Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

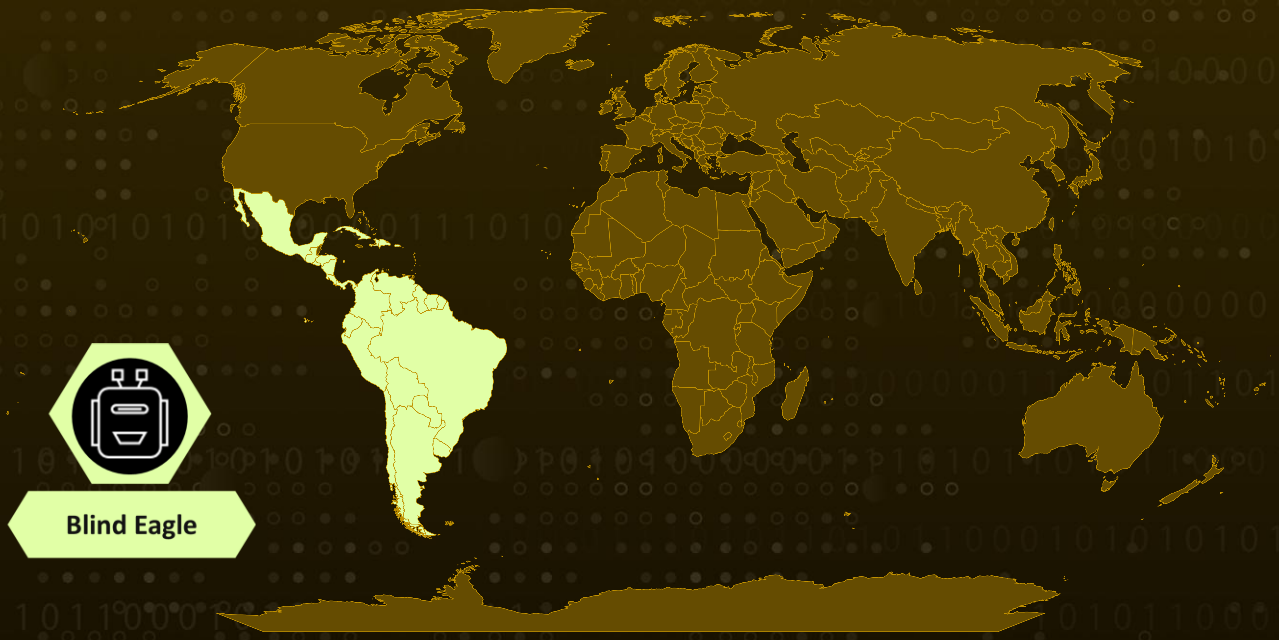
Blind Eagle’s Banking Trap: Phishing Colombia’s Financial Sector

Date of Publication	Admiralty Code	TA Number
July 2, 2025	A1	TA2025204

Summary

Attack Commenced: August 2024
Targeted Countries: Latin America
Targeted Industries: Financial institutions
Malware: Remcos, AsyncRAT
Actor: Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)
Attack: A cybercriminal group known as Blind Eagle has been running a crafty phishing campaign across Latin America, targeting users with fake emails that appear to come from trusted banks. These messages trick people into downloading malicious scripts hidden inside innocent-looking files. Once opened, the malware acts as a doorway, giving attackers control over the victim's computer through remote access tools like Remcos or AsyncRAT. What's striking is how open and sloppy the infrastructure is the attackers' reused domains, left directories exposed, and used basic obfuscation, proving that even low-effort setups can lead to serious breaches when phishing is done right.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 Blind Eagle has been uncovered operating through infrastructure linked to Proton66, leveraging a tightly connected network of domains and IPs to distribute malware. The campaign is initiated via phishing emails delivering obfuscated Visual Basic Script (VBS) files, which act as loaders for commodity remote access trojans (RATs) such as Remcos and AsyncRAT. Many of the domains registered as recently as mid-2024, follow a consistent naming scheme and resolve to IP addresses within Proton66's netblock, underscoring the organized nature of the operation.

#2 The group's infrastructure is built using low-cost yet evasive methods like free Dynamic DNS hosting, open directories exposing identical malware samples, and phishing pages masquerading as login portals for major Colombian banks, including Bancolombia, BBVA, Banco Caja Social, and Davivienda. These fraudulent pages are designed to harvest credentials and financial information. The VBS loaders are often protected using Vbs-Crypter, a commercial crypter service employed to evade static detection mechanisms.

#3 The infection chain decodes Base64-encoded strings, downloads and renames the payload, and launches a RAT that communicates with a Brazilian Portuguese-language botnet management panel. This backend provides attackers with the ability to exfiltrate data, monitor infected systems, and execute remote commands. Despite targeting high-value sectors, Blind Eagle's operational security appears minimal, evidenced by reused SSL certificates, overlapping domains, and shared infrastructure favoring speed and accessibility over stealth.

#4 This ongoing campaign exemplifies how relatively simple infrastructure, combined with localized social engineering, can enable large-scale compromise. Organizations in Latin America's financial sector are strongly advised to remain vigilant. Measures such as advanced email filtering, training employees to identify region-specific phishing tactics, and proactively tracking can significantly reduce risk exposure.

Recommendations

Be cautious with emails, especially those related to banking or taxes: Blind Eagle often sends phishing emails that look like messages from real banks or government agencies. If something feels off, don't click. Verify through official channels.

Monitor for unusual script activity: These attackers often rely on Visual Basic Scripts (VBS). Flag any unexpected script execution, especially those triggered from email attachments or unknown sources.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0010 Exfiltration	TA0011 Command and Control
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059.001 PowerShell
T1656 Impersonation	T1027 Obfuscated Files or Information	T1011 Exfiltration Over Other Network Medium	T1140 Deobfuscate/Decode Files or Information
T1053 Scheduled Task/Job	T1078 Valid Accounts	T1588 Obtain Capabilities	T1588.004 Digital Certificates
T1552 Unsecured Credentials	T1132 Data Encoding	T1132.001 Standard Encoding	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	testedark.writesthisblog[.]com, drgost.duckdns[.]org, asynpro.duckdns[.]org, dxpam.duckdns[.]org, driveswindows[.]duckdns[.]org, vm130833[.]goodtec[.]cloud
IPv4	159[.]148[.]88[.]218, 209[.]105[.]248[.]135, 107[.]172[.]31[.]5, 181[.]206[.]158[.]190, 45[.]135[.]232[.]38
SHA256	a99224d6aeda3dca01b79000cd51babd9f03edfbb78d3aea680d4bc07f6baaaa, a9c86b2ebd29ad0de8f5810a10b6f673a4cf9f2e72de0dc348dea6569624ab78, 187d9bc5bfcc597cdc63e450c1629216b6eaab80fbcee0fc45ebf7b7d6dc01bb, e71ff8bba14a0f6b8fd38341585580f0937c9fd8dd37faedbf9dc1cf49519590, b682e9964d89eb1bcfb3d1996c982b00d1a66ccaf9f8549689b39e7cd06f1d1a, a666a99f2056082802f459f7180f891582a527324a16d34b4755ed63e5467882, a15e5ddeb79251a97b724208b2fe45f5e0f9364eef02db5fdc151130755b5562, 811df06858d30da6c5b74117b2e95c6c12a013cf8156bf00dd15c67732a0350d, 378c1adf5107a507cae88c2b24ddd0bb18a46fca7ab561025e2bd582e67decd5, b519225636c9edb22746ed2c6d49bf1cccc4ae2bfdf933cd79af7ca69840ff7e, a399576c65029c88eba5440603afff4d977f288da66418131884b39aa428977d, dc7aa3d3e0d75d6e7a5169716635a1e69e19df828d849f8363be3195b29ea7e3, 394908cbe5ba04a3b772ef11ea6a2c6a0c8d3d9689c89ccd1410aaa583bb07d7,

TYPE	VALUE
SHA256	48ee878fefc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0, 2e432426a7a0a10a0068c035368f749c298e1ef1add61e31a8b25da74676fcaa, 2a84f9440f120edd032eddb4b61339ee184743d47805e2ed50572ca4905c1fdd, 66663cf3596b0e6fd2721d81f91cda058ca61feb46f9943ef1a91fec7a68590d, 666f0c305b0a6cc558192918bc144c3119d898c33656101395140d93e9e10e69, fa32ea24d1a6041be009ad0c59ce61f3d00e0588700c709c0222ecd8c8c3753, 81ffcabc8db8db4f42ee4d53f35d47e5cca9aba8fadf972a97596b79492cb03, 5cf4a8c83f8591950c24c8b5d79c5464e4cb1b608fc61775f605d6a3503c73c3, 1728133a5a75adc097d2b5dee5693c5b1b72d25832435213bada40be433b2f75

References

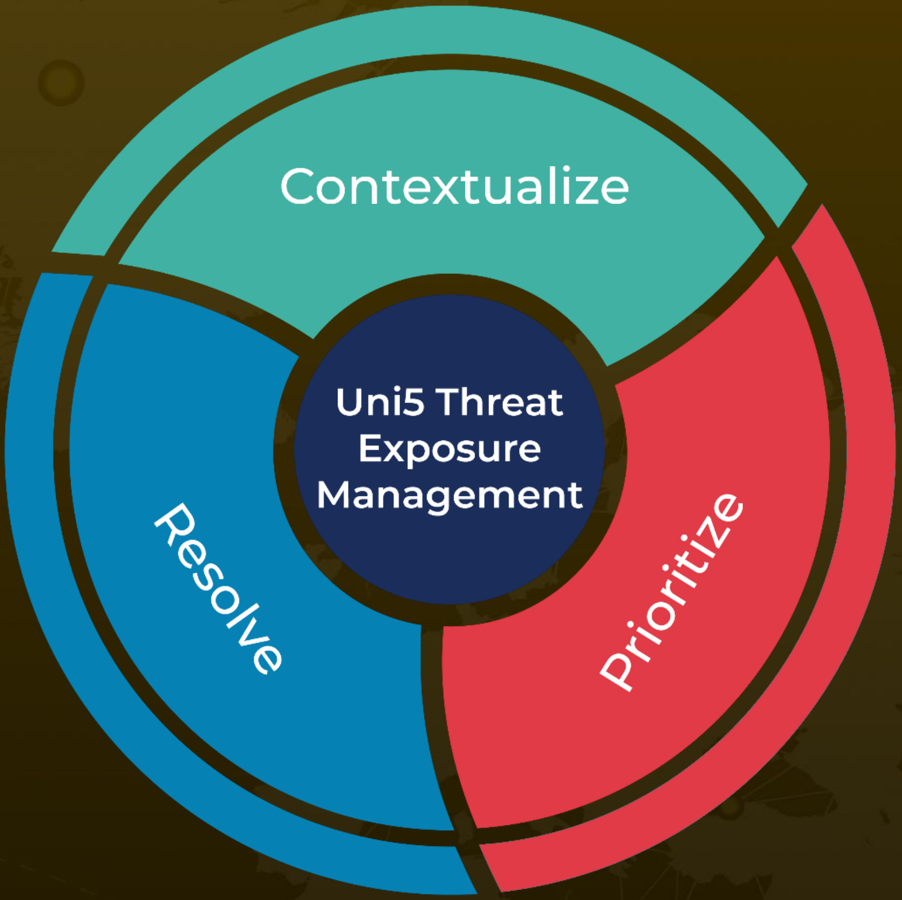
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracing-blind-eagle-to-proton66/

https://hivepro.com/threat-advisory/blind-eagle-cyber-reign-striking-before-you-can-blink/

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

July 2, 2025 • 11:30 PM

More at www.hivepro.com