Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

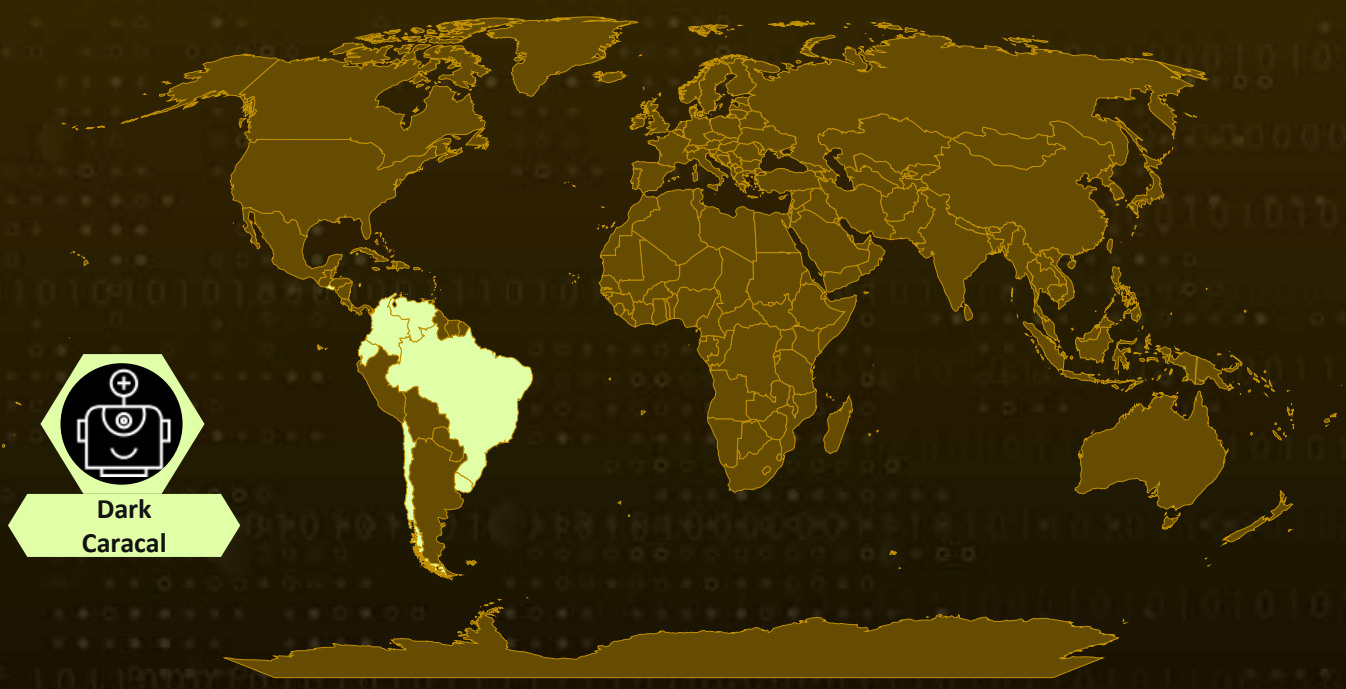
# Dark Caracal Modernizes Its Espionage Toolkit

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 27, 2026 | A1 | TA2026250 |

# Summary

**First Seen:** January 2026
**Targeted Regions:** Venezuela, Brazil, Ecuador, Chile, Colombia, El Salvador, Uruguay
**Targeted Platform:** Windows
**Targeted Products:** Google Chrome, Brave, Mozilla Firefox
**Targeted Industries:** Communications, Government, Military, Businesses, Journalists, Activists, Legal, Healthcare, Educational institutions
**Threat Actor:** Dark Caracal (aka ATK 27, TAG-CT3)
**Malware:** GoCaracal, Bandook, Delphi loader
**Attack:** Dark Caracal, a cyberespionage group associated with Lebanon's General Directorate of General Security, has introduced a previously undocumented modular framework written in Go, tracked as GoCaracal. The framework was uncovered during a June 2026 investigation into a targeted intrusion at a Venezuelan communications organization, where it was deployed alongside an updated Bandook variant. Delivery relied on the group's established ecosystem of Spanish-language financial and tax-themed lures, weaponized SVG files, URL shorteners, and document-themed hosting infrastructure.

## Attack Regions



# Attack Details

**#1**

In June 2026, a targeted intrusion at a communications organization in Venezuela recovered a previously undocumented modular framework written in Go, tracked as GoCaracal. The activity is assessed with medium confidence to belong to Dark Caracal, a cyberespionage group linked to Lebanon's General Directorate of General Security that has been active since at least 2012 against governments, businesses, journalists, and activists.

**#2**

GoCaracal was found alongside an updated variant of Bandook, the group's long-standing Windows remote access trojan, and analysis of 249 related samples shows the framework exists in two build profiles drawn from one shared architecture: a lightweight implant for access and payload delivery, and an extended build for sustained control and intelligence collection. No code-level evidence indicates that GoCaracal succeeds AsioGate, the C++ backdoor reported in the February 2026 Dark Caracal campaign, and nothing suggests it replaces Bandook. The two families currently operate in parallel.

**#3**

Dark Caracal gained access to the Venezuelan organization through the same delivery ecosystem it has used across its Latin American operations. The original phishing email and SVG attachment were not recovered, but the financial and tax-themed filename of the recovered artifact, the group's established delivery pattern, and more than one hundred related SVG files communicating with the same malicious hosting site support the assessment that the file arrived by phishing.

**#4**

The lightweight build establishes command-and-control using a custom packet protocol protected by AES-GCM encryption. During initialization, it collects user, hostname, operating system, uptime, active window, and installed security product data, then makes that profile available for registration with the C2 server. In this intrusion, the implant was followed by a Delphi loader carrying Bandook and an extended GoCaracal build, confirming the lightweight profile as a foothold rather than a final payload. The development timeline runs from core communications and host profiling in January 2026, through modularization and antivirus discovery between February and April, to broad post-compromise capability in May and June and blockchain-based C2 resilience between June and July.

**#5**

Once the extended build is resident, the operator has the pieces needed to expand inside the environment. Host discovery covers system profiling, process enumeration, drive discovery, directory listing, and recursive file search. Credential access comes from keylogging and from collection of browser cookie and login databases, with the parallel Bandook sample adding credential theft from Chrome, Brave, and Firefox. An in-band SOCKS5 proxy tunnels operator traffic through the compromised host, and remote interaction is available through WebRTC-based desktop access, hidden virtual network computing behavior, and cloning of a local Chrome profile into a separate concealed browser session. Privilege escalation, exploitation of domain infrastructure, and confirmed movement to additional hosts are not described in available reporting, so lateral movement beyond proxied operator access remains unreported.

**#6**

Collected files, browser data, and keystrokes returned over the same encrypted protocol used for tasking, and no separate exfiltration channel was identified. Twenty-four unique C2 addresses were extracted from GoCaracal samples; twenty-three were hosted on AEZA Group networks, while Bandook C2 addresses sat on AlexHost, a provider previously tied to Dark Caracal. That separation limits the damage a single infrastructure takedown can do to the wider operation. Resilience is reinforced by an Ethereum fallback: alongside primary HOST and PORT values, the extended configuration can hold a CONTRACT address, and after repeated failures to reach the primary server the implant issues an eth_getStorageAt request to a public Ethereum JSON-RPC endpoint and reads a stored value from that contract. If the value resolves to a valid address, the implant rewrites its in-memory configuration and retries.

# Recommendations

**Treat inbound SVG attachments as executable content:** Quarantine or strip SVG files arriving by email, since the delivery chain depends on script and link content embedded inside an image format that most users and many filters treat as benign. Where SVG is a business requirement, inspect the file body for Base64 blobs and redirect URLs before delivery.

**Block the URL shortener redirect path:** Block or force interstitial inspection on URL-shortening and redirector services at the web proxy. The chain routes the victim from the SVG through a shortened URL and an intermediate redirector before reaching the payload host, so interrupting the middle hop stops the download without needing to know the final domain.

**Alert on concealed NTUSER.MAN and Run-key changes:** Monitor for creation of a hidden NTUSER.MAN file and for registry hive modifications associated with Run-key persistence. This artifact pair is distinctive to the extended build and is one of the few high-fidelity persistence signals available.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Resource Development | T1583: Acquire Infrastructure | T1583.001: Domains |
| | | T1583.003: Virtual Private Server |
| | T1608: Stage Capabilities | T1608.001: Upload Malware |
| Initial Access | T1566: Phishing | T1566.001: Spearphishing Attachment |
| Execution | T1204: User Execution | T1204.002: Malicious File |
| | T1059: Command and Scripting Interpreter | T1059.003: Windows Command Shell |
| Persistence | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| Defense Evasion | T1112: Modify Registry | |
| | T1055: Process Injection | |
| | T1027: Obfuscated Files or Information | |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1564: Hide Artifacts | T1564.001: Hidden Files and Directories |
| | T1070: Indicator Removal | T1070.004: File Deletion |
| | T1036: Masquerading | T1036.005: Match Legitimate Name or Location |
| Credential Access | T1555: Credentials from Password Stores | T1555.003: Credentials from Web Browsers |
| | T1539: Steal Web Session Cookie | |
| | T1056: Input Capture | T1056.001: Keylogging |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Discovery | T1082: System Information Discovery | |
| | T1057: Process Discovery | |
| | T1083: File and Directory Discovery | |
| | T1518: Software Discovery | T1518.001: Security Software Discovery |
| | T1010: Application Window Discovery | |
| Collection | T1005: Data from Local System | |
| Command and Control | T1105: Ingress Tool Transfer | |
| | T1573: Encrypted Channel | T1573.001: Symmetric Cryptography |
| | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1102: Web Service | T1102.001: Dead Drop Resolver |
| | T1090: Proxy | T1090.001: Internal Proxy |
| | T1219: Remote Access Tools | T1219.002: Remote Desktop Software |
| Exfiltration | T1041: Exfiltration Over C2 Channel | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 1e499c815146124c4a6d2b48c99068b980ad74e1a2cfd16013f8d75a9425a0ca, 77f7ad29f4a8037ee5f38d3d87fb91cfd97cb8f7fa7883edf3fce506df5200c0, 8c03d072df2e1bf14b0c00a8ab99834138c8b69f301849bf09cb44394e916015, 0a6da70548f14834acb8960689a589b48ff422f8385ae445a281aab77045fe22, a2cdf2fe741de4b13ad2298b387a6c32da4a94da180ae75bf8547386aee7376b, c9da1b08a39491dfdbede6ff4c1a2d383f57cb29e2d3532aee08d6e0a5c1dda6 |
| Domains | getpdfdigital[.]cloud, getpdf[.]digital, visualizarpdf[.]online, contabilidad[.]icu, soportedigital[.]cloud, documentodigital[.]cloud, gestionadocs[.]me |
| IPv4 | 109[.]120[.]187[.]217, 109[.]172[.]95[.]121, 138[.]124[.]112[.]213, 138[.]124[.]14[.]130, 176[.]124[.]220[.]153, 185[.]125[.]101[.]181, 185[.]96[.]80[.]110, 185[.]96[.]80[.]54, 193[.]233[.]245[.]52, 193[.]233[.]245[.]45, 193[.]233[.]245[.]0, 62[.]60[.]237[.]22, 77[.]110[.]104[.]98, 77[.]110[.]105[.]244, 77[.]110[.]105[.]56, 77[.]110[.]105[.]59, 77[.]110[.]98[.]66 |

| TYPE | VALUE |
|---|---|
| IPv4 | 80[.]71[.]224[.]30,<br>82[.]117[.]87[.]138,<br>82[.]117[.]87[.]192,<br>85[.]192[.]30[.]211,<br>79[.]137[.]192[.]38,<br>46[.]226[.]162[.]68,<br>45[.]152[.]198[.]108,<br>91[.]208[.]197[.]80,<br>91[.]208[.]184[.]45,<br>91[.]208[.]206[.]88,<br>91[.]208[.]184[.]130,<br>176[.]123[.]1[.]174 |
| Filenames | TF-OFICINA004A9.exe,<br>VRJDL_21812.exe,<br>7676230602QQ.exe,<br>NTUSER.MAN |
| File Paths | %AppData%\Roaming\d30547514515\91ed375e.exe,<br>%AppData%\Roaming\e1d58f51c58a\5c0416e4.exe |
| HTTP Request | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) |
| Ethereum Contract Address | 0x03D605f13A74Bfb6149078122FcF62BD6d8799d8,<br>0x04aB453494381E60171BE04Ea6BE6E7C44EafAfd,<br>0xD7635f31620772882a6712472a6278c53247Bc44,<br>0xf165F26300BF65DFaC78BC9557326bDbB3C6d33C |
| Ethereum Wallet Address | 0x7D321FE277f8c25aaC14aF1BA3Fc34953242052F |

## References

https://arcticwolf.com/resources/blog/dark-caracal-reloaded-new-malware-same-hunting-grounds/

# 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

**August 27, 2026 • 06:00 AM**



More at www.hivepro.com