

This project has been added to <u>pupy</u> as a post-exploitation module. Python code will be interpreted in memory without touching the disk and it works on Windows and Linux host.

#### **Standalones**

Standalones are now available here: https://github.com/AlessandroZ/LaZagne/releases/

### Installation

pip install -r requirements.txt

### Usage

Launch all modules

laZagne.exe all

• Launch only a specific module

laZagne.exe browsers

• Launch only a specific software script

laZagne.exe browsers -firefox

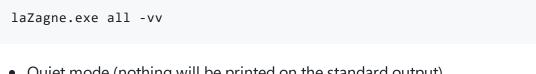
Write all passwords found into a file (-oN for Normal txt, -oJ for Json, -oA for All).
 Note: If you have problems to parse JSON results written as a multi-line strings, check this.

• Get help

laZagne.exe -h
laZagne.exe browsers -h

• Change verbosity mode (2 different levels)

Q



• Quiet mode (nothing will be printed on the standard output)

Q laZagne.exe all -quiet -oA

• To decrypt domain credentials, it could be done specifying the user windows password. Otherwise it will try all passwords already found as windows passwords.

Q laZagne.exe all -password ZapataVive

Note: For wifi passwords \ Windows Secrets, launch it with administrator privileges (UAC Authentication / sudo)

## Mac OS

Note: In Mac OS System, without the user password it is very difficult to retrieve passwords stored on the computer. So, I recommend using one of these options

• If you know the user password, add it in the command line

Q laZagne all --password SuperSecurePassword

• You could use the interactive mode that will prompt a dialog box to the user until the password will be correct

Q laZagne all -i

## Supported software

	Windows	Linux	Mac
Browsers	7Star	Brave	Chrome
	Amigo	Chromium	Firefox
	Basilisk	Dissenter-Browser	
	BlackHawk	Firefox	
	Brave	Google Chrome	
	Centbrowser	IceCat	
	Chedot	Microsoft Edge	
	Chrome Beta	Opera	
	Chrome Canary	SlimJet	
	Chromium	Vivaldi	
	Coccoc		
	Comodo Dragon		
	Comodo IceDragon		
	Cyberfox		
	DCBrowser		
	Elements Browser		
	Epic Privacy Browser		
	Firefox		
	Google Chrome		
	Icecat		
	K-Meleon		
	Kometa		
	Microsoft Edge		
	Opera		
	Opera GX		
	Orbitum		
	QQBrowser		

	pale Moon SogouExplorer Sputnik Torch Uran Vivaldi		
Chats	Pidgin Psi Skype	Pidgin Psi	
Databases	DBVisualizer Postgresql Robomongo Squirrel SQLdevelopper	DBVisualizer Squirrel SQLdevelopper	
Games	GalconFusion Kalypsomedia RogueTale Turba		
Git	Git for Windows		
Mails	Epyrus Interlink Outlook Thunderbird	Clawsmail Thunderbird	
Maven	Maven Apache		
Dumps from memory	Keepass Mimikatz method	System Password	
Multimedia	EyeCON		
PHP	Composer		
SVN	Tortoise		
Sysadmin	Apache Directory Studio CoreFTP CyberDuck FileZilla FileZilla Server FTPNavigator OpenSSH OpenVPN mRemoteNG KeePass Configuration Files (KeePass1, KeePass2) PuttyCM Rclone RDPManager VNC WinSCP Windows Subsystem for Linux	Apache Directory Studio AWS Docker Environnement variable FileZilla gFTP History files Shares SSH private keys KeePass Configuration Files (KeePassX, KeePass2) Grub Rclone	
Wifi	Wireless Network	Network Manager WPA Supplicant	

Internal mechanism passwords storage	Autologon MSCache Credential Files Credman DPAPI Hash Hashdump (LM/NT) LSA secret Vault Files	GNOME Keyring Kwallet Hashdump	Keychains Hashdump
---	---	--------------------------------------	-----------------------

# Compile

• Using Pyinstaller

pyinstaller --additional-hooks-dir=. -F --onefile laZagne.py

• Using Nuitka

python3 -m nuitka --standalone --onefile --include-package=lazagne 1:  $\Box$ 

## For developers

Please refer to the wiki before opening an issue to understand how to compile the project or to develop a new module. <a href="https://github.com/AlessandroZ/LaZagne/wiki">https://github.com/AlessandroZ/LaZagne/wiki</a>

#### Donation

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information