Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

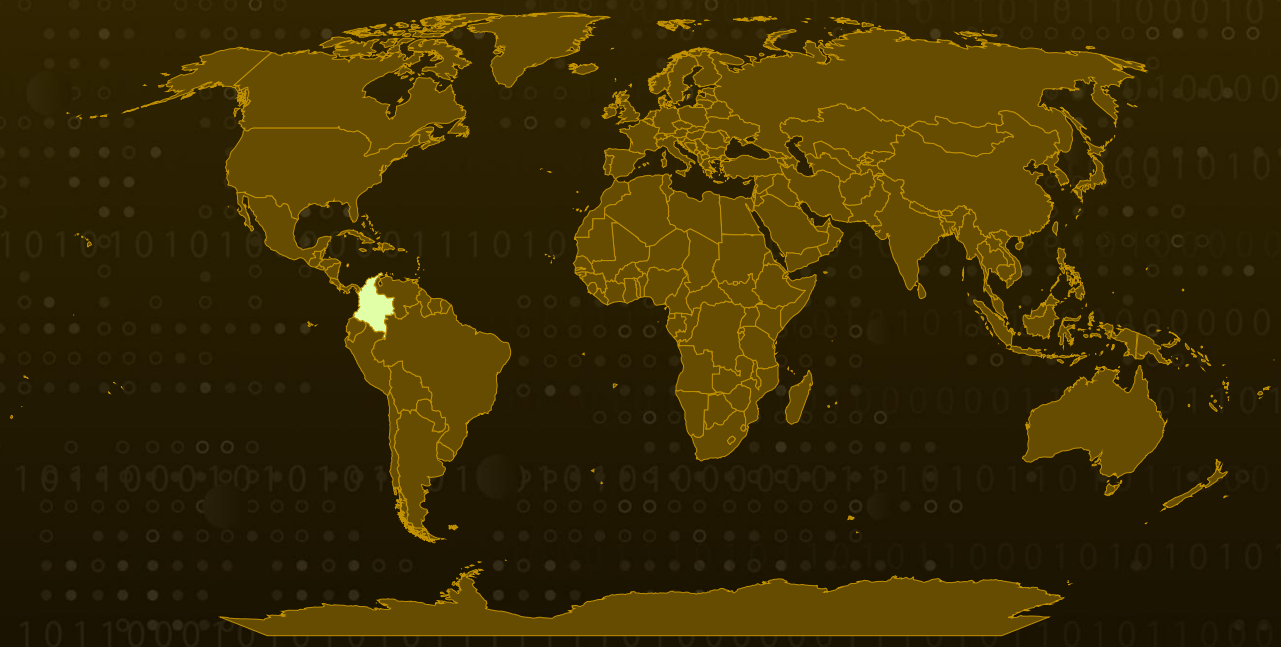
Hijackloader Strikes Colombia with PureHVNC

Date of Publication	Admiralty Code	TA Number
October 30, 2025	A1	TA2025333

Summary

Attack Discovered: August and October 2025
Targeted Country: Colombia
Affected Platform: Windows
Malware: Hijackloader, PureHVNC
Attack: A new phishing wave sweeping through Colombia has weaponized trust in authority, disguising itself as official communication from the Attorney General's office to trick users into downloading supposed legal documents. Behind these convincingly crafted emails lies Hijackloader, a stealthy malware loader that executes a complex, multi-stage infection chain to deploy the PureHVNC remote-access tool. This marks a troubling shift, as PureHVNC and Hijackloader, previously unseen in Latin America, converge in a campaign that blends social engineering, technical sophistication, and regional targeting to infiltrate unsuspecting victims with alarming precision.

Attack Regions



Attack Details

#1 Between August and October 2025, a convincing phishing campaign targeted people in Colombia by impersonating the Attorney General's office and promising official legal documents. Recipients received an SVG hosted on Google Drive that either failed to preview with a "Couldn't preview file" message or presented a download button leading to a password-protected ZIP. When victims extracted the archive and ran the included executable (after entering the supplied password), it launched Hijackloader, a flexible loader that then fetched follow-on tools, most notably PureHVNC, a remote-access tool commonly traded on underground forums and Telegram channels.

#2 The attackers rely on DLL side-loading to make the malicious program look like a legitimate application. A genuine executable is renamed so Windows' DLL search order causes it to load a tampered JLI.dll; that program then calls MSTH7EN.dll via LoadLibraryW(), which boots the second stage and hands control to the core payload while preserving the appearance of a normal process. This trick lets the malware run under the cover of an otherwise benign binary and avoids immediate suspicion.

#3 In the second stage, the malware takes steps to avoid detection and assemble its runtime components. It dynamically resolves and loads libraries, checks the working directory, and parses an encrypted artifact (observed as Plagkeg.zk) into marked chunks. After validating those chunks, it reconstructs decryption keys, applies a simple XOR routine, and uses LZNT1 decompression to rebuild executable shellcode. That shellcode is injected into a legitimate module, vssapi.dll in the sample, by changing memory protections and redirecting execution into the in-memory payload.

#4 The final stage, dubbed ti64, is a modular framework capable of hosting up to 40 discrete modules; the analyzed sample contained 35. Each module has a focused role, from code execution and persistence to information gathering. The campaign completes by performing another DLL hollowing step (targeting pla.dll) to place and run shellcode from the selected ti64 module, delivering a full-featured foothold for the attackers and enabling remote control or data theft.

#5 Hijackloader is engineered for stealth and survival. Its privilege escalation component (modUAC) either calls runas or abuses the CMSTPLUA COM interface to bypass User Account Control. For evasion, it uses stack-spoofing and indirect API calls to hide the true source of sensitive calls; newer variants instead load a legitimate DLL and patch a random offset with TinyCallProxy64 shellcode to invoke monitored APIs before restoring original bytes. It also compares the in-memory .text of ntdll.dll against a clean copy and patches any hooks it finds. For persistence the loader can create startup shortcuts, install scheduled tasks via modTask, or read PERSDATA configuration to reestablish tasks after reboot, all measures designed to keep the implant active and hard to remove. The blend of human-oriented deception and technical sophistication makes these operations especially dangerous.

Recommendations

- **Be Cautious With Unexpected Emails:** Do not open attachments or click on links in emails that claim to be from government offices or legal authorities, especially if they involve lawsuits or urgent requests. Always verify the sender through official channels.
- **Avoid Downloading Password-protected ZIP Files:** Cybercriminals often use these to hide malware. If you receive such a file unexpectedly, do not open it or enter the password provided in the email.
- **Use Trusted Document-sharing Platforms Carefully:** Even links to Google Drive or similar platforms can be malicious. Check the file type before downloading anything and avoid running executable (.exe) files from unknown sources.
- **Regularly Update Windows and Software:** Applying security patches reduces the risk of DLL side-loading and other exploit techniques used in these attacks.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0011** Command and Control	**T1566** Phishing	**T1566.001** Spearphishing Attachment
T1566.002 Spearphishing Link	**T1574** Hijack Execution Flow	**T1574.001** DLL	**T1055** Process Injection
T1055.012 Process Hollowing	**T1106** Native API	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1548 Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task

T1497 Virtualization/Sandbox Evasion	**T1036** Masquerading	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1204 User Execution	**T1204.002** Malicious File	**T1497.001** System Checks	**T1059** Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	troquelesmyj[@]gmail.com
Domains	nuevos777[.]duckdns[.]org, 7octubredc[.]duckdns[.]org, dckis13[.]duckdns[.]org, dckis7[.]duckdns[.]org enviopago[.]mysynology[.]net, maximo26[.]duckdns[.]org, sofiavergara[.]duckdns[.]org
URLs	hxxps[:]//drive[.]google[.]com/file/d/1haApB_GMwZb83nw1YPdIDTLMtksRjkh/view?pli=1, hxxps[:]//drive[.]google[.]com/file/d/1wzunPhL33jq_ZQug6k03hgxi4Eu57VfN/view?usp=sharing
SHA256	e7120d45ee357f30cb602c0d93ed8d366f4b11c251c2a3cd4753c5508c3b15e5, 7e641024054591928135414 48c8fbadc481997a2065f26c848f1e3594ca404c9, 14becb3a9663128543e1868d09611bd30a2b64c655dfb407a727a7f2d0fb8b7e, 57c49cff3e71bc75641c78a5a72d8509007a18032510f607c042053c9d280511, 7c3d9ad3f1bd890e3552dc67093e161395d4e1fab79ec745220af1e19a279722, ce42377d3d26853fd1718f69341c0631208138490decc8e71a5622df5e9e1f59, a0e4979b4e4a706286438d48f0e21b0d92cc7bd40c1c3ea5b9872089aaec0124,

TYPE	VALUE
SHA256	6d93a486e077858b75eb814e9a7bda181189d5833adce7cec75775cfda03f514, bdca9849d7263d508b7ed4dbbf86bd628932b117b45933cb28a7e78171d05cdd, 1ae61edf35127264d329b7c0e2bddb7077e34cc5f9417de86ab6d2d65bad4b4f, 2ec31a8a36d73fa8354a7ac0c39506dbe12638a0dc1b900f57620b8d53ae987f, 776bbaa44c7788e0ccd5945d583de9473b6246c44906692cb0a52e6329cb213a, 9e9997b54da0c633ffcf0a4fb94e67b482cf7a89522d1b254778d0c6c22c70ee, b2f733b67f1ef06d9e5ce76d3cc848f6e7e3ec2d0c363c76d5175c6cf85f979b, c93e70d20ba2948a6a8a013df68e5c4d14d59e5f549417d1a76833bd1c8efd22, d550a2a327394148c0c3d05df2fe0156783fc313b4038e454f9aa2cb2f0f2090, e668ca17fcdfa818aac35f12064d10a0288d7d9c6b688966b695125b760567d6, fe6d0ee45a70359008b2916e5116c411a955978b5694cc457683ab7b26590e47, 977f2f18ff13c93406c5702f83c04a9412760e02028aefc7c1cb7d6f2797a9b5, 768ca38878c5bb15650343ce49292315a9834eaf62fad14422d52510c3787228, 47245b7d2d8cb6b92308deb80399e0273193d5bca39da85a6b2a87a109d18d85, 4484b0ac51536890301a0e6573b962e069e31abc4c0c6f0f6fc1bf66bf588a93, 0113d9f3d93069a29458b3b4c33610aae03961014df60a9e859f3104086d886a, 22d474e729d600dcd84ce139f6208ce3e3390693afa7b52b0615174fca6d0fe2, 2cbfc482e27a2240a48d2fb6f6f740ff0f08598f83ae643a507c6f12a865dc28, 96ee786c5b6167c0f0f770efbace25e97d61e127ef7f58a879b6cf4b57e202c3, 33d0c63777882c9ec514be062612a56fdb1f291fcb6676c49480d3cd4501c508, afecefa6d9bd1e6d1c92144209eda320e1fe0f196ffa8e8bc114e7d3a25503f6, 85641c8fb94e8e4c5202152dcbb2bb26646529290d984988ecb72e18d63c9bc5, 1bf3a1cf9bc7eded0b8994d44cf2b801bf12bc72dc23fb337ddd3a64ac235782

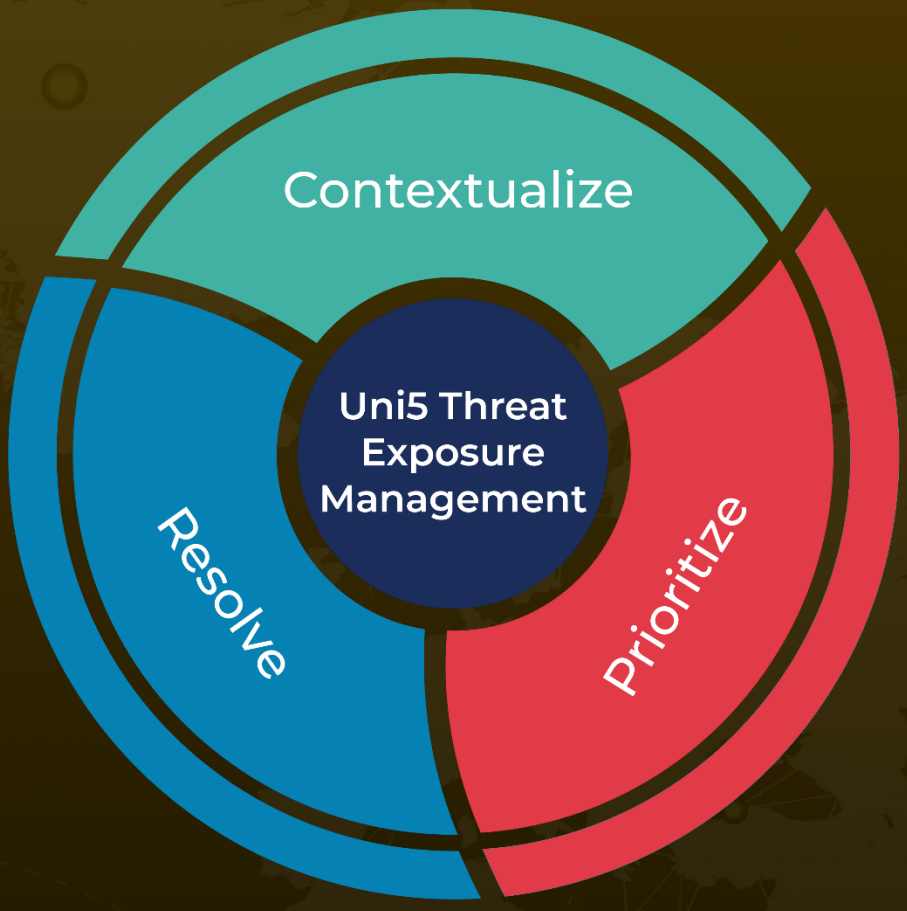
References

https://www.ibm.com/think/x-force/latam-baited-into-delivery-of-purehvnc

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 30, 2025 . 7:30 AM

More at www.hivepro.com