

Forum:[Hack Forums](#)

Thread: [Divulge Stealer | Umbral-Stealer Overhaul | 25 Wallets | Browser Passwords, Cookies](#)

Py_Dev - September 5, 2024, 5:57 pm

Divulge Stealer

a highly advanced info-stealer that outperforms its predecessor, Umbral-Stealer by [Blank-c](#). This new iteration is a complete overhaul with enhanced capabilities, targeting 25 major cryptocurrency wallets with precision.

What's New in Divulge Stealer:

1. Comprehensive Redesign: Divulge Stealer has been meticulously reworked from the ground up. Building on the foundation of Umbral-Stealer, it introduces advanced capabilities for targeting cryptocurrency wallets with unprecedented accuracy.
2. Expanded Wallet Support: Our stealer now supports 25 major cryptocurrency wallets, including well-known names like Bitcoin, Ethereum, and Monero. This expansion ensures a broader reach and higher effectiveness in data extraction.
3. Recursive Data Extraction: Utilizing a sophisticated recursive technique, Divulge Stealer ensures thorough scanning and retrieval of wallet files, leaving no trace behind.
4. Signature Appending Feature: In a notable upgrade, the new build includes a feature allowing you to append another .exe digital signature upon compilation. This adds a layer of customization and stealth, making detection even more challenging.
5. Optimized: Removed useless features to make the overall output file much smaller.

Key Features:

Spoiler ([Click to View](#))

Anti-Virtual Machine Detection: Detects and exits if running in a virtual machine to avoid analysis in controlled environments.

Ensures execution only on legitimate systems by integrating with the AntiVM component.

Admin Privileges Management: Requests elevated privileges if needed for certain operations like disabling security mechanisms or accessing restricted areas of the system.

Automatically adds itself to startup if configured, ensuring persistence across reboots.

Self-Protection Mechanisms: The payload uses techniques like hiding its own executable and excluding itself from Windows Defender scans.

Windows Defender is disabled to avoid detection during runtime.

Data Collection: Browser Passwords: Extracts credentials stored in major browsers.

Browser Cookies: Hijacks sessions for further access.
Google Chrome

Brave

Chromium-based browsers

Microsoft Edge

Opera (and Opera GX)

Yandex

Vivaldi

Comodo

Epic Privacy Browser, and more..

Discord Token Stealing: Extracts tokens from Discord sessions to compromise user accounts.

Cryptocurrency Wallet Theft: Scans the system for installed cryptocurrency wallets and attempts to steal private keys and wallet data.

Screenshot Capturing: Captures screenshots of the desktop environment for further insights into user activities.

System Information: Gathers detailed system data including IP, OS version, Anti-Virus, and hardware details.

Wallets

Bitcoin Core (wallets folder)

Armory

Bytecoin

Ethereum (Keystore and Wallet Files)

Litecoin

Dash

Dogecoin

ZCash

Monero

Ripple

Stellar

Binance

Tron

VeChain

Polkadot

Cardano

Tezos

Zilliqa

Neo

Jaxx Liberty (com.liberty.jaxx)

Exodus (exodus.wallet)

Electrum (wallets)

Atomic Wallet (Local Storage)

Guarda Wallet (Local Storage)

Coinomi

Real-Time Connection Monitoring: Monitors for an active internet connection before executing any network-related tasks, ensuring data exfiltration can be completed successfully.

Exfiltration of Stolen Data:Compresses collected data (credentials, cookies, screenshots, wallets) into a single archive and sends it to a specified webhook using the Postman component.

Sends statistical information on the number of credentials, cookies, and other items successfully stolen.

Stealth Operations:The payload can operate silently without user interaction or visible signs of execution.

Optional functionality for removing itself from the system after execution, leaving no trace behind.

Blocking Security Sites:Blocks access to well-known antivirus and security websites (e.g., VirusTotal, Avast, McAfee) to prevent users from uploading the payload for analysis or removing threats from the system.

file was detected by [11 / 39] engine(s)
Kleenscan Results [HERE](#)

Terms of Service (TOS) for Divulge Stealer (Developed by Py_Dev)

Spoiler ([Click to View](#)) 1. Acknowledgement of Research Purpose

The Divulge Stealer software is created solely for research, testing, and educational purposes. It is intended only for use in virtual machines or test environments. Any use of this software outside of these clearly defined settings is strictly prohibited. By using this software, you acknowledge and agree to adhere to these conditions.

2. No Liability

As the developer (Py_Dev), I disclaim any and all liability for any direct, indirect, incidental, or consequential damages that may result from the use, misuse, or inability to use the Divulge Stealer software. This includes, but is not limited to, loss of data, financial loss, security breaches, or any other harms. Py_Dev shall not be held responsible for any illegal or unethical use of this software, and the responsibility for compliance with applicable laws rests solely with the user.

3. Prohibition of Unauthorized Usage

Divulge Stealer is provided as a tool for research and should not be used in any production or live environments. You are required to use this tool solely within isolated, controlled, and non-public environments, such as virtual machines. Any application of Divulge Stealer for the purposes of unauthorized access, data theft, or illegal activities is strictly forbidden. Failure to comply with this may result in legal consequences, and Py_Dev is not responsible for the actions of the user.

4. No Warranties

This software is provided "as is," without any express or implied warranties, including but not limited to warranties of merchantability, fitness for a particular purpose, or non-infringement. I, Py_Dev, make no guarantees that the software will be free of bugs, errors, or vulnerabilities, or that it will function as expected in all test scenarios.

5. Indemnity

By using Divulge Stealer, you agree to indemnify and hold harmless Py_Dev from any claims, liabilities, damages, losses, or legal proceedings that may arise as a result of the misuse or unlawful use of this software. This includes, but is not limited to, any legal or regulatory actions brought against you due to violations of laws or policies regarding data security, privacy, or unauthorized access.

6. Anti-VM and Use Restriction Notice

This software includes an Anti-Virtual Machine Detection feature that prevents its use in certain environments. Despite this, you must ensure that the software is executed only within a virtual machine or test environment. Any activation of this software on a live system, without the explicit authorization of the system owner, is strictly prohibited and considered unlawful.

7. Amendments and Modifications

Py_Dev reserves the right to modify or update this Terms of Service at any time. Continued use of the software after any modifications constitutes acceptance of the revised terms.

8. Governing Law

This TOS shall be governed and construed in accordance with the laws of the jurisdiction where THE USER operates.

By using Divulge Stealer, you affirm that you have read, understood, and agreed to these terms. Any violation of these terms may result in termination of your rights to use this software and potential legal action.

[attachment=2013]

Kruzzn - September 5, 2024, 6:47 pm

im keen to test this

Py_Dev - September 6, 2024, 5:02 am

(Sep 5, 2024 06:47 PM)Kruzzn Wrote: [\[CITE\]](#) im keen to test this
Check your DM.

darkterror - September 6, 2024, 10:19 am

just checked the github repo, do you code c# as well? also if you need to test it i can give you feedback on it :) anyway, once again nice project

Py_Dev - September 6, 2024, 10:22 am

(Sep 6, 2024 10:19 AM)darkterror Wrote: [\[CITE\]](#) just checked the github repo, do you code c# as well? also if you need to test it i can give you feedback on it :) anyway, once again nice project
I am learning c# currently.

ozaik - September 8, 2024, 3:17 pm

Do you have the link of the GitHub repo ?

Py_Dev - September 8, 2024, 4:44 pm

(Sep 8, 2024 03:17 PM)ozaik Wrote: [\[CITE\]](#) Do you have the link of the GitHub repo ?
Yes I have sent you a dm, If anyone else wants this for free just PM me. I added the link just cause I dont want a million dms.

aaravs241 - September 10, 2024, 11:19 pm

please telegram me bro or pm me

i hve money makingmoppurtunity

Moonstone_48 - September 11, 2024, 5:15 pm

Do one still need to crypt this?

Py_Dev - September 11, 2024, 5:19 pm

(Sep 11, 2024 05:15 PM)Moonstone_48 Wrote: [\[CITE\]](#) Do one still need to crypt this?
If you want it to be undetectable, yes.

skynetT1000 - September 11, 2024, 11:40 pm

Chrome has upgraded security on the new version. Unable to get FB cookies.

Does your Stealer get FB cookies?

Py_Dev - September 11, 2024, 11:41 pm

(Sep 11, 2024 11:40 PM)skynetT1000 Wrote: [\[CITE\]](#) Chrome has upgraded security on the new version. Unable to get FB cookies.

Does your Stealer get FB cookies?

I have not tested. I only test on my vm and do not log into fb on my vm.

Zellow - September 12, 2024, 7:24 pm

Could it bypass the anti virus? btw nice project

Py_Dev - September 13, 2024, 4:37 pm

(Sep 12, 2024 07:24 PM)Zellow Wrote: [\[CITE\]](#) Could it bypass the anti virus? btw nice project
yeah some of them. If you want it encrypted, click my signature.

Greatx0 - September 15, 2024, 6:52 am

saving this one for later! thank you :)!

indamirrow - September 27, 2024, 5:55 am

where can i get i good crypter for this ?

lightyear - September 27, 2024, 4:41 pm

Hi

can you also please send me the link to github repo
for the stealers.

br

Biggy_Asian - September 28, 2024, 3:27 am

You're aware discord bans accounts from webhook logging now right? If not you do now. I
recommend you add telegram bot support or even support for other platforms/self hosted webpanel
for logs.

Shddjdh7282 - September 28, 2024, 10:26 am

?????? ???? ? ???? ???? ???? githab ?? [warn]

Hdev84clone - September 28, 2024, 11:12 pm

Can I have it? I can't PM because im newbie

?Rednix™ - September 29, 2024, 5:21 am

Hey! Looks interesting. I would not mind to check this one out and run some tests on it. Do you have a Github? I will follow you and maybe even fork the repository.

hoangdoan - September 29, 2024, 11:35 pm

I tried it, but no cookie data is sent

Lbawye - October 10, 2024, 1:51 am

I'm very interested in testing this. Looks very user friendly.

mdmdmhdnn - October 20, 2024, 1:45 am

Can it decrypt cookies chrome v129(Application-Bound)?

Jhoyce0820 - October 21, 2024, 5:31 pm

hmmmm gonna try this out

Pmagner0415 - November 21, 2024, 2:39 pm

It seems interesting

jason123 - November 22, 2024, 8:04 am

OP thanks and nice , but i tested it on Chrome and noticed it couldn't get cookies. You may work on it.

Binance - November 22, 2024, 10:55 am

(Nov 22, 2024 09:04 AM)jason123 Wrote: [\[CITE\]](#) OP thanks and nice , but i tested it on Chrome and noticed it couldn't get cookies. You may work on it.

Did you test on chrome 129+?

This was big issue for stealers.

Py_Dev - November 22, 2024, 10:58 am

(Nov 22, 2024 11:55 AM)Dryx Wrote: [\[CITE\]](#) Did you test on chrome 129+?

This was big issue for stealers.

does not capture cookies just passwords and autofills.

jason123 - November 26, 2024, 1:26 am

(Nov 22, 2024 11:55 AM)Dryx Wrote: [\[CITE\]](#) Did you test on chrome 129+?

This was big issue for stealers.

No i didn't but it's fine.

(Nov 22, 2024 11:58 AM)Py_Dev Wrote: [\[CITE\]](#) does not capture cookies just passwords and autofills.

Noted, thanks.

henki11 - December 21, 2024, 3:58 pm

Hi guys, im new here! and finding my way a bit!

I love to try the prog, looks very good

xiaoran5458 - January 17, 2025, 5:44 am

I want to buy stealer software?

xs0day - January 17, 2025, 11:11 am

If you don't mind can I get the github repo for this?

fscammers - January 17, 2025, 5:30 pm

Great, id love to try this

Tyr - January 17, 2025, 6:26 pm

How well do the cookie capturing functionalities work when it comes to Brave on the other machine? Will take a peak at this. Thanks.

(Jan 17, 2025 12:11 PM)xs0day Wrote: [\[CITE\]](#) If you don't mind can I get the github repo for this? Just google for something similar if you're trying to get code for a skeleton to build your own project. XD

Pr0m3th3us - January 17, 2025, 6:42 pm

Got it, thanks man. will post when i use it

TehGrind - January 19, 2025, 10:05 pm

If around and its possible i would love to give this a spin.

cipher2020 - February 1, 2025, 9:36 am

Does your tool have the option to recover cookies? Does it work perfectly?

ForgottenFoe - February 1, 2025, 2:49 pm

If you are still active on HF and wouldn't mind DMing me the repo I would be very appreciative.

ServersFucked - February 1, 2025, 6:17 pm

Cant wait to test 2.0 i used the first version after finding your github a while back, cant wait for the dm hahaha

mdmaty - February 2, 2025, 1:33 am

(Sep 5, 2024 05:57 PM)Py_Dev Wrote: [\[CITE\]](#) [/align]

Key Features:

[spoiler]

Anti-Virtual Machine Detection: Detects and exits if running in a virtual machine to avoid analysis in controlled environments.

Ensures execution only on legitimate systems by integrating with the AntiVM component.

Admin Privileges Management: Requests elevated privileges if needed for certain operations like disabling security mechanisms or accessing restricted areas of the system.

Automatically adds itself to startup if configured, ensuring persistence across reboots.

Self-Protection Mechanisms: The payload uses techniques like hiding its own executable and excluding itself from Windows Defender scans.

Windows Defender is disabled to avoid detection during runtime.

Data Collection:Browser Passwords: Extracts credentials stored in major browsers.

Browser Cookies: Hijacks sessions for further access.

Google Chrome

Brave

Chromium-based browsers

Microsoft Edge

Opera (and Opera GX)

Yandex

Vivaldi

Comodo

Epic Privacy Browser, and more..

Discord Token Stealing: Extracts tokens from Discord sessions to compromise user accounts.

Cryptocurrency Wallet Theft: Scans the system for installed cryptocurrency wallets and attempts to steal private keys and wallet data.

Screenshot Capturing: Captures screenshots of the desktop environment for further insights into user activities.

System Information: Gathers detailed system data including IP, OS version, Anti-Virus, and hardware details.

Wallets

Bitcoin Core (wallets folder)

Armory

Bytecoin

Ethereum (Keystore and Wallet Files)

Litecoin

Dash

Dogecoin

ZCash

Monero

Ripple

Stellar

Binance

Tron

VeChain

Polkadot

Cardano

Tezos

Zilliqa

Neo

Jaxx Liberty (com.liberty.jaxx)

Exodus (exodus.wallet)

Electrum (wallets)

Atomic Wallet (Local Storage)

Guarda Wallet (

Thank u!!

csslll - February 2, 2025, 3:30 am

DOES IT STEAL WALLETS EXTENSIONS

jason123 - February 2, 2025, 5:51 am

Are you working on a new update?

XaviDish - February 2, 2025, 8:30 am

I need this, I sent you a private message

Learning Hacking - February 19, 2025, 8:11 pm

it steals chrome cookies after the latest update?

Socma849 - February 20, 2025, 11:18 am

dm, Write to me, I'm ready to buy! Write your telegram

Py_Dev - February 21, 2025, 4:56 am

There is nothing to buy just search it on Google

aweroamsd - February 21, 2025, 9:17 pm

this is a very good build, works well thanks bro

arabrisa - February 22, 2025, 10:38 am

does this still work? PM me. I want to try it

bilalkhanicom - February 24, 2025, 5:27 am

how can i buy it what is your contact

jason123 - April 1, 2025, 4:31 pm

The built file is detected by WD , any update?

boow5 - April 1, 2025, 10:50 pm

really want to try this!

dexxesb - April 1, 2025, 11:26 pm

I am interested and would like to contact you. Please let me know your tg.

helloguys5678 - April 13, 2025, 3:41 am

We need to look What is it like?

Hopsin - April 15, 2025, 7:32 am

(Sep 8, 2024 04:44 PM)Py_Dev Wrote: [\[CITE\]](#) Yes I have sent you a dm, If anyone else wants this for free just PM me. I added the link just cause I dont want a million dms.

'?' like to as well. For educational purposes.

Thanks.

drunkown416 - April 15, 2025, 5:23 pm

im looking for someone that have bot logs from canada if you have this message me lets work