Dec 14 2023

NETMANAGEIT

Intelligence Report

Kaspersky crimeware report: FakeSG, Akira and AMOS

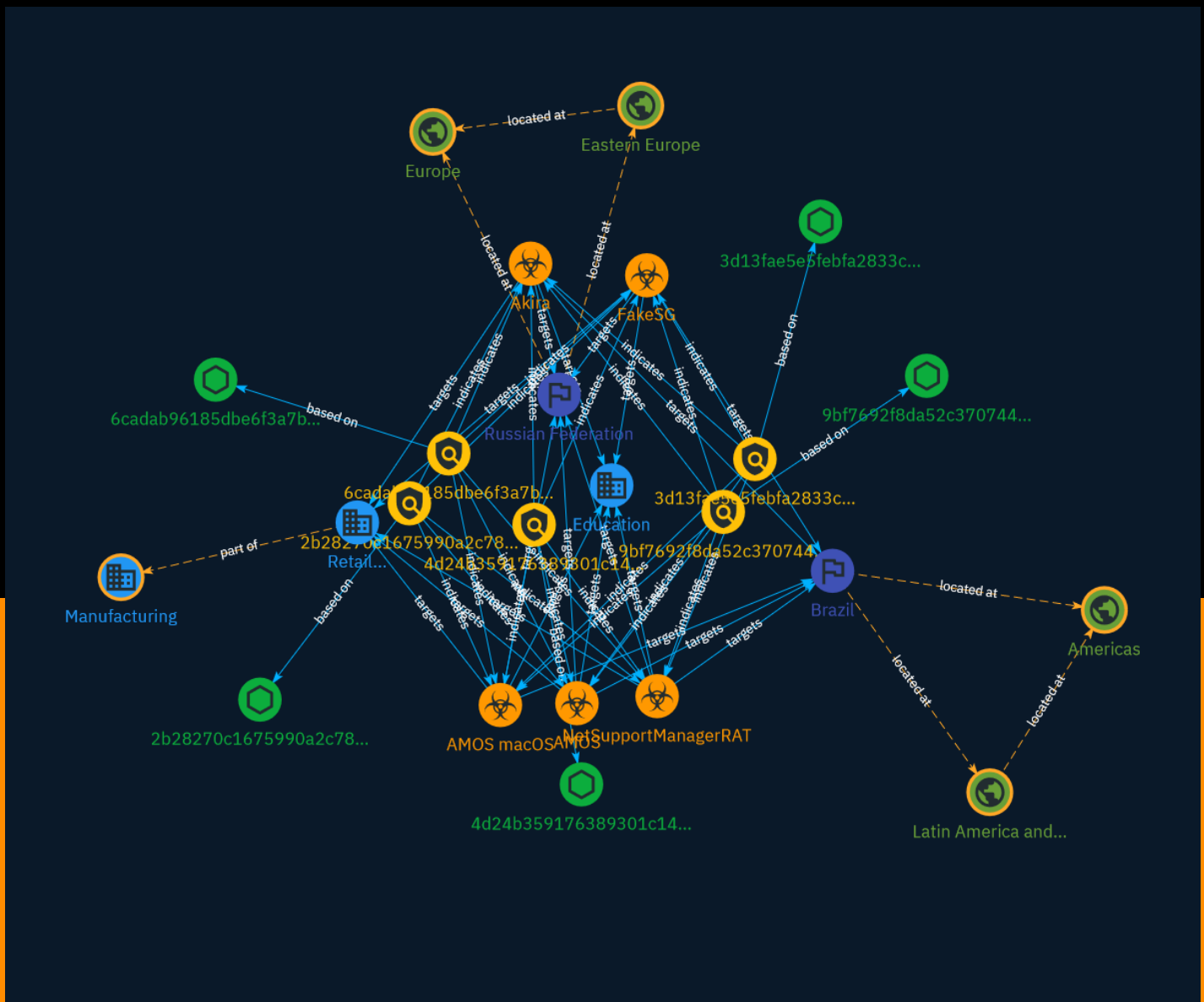

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Sector 6
- Indicator 7
- Country 10
- Region 11
- Malware 12

Observables

- StixFile 13

External References

- External References 14

Overview

Description

Kaspersky has published a series of reports on new cross-platform ransomware, malware distribution campaigns and the AMOS stealer, which it describes as the “FakeSG” campaign.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Retail (distribution)
Description
Distribution and sale of goods directly to the consumer.

Indicator

Name
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
Description
stack_string SHA256 of 0885b3153e61caa56117770247be0444
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360']
Name
9bf7692f8da52c3707447deb345b5645050de16acf917ae3ba325ea4e5913b37
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '9bf7692f8da52c3707447deb345b5645050de16acf917ae3ba325ea4e5913b37']

Name

2b28270c1675990a2c78b31faab547fb75948dd1c2b22e892377ee5e40abebc2

Description

stack_string SHA256 of 2cda932f5a9dafb0a328d0f9788bd89c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b28270c1675990a2c78b31faab547fb75948dd1c2b22e892377ee5e40abebc2']

Name

3d13fae5e5febfa2833ce89ea1446607e8282a2699aafd3c8416ed085266e06f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d13fae5e5febfa2833ce89ea1446607e8282a2699aafd3c8416ed085266e06f']

Name

4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87

Description

SHA256 of c60ac6a6e6e582ab0ecb1fdbd607705b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87']

Country

Name
Brazil

Name
Russian Federation

Region

Name
Europe
Name
Eastern Europe
Name
Americas
Name
Latin America and the Caribbean

Malware

Name
AMOS
Name
Akira
Name
NetSupportManagerRAT
Name
AMOS macOS
Name
FakeSG

StixFile

Value
3d13fae5e5febfa2833ce89ea1446607e8282a2699aafd3c8416ed085266e06f
4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87
9bf7692f8da52c3707447deb345b5645050de16acf917ae3ba325ea4e5913b37
2b28270c1675990a2c78b31faab547fb75948dd1c2b22e892377ee5e40abebc2
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360

External References

- https://otx.alienvault.com/pulse/657b34f330a288e473f448c0
- https://securelist.com/crimeware-report-fakesg-akira-amos/111483/