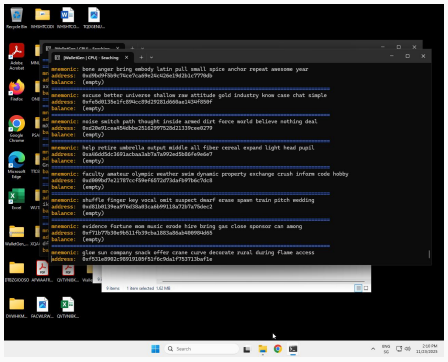
Windows Analysis Report

WalletGen_windows_x64-23NOVEMBER2025.zip

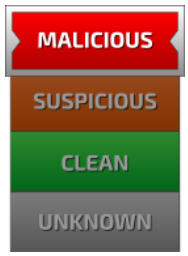
Time: 20:07:56
Date: 23/11/2025
Version: 43.0.0 Green Sapphire

General Information

Sample name:	WalletGen_windows_x64-23NOVEMBER2025.zip
Analysis ID:	5078708
Has dependencies:	false
MD5:	ae41ec6bcf20baf4c76…
SHA1:	3cf3e04b6a5e8552073..
SHA256:	acb88845f08b28c2e58..
Infos:	

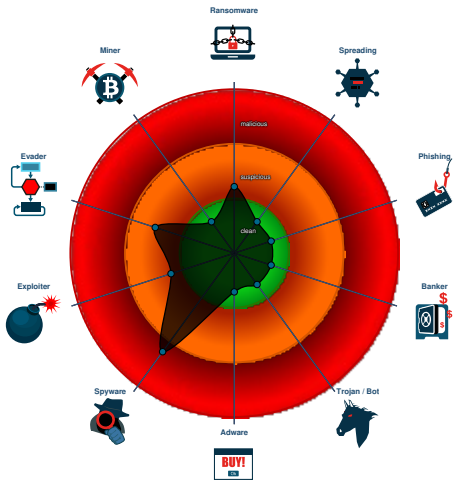


Detection



Score:	48
Range:	0 - 100
Confidence:	100%

Classification



Process Tree

- **System is w11x64_office2021**
- rundll32.exe (PID: 5412 cmdline: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding MD5: B1BB2F6519DB1F087F45EC70638B99A6)
- SingleClientServicesUpdater.exe (PID: 6668 cmdline: --postMsg MD5: FC9E6DF0E57B8116073BC5A94BA8B867)
- WalletGen.exe (PID: 3916 cmdline: "C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe" MD5: A5CEE52B774AC909D62815130710CE6B)
  - conhost.exe (PID: 3992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 2447D7A01919B47AB7A009C0CA79A1AF)
- OpenConsole.exe (PID: 5428 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding MD5: ED52DFA7DDEE29475240FBEC2AC2A096)
- WindowsTerminal.exe (PID: 3812 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe" -Embedding MD5: 97E5964AD41B33E7291E97B51D59E4A6)
- WalletGen.exe (PID: 1620 cmdline: "C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe" MD5: A5CEE52B774AC909D62815130710CE6B)
  - conhost.exe (PID: 6392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 2447D7A01919B47AB7A009C0CA79A1AF)
- OpenConsole.exe (PID: 5856 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding MD5: ED52DFA7DDEE29475240FBEC2AC2A096)
- WindowsTerminal.exe (PID: 6596 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

Found many strings related to Crypto-Wallets (likely being stolen)

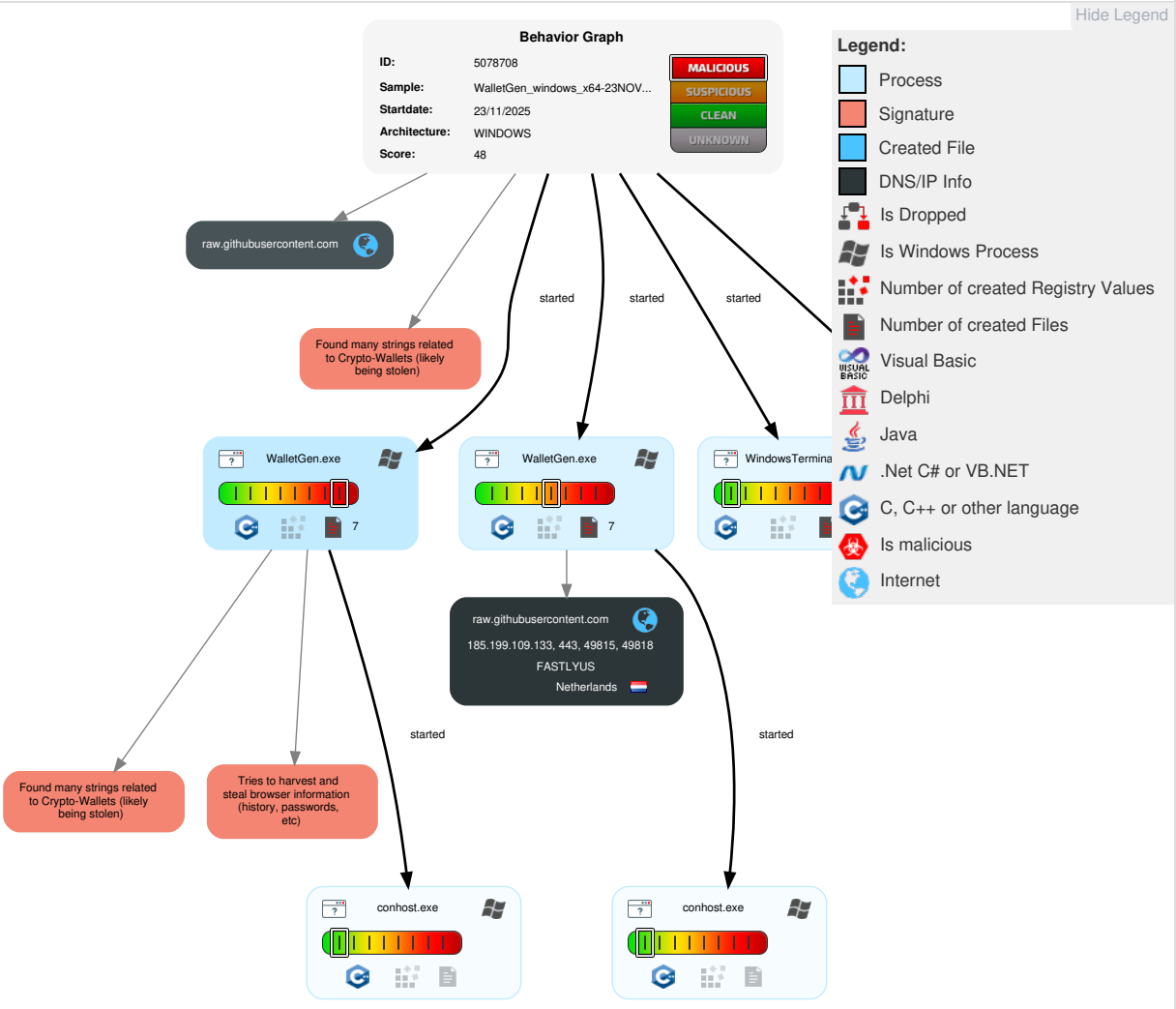
Tries to harvest and steal browser information (history, passwords, etc)

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	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 Process Injection	1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	1 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	2 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	3 Obfuscated Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	3 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 Account Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	Compile After Delivery	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 3 System Information Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

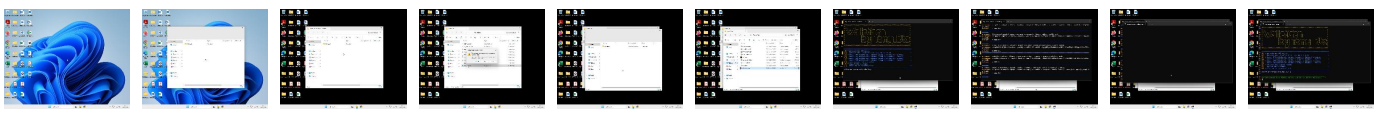
Behavior Graph

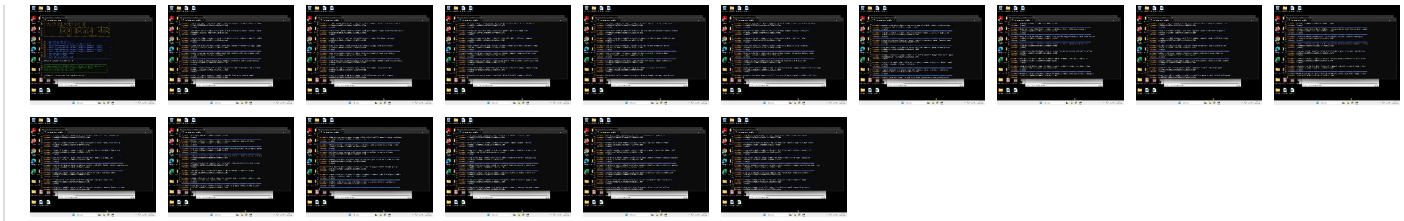


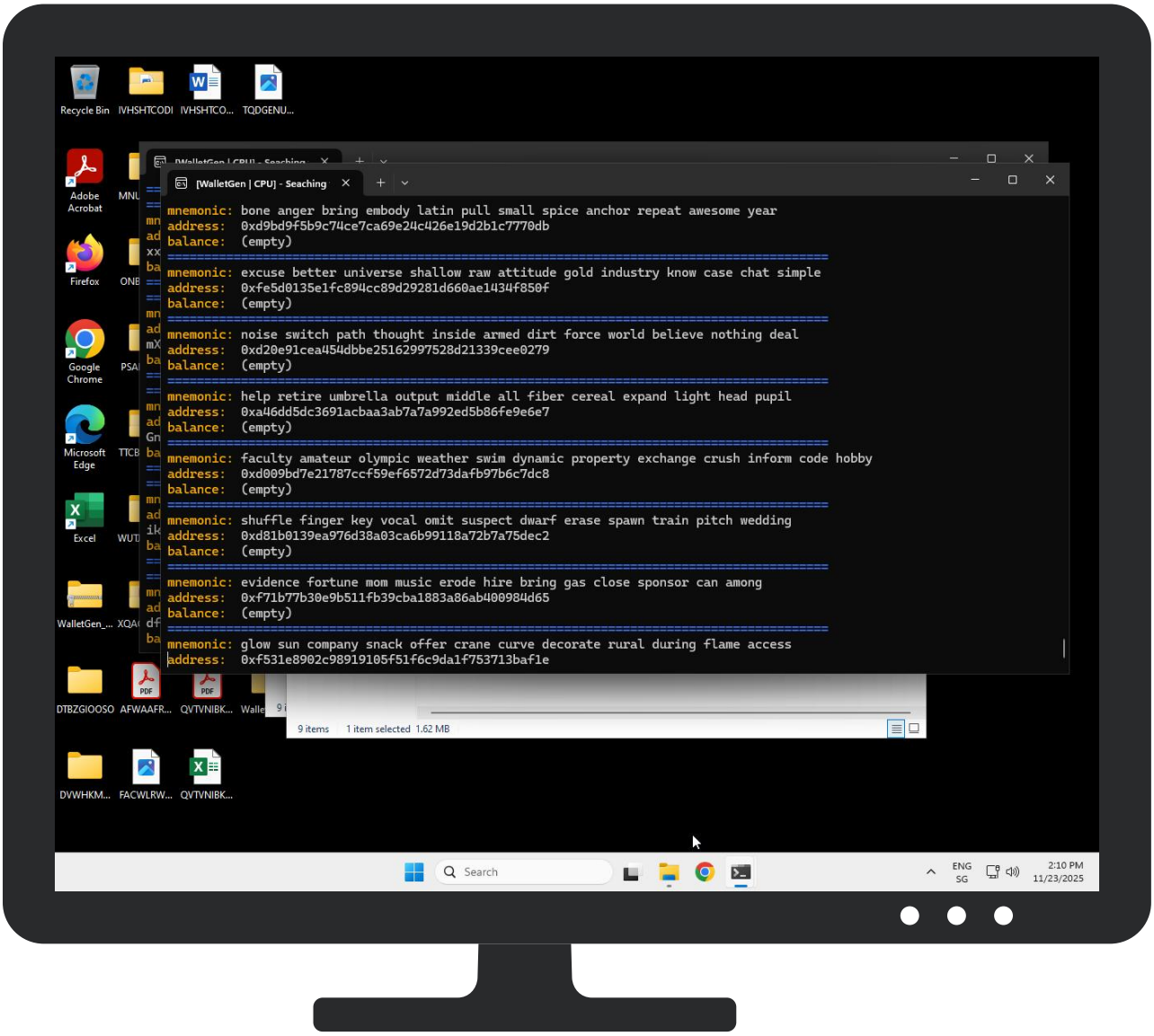
Screenshots

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

No Antivirus matches

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	52.123.129.14	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://raw.githubusercontent.com/wookalsxadsl/config/refs/heads/main/config.ini	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gcc.gnu.org/bugs/):	WalletGen.exe	false		high
http://https://yandex.com/images/search?rpt=imageviewupfile=	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://raw.githubusercontent.com/wookalsxadsl/config/refs/heads/main/config.ini=zg	WalletGen.exe, 00000005.00000002.5166623225.000002E79C4B4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://scripts.sil.org/OFL	WindowsTerminal.exe, 00000008.00000002.5248172252.000001818DA22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpv20	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://raw.githubusercontent.com/n	WalletGen.exe, 00000005.00000002.5166623225.000002E79C507000.00000004.00000020.00020000.00000000.sdmp	false		high
http://sajatypeworks.comi	WindowsTerminal.exe, 00000008.00000002.5248172252.000001818DA22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://scripts.sil.org/OFL)	WindowsTerminal.exe, 00000008.00000002.5248172252.000001818DA22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.openssl.org/H	libcrypto-3-x64.dll, libssl-3-x64.dll	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://suggest.yandex.com/suggest-ff.cgi?part=	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/tonybtc1/walletgen/releases/tag/database	WalletGen.exe	false		high
http://https://raw.githubusercontent.com/wookalsxadsl/config/refs/heads/main/config.iniw	WalletGen.exe, 0000000B.00000002.5166621899.0000025E9DF67000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtabv20(	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://yastatic.net/lego/_/rBTjd6UOPk5913OSn5ZQVYMTQWQ.icohttps://yandex.com/	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://raw.githubusercontent.com/wookalsxadsl/config/refs/heads/main/config.iniZ	WalletGen.exe, 00000005.00000002.5166623225.000002E79C4B4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/tonybtc1/walletgen	readme.txt	false		high
http://https://github.com/microsoft/cascadia-code/blob/main/LICENSE).	WindowsTerminal.exe, 00000008.00000002.5248172252.000001818DA22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	WalletGen.exe, 00000005.00000003.4206798076.000002E7AA65C000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4207398889.000002E7A9F57000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000005.00000003.4206798076.000002E7AA67E000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6226000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gemini.google.com/app?q=	WalletGen.exe, 0000000B.00000003.4377004362.0000025EA6229000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://raw.githubusercontent.com/	WalletGen.exe, 00000005.00000002.5166623225.000002E79C507000.00000004.00000020.00020000.00000000.sdmp, WalletGen.exe, 00000000B.00000002.5166621899.0000025E9DFB0000.00000004.00000020.00020000.00000000.sdmp	false		high

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:	5078708
Start date and time:	2025-11-23 20:07:56 +01:00
Joe Sandbox product:	Cloud
Overall analysis duration:	0h 7m 11s
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:	16
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	WalletGen_windows_x64-23NOVEMBER2025.zip
Detection:	MAL
Classification:	mal48.spyw.winZIP@10/2@1/1

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .zip

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, SIHClient.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.147.0
- Excluded domains from analysis (whitelisted): ecs.office.com, client.wns.windows.com, dual-s-0005-office.config.skype.com, slscr.update.microsoft.com, login.live.com, ecs.office.trafficmanager.net, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\ConDrv

Process:	C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe
File Type:	ASCII text, with CRLF, CR line terminators, with escape sequences
Category:	dropped

Size (bytes):	121710
Entropy (8bit):	4.5148684191262
Encrypted:	false
SSDEEP:	768:W438ILDdcL++sozka1RmBH3X029PV/0P9zmIVuOZOk260T4hc9s7UxbmFBAXtgG3:Z8yhGkmRsl9NsPp/dcFWiKFEJ5
MD5:	250B5BC8298025A223C7C4D72FDD1839
SHA1:	89E56025BC2BF5BC7FBC362D3B13243C87740C50
SHA-256:	D6B7707A9E06D34C287F57BDC8CC4DE5EE30092064FA5B29D94ADC172E2AE411
SHA-512:	B3FA69B8BCD3B6F8384EBD40A7F7B58875FC189DB594C9367F4CABD0EDAFAF36A3155B929FA8A80E16973B05B70F47752CE91DA2E7ED7BA8973E910138A4EC16
Malicious:	false
Reputation:	low
Preview:	**********..*__ __ _ _ _ ____ *..*\ \ / /_ _|		___| |_ / ___| ___ _ __ *..* \ \ /\ / / _ \ '__|	|/ _ \ __|| _ / _ \ '_ \ *..* \ V V / (_| | | | __/ |_| |_| | __/ | | | *..* _/_/ __,_|_|_|___|__|___|___|___|_| |_| ____ _ *..* | |___ _ _ |_ _|___ _ ___ _ _ | __)| |_ ___ *..*	'_ |				|/ _ | '_ |			_ | __/ __|*..*	|_)	|_|		(_)			|_|				|_)	|| (__ *..* |_.__/ __,	|_|___/|_| |_|__, |___|____/ _____|*..* |___/ |___/_____| *..********** **********.....[34m==========

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract, compression method=store
Entropy (8bit):	7.995496055174563
TrID:	• ZIP compressed archive (8000/1) 99.91% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.09%
File name:	WalletGen_windows_x64-23NOVEMBER2025.zip
File size:	3'529'228 bytes
MD5:	ae41ec6bcf20baf4c76c1c0f6d25c1a1
SHA1:	3cf3e04b6a5e8552073ded4ce56778ad30754066
SHA256:	acb88845f08b28c2e58ca60b77126a49ea4a24df5469b3fecb46b5094f8dcef3
SHA512:	e0832563c84fdf587156b99fee6f164af06bc2458f56e2efb2860839f93e4e1527f2c97d1eaa60739bd23b987c211bdfb33e5b9224d71ae51d3844d3c2a56a55
SSDEEP:	98304:aAubtWnrXX4VNpRmC49+iULORAS8pJJHIXgl3nt+hi:agqpRmb9+JLORAS8fZ8Qdd
TLSH:	9AF533F8464A54B9D2DC8EB411F52A61EF9FDF14AA832F73F358D1A431EB7C190148A2
File Content Preview:	PK.....u[.....WalletGen/PK.....n[c...@...:;.....WalletGen/bip39-words.txt=....(.E.O.<.Qb. 8.I.O?{..7.U{.....T.V..kz....Fl.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

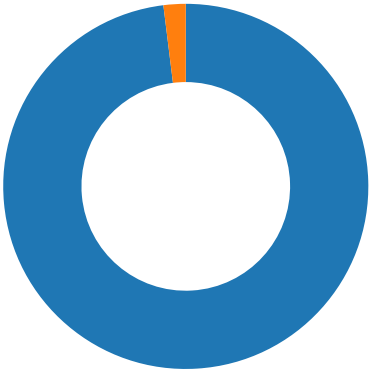
Icon Hash:	03f1b9752babe989

Network Behavior

Network Port Distribution

Total Packets: 51

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2025 20:08:56.467926979 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.467983961 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.468136072 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.490324974 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.490346909 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.521677971 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.521764994 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.531368017 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.531930923 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.531985998 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.792962074 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.835706949 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.987787962 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.987865925 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.988207102 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.988282919 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.988524914 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.988584995 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.989139080 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.989204884 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.989543915 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.989593983 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.993482113 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.993494034 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.993556023 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:56.993571043 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:56.993626118 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.002394915 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.002407074 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.002481937 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.004899979 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.004976988 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.007399082 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.007498026 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.009154081 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.009257078 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.016742945 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.016832113 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.018203020 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.018280029 CET	49815	443	192.168.2.12	185.199.109.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2025 20:08:57.019047022 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.019138098 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.020752907 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.020840883 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.021840096 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.021925926 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.022465944 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.022556067 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.023366928 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.023447990 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.024317026 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.024388075 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.030232906 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.030309916 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.031285048 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.031369925 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.032084942 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.032191992 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.032761097 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.032809019 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.032852888 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.033399105 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.033493042 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.034006119 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.034102917 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.034707069 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.034782887 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.035325050 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.035408020 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.035943985 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.036021948 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.036892891 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.036994934 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.037628889 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.037702084 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.038573027 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.038589001 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.038687944 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.039479017 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.039577961 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.040443897 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.040574074 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.044644117 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.044737101 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.045829058 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.045921087 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.046509981 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.046583891 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.047836065 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.047852039 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.047966957 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.048502922 CET	443	49815	185.199.109.133	192.168.2.12
Nov 23, 2025 20:08:57.048579931 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:08:57.051738977 CET	49815	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:09:08.734827995 CET	49818	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:09:08.734875917 CET	443	49818	185.199.109.133	192.168.2.12
Nov 23, 2025 20:09:08.734960079 CET	49818	443	192.168.2.12	185.199.109.133
Nov 23, 2025 20:09:08.740901947 CET	49818	443	192.168.2.12	185.199.109.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2025 20:09:08.740926981 CET	443	49818	185.199.109.133	192.168.2.12
Nov 23, 2025 20:09:08.773642063 CET	443	49818	185.199.109.133	192.168.2.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2025 20:08:56.439850092 CET	59153	53	192.168.2.12	1.1.1.1
Nov 23, 2025 20:08:56.461206913 CET	53	59153	1.1.1.1	192.168.2.12

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 23, 2025 20:08:56.439850092 CET	192.168.2.12	1.1.1.1	0xd28f	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 23, 2025 20:08:21.728482962 CET	1.1.1.1	192.168.2.12	0xf4fc	No error (0)	ecs-office.s-0005.dual-s-msedge.net	s-0005.dual-s-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 23, 2025 20:08:21.728482962 CET	1.1.1.1	192.168.2.12	0xf4fc	No error (0)	s-0005.dual-s-msedge.net		52.123.129.14	A (IP address)	IN (0x0001)	false
Nov 23, 2025 20:08:21.728482962 CET	1.1.1.1	192.168.2.12	0xf4fc	No error (0)	s-0005.dual-s-msedge.net		52.123.128.14	A (IP address)	IN (0x0001)	false
Nov 23, 2025 20:08:56.461206913 CET	1.1.1.1	192.168.2.12	0xd28f	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)	false
Nov 23, 2025 20:08:56.461206913 CET	1.1.1.1	192.168.2.12	0xd28f	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)	false
Nov 23, 2025 20:08:56.461206913 CET	1.1.1.1	192.168.2.12	0xd28f	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)	false
Nov 23, 2025 20:08:56.461206913 CET	1.1.1.1	192.168.2.12	0xd28f	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)	false

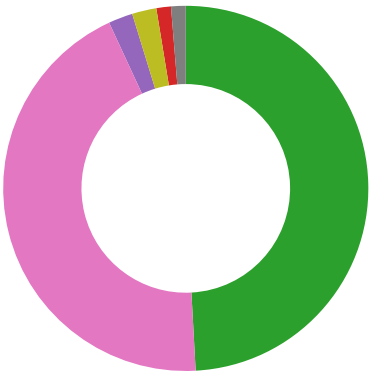
HTTP Request Dependency Graph

- raw.githubusercontent.com

Statistics

Behavior

- rundll32.exe
- SingleClientServicesUpdater.exe
- WalletGen.exe
- conhost.exe
- OpenConsole.exe
- WindowsTerminal.exe
- WalletGen.exe
- conhost.exe
- OpenConsole.exe
- WindowsTerminal.exe



Click to jump to process

System Behavior

Analysis Process: rundll32.exe PID: **5412**, Parent PID: **840**

General

Target ID:	0
Start time:	14:08:27
Start date:	23/11/2025
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
Imagebase:	0x7ff697b90000
File size:	90'112 bytes
MD5 hash:	B1BB2F6519DB1F087F45EC70638B99A6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: SingleClientServicesUpdater.exe PID: **6668**, Parent PID: **5092**

General

Target ID:	2
Start time:	14:08:36
Start date:	23/11/2025
Path:	C:\Program Files\Adobe\Acrobat DC\Acrobat\AcroCEF\SingleClientServicesUpdater.exe
Wow64 process (32bit):	false
Commandline:	--postMsg
Imagebase:	0x7ff60fd00000
File size:	240'258'520 bytes
MD5 hash:	FC9E6DF0E57B8116073BC5A94BA8B867
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: WalletGen.exe PID: **3916**, Parent PID: **4124**

General

Target ID:	5
Start time:	14:08:45
Start date:	23/11/2025
Path:	C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe"
Imagebase:	0x7ff7e56f0000
File size:	1'703'936 bytes
MD5 hash:	A5CEE52B774AC909D62815130710CE6B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

Analysis Process: conhost.exe PID: **3992**, Parent PID: **3916**

General

Target ID:	6
Start time:	14:08:46
Start date:	23/11/2025
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60fd00000
File size:	1'040'384 bytes
MD5 hash:	2447D7A01919B47AB7A009C0CA79A1AF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	1	success or wait	1	7FF60FD96C53	ReadFile
\pipe	0	8	success or wait	1	7FF60FD96C53	ReadFile
\pipe	0	1	unknown	1	7FF60FD96C53	ReadFile

Analysis Process: OpenConsole.exe PID: **5428**, Parent PID: **840**

General

Target ID:	7
Start time:	14:08:46
Start date:	23/11/2025
Path:	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding

Imagebase:	0x7ff644d30000
File size:	1'261'112 bytes
MD5 hash:	ED52DFA7DDEE29475240FBEC2AC2A096
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	2	success or wait	2	7FF644D6E7C1	ReadFile
\pipe	0	4	success or wait	1	7FF644D6E878	ReadFile
\pipe	0	4096	success or wait	1	7FF644D94FE7	ReadFile
\pipe	0	2	unknown	1	7FF644D6E7C1	ReadFile
\pipe	0	4096	unknown	1	7FF644D94FE7	ReadFile

Analysis Process: WindowsTerminal.exe PID: **3812**, Parent PID: **840**

General

Target ID:	8
Start time:	14:08:46
Start date:	23/11/2025
Path:	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe" -Embedding
Imagebase:	0x7ff678bc0000
File size:	719'416 bytes
MD5 hash:	97E5964AD41B33E7291E97B51D59E4A6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WalletGen.exe PID: **1620**, Parent PID: **4124**

General

Target ID:	11
Start time:	14:08:57
Start date:	23/11/2025
Path:	C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\WalletGen_windows_x64-23NOVEMBER2025\WalletGen\WalletGen.exe"
Imagebase:	0x7ff7e56f0000
File size:	1'703'936 bytes

MD5 hash:	A5CEE52B774AC909D62815130710CE6B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7E5766C32	InternetOpenUrlA

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>\Device\ConDrv</td><td>1</td><td>1</td><td>2a</td><td>*</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>77</td><td>76</td><td>2a 5f 5f 20 20 20 20 20 20 20 20 5f 5f 20 20 20 20 5f 20 5f 20 20 20 20 20 20 20 5f 20 20 20 20 5f 5f 5f 5f 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 0d</td><td>*__   __ _ _   _
_____
*</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>78</td><td>1</td><td>5f</td><td>_</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>154</td><td>76</td><td>2a 5c 20 5c 20 20 20 20 20 20 2f 20 2f 5f 20 5f 7c 20 7c 20 7c 20 5f 5f 5f 7c 20 7c 5f 20 2f 20 5f 5f 5f 7c 20 5f 5f 5f 20 5f 20 5f 5f 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 0d</td><td>*\ \   / /_ _| | | ___| |_ /
___| ___ _ __
*</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>155</td><td>1</td><td>5c</td><td>\</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	231	76	2a 20 5c 20 5c 20 2f 5c 20 2f 20 2f 20 5f 60 20 7c 20 7c 20 7c 2f 20 5f 20 5c 20 5f 5f 7c 20 7c 20 20 5f 20 2f 20 5f 20 5c 20 27 5f 20 5c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 0d	* \ \ /\ / / _` | | |/ _ \ __| | _ / _ \ '_ \ *	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	232	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	308	76	2a 20 20 5c 20 56 20 20 56 20 2f 20 28 5f 7c 20 7c 20 7c 20 7c 20 20 5f 5f 2f 20 7c 5f 7c 20 7c 5f 7c 20 7c 20 20 5f 5f 2f 20 7c 20 7c 20 7c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 0d	* \ V V / (_| | | __/ |_| |_| | __/ | | *	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	309	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	385	76	2a 20 20 20 5c 5f 2f 5c 5f 2f 20 5c 5f 5f 2c 5f 7c 5f 7c 5f 7c 5c 5f 5f 5f 7c 5c 5f 5f 5f 7c 5c 5f 5f 5f 5f 7c 5c 5f 5f 5f 7c 5f 7c 20 7c 5f 7c 20 20 20 20 20 20 20 20 20 20 20 20 20 5f 5f 5f 5f 20 20 5f 20 20 20 20 20 20 20 2a 0d	* _/_/ __,_|_|_|___|__|____|_ __|_| |_| ____ _ *	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	386	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	462	76	2a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 20 7c 5f 5f 20 20 5f 20 20 20 5f 20 20 7c 5f 20 20 20 5f 7c 5f 5f 20 20 5f 20 5f 5f 20 20 5f 20 20 20 20 5f 20 20 20 20 7c 20 5f 5f 20 29 7c 20 7c 5f 20 5f 5f 5f 20 2a 0d	* | |__ _ _ |_ _|__ _ __ _ _ | __)| |_ ___ *	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	463	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	539	76	2a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 20 27 5f 20 5c 7c 20 7c 20 7c 20 7c 20 20 20 7c 20 7c 2f 20 5f 20 5c 7c 20 27 5f 20 5c 7c 20 7c 20 7c 20 7c 20 20 20 20 7c 20 20 5f 20 5c 7c 20 5f 5f 2f 20 5f 5f 7c 2a 0d	* | '_ \\| | | | | _ \\| '_ \\| | | | | _ \\| __/ __|*	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	540	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	616	76	2a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 20 7c 5f 29 20 7c 20 7c 5f 7c 20 7c 20 20 20 7c 20 7c 20 28 5f 29 20 7c 20 7c 20 7c 20 7c 20 7c 20 7c 5f 7c 20 7c 20 20 20 7c 20 7c 5f 29 20 7c 20 7c 7c 20 28 5f 5f 20 2a 0d	* | _) | |_| | | (_) | | | | _| | | _) | || (__ *	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	617	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	693	76	2a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 5f 2e 5f 5f 2f 20 5c 5f 5f 2c 20 7c 20 20 20 7c 5f 7c 5c 5f 5f 5f 2f 7c 5f 7c 20 7c 5f 7c 5c 5f 5f 2c 20 7c 5f 5f 5f 7c 5f 5f 5f 5f 2f 20 5c 5f 5f 5c 5f 5f 5f 7c 2a 0d	* |_.__/ __, | |_|___/|_| |_|__, |___|____/ _____|*	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	694	1	20		success or wait	1	7FF7E5818DD3	fwrite

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>\Device\ConDrv</td><td>770</td><td>76</td><td>2a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 5f 5f 5f 2f 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 5f 5f 5f 2f 5f 5f 5f 5f 5f 7c 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 0d</td><td>* |___/ |___/_____| *</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>771</td><td>1</td><td>20</td><td></td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>847</td><td>76</td><td>2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d</td><td>***</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>848</td><td>1</td><td>2a</td><td>*</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>924</td><td>76</td><td>0d 0a 1b 5b 33 34 6d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d</td><td>[34m===</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>926</td><td>2</td><td>1b 5b</td><td>[</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>927</td><td>1</td><td>5b</td><td>[</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1009</td><td>82</td><td>1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 31 5d 1b 5b 39 34 6d 20 2d 20 67 65 6e 65 72 61 74 65 20 6f 6e 65 20 42 54 43 20 77 61 6c 6c 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20</td><td>[38;5;214m[1][94m - generate one BTC wallet</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1010</td><td>1</td><td>5b</td><td>[</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1108</td><td>98</td><td>1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 32 5d 1b 5b 39 34 6d 20 2d 20 67 65 6e 65 72 61 74 65 20 6f 6e 65 20 45 56 4d 20 77 61 6c 6c 65 74 20 28 45 54 48 2c 20 42 4e 42 2c 20 4d 41 54 49 43 20 65 2e 74 2e 63 29 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d</td><td>[38;5;214m[2][94m - generate one EVM wallet (ETH, BNB, MATIC e.t.c) [34m=</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1109</td><td>1</td><td>5b</td><td>[</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1207</td><td>98</td><td>1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 33 5d 1b 5b 39 34 6d 20 2d 20 73 65 61 72 63 68 20 42 54 43 20 77 61 6c 6c 65 74 73 20 77 69 74 68 20 62 61 6c 61 6e 63 65 20 28 75 73 69 6e 67 20 74 68 65 20 49 6e 74 65 72 6e 65 74 20 2d 20 73 6c 6f 77 65 72 29 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d</td><td>[38;5;214m[3][94m - search BTC wallets with balance (using the Internet - slower) [34m=</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
<tr><td>\Device\ConDrv</td><td>1208</td><td>1</td><td>5b</td><td>[</td><td>success or wait</td><td>1</td><td>7FF7E5818DD3</td><td>fwrite</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1306	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 34 5d 1b 5b 39 34 6d 20 2d 20 73 65 61 72 63 68 20 42 54 43 20 77 61 6c 6c 65 74 73 20 77 69 74 68 20 62 61 6c 61 6e 63 65 20 28 75 73 69 6e 67 20 74 68 65 20 64 61 74 61 62 61 73 65 20 2d 20 66 61 73 74 65 72 29 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[4][94m - search BTC wallets with balance (using the database - faster) [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1307	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1405	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 35 5d 1b 5b 39 34 6d 20 2d 20 73 65 61 72 63 68 20 45 56 4d 20 77 61 6c 6c 65 74 73 20 77 69 74 68 20 62 61 6c 61 6e 63 65 20 28 75 73 69 6e 67 20 74 68 65 20 49 6e 74 65 72 6e 65 74 20 2d 20 73 6c 6f 77 65 72 29 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[5][94m - search EVM wallets with balance (using the Internet - slower) [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1406	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1504	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 36 5d 1b 5b 39 34 6d 20 2d 20 73 65 61 72 63 68 20 45 56 4d 20 77 61 6c 6c 65 74 73 20 77 69 74 68 20 62 61 6c 61 6e 63 65 20 28 75 73 69 6e 67 20 74 68 65 20 64 61 74 61 62 61 73 65 20 2d 20 66 61 73 74 65 72 29 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[6][94m - search EVM wallets with balance (using the database - faster) [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1505	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1603	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 37 5d 1b 5b 39 34 6d 20 2d 20 72 65 63 6f 76 65 72 79 20 79 6f 75 72 20 62 69 74 63 6f 69 6e 20 77 61 6c 6c 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[7][94m - recovery your bitcoin wallet [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1604	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1702	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 38 5d 1b 5b 39 34 6d 20 2d 20 73 75 70 70 6f 72 74 20 74 68 65 20 64 65 76 65 6c 6f 70 65 72 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[8][94m - support the developer [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1703	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1801	98	1b 5b 33 38 3b 35 3b 32 31 34 6d 5b 39 5d 1b 5b 39 34 6d 20 2d 20 62 72 61 69 6e 20 77 61 6c 6c 65 74 20 67 65 6e 65 72 61 74 65 2f 63 68 65 63 6b 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1b 5b 33 34 6d 3d 0d	[38;5;214m[9][94m - brain wallet generate/check [34m=	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1802	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1900	98	1b 5b 33 34 6d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 0d 0a 73 65 6c 65 63 74 20 61 6e 20 61 63 74 69 6f	[34m================ =================== =================== =================== ===select an actio	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1901	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1983	82	73 65 6c 65 63 74 20 61 6e 20 61 63 74 69 6f 6e 20 75 73 69 6e 67 20 74 68 65 20 6b 65 79 3a 20 0d 0a 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f	select an action using the key: ______________________ ______________________ ______	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	1984	1	65	e	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2015	31	0d 0a 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f	______________________ ________	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2017	2	5f 5f	__	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2018	1	5f	_	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2090	72	41 72 65 20 79 6f 75 20 73 65 72 69 6f 75 73 20 61 62 6f 75 74 20 66 69 6e 64 69 6e 67 20 77 61 6c 6c 65 74 73 20 61 6e 64 20 77 61 6e 74 20 74 6f 20 75 73 65 20 47 50 55 20 57 61 6c 6c 65 74 47 65 6e 2c 20 20 20 7c	Are you serious about finding wallets and want to use GPU WalletGen, |	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2091	1	72	r	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2164	73	77 68 65 72 65 20 74 68 65 20 63 68 61 6e 63 65 20 69 73 20 6d 69 6c 6c 69 6f 6e 73 20 6f 66 20 74 69 6d 65 73 20 68 69 67 68 65 72 20 74 68 61 6e 20 6f 6e 20 43 50 55 3f 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 0d	where the chance is millions of times higher than on CPU? |	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2165	1	68	h	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2238	73	57 72 69 74 65 20 74 6f 20 6d 65 20 6f 6e 20 44 69 73 63 6f 72 64 3a 20 74 6f 6e 79 64 65 76 62 74 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7c 0d	Write to me on **Discord:** tonydevbtc |	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2239	1	72	r	success or wait	1	7FF7E5818DD3	fwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	2312	73	5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 7c 0d	____|	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2313	1	5f	_	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2388	75	4c 6f 61 64 69 6e 67 20 74 68 65 20 45 54 48 20 64 61 74 61 62 61 73 65 20 66 72 6f 6d 20 65 76 6d 5f 64 61 74 61 62 61 73 65 2e 74 78 74 2e 2e 2e 0d 0a 0d 5b 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	Loading the ETH database from evm_database.txt...[>	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2389	1	6f	o	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2434	45	2e 2e 2e 0d 0a 0d 5b 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	...[>	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2435	1	2e	.	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2439	4	0d 5b 3e 20	[>	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2440	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2441	1	3e	>	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2442	1	20		success or wait	50	7FF7E5818DD3	fwrite
\Device\ConDrv	2492	1	5b	[	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2497	5	30 25 20 28 31	0% (1	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2498	1	25	%	success or wait	1	7FF7E57AD18E	fwrite
\Device\ConDrv	2499	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2501	2	31 30	10	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2502	1	30	0	success or wait	1	7FF7E57ADA08	fwrite
\Device\ConDrv	2506	4	2f 32 35 39	/259	success or wait	1	7FF7E57ADA08	fwrite
\Device\ConDrv	2507	1	32	2	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2508	1	35	5	success or wait	1	7FF7E57ADA08	fwrite
\Device\ConDrv	2515	7	29 20 20 20 1b 5b 33	) [3	success or wait	1	7FF7E57ADA08	fwrite
\Device\ConDrv	2516	1	20		success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2519	3	1b 5b 33	[3	success or wait	1	7FF7E5818DD3	fwrite
\Device\ConDrv	2520	1	5b	[	success or wait	389	7FF7E5818DD3	fwrite
\Device\ConDrv	2544	24	61 73 70 65 63 74 20 73 65 6d 69 6e 61 72 20 66 75 72 6e 61 63 65 20 61	aspect seminar furnace a	success or wait	389	7FF7E5818DD3	fwrite
\Device\ConDrv	2545	1	73	s	success or wait	389	7FF7E5818DD3	fwrite
\Device\ConDrv	2620	75	0d 0a 1b 5b 33 38 3b 35 3b 32 31 34 6d 61 64 64 72 65 73 73 3a 1b 5b 30 6d 20 20 30 78 34 32 38 35 30 30 37 63 38 61 62 32 62 35 37 61 32 35 61 64 36 36 65 63 33 31 31 35 61 33 64 39 39 35 66 30 36 31 63 34 0d 0a 1b 5b 33 38	[38;5;214maddress:[0m 0x4285007c8ab2b57a25ad66ec3115a3d995f061c4[38	success or wait	389	7FF7E5818DD3	fwrite
\Device\ConDrv	2622	2	1b 5b	[	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2647	25	30 78 34 32 38 35 30 30 37 63 38 61 62 32 62 35 37 61 32 35 61 64 36 36 65	0x4285007c8ab2b57a25ad66e	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2648	1	78	x	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2689	41	0d 0a 1b 5b 33 38 3b 35 3b 32 31 34 6d 62 61 6c 61 6e 63 65 3a 1b 5b 30 6d 20 20 28 65 6d 70 74 79 29 0d 0a 1b 5b 39 34 6d	[38;5;214mbalance:[0m (empty)[94m	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2691	2	1b 5b	[	success or wait	388	7FF7E5818DD3	fwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	2716	25	28 65 6d 70 74 79 29 0d 0a 1b 5b 39 34 6d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d	(empty) [94m==========	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2717	1	65	e	success or wait	388	7FF7E5818DD3	fwrite
\Device\ConDrv	2826	109	1b 5b 33 38 3b 35 3b 32 31 34 6d 6d 6e 65 6d 6f 6e 69 63 3a 1b 5b 30 6d 20 63 61 72 74 20 73 70 61 63 65 20 6e 65 78 74 20 65 72 61 73 65 20 6f 72 67 61 6e 20 6d 6f 75 73 65 20 64 61 77 6e 20 73 63 69 65 6e 63 65 20 74 72 75 65 20 64 75 73 74 20 74 77 69 73 74 20 63 6f 6c 6c 65 63 74 0d 0a 1b 5b 33 38 3b 35 3b 32 31 34 6d 61	[38;5;214mmnemonic:[0m cart space next erase organ mouse dawn science true dust twist collect[38;5;214ma	success or wait	388	7FF7E5818DD3	fwrite

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\src37dsj.default-release\cookies.sqlite	0	98304	success or wait	1	25EACCEE9F0	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\src37dsj.default-release\key4.db	0	294912	success or wait	1	25EACCEE9F0	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\src37dsj.default-release\prefs.js	0	7116	success or wait	1	25EACCE3095	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	0	112640	success or wait	1	25EACCE2FF0	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	143360	success or wait	1	25EACCE2FF0	ReadFile

Analysis Process: conhost.exe PID: **6392**, Parent PID: **1620**

General

Target ID:	12
Start time:	14:08:57
Start date:	23/11/2025
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60fd00000
File size:	1'040'384 bytes
MD5 hash:	2447D7A01919B47AB7A009C0CA79A1AF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	1	success or wait	1	7FF60FD96C53	ReadFile
\pipe	0	8	success or wait	1	7FF60FD96C53	ReadFile
\pipe	0	1	unknown	1	7FF60FD96C53	ReadFile

Analysis Process: OpenConsole.exe PID: **5856**, Parent PID: **840**

General

Target ID:	13

Start time:	14:08:58
Start date:	23/11/2025
Path:	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.exe" -Embedding
Imagebase:	0x7ff644d30000
File size:	1'261'112 bytes
MD5 hash:	ED52DFA7DDEE29475240FBEC2AC2A096
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	2	success or wait	3	7FF644D6E7C1	ReadFile
\pipe	0	4	success or wait	1	7FF644D6E878	ReadFile
\pipe	0	4096	success or wait	2	7FF644D94FE7	ReadFile
\pipe	0	4096	unknown	1	7FF644D94FE7	ReadFile
\pipe	0	2	unknown	1	7FF644D6E7C1	ReadFile

Analysis Process: WindowsTerminal.exe PID: **6596**, Parent PID: **840**

General

Target ID:	14
Start time:	14:08:59
Start date:	23/11/2025
Path:	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe" -Embedding
Imagebase:	0x7ff678bc0000
File size:	719'416 bytes
MD5 hash:	97E5964AD41B33E7291E97B51D59E4A6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly