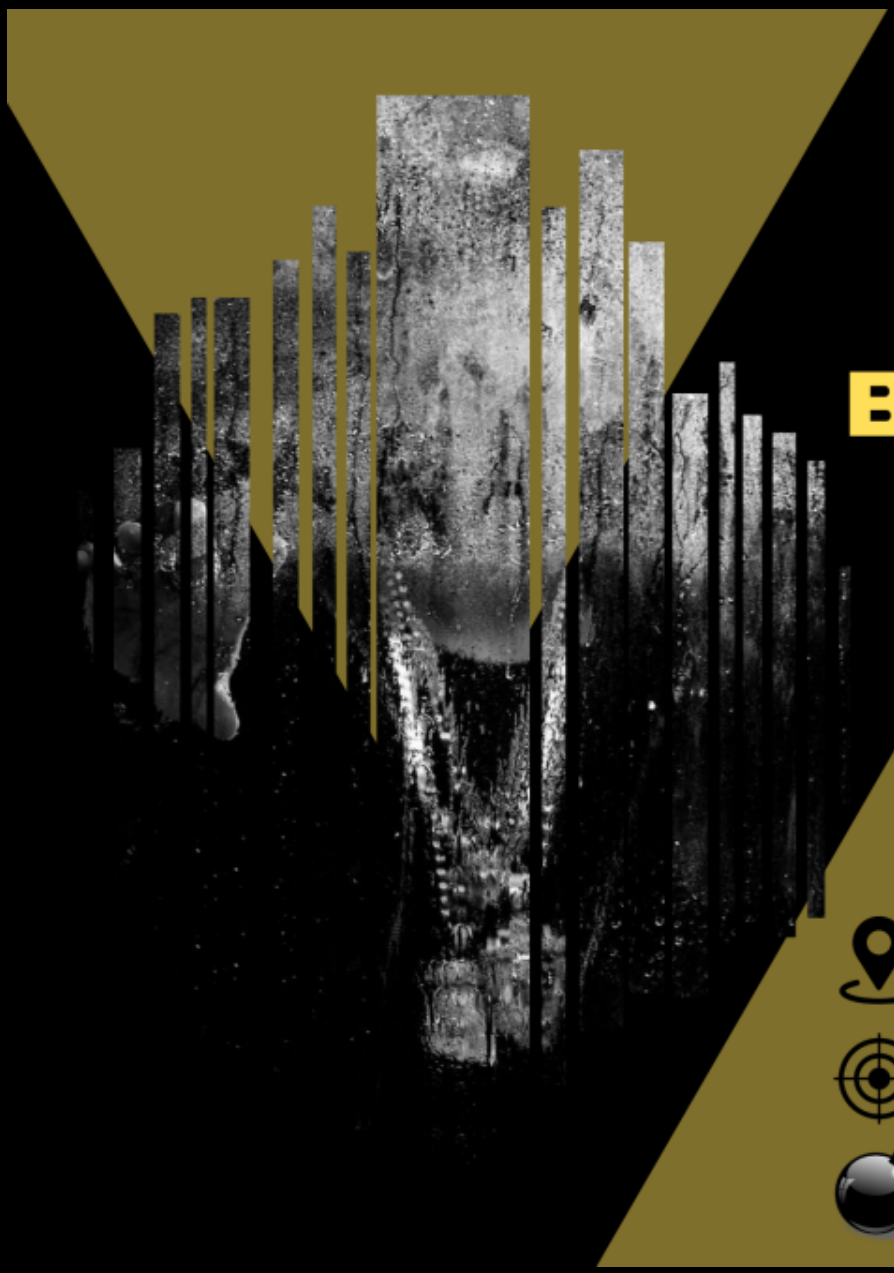
APT C-36



AXIAL

APT C-36
BLIND EAGLE

SOUTH AMERICA

COLUMBIA

LIMERAT

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT C-36 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT C-36 is a threat group based out of South America focused on information theft and espionage.

II. TARGETS

The targets of this threat group has been focused on Financial, Government and large domestic companies and multinational corporation branches of Colombia.

III. METHODS USED

This group has been using tools like Imminent Monitor RAT , LimeRAT against its targets.

IV. CAMPAIGNS

This group has been involved in sophisticated attacks on Colombian Government institutions as well as important corporations in financial sector, petroleum industry, and manufacturing.

ATTRIBUTION

This threat actor is a state sponsored threat group based out of South America, and its targets are only focused on big comapnies in Colombia.

V. IOCS

Hashes , Network & IPs

To be added

VI. REFRENCES

https://malpedia.caad.fkie.fraunhofer.de/actor/apt-c-36
https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Blind%20Eagle