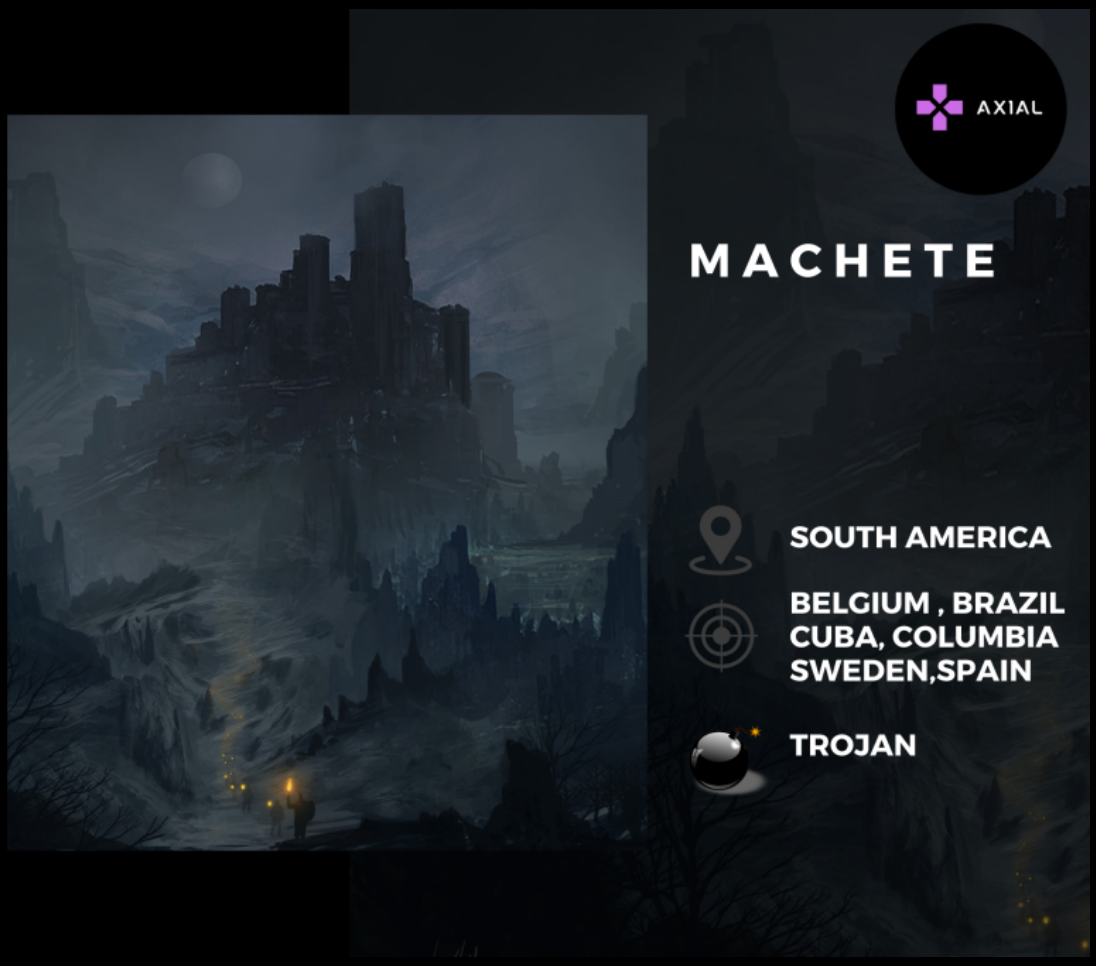
MACHETE



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON MACHETE: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

The group has been active since 2010 and hit military organizations and other high-profile targets worldwide. Since the beginning of 2019, the group is focusing on Venezuela, according to the experts, it is still very active at the time of the publication of the report. Experts noticed the group regularly upgrade the malware in its arsenal and its infrastructure.

II. TARGETS

Governments and Military Organizations at Venezuala & Colombia

III. METHODS USED

- This group is known for it's Python-based toolset also known as machete that was detected by Kaspersky and Cylance .
- Machete cyberespionage group hits victim with effetive spear phising techniques that changes from target to target .
- These emails contain either a link to, or an attachment of, a compressed self-extracting archive that runs the malware and opens a document that serves as a decoy

.

AXIAL

IV. ATTRIBUTIONS

Various artifacts that we have seen in Machete's code and the underlying infrastructure lead to the researchers at ESET think that this is a Spanish-Speaking group.

[Cited from ESET]

VII. IOCS

Some Powerpoint attachments :

Hermosa XXX.pps.rar
Suntzu.rar
El arte de la guerra.rar
Hot brazilian XXX.rar

Domains :

java.serveblog.net
agaliarept.com
frejabe.com
grannegral.com
plushbr.com
xmailliwx.com
blogwhereyou.com

Infection artifacts:

61d33dc5b257a18eb6514e473c1495fe
AwgXuBV31pGV.eXe

b5ada760476ba9a815ca56f12a11d557
EL ARTE DE LA GUERRA.exe

d6c112d951cb48cab37e5d7ebed2420b
Hermosa XXX.rar

df2889df7ac209e7b696733aa6b52af5
Hermosa XXX.pps.rar

e486eddffd13bed33e68d6d8d4052270
Hermosa XXX.pps.rar

e9b2499b92279669a09fef798af7f45b
Suntzu.rar

f7e23b876fc887052ac8e2558f0d6c38
Hot Brazilian XXX.rar

b26d1aec219ce45b2e80769368310471
Signed_Update.jar

V. REFERENCES

1. www.malpedia.com
2. www.attack.mitre.org
3. www.securelist.com