

From fake Proton VPN sites to gaming mods, this Windows infostealer is everywhere

malwarebytes.com/blog/threat-intel/2026/04/from-fake-proton-vpn-sites-to-gaming-mods-this-windows-infostealer-is-everywhere

Gabriele Orini

April 15, 2026



We've uncovered multiple campaigns distributing an infostealer we track as **NWHStealer**, using everything from fake VPN downloads to hardware utilities and gaming mods. What makes this campaign stand out isn't just the malware, but how widely and convincingly it's being spread.

Once installed, it can collect browser data, saved passwords, and cryptocurrency wallet information, which attackers may use to access accounts, steal funds, or carry out further attacks.

We detected multiple campaigns using different platforms and lures to distribute NWHStealer. The stealer is loaded and executed in several ways, such as self-injection or injection into other processes like [RegAsm](#) (Microsoft's Assembly Registration Tool). Often, additional wrappers such as MSI or Node.js are used as the initial loader.

The stealer is distributed using lures (what the file claims to be) such as:

- VPN installers
- Hardware utilities (e.g. [OhmGraphite](#), [Pachtop](#), [HardwareVisualizer](#), [SidebarDiagnostics](#))

- Mining software
- Games, cheats, and mods (e.g. [Xeno](#))

It's hosted or shared across multiple distribution channels, including:

- Fake websites impersonating legitimate services, like Proton VPN
- Code hosting platforms like GitHub and GitLab
- File hosting services such as MediaFire and SourceForge
- Links and redirects from gaming- and security-related YouTube videos

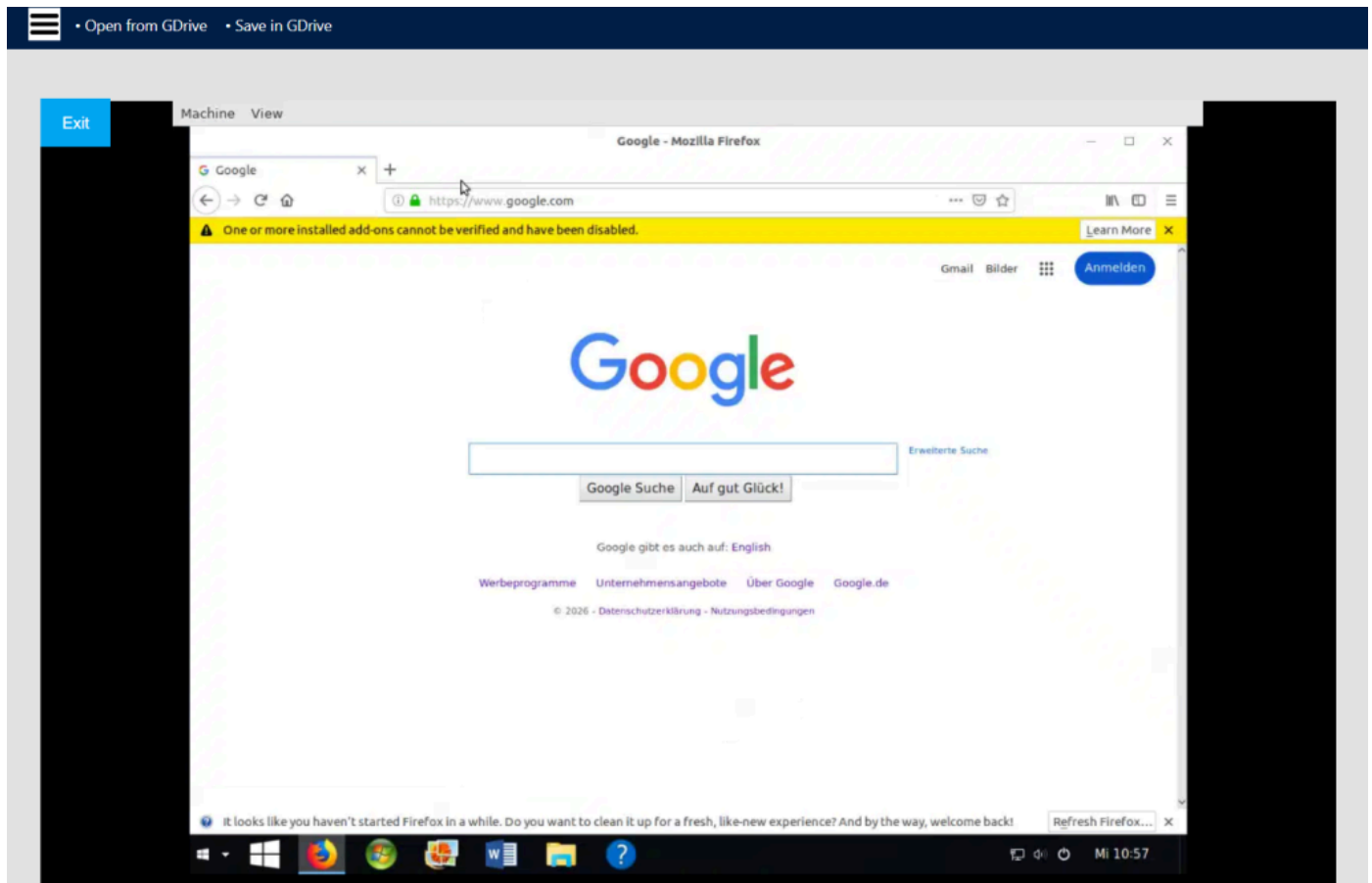
Although there are many distribution methods, in this blog we look at two cases:

- Case 1: A free web hosting provider distributing a malicious ZIP file that loads the stealer using self-injection
- Case 2: Fake websites that load the stealer using DLL hijacking and injection into the RegAsm process

Case 1: Free web hosting provider distributes the stealer

The first case is the most unexpected. We found that a free web hosting provider, [onworks\[.\]net](#), hosts ZIP files in its download section that ultimately distribute the stealer.

The website, ranked in the top 100,000, allows users to run virtual machines entirely in the browser.



Virtual machine running in the browser

Through this site, users download a malicious ZIP with names like:

- OhmGraphite-0.36.1.zip
- Sidebar Diagnostics-3.6.5.zip
- Pachtop_1.2.2.zip
- HardwareVisualizer_1.3.1.zip

HARDWARE VISUALIZER DOWNLOAD FOR WINDOWS



This is the Windows app named Hardware Visualizer whose latest release can be downloaded as HardwareVisualizer_1.3.1.zip. It can be run online in the free hosting provider OnWorks for workstations.

Download and run online this app named Hardware Visualizer with OnWorks for free.

Follow these instructions in order to run this app:

- 1. Downloaded this application in your PC.
- 2. Enter in our file manager <https://www.onworks.net/myfiles.php?username=XXXXX> with the username that you want.
- 3. Upload this application in such filemanager.
- 4. Start any OS OnWorks online emulator from this website, but better Windows online emulator.
- 5. From the OnWorks Windows OS you have just started, goto our file manager <https://www.onworks.net/myfiles.php?username=XXXXX> with the username that you want.
- 6. Download the application and install it.
- 7. Download Wine from your Linux distributions software repositories. Once installed, you can then double-click the app to run them with Wine. You can also try PlayOnLinux, a fancy interface over Wine that will help you install popular Windows programs and games.

Wine is a way to run Windows software on Linux, but with no Windows required. Wine is an open-source Windows compatibility layer that can run Windows programs directly on any Linux desktop. Essentially, Wine is trying to re-implement enough of Windows from scratch so that it can run all those Windows applications without actually needing Windows.

Download App

Run Online

One of the pages that downloads the malicious archive

In this case, the malicious code responsible for loading the stealer is embedded in the executable, for example **HardwareVisualizer.exe**.

 Modules	4/10/2026 1:30 AM	File folder	
 common.dll	4/10/2026 1:30 AM	Application exten...	1,336 KB
 Common.Logging.dll	4/10/2026 1:30 AM	Application exten...	39 KB
 CommonServiceLocator.dll	4/10/2026 1:30 AM	Application exten...	10 KB
 ControlzEx.dll	4/10/2026 1:30 AM	Application exten...	176 KB
 ENPMessagingContract.dll	4/10/2026 1:30 AM	Application exten...	12 KB
 EntityFramework.dll	4/10/2026 1:30 AM	Application exten...	4,939 KB
 EntityFramework.SqlServer.dll	4/10/2026 1:30 AM	Application exten...	568 KB
 EntityFramework.SqlServerCompact.dll	4/10/2026 1:30 AM	Application exten...	277 KB
 GalaSoft.MvvmLight.dll	4/10/2026 1:30 AM	Application exten...	30 KB
 GalaSoft.MvvmLight.Extras.dll	4/10/2026 1:30 AM	Application exten...	21 KB
 GalaSoft.MvvmLight.Platform.dll	4/10/2026 1:30 AM	Application exten...	14 KB
 HardwareVisualizer.exe	4/10/2026 1:30 AM	Application	6,692 KB
 Ionic.Zip.Reduced.dll	4/10/2026 1:30 AM	Application exten...	248 KB
 MahApps.Metro.dll	4/10/2026 1:30 AM	Application exten...	1,072 KB
 Microsoft.Expression.Interactions.dll	4/10/2026 1:30 AM	Application exten...	106 KB
 Microsoft.Xaml.Behaviors.dll	4/10/2026 1:30 AM	Application exten...	142 KB
 Newtonsoft.Json.dll	4/10/2026 1:30 AM	Application exten...	684 KB
 O2S.Components.PDF4NET.dll	4/10/2026 1:30 AM	Application exten...	2,140 KB
 O2S.Components.PDFRender4NET.WPF.dll	4/10/2026 1:30 AM	Application exten...	1,558 KB
 O2S.Components.PDFView4NET.WPF.dll	4/10/2026 1:30 AM	Application exten...	2,236 KB
 Polly.dll	4/10/2026 1:30 AM	Application exten...	240 KB
 Prism.dll	4/10/2026 1:30 AM	Application exten...	75 KB
 Prism.Unity.Wpf.dll	4/10/2026 1:30 AM	Application exten...	30 KB
 Prism.Wpf.dll	4/10/2026 1:30 AM	Application exten...	144 KB
 Quartz.dll	4/10/2026 1:30 AM	Application exten...	936 KB
 System.ComponentModel.Composition....	4/10/2026 1:30 AM	Application exten...	109 KB
 System.Data.SqlServerCe.dll	4/10/2026 1:30 AM	Application exten...	460 KB
 System.IO.Abstractions.dll	4/10/2026 1:30 AM	Application exten...	46 KB
 System.Reactive.Core.dll	4/10/2026 1:30 AM	Application exten...	112 KB
 System.Reactive.Interfaces.dll	4/10/2026 1:30 AM	Application exten...	23 KB
 System.Reactive.Linq.dll	4/10/2026 1:30 AM	Application exten...	693 KB
 System.Reactive.PlatformServices.dll	4/10/2026 1:30 AM	Application exten...	38 KB
 System.Reactive.Windows.Threading.dll	4/10/2026 1:30 AM	Application exten...	28 KB
 System.Runtime.CompilerServices.Unsaf...	4/10/2026 1:30 AM	Application exten...	24 KB
 System.Threading.Tasks.Extensions.dll	4/10/2026 1:30 AM	Application exten...	33 KB
 System.ValueTuple.dll	4/10/2026 1:30 AM	Application exten...	25 KB
 System.Windows.Interactivity.dll	4/10/2026 1:30 AM	Application exten...	55 KB
 Telerik.Windows.Controls.dll	4/10/2026 1:30 AM	Application exten...	3,874 KB

The loader that starts the infection chain

The loader contains junk code to make analysis more difficult and performs several operations, including:

- Checking the environment for analysis tools and terminating if detected
- Implementing a custom decryption function for strings

- Resolving functions using `LoadLibraryA` and `GetProcAddress`
- Decrypting and loading the next stage using AES-CBC via BCrypt APIs

This isn't the only way the stealer is distributed. We found similar lures, with the same ZIP names, that instead distribute the stealer via DLL hijacking.

In this case, `HardwareVisualizer.exe` is actually the WinRAR executable, and the malicious code resides in `WindowsCodecs.dll`.

 HardwareVisualizer.exe	5/14/2024 2:35 PM	Application	3,210 KB
 Ionic.Zip.Reduced.dll	8/17/2011 6:59 PM	Application exten...	248 KB
 MahApps.Metro.dll	6/18/2018 7:31 PM	Application exten...	1,072 KB
 Microsoft.Expression.Interactions.dll	8/13/2015 11:26 PM	Application exten...	106 KB
 Microsoft.Xaml.Behaviors.dll	1/15/2020 7:50 AM	Application exten...	142 KB
 Newtonsoft.Json.dll	11/8/2019 7:56 AM	Application exten...	684 KB
 O2S.Components.PDFView4NET.WPF.dll	7/10/2017 7:35 PM	Application exten...	2,236 KB
 Polly.dll	8/5/2017 5:54 PM	Application exten...	240 KB
 Prism.dll	11/20/2019 11:58 PM	Application exten...	75 KB
 Prism.Unity.Wpf.dll	11/20/2019 11:58 PM	Application exten...	30 KB
 Prism.Wpf.dll	11/20/2019 11:58 PM	Application exten...	144 KB
 Quartz.dll	11/24/2013 12:01 AM	Application exten...	936 KB
 System.ComponentModel.Composition....	3/25/2018 11:24 PM	Application exten...	109 KB
 System.Data.SqlServerCe.dll	8/8/2012 1:02 AM	Application exten...	460 KB
 System.IO.Abstractions.dll	9/9/2019 2:13 AM	Application exten...	46 KB
 System.Reactive.Core.dll	11/20/2016 9:01 PM	Application exten...	112 KB
 System.Reactive.Interfaces.dll	11/20/2016 9:02 PM	Application exten...	23 KB
 System.Reactive.Linq.dll	11/20/2016 9:02 PM	Application exten...	693 KB
 System.Reactive.PlatformServices.dll	11/20/2016 9:02 PM	Application exten...	38 KB
 System.Reactive.Windows.Threading.dll	11/20/2016 9:03 PM	Application exten...	28 KB
 System.Runtime.CompilerServices.Unsaf...	9/18/2018 2:38 AM	Application exten...	24 KB
 System.Threading.Tasks.Extensions.dll	11/28/2018 10:39 PM	Application exten...	33 KB
 System.ValueTuple.dll	5/14/2018 8:29 PM	Application exten...	25 KB
 System.Windows.Interactivity.dll	9/14/2017 3:32 AM	Application exten...	55 KB
 Telerik.Windows.Controls.dll	2/19/2019 9:05 AM	Application exten...	3,874 KB
 Telerik.Windows.Controls.Docking.dll	2/19/2019 9:06 AM	Application exten...	232 KB
 Telerik.Windows.Controls.FixedDocumen...	2/19/2019 9:05 AM	Application exten...	461 KB
 Telerik.Windows.Controls.GridView.dll	2/19/2019 9:06 AM	Application exten...	1,187 KB
 Telerik.Windows.Controls.Input.dll	2/19/2019 9:05 AM	Application exten...	599 KB
 Telerik.Windows.Controls.Navigation.dll	2/19/2019 9:05 AM	Application exten...	1,152 KB
 Telerik.Windows.Data.dll	2/19/2019 9:05 AM	Application exten...	476 KB
 Telerik.Windows.Documents.Core.dll	2/14/2019 8:59 PM	Application exten...	458 KB
 Telerik.Windows.Documents.Fixed.dll	2/14/2019 9:00 PM	Application exten...	2,518 KB
 Telerik.Windows.Themes.Windows8Touc...	2/19/2019 9:13 AM	Application exten...	2,330 KB
 Telerik.Windows.Zip.dll	2/14/2019 8:59 PM	Application exten...	142 KB
 Unity.Abstractions.dll	6/20/2019 2:38 AM	Application exten...	64 KB
 Unity.Container.dll	6/20/2019 2:55 AM	Application exten...	143 KB
 WindowsCodecs.dll	3/1/2026 8:19 PM	Application exten...	5,526 KB

The WinRAR executable with the malicious DLL

While tracking the DLL loader, we also saw it distributed in other campaigns with different lures. For example, in the second case analyzed, this malicious DLL is delivered through fake websites.

Case 2: Fake Proton VPN website and DLL loader

In the second case, we detected a website impersonating Proton VPN that delivers a malicious ZIP. This archive executes the stealer using DLL hijacking or an MSI file. To be clear, this has no affiliation with Proton VPN, and we’ve contacted them to let them know what we found.

Links to the website appear in several compromised YouTube channels, along with AI-generated videos demonstrating the installation process:



Tech Shield Insights

@kvdoyle · 28 subscribers · 102 videos

Channel about protecting your digital life in 2025. VPN tutorials, privacy hacks, and review...more

guide.vpn-proton-setup.com

Subscribe

- Youtube channels with malicious Proton VPN links.

Free VPN for Windows PC – How to Install and Use Step by Step



AI Secure Future
41 subscribers

Subscribe

1

Share

Save

...

66 views 3 months ago #vpnfree #freevpn #freevpnforpc

In this video, I show you how to install and use a free VPN on a Windows PC step by step. This tutorial is perfect if you are looking for a free VPN for PC, want better privacy, or need a safe Windows VPN for everyday use. ...more

1 Comment

Sort by



Add a comment...



@caitlyn418 · 2 months ago (edited)

Link to the recommended option is in the description.

desktop.vpn-proton-setup.com

(Disclosure: affiliate link – I may earn a commission.)

Like

Dislike

Reply

- Youtube channels with malicious Proton VPN links.

8/17

Description

Exploring how artificial intelligence changes security, business, and online privacy. Learn about VPNs, data protection, and why secure internet matters more than ever in 2025. Protect your privacy online – download Proton VPN for free here.

Links



Try Proton VPN Free

desktop.vpn-proton-setup.com

More info



www.youtube.com/@caitlyn418



United States



Joined Nov 29, 2007



41 subscribers



108 videos



122,946 views



Share channel

- Youtube channels with malicious Proton VPN links.



Digital Armor Network

@pandorasykes · 61 subscribers · 105 videos

Protect your devices with tech that works. From VPN tutorials to cyber-safety guides, we s...more

help.vpn-proton-setup.com

Subscribe

- Youtube channels with malicious Proton VPN links.



NextGen VPN Hub

@natekauric · 25 subscribers · 99 videos

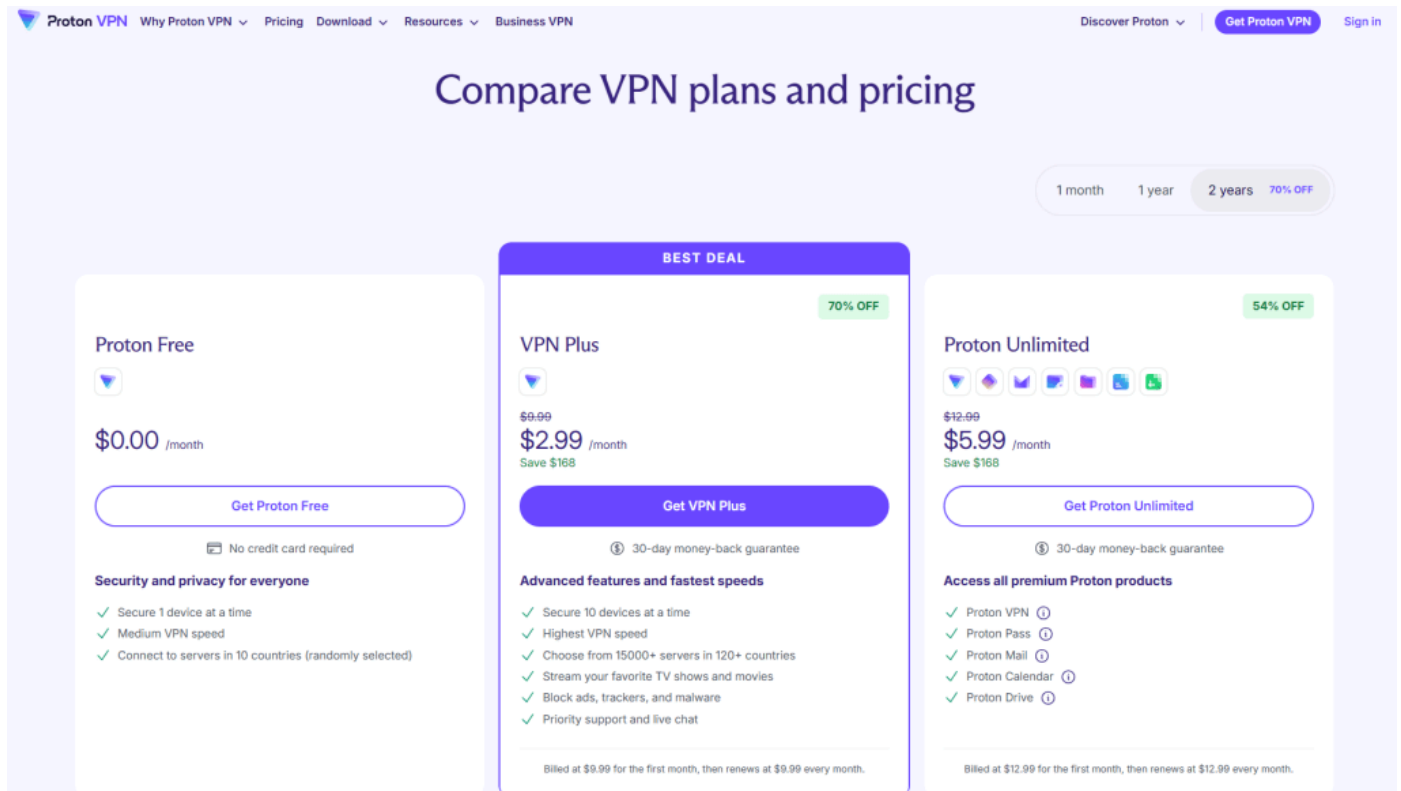
All about VPNs and the future of online security. Honest comparisons, beginner guides, ar...more

download.vpn-proton-setup.com

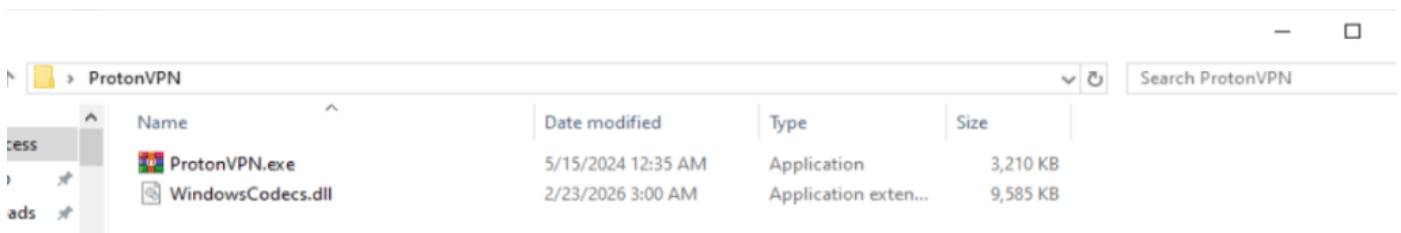
Subscribe

- Youtube channels with malicious Proton VPN links.

- Youtube channels with malicious Proton VPN links.



Fake website distributes the stealer via DLL hijacking



Folders containing the malicious DLL

In other infection chains, this DLL appears under different names, such as:

- `iviewers.dll`
- `TextShaping.dll`
- `CrashRpt1403.dll`

This DLL decrypts two embedded resources. The decryption method varies between samples: Some use custom AES implementations, while others rely on the OpenSSL library.

One of the decrypted resources is a second-stage DLL, `runpeNew.dll`, which is loaded and executed via the `GetGet` method.

The second-stage DLL starts a process (such as `RegAsm`) and performs process hollowing using low-level APIs, including:

- `NtProtectVirtualMemory`

- `NtCreateUserProcess`
- `NtUnmapViewOfSection`
- `NtAllocateVirtualMemory`
- `NtResumeThread`

The final payload: NWHStealer

At the end of these infection chains, the attacker deploys NWHStealer. The stealer runs directly in memory or injects itself into other processes such as `RegAsm.exe`.

It enumerates more than 25 folders and registry keys associated with cryptocurrency wallets.

 <code>QueryAllInforma...</code>	<code>\\vmware-host\Shared Folders\</code>	<code>BUFFER OVERFL...</code>	<code>CreationTime: 4/10...</code>
 <code>CloseFile</code>	<code>\\vmware-host\Shared Folders\</code>	<code>SUCCESS</code>	
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Local\Coinomi\Coinomi\wallets</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\com.tari.universe\app_configs\mainnet</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Local\com.tari.universe\wallet\mainnet\data\wallet</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\MyMonero</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Monero</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Vertcoin</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Groestlcoin</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Komodo</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\PIVX</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\BitcoinGold</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Binance</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Phantom</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Coin98</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\MathWallet</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Ledger Live</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\TrezorSuite</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\@trezor\suite-desktop</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\MyEtherWallet</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\MyCrypto</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\MetaMask</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\TrustWallet</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\NOW Wallet</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Sollet-Wallet</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\wombat-desktop</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\io.solarwallet.app</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Amory</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\atomic\Local Storage\leveldb\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Electrum\wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Electrum-LTC\wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\ElectrumSV\wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Ethereum\keystore\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Exodus\exodus.wallet\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Guarda\Local Storage\leveldb\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\com.libertyjazz\IndexedDB\file__0.indexeddb.leveldb\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Sparrow\wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\WalletWasabi\Client\Wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Zcash</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Daedalus Mainnet\wallets\</code>	<code>PATH NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\bytecoin</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>
 <code>CreateFile</code>	<code>C:\Users\root\AppData\Roaming\Dogecoin</code>	<code>NAME NOT FOUND</code>	<code>Desired Access: R...</code>

```

4712 RegOpenKey HKCU
4712 RegQueryKey HKCU
4712 RegOpenKey HKCU\Software\Bitcoin\Bitcoin-Qt
4712 RegQueryKey HKCU
4712 RegOpenKey HKCU\Software\Dash\Dash-Qt
4712 RegQueryKey HKCU
4712 RegOpenKey HKCU\Software\Litecoin\Litecoin-Qt
4712 RegQueryKey HKCU
4712 RegOpenKey HKCU\Software\monero-project\monero-core

```

Enumeration phase of wallets

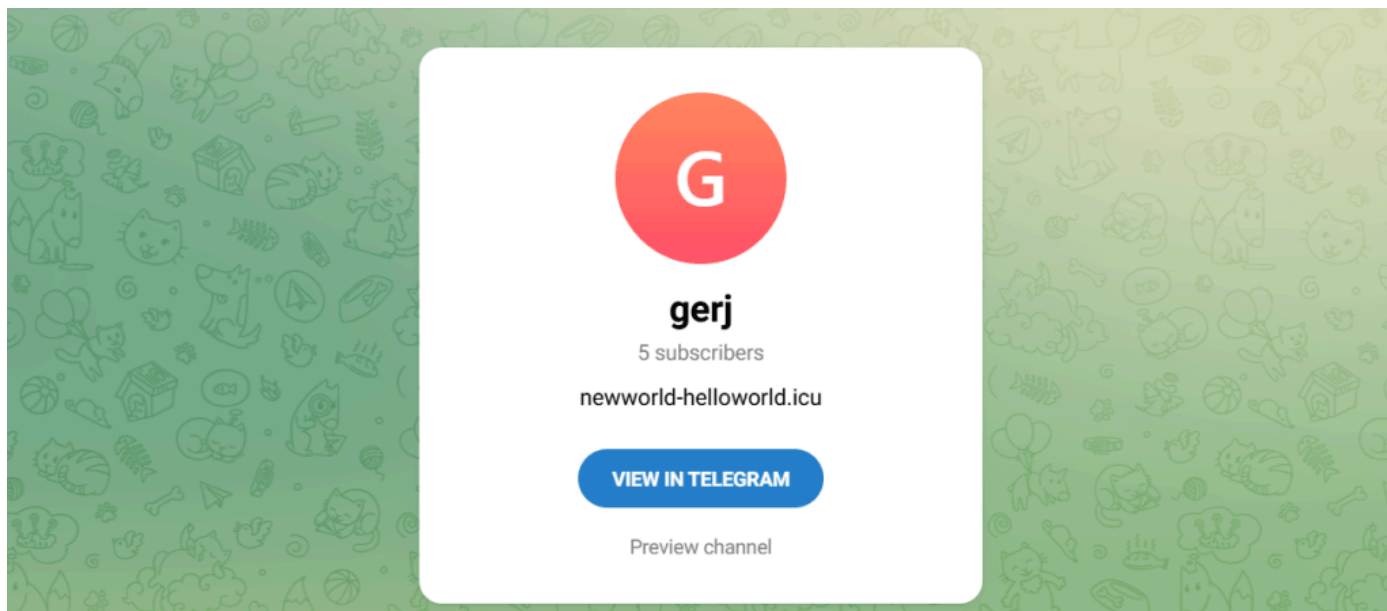
The stealer also collects and exfiltrates data from multiple browsers, including Edge, Chrome, Opera, 360 Browser, K-Melon, Brave, Chromium, and Chromodo.

Operation	Path	Result	Detail
CreateFile	C:\Users\root\AppData\Roaming\Opera Software\Opera Stable_side_profiles	PATH NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Roaming\Opera Software\Opera Stable\Snapshots	PATH NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data	SUCCESS	Desired Access: R...
QueryDirectory	C:\Users\root\AppData\Local\Microsoft\Edge\User Data*	SUCCESS	FileInformationClas...
QueryDirectory	C:\Users\root\AppData\Local\Microsoft\Edge\User Data	SUCCESS	FileInformationClas...
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data	SUCCESS	Offset: 16,384, Len...
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data	SUCCESS	Offset: 4,096, Leng...
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data	SUCCESS	Offset: 12,288, Len...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Ad Blocking	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Ad Blocking	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Ad Blocking	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Ad Blocking	SUCCESS	
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Ad Blocking\Local Extension Settings	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Autofill	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Autofill	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Autofill	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Autofill	SUCCESS	
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Autofill\Local Extension Settings	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent	SUCCESS	
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent\Local Extensio...	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics	SUCCESS	
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics	SUCCESS	Offset: 0, Length: 4...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\Local Extension Settings	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation	SUCCESS	
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation\Local Extension Settings	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	SUCCESS	
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	SUCCESS	Offset: 16,384, Len...
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache	SUCCESS	Offset: 12,288, Len...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\Local Extension Settings	NAME NOT FOUND	Desired Access: R...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad	SUCCESS	Desired Access: R...
QueryInformatio...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad	SUCCESS	VolumeCreationTim...
QueryAllInforma...	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad	BUFFER OVERFL...	CreationTime: 2/26...
CloseFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad	SUCCESS	
ReadFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad	SUCCESS	Offset: 0, Length: 4...
CreateFile	C:\Users\root\AppData\Local\Microsoft\Edge\User Data\Crashpad\Local Extension Settings	NAME NOT FOUND	Desired Access: R...

Enumeration of browser folders

- Encrypts a **getPayload** request and sends it to the C2
- Receives and executes additional payloads disguised as system processes (e.g., **svchost.exe**, **RuntimeBroker.exe**)
- Creates scheduled tasks to run the payload at user logon with elevated privileges

Data sent to the C2 is encrypted using AES-CBC. If the primary server is unavailable, the malware can retrieve a new C2 domain via a Telegram-based dead drop.



Dead drop resolver via Telegram

```
{
  "type": "system_info",
  "username": "root",
  "computer_name": "DESKTOP-TSKTHVJ",
  "os": "Windows 10.0.19045 (Workstation) Windows 10 Pro (Build 19045)",
  "hwid": "9dae92ca-f2ee-4d02-a933-2b7d4b4bb58e",
  "local_time": "2026-04-10 07:32:01",
  "utc_time": "2026-04-10 14:32:01 UTC",
  "timezone": "UTC-7",
  "language": "en-US",
  "system_language": "English",
  "keyboard_layouts": "English",
  "running_path": "C:\\Users\\root\\Desktop\\HardwareVisualizer_1.3.1\\HardwareVisualizer.exe",
  "cpu": "Intel(R) Core(TM) Ultra 9 185H",
  "cpu_cores": 3,
  "cpu_threads": 6,
  "ram": "2.0",
  "gpu": "VMware SVGA 3D",
  "displays": "1918x998",
  "injected_browsers": [
    "Microsoft Edge"
  ],
  "screenshots": [
    "iVBORw0KGgoAAAANSUHEUgAAB34AAAPmCAIAAAACEp6nvAAQexklEQVR42uy9CZQyVkmAOZXRORRMXVXV/VV3V1d1a2+po6W0AmSEEjAAOLcQc0i3WVYG3IbldkZFaGM5klivEqWt8zM7kE,
    Cpjdod+umB12dsQxIAGSkISQ1FKr1Uf1XdVldB2ZdeQZ4e5mts/9d//999/MIYMyI4/qSnutVFSEH2a//WZu/v3f/5kUjyyL66lIKYc63mddKENqrExG3SjDslYzK3xNrapfZtpuQd8g9/L
    MAHkxetdf7/Cg4w0O9l70vPM+gJtkYXzR5p5G6ukLfvdgEK92JaxD0zgyo3LXpus0jbuG46VZxZ8Ztr2j8v/G+xozlNTUZJlR9SntL73muvtPwwXxvgPeaNj+Grb+3gChj9wmYn0eK4PU0
    Pjascf1tRevc6Pyx6Fddi629+k32T2M8sclLpWcZy4Zdz8gRXaepjzWz3FFy2OMHtmf/66y6qSNvb/8bSemaZazTeKIzW9GMp/URm7x/9r+NVvirNt4hLvIpu8b/FnqIZ87WlXnuq7Jx1HtXg
    MKWnct0Z/luULCKWY+/dddjAcIiVilRWDUvliq/p9elylFbGK9ef9BQhRCLL7z3PgwrA0tb3fdYR8H0UhnAMvZTnefS5jNfP5iVtmQKuqVTRI3hH+Ak007qoLb0tbsN+A3cMpCgX3gbX5EK
    NemyqQFjI/alVu09iW0JwgCZmE4xfD9Ue8CPz/XGBMEQXajNIXDiuakC19Cb432pxeHKjnfLLAH4cqVKVT16kFNgbZVSaE/s7GrdRRFSqk0TTOzG4M2oX0ENyqNpcEmSmUNWZ6FY6BR2HF0
    moi+YkhDdurjxeE27wUrTyAlwZzgJX9H1faw2tgAq0Wq2lpSWjVNHqeZ4Xx7EQIooInaToIYnneXhZuAXeF5tPm0B9GypfnJvFWCml1ZKeFwQBNW4eEfBlFLXBmFgTqAZck/Y11CdNs/zDZ
    VSSZKA4dnjC871haQ9hVFXSHdwA2yCuf3DUKpVbR6ngc+Bp4M/0Rv92RAhw/eFlxLShnHMFQRWFjULV+NmtzU1Lx0TKHb0CGMhqL294ShzoMV63Q640dwKfRSKWWSDAooNpe3mtgcFpD5r
    Q2TgvYZ3t2YnZBw6AlKd3xiFslLKdk45oBY4C+5FuWADaNwcXFRGNNqt6WUvV5PCNFut1WS0akfaoLeCPVE2zKng0OhAuiflP7oqDAYoRrwT/geRzS6Qjxf0L3BpcHhAI+D86R5CYIGDEF
    87BDoc44s8FEV85yPrYLJlXsJmrVv8DD1wXZowwDKE+cDv0t8on6/gDnXLBi5IKgeVACLIXD2hbOnyK0aQ0Jp0h4QBoIH0igD19Wxv/Qidst9tgPbgX+q2QGP0ZLoJDFS2Gfg6PM5z/Pc8L
    xcfdQ2suavuDZ6lZXGV4KmZeKGQczb5VVUbIiWLYLxkYAFRjJ9KNKpgYdA6mW0vID/CJEUq5aDK4VdXo9YLDt:uay/b89V22S7XRkxWl17v62x12X4ebRdamkMKG+fqg0R0muppo6WD1
    JSrqq84duxFWYH0YKLOIhdK7tRNoRt15mubOlhCEywmhRXVhre6p3sDXrZ8m/tN3hZbDw3OK+KqUv5xW8RXAHRDdEGXpk6A+Fzp1BnHg9o13aAHYYPZ51H4PkWEHIu0SrFok4aS/jEYthgA
    4jx0eQHTGGUCFXwFYt+MQ90J21IFCJ7bJQ5iC0mEFcRKIJZ4F17H7AkykSuAPzQV4ECJNCJQwXAnrjPdLDeD6BXsWI2gC+c2LECKOY4ocIahNkXeEn2ijaK9BPREFgXMRf2buVLi00nhfGqJ
    XAmRSvgpSx0ImJjUoASWG3sRzqOPM9LkoSeVaF1DdMa9TQak6OQHJ0tsR9pPbNf88+0BxEyw2pQ1B9c141xbAsdX3BMGIbQBeD/1A17o1/wT+hrhk3T+Yq6sa7PhCyQh6j6tsVxxfB13/fR
    NTfnF2xgRcr6EwLrv+yGJlLoExFGnC7o0IoFAkykWDQ7vbi7riYKxDfBn2noEU6BCBN6IHlq4BinIQGYh+3gK5v6aySpjGbZDDW4oyeMkvS6zsJezudD6hASpWFTpGnDMt7VawAzq8l
    JAZxglTKeoT7JHJP3MIqAYJ0Ykmk5QePhRdnoetmYO+/VVoZkpl7rZUA6sD0lsbnG9w02GRXPHfJ3yNhCJ8tN359hdefL8a+GYSJue5lWDSkieUktafvdV2GenXfLtl15dtf96Ysm3nAQ
  ]
}
```

JSON containing various information about the compromised system

The stealer also uses a known CMSTP User Account Control (UAC) bypass technique to execute PowerShell commands:

- Generates a random `.inf` file in the temp folder
- Uses `cmstp.exe` to elevate privileges
- Automatically confirms the prompt using Windows APIs

How to stay safe

Instead of relying on phishing emails or obvious scams, the attackers behind this campaign are hiding malware inside tools people actively search for and trust. By spreading through platforms like GitHub, SourceForge, and YouTube, they increase the chances that users will let their guard down.

Once installed, the impact can be serious. Stolen browser data, saved passwords, and cryptocurrency wallet information can lead to account takeovers, financial loss, and further compromise.

Here are our tips for avoiding being caught out:

- Download software only from official websites
- Be cautious with downloads from GitHub, SourceForge, or file-sharing platforms unless you trust the source
- Check file signatures and publisher details before running anything
- Avoid downloading tools from links in YouTube descriptions
- **Pro tip:** Install [Malwarebytes Browser Guard](#) on your browser to block malicious URLs.

Indicators of Compromise (IOCs)

Check the signature and version of software in suspicious archives.

Hashes

`e97cb6cbcf2583fe4d8dcabd70d3f67f6cc977fc9a8cbb42f8a2284efe24a1e3`
`2494709b8a2646640b08b1d5d75b6bf3167540ed4acdb55ded050f6df9c53b3`

Domains

`vpn-proton-setup[.]com` (fake website)
`get-proton-vpn[.]com` (fake website)
`newworld-helloworld[.]icu` (C2 domain)
`https://t[.]me/gerj_threuh` (Telegram dead drop)

URLS

[https://www.onworks\[.\]net/software/windows/app-hardware-visualizer](https://www.onworks[.]net/software/windows/app-hardware-visualizer)

[https://sourceforge\[.\]net/projects/sidebar-diagnostics/files/Sidebar%20Diagnostics-3.6.5.zip](https://sourceforge[.]net/projects/sidebar-diagnostics/files/Sidebar%20Diagnostics-3.6.5.zip)

[https://github\[.\]com/PieceHydromancer/Lossless-Scaling-v3.22-Windows-Edition/releases/download/Fps/Lossless.Scaling.v3.22.zip](https://github[.]com/PieceHydromancer/Lossless-Scaling-v3.22-Windows-Edition/releases/download/Fps/Lossless.Scaling.v3.22.zip)

This is only a partial list of malicious URLs. Download the [Malwarebytes Browser Guard plugin](#) for full protection and to block the remaining malicious URLs.