now. Weirdly, it doesn't use the system masterkeys, but it works.

Thanks for sharing, it does work surprisingly well.