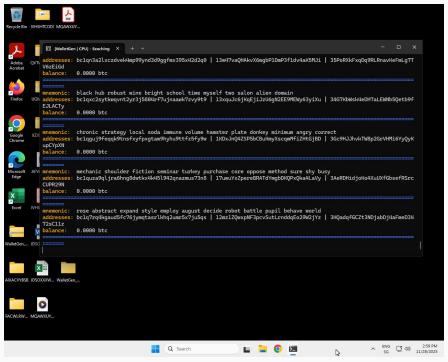
Windows Analysis Report

WalletGen_windows_x64-28NOVEMBER2025.zip

Time: 20:57:03
Date: 28/11/2025
Version: 43.0.0 Green Sapphire

General Information

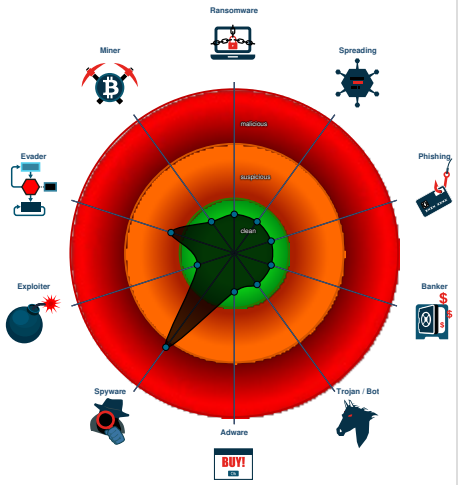
Sample name:	WalletGen_windows_x64-28NOVEMBER2025.zip
Analysis ID:	5091194
Has dependencies:	false
MD5:	291843fd3759f6c4ec6..
SHA1:	c2ee615e8002d09e3b..
SHA256:	1c7e3807e942423c9b..
Infos:	



Detection

Score:	21
Range:	0 - 100
Confidence:	80%

Classification



Process Tree

- **System is w11x64_office2021**
- rundll32.exe (PID: 6780 cmdline: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding MD5: B1BB2F6519DB1F087F45EC70638B99A6)
- WalletGen.exe (PID: 5584 cmdline: "C:\Users\user\Desktop\WalletGen_windows_x64-28NOVEMBER2025\WalletGen\WalletGen.exe" MD5: A185984A08BC4A171660D1B8B2F4D927)
  - conhost.exe (PID: 3804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 2447D7A01919B47AB7A009C0CA79A1AF)
- OpenConsole.exe (PID: 4840 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding MD5: ED52DFA7DDEE29475240FBEC2AC2A096)
- WindowsTerminal.exe (PID: 5428 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe" -Embedding MD5: 97E5964AD41B33E7291E97B51D59E4A6)
- WalletGen.exe (PID: 3252 cmdline: "C:\Users\user\Desktop\WalletGen_windows_x64-28NOVEMBER2025\WalletGen\WalletGen.exe" MD5: A185984A08BC4A171660D1B8B2F4D927)
  - conhost.exe (PID: 2896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 2447D7A01919B47AB7A009C0CA79A1AF)
- OpenConsole.exe (PID: 4292 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding MD5: ED52DFA7DDEE29475240FBEC2AC2A096)
- WindowsTerminal.exe (PID: 5340 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe" -Embedding MD5: 97E5964AD41B33E7291E97B51D59E4A6)
- **cleanup**

AI Reasoning

No reasoning have been found

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

Stealing of Sensitive Information

Tries to harvest and steal browser information (history, passwords, etc)

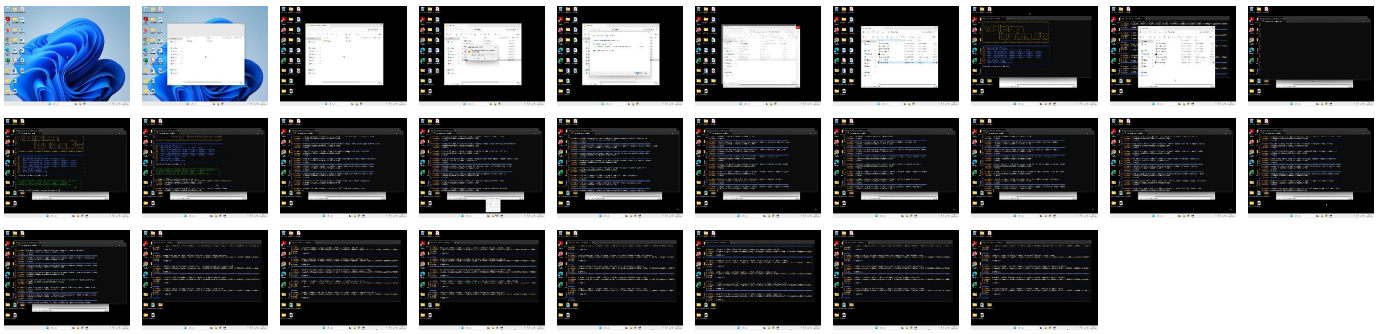
Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 Process Injection	1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	1 Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Rundll32	LSASS Memory	1 2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	2 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	3 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
https://raw.githubusercontent.com/vadbmbz3/version/refs/heads/main/1.1	0%	Avira URL Cloud	safe	

Domains and IPs

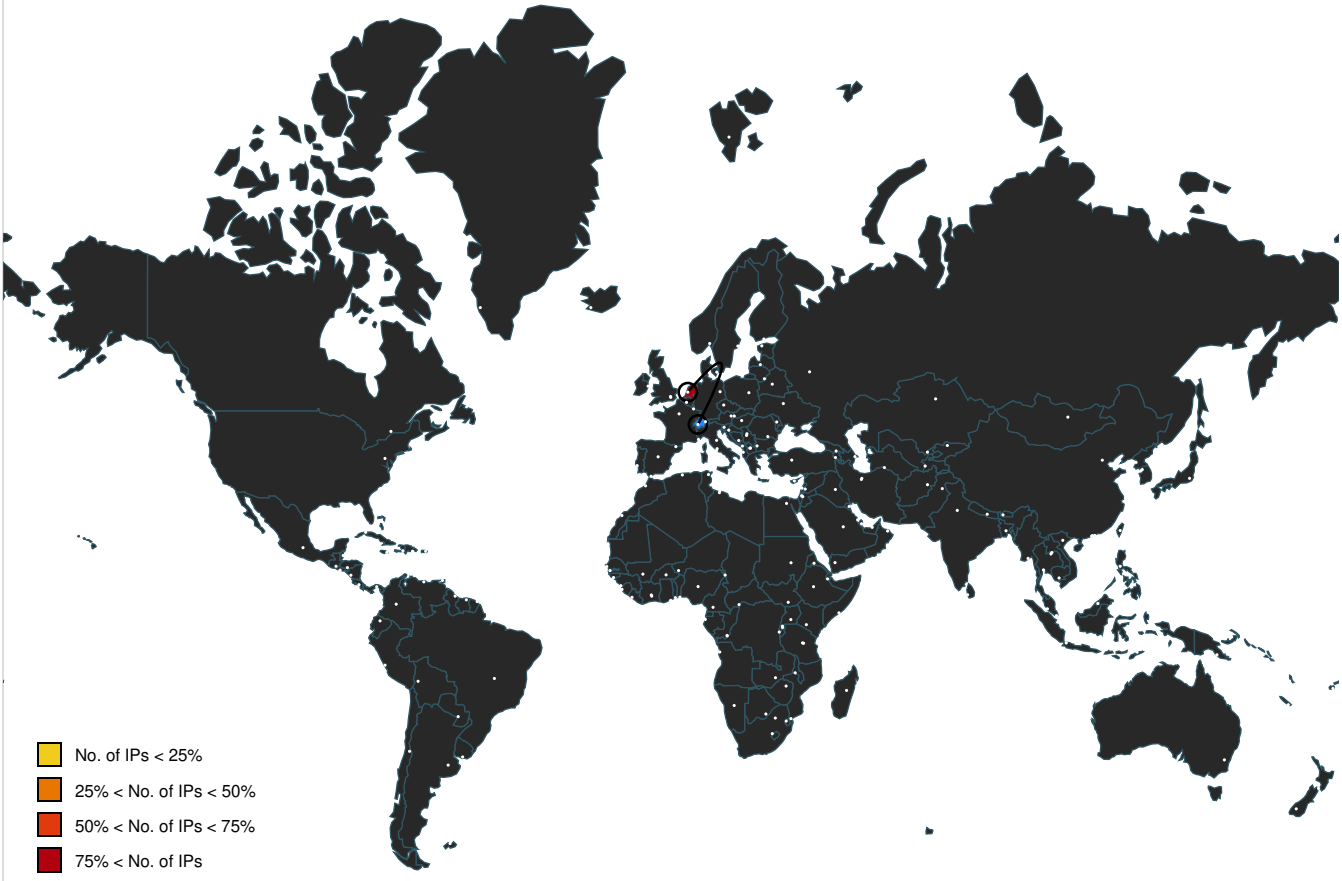
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
raw.githubusercontent.com	185.199.109.133	true	false		high
s-0005.dual-s-msedge.net	52.123.128.14	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://raw.githubusercontent.com/vadbmbz3/version/refs/heads/main/1.1	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.199.109.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	false

General Information

Joe Sandbox version:	43.0.0 Green Sapphire
Analysis ID:	5091194
Start date and time:	2025-11-28 20:57:03 +01:00
Joe Sandbox product:	Cloud
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 11 23H2 (Office Professional Plus 2021, Chrome 132, Firefox 135, Adobe Acrobat 24, Java 8 Update 431, 7-Zip 24.09, Python 3.13.5)
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample name:	WalletGen_windows_x64-28NOVEMBER2025.zip
Detection:	SUS
Classification:	sus21.spyw.winZIP@9/2@1/11
Cookbook Comments:	• Found application associated with file extension: .zip

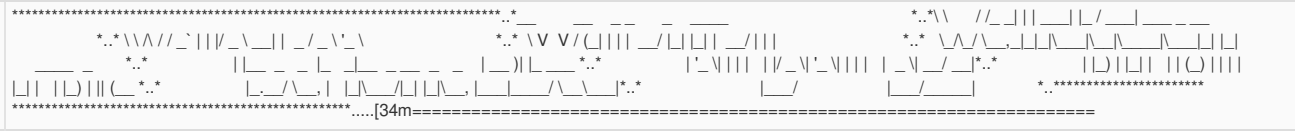
Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, SIHClient.exe
- Excluded IPs from analysis (whitelisted): 20.242.39.171, 20.3.187.198, 74.179.77.204, 20.190.147.0
- Excluded domains from analysis (whitelisted): ecs.office.com, client.wns.windows.com, fe3.delivery.mp.microsoft.com, dual-s-0005-office.config.skype.com, slscr.update.microsoft.com, login.live.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, ecs.office.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- VT rate limit hit for: https://raw.githubusercontent.com/vadbmbz3/version/refs/heads/main/1.1

Created / dropped Files

\Device\ConDrv

Process:	C:\Users\user\Desktop\WalletGen_windows_x64-28NOVEMBER2025\WalletGen\WalletGen.exe
File Type:	ASCII text, with CRLF line terminators, with escape sequences
Category:	dropped
Size (bytes):	171682
Entropy (8bit):	4.506489912182549
Encrypted:	false
SSDEEP:	
MD5:	26BBB87D133251BA901A7ADC23924996
SHA1:	D7E9121CC09DC0CCC5DDE1F5FD6D26C66814F52D
SHA-256:	F920AF3748BBC93EB3901CCE02D3B77EA256C25C15F3601A16B11DA23DE6751B
SHA-512:	A3A94AD0C29955B48109126BD23CB796D5C00C8B73763A957C85A5BACE38673C873E3D7781E8012702CAF16B397D4FA5E887D886823E1FC9CC3975B960BEAB8
Malicious:	false
Reputation:	unknown

Preview:	

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract, compression method=store
Entropy (8bit):	7.9951718019207565
TrID:	• ZIP compressed archive (8000/1) 99.91% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.09%
File name:	WalletGen_windows_x64-28NOVEMBER2025.zip
File size:	3'047'947 bytes
MD5:	291843fd3759f6c4ec694b81bba1d133
SHA1:	c2ee615e8002d09e3b44605552d3a6fe3142dbbb
SHA256:	1c7e3807e942423c9b6745ec3535e77153c8cdc5196509275324a19fc9f3ecf3
SHA512:	e92d89a39d8b7f6e96d8a5bbda53846006143ada07967b28c0b781ad7ffdf60da0a20cca27038aea5306b1b4bb5000a5b39f9ffc7905c1000a4637fbf612a21e
SSDEEP:	49152:WAakR2H7tWu3wFszKXX4BHrNplesmC499Ms6mDYLORA8diWtapJroNL0PKK4PQ0y:WAubtWnrXX4VNpRmC49+iULORAS8pJrn
TLSH:	D9E533655359A571EADF8FB0209416B48BAAEA1DBB652D17B3F8F0341ECF3C0A861470
File Content Preview:	PK.....yk|[.....WalletGen/PK.....n[c...@...:;.....WalletGen/bip39-words.txt=....(.E.O.<.Qb. 8.I.O?{..7.U{.....T.V..kz....FI.v..Ch.z.....1g_.s8. <.1`^t.V;o.N...L.D.....[dr .U.:...xNE\..0.$....-.(ss..,.3.9ad.z{P..s..6...'..N..

File Icon

Icon Hash:	03f1b9752babe989