

Forum:[Hack Forums](#)

Thread: [How do wallet stealers work for normal wallets and extensions?](#)

linkman46 - March 13, 2024, 3:11 am

Hey guys, glad to be here. Maybe someone who used such a tool like PureStealer, Akira and all these tools which are on this forum and other forums can explain this part to me:

How do I use the files the stealers give me?

I think there is a wallet.dat file but I'm not sure what it contains. What are the steps someone needs to take, let's say I compromised Exodus of a victim, how would I go with recovering this on my own end, does it already provide the private keys?

Also what about extensions like Metamask? Would I just install the extension on my browser and then I still need to figure out their password or how is it done?

Would love to learn more about this as I can potentially infect many with these

DramaKing - March 13, 2024, 7:56 am

(Mar 13, 2024 03:11 AM)linkman46 Wrote: [\[CITE\]](#) Hey guys, glad to be here. Maybe someone who used such a tool like PureStealer, Akira and all these tools which are on this forum and other forums can explain this part to me:

How do I use the files the stealers give me?

I think there is a wallet.dat file but I'm not sure what it contains. What are the steps someone needs to take, let's say I compromised Exodus of a victim, how would I go with recovering this on my own end, does it already provide the private keys?

Also what about extensions like Metamask? Would I just install the extension on my browser and then I still need to figure out their password or how is it done?

Would love to learn more about this as I can potentially infect many with these
Maybe you should actually try one and then ask questions. Stealers decrypt data as part of their functions and hand you the stolen data. That is how they work in a universal nutshell.

zeroday12 - March 13, 2024, 8:13 am

(Mar 13, 2024 03:11 AM)linkman46 Wrote: [\[CITE\]](#) Hey guys, glad to be here. Maybe someone who used such a tool like PureStealer, Akira and all these tools which are on this forum and other forums can explain this part to me:

How do I use the files the stealers give me?

I think there is a wallet.dat file but I'm not sure what it contains. What are the steps someone needs to take, let's say I compromised Exodus of a victim, how would I go with recovering this on my own end, does it already provide the private keys?

Also what about extensions like Metamask? Would I just install the extension on my browser and then I still need to figure out their password or how is it done?

Would love to learn more about this as I can potentially infect many with these
You pretty much import the wallet data into your wallet, not sure which part you're struggling with?

Anon158 - March 13, 2024, 4:11 pm

You could probably just download exodus and import the wallet.dat and access the entire wallet...

linkman46 - March 14, 2024, 2:42 am

would appreciate a reply by someone who actually used it. I think there's more to it, like there should always be a password which still needs to be figured out at minimum?

dathris - March 17, 2024, 7:37 pm

Yeah, most Stealers suck for gathering crypto-wallets, they will just exfill encrypted wallet files to you, completely useless if you don't know the victim's password to decrypt it.

linkman46 - March 18, 2024, 4:03 am

would be important to go more in details, I am also open for cooperation, I can get many HQ wallets so if you are in this business you can also DM me.

I believe that whether it's a Metamask, Exodus or other, it will always require to know their password as well right? (which sometimes should be in the stealer log)

Still I see some running this successfully with bruteforce and other stuff as well