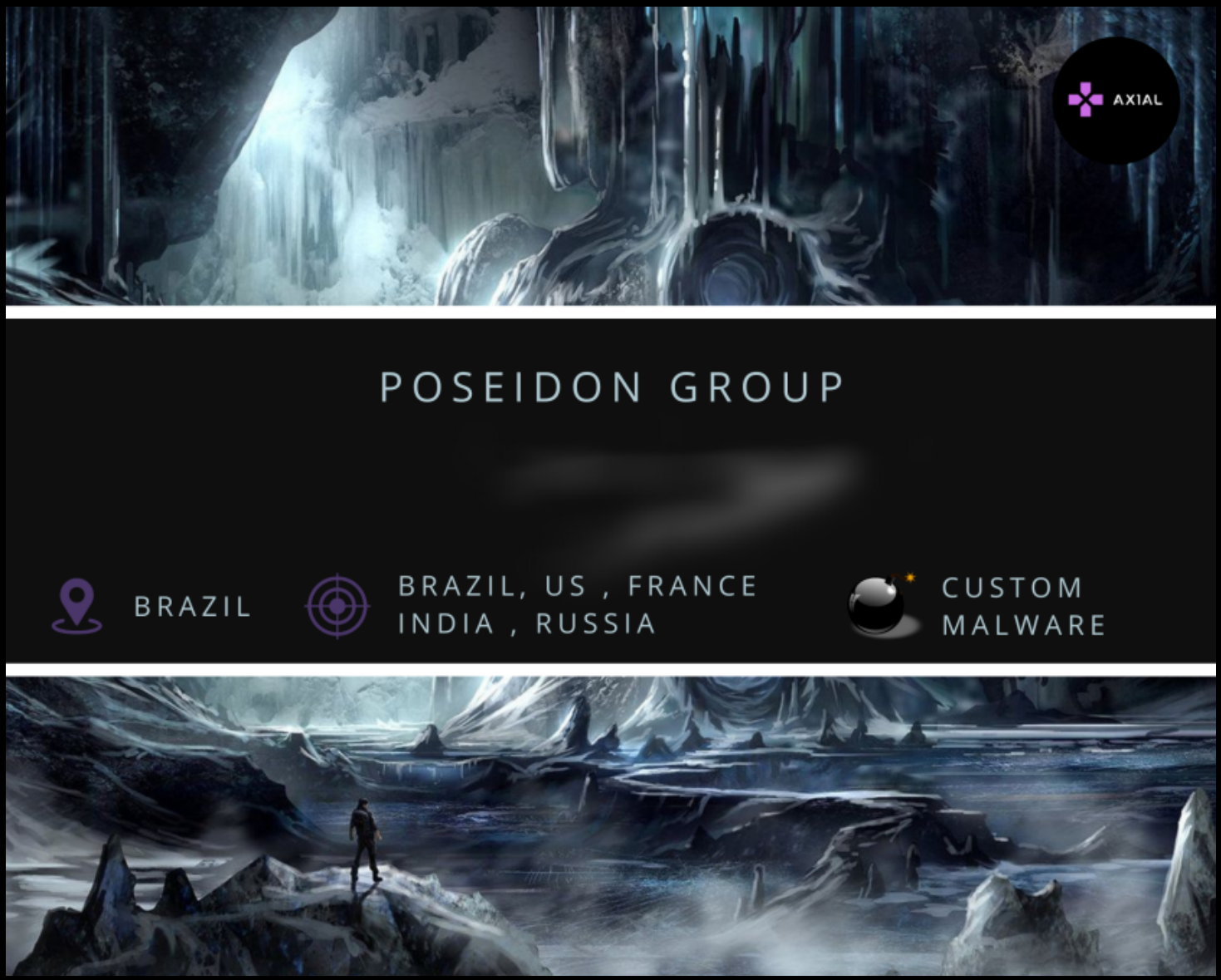
POSEIDON GROUP



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON POSEIDON GROUP ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Poseidon group is a threat group which is attributed to Brazil , they are motivated towards information theft and espionage.

II. TARGETS

Energy, Financial, Government, Media, Manufacturing, Telecommunications, Utilities.

III. METHODS USED

Poseidon group aggressively collects information through spear phishing packaged with embedded , executable elements inside office documents and extensive lateral movement tools.

Poseidon group uses exfiltration methods which include hijacked satelite connections .
Poseidon group uses IGT(Information Gathering toolkit) tool which is coded in Delphi .

IV. CAMPAIGNS

The campaigns of this threat group hbas been attributed to multiple countries involving critical sectors like energy onto various countries like Brazil , France , India along with other countries like the US.

ATTRIBUTION

Poseidon group is attributed to being a commercial threat players also language code used to compile implants, as well as the language used to describe certain commands used by the group, actually corresponds to Portuguese from Brazil. The inclusion of Portuguese language strings and preference for Portuguese systems is prominent throughout the samples.

[cited from Volexity]

AX1AL

V. IOCS

Hashes

2ce818518ca5fd03cbacb26173aa60ce
f3499a9d9ce3de5dc10de3d7831d0938
0a870c900e6db25a0e0a65b8545656d4
2fd8bb121a048e7c9e29040f9a9a6eee
4cc1b23daaaac6bf94f99f309854ea10
2c4aeacd3f7b587c599c2c4b5c1475da
f821eb4be9840feaf77983eb7d55e5f6
2ce818518ca5fd03cbacb26173aa60ce

C2

akamaihub[.]com
igdata[.]net
mozillacdn[.]com
msupdatecdn[.]com
sslverification[.]net

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Poseidon%20Group

https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

AXIAL