


Blind Eagle - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:40:12 UTC

APT group: Blind Eagle

Names	Blind Eagle (<i>Qihoo 360</i>) APT-C-36 (<i>Qihoo 360</i>) AguilaCiega (?) APT-Q-98 (?) G0099 (<i>MITRE</i>)	
Country	 Colombia	
Motivation	Information theft and espionage , Financial crime	
First seen	2018	
Description	<p>(Qihoo 360) Since April 2018, an APT group (Blind Eagle, APT-C-36) suspected coming from South America carried out continuous targeted attacks against Colombian government institutions as well as important corporations in financial sector, petroleum industry, professional manufacturing, etc.</p> <p>Till this moment, 360 Threat Intelligence Center captured 29 bait documents, 62 Trojan samples and multiple related malicious domains in total. Attackers are targeting Windows platform and aiming at government institutions as well as big companies in Colombia.</p>	
Observed	Sectors: Education , Energy , Financial , Government , Healthcare , Manufacturing , Transportation and large domestic companies and multinational corporation branches. Countries: Chile , Colombia , Ecuador , Panama , Spain , USA .	
Tools used	AsyncRAT , BitRAT , BlotchyQuasar , Imminent Monitor RAT , njRAT , LimeRAT , RemcosRAT , Warzone RAT .	
Operations performed	Sep 2021	APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs < https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html >
	2022	BlindEagle Targeting Ecuador With Sharpened Tools < https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-

	<p>with-sharpened-tools/></p>
Feb 2023	<p>Blind Eagle Deploys Fake UAE Files and Fociety to Target Colombia's Judiciary, Financial, Public, and Law Enforcement Entities</p> <p><https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia></p>
Mar 2023	<p>BlindEagle flying high in Latin America</p> <p><https://securelist.com/blindeagle-apt/113414/></p>
Jul 2023	<p>Blind Eagle's North American Journey</p> <p><https://www.esentire.com/blog/blind-eagles-north-american-journey></p>
Jun 2024	<p>BlindEagle Targets Colombian Insurance Sector with BlotchyQuasar</p> <p><https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar></p>
Nov 2024	<p>The Growing Danger of Blind Eagle: One of Latin America's Most Dangerous Cyber Criminal Groups Targets Colombia</p> <p><https://blog.checkpoint.com/research/the-growing-danger-of-blind-eagle-one-of-latin-americas-most-dangerous-cyber-criminal-groups-targets-colombia/></p>
Information	<p><https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/></p> <p><https://threatmon.io/apt-blind-eagles-malware-arsenal-technical-analysis/></p> <p><https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracing-blind-eagle-to-proton66/></p>
MITRE ATT&CK	<p><https://attack.mitre.org/groups/G0099/></p>

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=1421d8ca-9aff-4245-8ee4-cdf72c4c65c5