Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

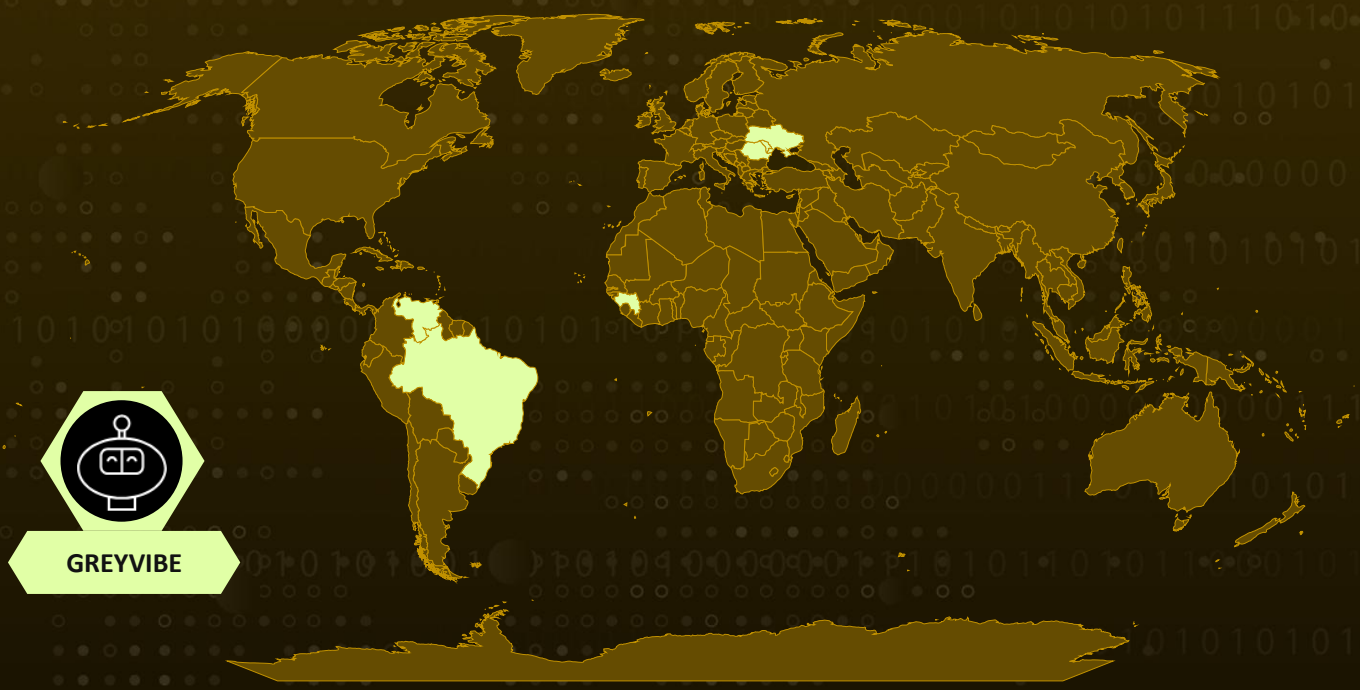
Vibe-Coding the Kill Chain: The GREYVIBE Story

Date of Publication	Admiralty Code	TA Number
June 3, 2026	A1	TA2026153

Summary

Attack Commenced: August 2025
Targeted Regions: Ukraine, Moldova, Romania, Brazil, Venezuela, Guinea
Targeted Platforms: Microsoft Windows, Android
Targeted Products: Web browsers (Chromium-based), Telegram Desktop, WhatsApp Desktop, Remote Desktop Protocol (RDP) targeted during post-compromise activity
Targeted Industries: Military, Government, Defense, Energy, Civilian individuals, NGOs, Business entities, Software supplier
Threat Actor: GREYVIBE
Malware: PhantomRelay (variants: PhantomRelayLite, PhantomRelayV1, PhantomRelayV2), FallSpy, LegionRelay, LOOKVALPS, LOOKVALJS, DAYLIGHT, TEASOUP
Campaigns: PhantomMail, PhantomClick, PrincessClub, DroneLink, Nebo

Actor Map



Actor Details

#1

GREYVIBE is a Russia-nexus group that has targeted Ukraine and Ukraine-related entities since at least August 2025, with development and testing dating back to April 2025. WithSecure assesses with high confidence that its operators are Russian-speaking and work in the Moscow time zone, and its lures, victimology, and objectives align with Russian state interests, chiefly intelligence collection tied to the Russia-Ukraine war.

#2

Initial access runs through five vectors: spear-phishing emails linking to malicious ZIP/RAR archives on Google Drive and 4sync (PhantomMail); ClickFix fake-CAPTCHA pages impersonating Zoom and LAPAS (PhantomClick); fake Ukrainian adult-club sites paired with fake female Telegram personas (PrincessClub); drone-themed fake charity sites (DroneLink); and a Russian-language "SPO NEBO" lure (Nebo).

#3

Every campaign follows the same Windows chain: lure, bundle, loader, payload, decoy. The loader shows a decoy: a PDF, a fake error pop-up, or a lure site while the infection runs silently in the background. The primary Windows payloads are PhantomRelay, a PowerShell RAT using a two-stage fingerprint-then-client model over WebSockets, and LegionRelay, a lightweight PowerShell RAT over a REST API; FallSpy is the Android spyware used in PrincessClub and Nebo.

#4

Payloads are obfuscated with custom obfuscators (LOOKVALPS, LOOKVALJS, DAYLIGHT, TEASOUP), and the PhantomRelayLite base variant adds SAWDUST and CRUDEDUST, which patch AMSI and tamper with the ETW provider. Persistence runs mainly through scheduled tasks driven by a "watchdog" script, with a short-lived Startup folder shortcut variant; PhantomRelay also spreads via USB using hidden files and malicious shortcuts.

#5

Privilege escalation uses shortcut hijacking that fires a UAC prompt from a trusted icon, a CMSTP-based UAC bypass, and a custom .NET component posing as "Windows Update" that baits a UAC approval to re-register LegionRelay's scheduled task as SYSTEM. For lateral movement, operators enable persistent RDP, create hidden local administrator accounts, and share local disks over SMB.

#6

PhantomRelay C2 has rotated across EDIS Global, KVMka, Cloudzy, and the suspected bulletproof host Global Connectivity Solutions LLP, while FallSpy and LegionRelay C2 stayed on Baxet Group Inc. infrastructure with Russian-language admin panels. The defining trait is the systematic use of GenAI/LLMs Ideogram AI, ChatGPT, and Google Gemini for lure imagery and site building, obfuscator/loader and full-stack RAT development, infrastructure setup, and post-compromise scripting.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
GREYVIBE	Russia **MOTIVE** Information theft, and Espionage	Ukraine, Moldova, Romania, Brazil, Venezuela, Guinea	Military, Government, Defense, Energy, Civilian individuals, NGOs, Business entities, Software supplier

Recommendations

Restrict Archive and Script Execution from Email and File-Sharing Links: Treat ZIP/RAR archives delivered via links to Google Drive, 4sync, and similar services as high-risk. Block or sandbox execution of double-extension files (e.g., `.pdf.js`, `.XLS.js`, `.Docx.rar`), and disable or tightly control the Windows Script Host (`wscript.exe`/`cscript.exe`) for JavaScript loaders.

Constrain PowerShell and LOLBIN Abuse: Enable PowerShell Constrained Language Mode, script block and module logging, and transcription. Hunt for `conhost.exe` launched with the `--headless` parameter spawning PowerShell, for `Invoke-Expression` on remotely fetched content, and for command-history suppression (`Set-PSReadlineOption -HistorySaveStyle SaveNothing` and `Remove-Module PSReadline`).

Hunt for Watchdog and Scheduled-Task Persistence: Alert on creation of scheduled tasks that re-execute scripts on short intervals (e.g., one minute after creation, then every three minutes) and on tasks/loaders masquerading as vendor utilities (Razer, AMD, Adobe, "System Health Service," "Windows Check Updater"). Inspect `%ProgramData%` and `%LOCALAPPDATA%` staging directories and Startup folder shortcuts for dropped `.ps1` payloads.

Enforce Strong UAC and Privilege Controls: Set UAC always to prompt, monitor for `cmstp.exe` invoked with custom `.INF` files, watch for unexpected `runas`/`RunAsInvoker` shortcut modifications, and treat sudden "Windows Update"-themed UAC prompts as suspicious. Audit creation of new local administrator accounts and accounts hidden via the `SpecialAccounts\UserList` registry key.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.001: Domains
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
	T1608: Stage Capabilities	T1608.001: Upload Malware
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
		T1566.003: Spearphishing via Service
	T1091: Replication Through Removable Media	
Execution	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
		T1204.004: Malicious Copy and Paste

Tactic	Technique	Sub-technique
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1202: Indirect Command Execution	
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1136: Create Account	T1136.001: Local Account
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
Defense Evasion	T1027: Obfuscated Files or Information	T1027.006: HTML Smuggling

Tactic	Technique	Sub-technique
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1070: Indicator Removal	T1070.003: Clear Command History
	T1497: Virtualization/Sandbox Evasion	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.002: Hidden Users
	T1218: System Binary Proxy Execution	T1218.003: CMSTP
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1480: Execution Guardrails	
Credential Access	T1003: OS Credential Dumping	T1003.002: Security Account Manager
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	

Tactic	Technique	Sub-technique
Credential Access	T1056: Input Capture	T1056.001: Keylogging
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
	T1083: File and Directory Discovery	
	T1016: System Network Configuration Discovery	
	T1518: Software Discovery	
Collection	T1113: Screen Capture	
	T1005: Data from Local System	
	T1119: Automated Collection	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1123: Audio Capture	
	T1125: Video Capture	
	T1636: Protected User Data	T1636.003: Contact List
		T1636.002: Call Log
	T1430: Location Tracking	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.001: Dead Drop Resolver
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1572: Protocol Tunneling	
	T1090: Proxy	
	T1219: Remote Access Software	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1496: Resource Hijacking	T1496.001: Compute Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	476334f9254ef0277b3462b6086655f38358a983b95991cfe4dcdd787740906a, 78773eb9738bc3306a56bf39adc8212226479c24af8bf453be9d57103a91a904, 62b585f36d4b14fa1e036feed692267aa098e7fc6cabb468a07997a025309299, d60dd96ef92b43e2e4f955dd76448fc320c3f8445b661d9a4a3c40caca0aa8a5, 687629ca9dc5b9b4bdf6c06fb1405449638b905f3a0c08bccac1c519ef22964d, 8a7401444dd7c85b36ff7b1d0b36c5953692ef32dbeac7642fb7c1034bd8a726, e81af6ae6862d905d8634a1f6e0a8893ba28e3ce61d12ccac020ef6fae802e8b, 93111e523c38d98247a78a0d1d9ae163e9874acb70721f6fe0bf451c62fff283, c823a315c2c78d2fd345c9b38bb7fc31a8cbff96c534ce9cc66c4e54bc7935a2, 5115eca388860371d994457793f3a3c2c3d106da48ca12ecccb9432522c56cc3, bd3f35b91bf83427e953d4cf531a0ee4b5ec9fc76b91700274effe0eba22510f, 2abb318455960b446d034967c8403ec4339ba248b946f02cb1307ed7e6f4e327, e8d0943042e34a37ae8d79aeb4f9a2fa07b4a37955af2b0cc0e232b79c2e72f3, 42464c188cb8116b63938b3236504ec4ae31c7cadb9063085b30dd468d88860f, 7ac06aaf0cdc1c1f0f14b0e8ccc550f9df20e79f3ce321207ec7a1867d6227ef, f79b9d14b93d4c509386684f2aeebe53ab088e704b38b359db3ee7991942aec6, 08eba15964cae61156a99d7ac33eedebdd6e9f3465dc77b5d8dc17dbedc2194a, 18db95f2ae20a4ea86b3296f409eb3fc1131d2758c5bfdbda16a424a64e97d18, e9634032df81334e9e960ab8b88ff05a0f7ec9c034dc012f816f09e23c18d41b, 40f9399ea067d69c0985aecdc54beddbcb585d7f660606e5bb4be981811c28ba,

TYPE	VALUE
SHA256	f8fd89b4d0d2608dbdf6e79282b7dc3fa3bef9b199a0dd02f15660cd02c73361, 5e6c5b6604d88f044bff53b6576f7b15046baa666fa72bafe62069a8b9e9452f, 48a371a3973983a9bdb395cb33d6fce68d75b41d4bfd86d3f923cff79b545efc, f56170fc141e2fce7449a01af9bda7b22b8909b6c8eaf698e5a149e3da75eeac, 1b916c486ec621fb66bd4521dddad5df69bd35c4b76a980c0b924babf566cb84, cbaf6cdb2acbd293d7e58cabe41449027a28b84223ba88f19e4463ec4176dad0, bcb9e99021f88b9720a667d737a3ddd7d5b9f963ac3cae6d26e74701e406dcdc, 87b8abb05c7ee5642a5e801e7825dfa5ee4c1393ac998e87470ab53cc75e1842, b189b6099e6ad190fd67e0dfa41f0adf29f75bb46d541dce6d4d4c632b58d42f, e1f86fe0d103979da38a2be7fe3bf1d3eb63c5b60b5b952e02334559396a72b6, a1a67fbceac6b3b840893e375da5c449d0dacb22b4a914c5ff9827d42c991758, c9dfd29fba3eb8a3325faea0be46c41dfe2b44cdee94ae65658c4b0a9b85ffc7, db1776cc96cb89c3bb39314363ae8476fea3421877214f362005d1ed59574c10, d9810fa6aa59864ceef509ed551da85fce31d69cfcd78f2f8b146c761387370e, 4e6f85802d365751fa25c7014002ae44329a2d037d7b21f4bc34091b0c01b7b7, 07d9deaace25d90fc91b31849dfc12b2fc3ac5ca90e317cfa165fe1d3553eead, 7db11cf6a0417d5e20cd6720687ba86045b2fb758a7b585a49f572df2dc40c5e, a695a70c2efd11e1daa93997c1aaf976a205476839f553f2c8e64fb73123b853, 920e8a8e06a1559ba0b4a1be5f6c290ed8e305fd130675ceadc655c79c1cb369, db05db462a0e8ba40c656dd0b8bd11f6fdc85895b54904df1dc83bb0609e2ff2, ee144c883784c635ef84e0ae6a12b03553c1fd65646621f22d08511bd3e6d42a,

TYPE	VALUE
SHA256	03beb07ce116a2a69f360dd3fab8c3aa55bb42ce580d43f1924642874e388efe, c716dabe228f89e58835d2c93dbaa5719dc77f62c9e84f3e3d54ef82ded621e1, 286de17c2e8017241bee12b0935ed5e1e5d5216f4311be781ca1a69ad81188b3, d814564ab8b905c3b9b7a42e757228d9d30f8ffd4fa6b3c48f4aa7e2b1e44594, b0c07b265c9d9046038ffa48d5b8e17b8ba0791503beba85196cdbe0ac2fcb27, 63047083db26ec6a8aa2d0d008ca4c067855a952a89f9e3e878b2215e26841cf, ee87fae14e3cc64d894f0a677af8832f8669f11853374c18b7110df1fc52f4e5, 1d69523a20b9c1180bba6a2cc9959d555e2ee9e78440fd79cfbaf31ad35a09fc, eb2c32b3d1aed95266b0b75704d4570b37b2d77e6c5d8401122ef4daf762f186, 0005c16f04ce7d5a1a9966069f4a291de5506e77490926d7fb177efa677fe588, ccc7f039e1afd55fe8bc767ae688e71e66f162aba0c0d1650face02f15e9c7d0, 908619929db75b0d2592ba6fb0a65be6c894592907c83f664f3b130108d98d6a, e67a883595e95d357f92c2ab6cd34d4708e5ee711861c59192d9c23d7d20d0c7, 1e20e95b351a5bd26a3dcf1ead8cab133e3e473d2912b6e2ff285a09e855b60f, 2a18935e758d6a0f5bc5ebb8e43da0d1fb0cb57f7be5ab7eb050e82a51bdc5b5, bc43504669966b0add6e4ec12022626126b80b8ee8d57ae95a953ee74d8df702, 35f3f1ead293ecc14ab03c96b0505c444b6cd0e7a48b4d099b53c8fe91cafc5e, 51b92c81a44f5d242519032c56601d3ee3f5699112d8fbf40323b825dfa9feda, e8ff33344b9aef15df02e03f4a5d8459b520d18011e39c179e19c629171122a5, 26d1a616b9332c34f1884ed000751833a9d9d17fb737e637636bf4acb4339a22, dec9c0213e1259c5aa5f86f6fef2c73e87c6a2c01773e2e99b8e1a0dd2eb149f, d63cdac3e3623ae3072393f33a658537af71ded3109aacb3006f45cc7c94de05,

TYPE	VALUE
SHA256	9e443d773df5adf0ab9e622bb8179ce899f46b2166f2faa09d54a4622a9ac5cc, 296932373f9c54fcf4eb285f81a17b1b93c5a96e5ff6dfa097b4d8c4b8f53b81, 89e052bd182df8de5960784c663f962d44e058c8920a437f54ab75d03a7da3bd, 9b7008c43814c7bf18375774bd2ed5f3bda9316dbef20b7e086fe921838f1186
Domains	lapas[.]live, zoomconference[.]click, zoomconference[.]app, strip-mens[.]tilda[.]ws, princess-mens[.]fun, princess-mens-club[.]com, princess-mens[.]click, princessclub[.]click, princessclub[.]best, princessclub[.]online, princessclub[.]cyou, clubprincess[.]click, frontforce[.]org, ukrguard[.]org, ukrbezpeka[.]online, ironbrave[.]online, ukrvarta[.]online, edbo[.]linkpc[.]net, edbo[.]publicvm[.]com, edbo[.]work[.]gd, dsszzi[.]linkpc[.]net, declaration[.]linkpc[.]net, goodhillsenterprise[.]com, ny-car-dealership[.]it[.]com, doct0rsim[.]com, routinesyscheckup[.]com, serotoninenterprise[.]com, newstarcommunity[.]com, jackscommunications[.]com, fasterscommunications[.]com, bsnowcommunications[.]com, highfleetenterprise[.]com, flyskyenterprise[.]com, newsolutionsxsenterprise[.]icu, nycpartnersenterprise[.]com, chiselworksenterprise[.]com, newrentalsenterprise[.]com,

TYPE	VALUE
Domains	bluelagoonaenterprise[.]com, heltaskeltahenterprise[.]com, neuromancersolutionsenterprise[.]icu, newequipmentsolutions[.]com, j4jobspk[.]com, aerobionix[.]com, prosearium[.]net, saidozdemir[.]com, tucsonanimalallergy[.]com, halungroup[.]com, khanvas[.]com, maxolutions243[.]com, thirdmetrics[.]com, resutato[.]com, red-viper[.]com, emballeplus[.]com, meadowsantiques[.]com, seahorsemethod[.]com, intrawld[.]com, emovietheater[.]com, robotic-toys[.]com, kentfiresafe[.]com, artsselection[.]com, zeftasarim[.]com, xpertlearninghub[.]com
Email	centrenergo[.]ukr[@]gmail[.]com, centrenergo[.]ua[@]gmail[.]com, office[.]dsns[.]dp[@]gmail[.]com, kanc[.]kh[.]dsns[@]gmail[.]com, office[.]cip[.]ua[.]gov[@]gmail[.]com, office[.]gov[.]cips[@]gmail[.]com
FileNames	форма акта перевірки.XLS.js, форма акта перевірки територій.rar, матеріали конференції з кіберзахисту_pdf.exe, пріоритетні теми співпраці.exe, зразок заявки на отримання фінансової підтримки.Docx.rar, Заявка на забезпечення.rar, SysCheckupService.ps1, SystemHealthSvc.ps1, Configuration.ps1, Configurate.ps1, WUDFHost.ps1, razer_update.log, RzUpdateManager.ps1, RzTelemetry.ps1

TYPE	VALUE
File Paths	%ProgramData%\WindowSystem, %ProgramData%\Microsoft Windows, C:\ProgramData\AMD\amd.ps1, C:\ProgramData\BackUp\backup.ps1, C:\ProgramData\Adobe\dfDgrr3.ps1
IPv4	188[.]124[.]59[.]120, 193[.]233[.]23[.]81
IPv4:Port	89[.]37[.]185[.]60[:]14000, 74[.]112[.]102[.]120[:]14000, 194[.]87[.]128[.]243[:]8000, 194[.]87[.]108[.]110[:]8000, 89[.]125[.]189[.]118[:]8000, 89[.]125[.]189[.]85[:]8000, 91[.]149[.]221[.]124[:]8000
Scheduled task name	System Health Service, Microsoft System Health Service, Razer Synapse Service Helper, Adobe working, BackUp checker, AMD Checker
Staging directory	%LOCALAPPDATA%\Razer Update
URLs	hxxps[:]//storage[.]vlasiuk[.]kiev[.]ua/SW90D0qhta/матеріали_конференції[.]zip, hxxps[:]//share[.]secureinfo[.]eu/get/ypMXMG58xH/Матеріали_конференції_доп[.]zip, hxxps[:]//www[.]4sync[.]com/web/directDownload/tcqtmocL/MyE7HPqt[.]11b47e3a02edac898638b1906774210d, hxxps[:]//drive[.]google[.]com/file/d/1RDXHPZtCzOXn6GN7UidXPo4qqZOA_UGd, hxxps[:]//drive[.]google[.]com/file/d/12ffiBTWHm6GW8chJNIXuOeALPI82VnNs, hxxps[:]//drive[.]google[.]com/file/d/1wkgvtTw_g5CvK84rWiHCr6HPZZb_OeKd, hxxps[:]//drive[.]google[.]com/file/d/1aSIXJgZUT7AQEp5B_D7gyHRq74EFUxoz, t[.]me/s/sdgsersergser
Usernames	vikagogogo111, nastyaa2001lov, lilymihalyk

References

https://www.withsecure.com/en/resources-hub/w-labs/greyvibe/

https://www.withsecure.com/content/dam/labs/docs/WithSecure_GREYVIBE.pdf

https://github.com/WithSecureLabs/iocs/blob/master/GREYVIBE/greyvibe_iocs.csv

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 3, 2026 • 11:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com