APT-C-36

[/ˌeɪ piː ˈtiː siː ˈθɜːrti sɪks/]

APT-C-36 (Blind Eagle / Blind Spider) is a Colombia-linked cyber-espionage group active since 2018, conducting phishing and credential theft against government and financial sectors in Latin America. It has evolved from basic phishing to modular post-compromise tools and improved operational security, mainly targeting Colombia, Ecuador, and Peru.

IDENTITY

Attribution	: Suspected Colombian or Latin American threat actor with espionage and financial motives.
Active Since	: ~2018
Aliases	: TAG-144, Blind Eagle, Blind Spider
Motivation	: Intelligence collection and financial theft targeting public and private sector entities across Latin America.

TTPs

Initial Access	: Spearphishing with weaponized PDFs or ZIP files; lures impersonating government tax agencies, customs authorities, or telecoms.
Persistence	: Scheduled tasks, malicious PowerShell scripts, and use of legitimate remote-management tools.
Command & Control (C2)	: HTTPS-based channels; use of commercial VPNs, dynamic DNS, and cloud services.
Malware & Tools	: AsyncRAT, QuasarRAT, njRAT, BitRAT; custom droppers for information theft and remote access.
Techniques	: Credential harvesting, system reconnaissance, and exfiltration of documents from compromised government and financial networks.

TARGET PROFILE

Primary Sectors	: Government, Finance, Telecommunications, Education, Energy.
Geographic Focus	: Colombia, Ecuador, Peru, with additional activity in Chile and Spain.

THREAT ASSESSMENT

Risk Level	: High (Regional)
Recent Activity	: 2025 campaigns delivering phishing emails with embedded links leading to credential-stealing payloads.
Evolution	: Increasing operational security and diversification of infrastructure; adoption of off-the-shelf RATs for scalability and stealth.

NOTABLE OPERATIONS

- **2023 – Tax Authority Phishing:** Impersonated Colombian DIAN to harvest credentials and deploy AsyncRAT.
- **2024 – Financial Institution Breach:** Used fake government communication to compromise internal networks of South American banks.
- **2025 – Public Sector Espionage:** Conducted spearphishing campaign against Colombian ministries using PowerShell loaders and encrypted C2 channels.