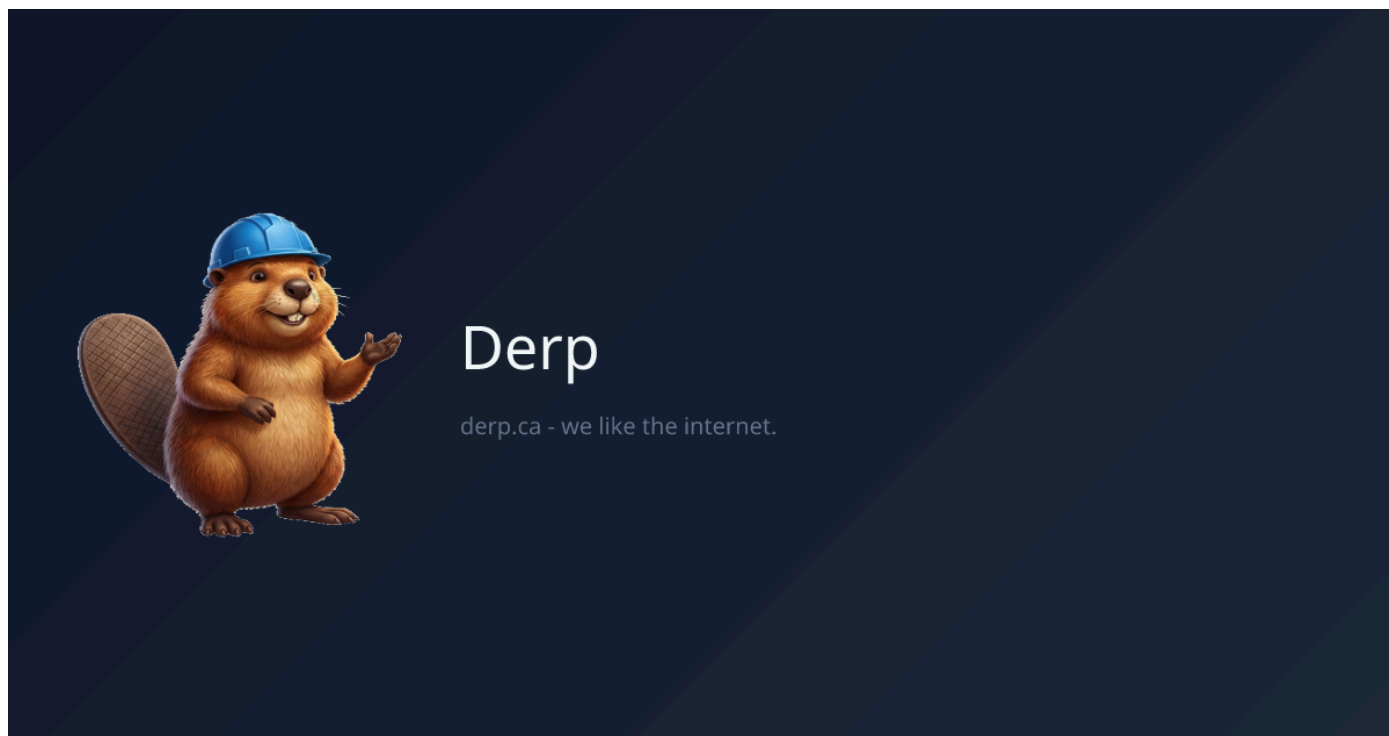


Tranium wiper: static analysis of a Go binary

 derp.ca/research/tranium-wiper-analysis

Kirk

March 10, 2026



malware wiper ransomware go reverse-engineering

Tranium is a 6 MB Go binary that encrypts files with AES-CBC, overwrites the MBR on three physical drives, and corrupts 30+ system files including the registry hives and boot chain. It triggers a Blue Screen of Death and sets the desktop wallpaper to a photo of an American YouTuber. The source file is named `wiper.go`. There are no wallet addresses, no contact email, no `.onion` URL, no payment mechanism of any kind. Every vendor that detects it calls it ransomware.

It is not ransomware. Even if the encryption key could be recovered, the MBR is gone. The boot chain is destroyed, the registry hives are corrupted, and the system files required to start Windows no longer exist. The machine will not boot. This is a wiper.

If you operate a threat intelligence platform with API access and can provide a researcher account, please reach out to . Additional data sources directly increase the quality and coverage of the threat intel published here.

Binary identification

Field	Value
SHA256	06430cf9e0ec9fb5b783db7c01fd59bd651d8877143fc45d2bcd7e4dedaf94a6
MD5	5dc62f4c65df422f1e7a0e691b1a075b
Type	PE32+ GUI executable (x86-64)
Size	6,192,640 bytes (6 MB)
Language	Go 1.26.0
Source file	wiper.go (1,037 lines)
Build path	C:/Users/Admin/Downloads/wiper.go
Dependency	golang.org/x/sys@v0.41.0
Compiler flags	-s -w -H windowsgui (stripped, GUI subsystem)
AV detection	9/76 at time of analysis

Kaspersky detects it as **VH0:Trojan-Ransom.Win32.Agent.gen**. Microsoft calls it **Ransom:Win32/Genasom**. huorong labels it **Ransom/LockFile.mf**. All generic ransomware signatures. No vendor identifies it as a wiper or assigns a family name.

The binary was compiled from a single source file in the Downloads folder with symbols stripped. Go 1.26.0 was released on 2026-02-10, one month before the sample appeared. The **.symtab** section, zeroed PE timestamp, and linker version 3.0 are standard Go compiler markers.

Function map

The main package contains 29 functions named `main.a1` through `main.a29` (no `a21`), plus `main.main`, `main.boxWndProc`, and `main.createMessageBoxClass`. We mapped every function to its behaviour using GoReSym virtual address boundaries and RIP-relative LEA cross-references against the string blob.

`main.main` orchestrates the execution. It prints "Hello Tranium," displays "Where hath your files gone?" in a custom window, includes the string "Good luck.", and calls the 29 functions roughly in sequence. The execution chain is:

```
Mutex check (a1)
-> Defender kill (a2)
-> Shadow copy / recovery destruction (a3)
-> UAC bypass via fodhelper (a4)
-> Persistence: Run/RunOnce keys (a6)
-> Persistence: startup folder (a8)
-> Persistence: scheduled tasks x3 (a9)
-> Persistence: Windows service (a10)
-> Persistence: IFE0 debugger hijack (a11)
-> Persistence: BootExecute (a12)
-> Taskbar hiding (a13)
-> File download: wallpaper + audio (a14)
-> MBR overwrite (a15)
-> Raw disk overwrite, second pass (a16)
-> System file corruption (a17)
-> User directory + system component wipe (a18)
-> Full system lockdown: 16+ policies (a19)
-> Wallpaper and audio setup (a20)
-> Certificate store manipulation (a24, a25)
-> File encryption: AES-CBC via goroutines (a26)
-> Audio playback (a27)
-> BSOD trigger (a28)
-> Final boot cleanup (a29)
```

The ordering matters. Tranium destroys the MBR and corrupts system files *before* it encrypts user data. By the time the encryption goroutines finish, the machine is already unrecoverable. The encryption is a cosmetic layer on top of irreversible destruction.

Encryption

`main.a26` is the encryption orchestrator. It spawns goroutine workers (`main.a26.func1`, 6.1 KB) that perform AES-CBC encryption using Go's `crypto/cipher` stdlib. The AES S-box, inverse S-box, and Rcon tables are present in the `.data` section at their standard offsets.

Key generation uses `crypto/rand` -- the OS CSPRNG. Both `CryptProtectData` and `CryptUnprotectData` are imported, indicating the key is stored via DPAPI. The binary also links decryption routines (`NewCBCDecrypter`, `CryptBlocks`). In theory, the key could be recovered from DPAPI if the user profile is intact.

In practice, the boot chain is destroyed before the user could attempt recovery. The registry hives (`SAM`, `SYSTEM`, `SOFTWARE`, `SECURITY`, `DEFAULT`) that DPAPI depends on are among the files corrupted in `main.a17`.

No file extension for encrypted files was found in the binary. A search for `.tranium`, `.locked`, `.encrypted`, `.enc`, `.crypt`, and other common ransomware extensions returned nothing. Files may be overwritten in place without renaming.

MBR and disk destruction

`main.a15` opens `\\\\.\\PhysicalDrive0`, `\\\\.\\PhysicalDrive1`, and `\\\\.\\PhysicalDrive2` for direct write access, along with raw volume handles `\\\\.\\C:` and `\\\\.\\D:`. The MBR is overwritten on all three drives.

`main.a16` performs a second raw disk overwrite pass on the C: and D: volumes. This is separate from the MBR operation -- it targets the volume data directly.

`main.a29` handles final boot cleanup after everything else has run: `bootmgr`, `ntldr`, `pagefile.sys`, and `hiberfil.sys`.

System file corruption

`main.a17` (4.4 KB) and `main.a18` (5.3 KB) between them target over 30 files and directories:

Boot chain:

bootmgr, bootmgr.efi, BOOTNXT, bootsect.bak
winload.exe, winload.efi, winresume.exe, winresume.efi
bootvid.dll, BCD-Template, boot.ini

System executables:

ntoskrnl.exe, hal.dll, smss.exe, winlogon.exe, wininit.exe

Registry hives:

SAM, SYSTEM, SOFTWARE, SECURITY, DEFAULT

Filesystem and storage drivers:

ntfs.sys, fastfat.sys, partmgr.sys, volmgr.sys, volmgrx.sys

Configuration:

win.ini, system.ini, hosts

User directories (main.a18): Desktop, Documents, Downloads, Favourites, Pictures, Videos, Music, Contacts, Searches, OneDrive, Saved Games, 3D Objects. Also targets system components: [CodeIntegrity](#), [DriverStore](#), [catroot2](#), [dllcache](#), [SysWOW64](#).

The string "Good luck." appears in [main.a17](#).

Recovery destruction

Before any persistence or encryption begins, [main.a3](#) eliminates recovery options:

```
cmd.exe /c wmic shadowcopy delete
cmd.exe /c vssadmin delete shadows /all /quiet
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
cmd.exe /c bcdedit /set {default} recoveryenabled no
```

System Restore is disabled via the `SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore` registry key.

Persistence

Ten mechanisms across six functions:

#	Mechanism	Function	Detail
1	Run key (HKLM)	a6	{D4E5F6A1-B2C3-4D5E-6F7A-8B9C0D1E2F3A} -> Tranium.exe
2	Run key (HKCU)	a6	Same GUID
3	RunOnce key (HKLM)	a6	Same GUID
4	RunOnce key (HKCU)	a6	Same GUID
5	Startup folder	a8	Copies as {E5F6A1B2-C3D4-4E5F-6A7B-8C9D0E1F2A3B}.exe
6	Scheduled task x3	a9	Three nested tasks, every minute, SYSTEM, highest privileges
7	Windows service	a10	sc create {C3D4E5F6-A1B2-4C9D-0E1F-2A3B4C5D6E7F}
8	IFEO debugger hijack	a11	sethc.exe, osk.exe, magnify.exe, narrator.exe, utilman.exe

#	Mechanism	Function	Detail
9	BootExecute	a12	<code>autocheck autochk * Tranium.exe</code> -- runs pre-boot
10	UAC bypass	a4	fodhelper via <code>ms-settings\Shell\Open\command + DelegateExecute</code>

The scheduled task persistence (#6) uses a triple-nesting technique. The outer task creates the middle task, the middle creates the inner, and the inner runs the payload every minute as SYSTEM with highest privileges. Deleting one task leaves the others to recreate it.

The IFEO hijack (#8) replaces the Debugger value for five accessibility tools. Pressing Shift five times at the lock screen, clicking the on-screen keyboard, or launching any of these utilities will execute Tranium instead.

Defence evasion and system lockdown

`main.a2` disables Windows Defender:

```
DisableAntiSpyware = 1
DisableRealtimeMonitoring = 1
DisableBehaviorMonitoring = 1
DisableOnAccessProtection = 1
```

`main.a19` (1.2 KB) applies a full system lockdown via 16+ registry policies:

Policy	Effect
<code>DisableTaskMgr = 1</code>	Blocks Task Manager
<code>DisableRegistryTools = 1</code>	Blocks regedit
<code>DisableCMD = 2</code>	Blocks cmd.exe (batch files allowed)

Policy	Effect
EnableLUA = 0	Disables UAC
ConsentPromptBehaviorAdmin = 0	No elevation prompt
DisableLockWorkstation	Blocks Win+L
DisableChangePassword	Blocks password change
NoRun	Removes Run dialog
NoFind	Removes search
NoControlPanel	Blocks Control Panel
NoClose	Removes shutdown option
NoLogoff	Removes log off
NoSetTaskbar	Blocks taskbar changes
NoFileMenu	Removes file menus
NoFolderOptions	Blocks folder options
NoTrayContextMenu	Disables tray right-click
NoViewContextMenu	Disables explorer right-click

`main.a13` hides the taskbar by calling `FindWindow` on `Shell_TrayWnd`.

Certificate manipulation occurs in `main.a24` and `main.a25` -- certificates are added to both the ROOT and AuthRoot stores.

Wallpaper, audio, and the YouTuber connection

`main.a14` downloads two files from up to four sources:

URL	File
<code>https://autism[.]lat/v73d2.bmp</code>	Wallpaper (primary)
<code>https://autism[.]lat/UPiQj.wav</code>	Audio (primary)
<code>https://file.marafire[.]cc/3months/1773106600_716fdd44_0.bmp</code>	Wallpaper (backup)
<code>https://file.marafire[.]cc/3months/1773106676_5f65a166_0.wav</code>	Audio (backup)
<code>https://biteblob[.]com/Download/gsaqlrX1mH0a5V/#bat.wav</code>	Audio (backup)
<code>https://thegumonmyshoe[.]me/b77/gYKRXBNDVcuBUeNlQGhu.bmp?md5=...&expires=...</code>	Wallpaper (auth-gated)

The wallpaper is a 225x225 BMP -- a selfie photo of **Tranium**, an American YouTuber with 1.3 million subscribers who makes virus testing content. The binary sets this as the desktop wallpaper via `SystemParametersInfo` and the `Control Panel\Desktop\Wallpaper` registry key. The string "Hello Tranium" appears in `main.main`. The malware is named after him.

The audio file (`bat.wav`) is 145.9 seconds of PCM 16-bit stereo at 44100 Hz (24.5 MB). `main.a27` plays it via `PlaySoundW`.

Ransom dialog

`main.createMessageBoxClass` registers a custom window class called `BoxClass` via `RegisterClassExW`. The window procedure `main.boxWndProc` renders a BMP image using `BitBlt` and `StretchBlt`.

No text rendering APIs are present -- `DrawTextW`, `TextOutW`, `BeginPaint`, `CreateFont`, and `SetTextColor` are all absent. The "ransom note" is the downloaded BMP itself, displayed as an image. The text "Where hath your files gone?" appears in the string blob but is not rendered via GDI text functions.

BSOD trigger

`main.a28` calls `RtlAdjustPrivilege` to acquire `SeShutdownPrivilege`, then triggers a Blue Screen of Death via `NtRaiseHardError`. The binary also imports `ExitWindowsEx` and `InitiateSystemShutdownExW` as additional shutdown paths.

Infrastructure

Domain	Notes	
<code>autism[.]lat</code>	Primary file host, behind Cloudflare. Created 2026-02-13.	
<code>thegumonmyshoe[.]me</code>	Wallpaper hosting. Round-robins across <code>91.193.56.10-14</code> (AS207616 Altrosky Technology, Amsterdam). Created 2026-01-03.	
<code>file.marafile[.]cc</code>	Backup file hosting. Generic service.	
<code>biteblob[.]com</code>	Backup file hosting. Generic service.	
IP	ASN	Location
<code>91.193.56.10</code>	AS207616 Altrosky Technology	Amsterdam, NL
<code>91.193.56.11</code>	AS207616 Altrosky Technology	Amsterdam, NL
<code>91.193.56.12</code>	AS207616 Altrosky Technology	Amsterdam, NL

IP	ASN	Location
91.193.56.14	AS207616 Altrosky Technology	Amsterdam, NL
71.179.14.4	AS701 Verizon Business	Bel Air, MD, US (residential FIOS)

All network traffic is HTTPS on port 443. The [thegumonmyshoe.me](#) URL includes an MD5 auth token and epoch expiry (1773117667, approximately 2026-03-07). No C2 channel exists -- these are download-only URLs for the wallpaper and audio files.

The residential Verizon FIOS IP (71.179.14.4) appeared in sandbox network flows.

No related samples were found on any platform. Domain searches, IP searches, tag searches, and GitHub source searches all returned zero results. This appears to be a single build from a single author.

IOC summary

Network

Type	Value	Context
Domain	autism[.]lat	Primary file hosting
Domain	thegumonmyshoe[.]me	Wallpaper hosting
Domain	file.marafire[.]cc	Backup file hosting
Domain	biteblob[.]com	Backup file hosting
IP	91.193.56.10	Altrosky Technology, Amsterdam (thegumonmyshoe.me)
IP	91.193.56.11	Altrosky Technology, Amsterdam

Type	Value	Context
IP	91.193.56.12	Altrosky Technology, Amsterdam (thegumonmyshoe.me)
IP	91.193.56.14	Altrosky Technology, Amsterdam (thegumonmyshoe.me)
IP	71.179.14.4	Verizon FIOS residential, Bel Air MD

Host

Indicator	Value
Mutex	Global\{F9E3B4A1-2D5C-4F8B-9A6E-1C7D3B5A8F2E}
Wallpaper	%TEMP%\1773106600_716fdd44_0.bmp (225x225 YouTuber selfie)
Audio	bat.wav (145.9s PCM)
Window class	BoxClass
Build path	C:/Users/Admin/Downloads/wiper.go

Hashes

Hash	Value
SHA256 (binary)	06430cf9e0ec9fb5b783db7c01fd59bd651d8877143fc45d2bcd7e4dedaf94a6
MD5 (binary)	5dc62f4c65df422f1e7a0e691b1a075b

Hash	Value
SHA1 (binary)	621551552d8ebcf1c5b8e23246726cc589eda56d
Imphash	4e2bd2c481372f7ab13b83b63b424e97
SHA256 (wallpaper)	0fd1cd57e37b3c312ed66c2dda1e9548dfccdf1d8fcf57416b67118e072b38a4
SHA256 (bat.wav)	3bfeaa70b0df65969d5ac7fb2ae6e110fbd3cd2901658ff4ac0cbf8569a2ff38

Registry

Key	Value	Purpose
HKLM\...\Run\{D4E5F6A1-...}	Tranium.exe	Persistence
HKCU\...\Run\{D4E5F6A1-...}	Tranium.exe	Persistence
HKLM\...\RunOnce\{D4E5F6A1-...}	Tranium.exe	Persistence
HKCU\...\RunOnce\{D4E5F6A1-...}	Tranium.exe	Persistence
HKLM\...\IFE0\sethc.exe\Debugger	Tranium.exe	IFE0 hijack
HKLM\...\IFE0\osk.exe\Debugger	Tranium.exe	IFE0 hijack
HKLM\...\IFE0 magnify.exe\Debugger	Tranium.exe	IFE0 hijack
HKLM\...\IFE0\narrator.exe\Debugger	Tranium.exe	IFE0 hijack
HKLM\...\IFE0\utilman.exe\Debugger	Tranium.exe	IFE0 hijack

Key	Value	Purpose
..\Session Manager\BootExecute	autocheck autochk * Tranium.exe	Pre-boot persistence
..\Windows Defender\DisableAntiSpyware	1	Defence evasion
..\Policies\System\EnableLUA	0	UAC disable

Behavioural

Behaviour	Detail
MBR overwrite	\\.\PhysicalDrive0/1/2
Raw disk overwrite	\\.\C:, \\.\D: (two passes)
Shadow copy deletion	wmic + vssadmin
Recovery disabled	bcdedit bootstatuspolicy + recoveryenabled
System Restore disabled	Registry: DisableSR
BSOD trigger	RtlAdjustPrivilege + NtRaiseHardError
Scheduled tasks	3 nested tasks, every minute, SYSTEM
Windows service	sc create with GUID name
Taskbar hidden	FindWindow(Shell_TrayWnd)
Certificate injection	ROOT + AuthRoot store additions

Assessment

Tranium uses AES-CBC encryption with DPAPI key protection, MBR overwriting across three physical drives, raw volume data destruction, and system file corruption targeting the boot chain and registry hives. It adds IFEO debugger hijacking on five accessibility tools, the fodhelper UAC bypass, BootExecute persistence, and a forced BSOD via `NtRaiseHardError`. 10 persistence mechanisms. 16+ lockdown policies.

The source file is named `wiper.go`, compiled from a Downloads folder, with no payment infrastructure. The wallpaper is a photo of a YouTuber who tests malware on camera. 9 of 76 vendors detect it. All of them classify it as ransomware.

A YARA rule (`Tranium_Wiper`) is available at .

See also: [IronChain](#), [GhostWeaver](#).

Kirk

I like the internet. Want to get in touch? ·