Mar 26 2024

NETMANAGEIT

Intelligence Report

Agenda Ransomware Propagates to vCenters and ESXi via Custom PowerShell Script

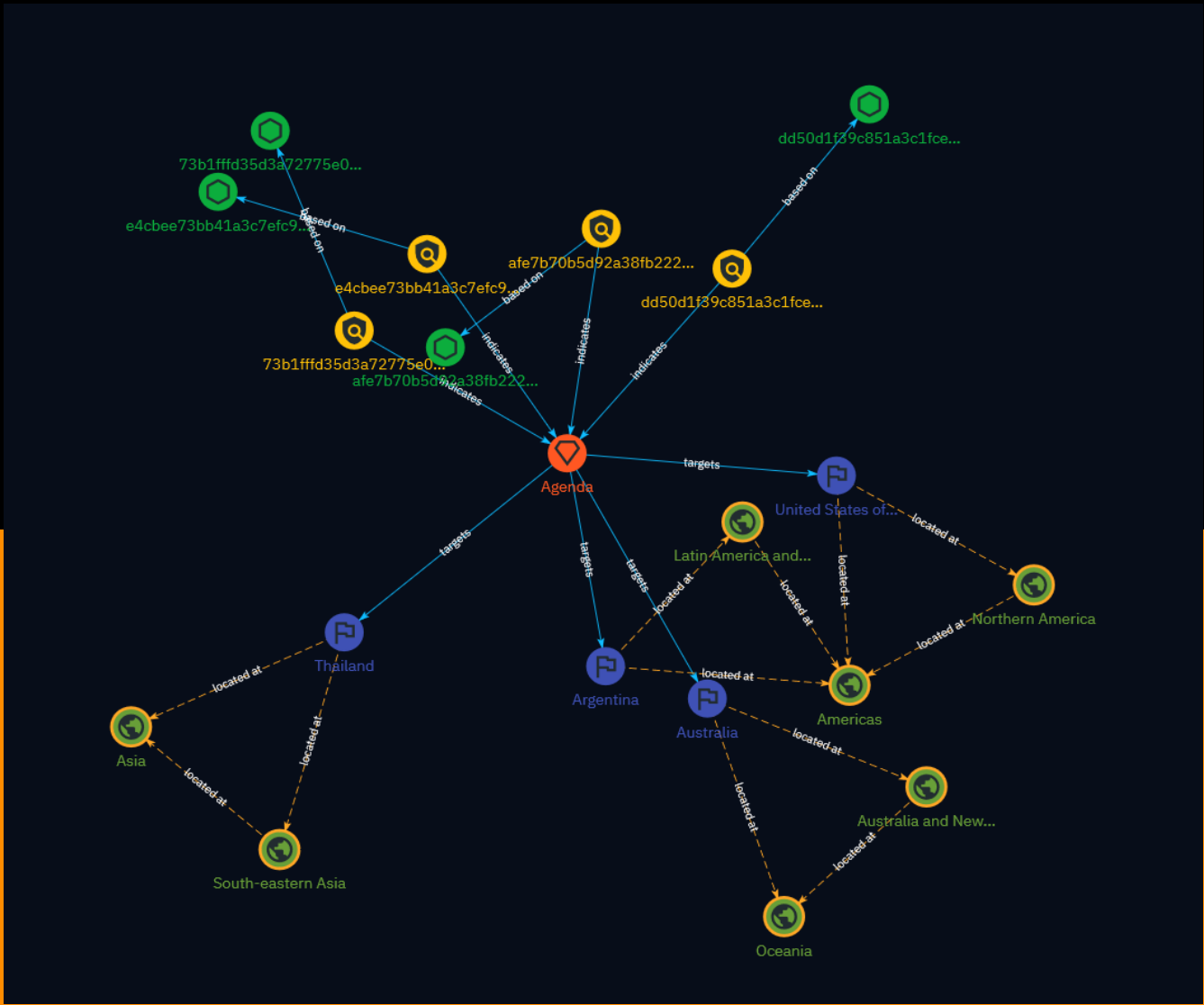

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since its discovery in 2022, the Agenda Ransomware group (also known as Qilin) has been active and in development. Agenda, which Trend Micro tracks as Water Galura, continues infecting victims globally with the US, Argentina, and Australia, and Thailand being among its top targets (based on the threat actor's leak site data). Meanwhile the Agenda ransomware was used to target several industries, such as finance and law.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70']
Name
dd50d1f39c851a3c1fce8abdf4ed84d7dca2b7bc19c1bc3c483c7fc3b8e9ab79
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'dd50d1f39c851a3c1fce8abdf4ed84d7dca2b7bc19c1bc3c483c7fc3b8e9ab79']
Name

afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38']

Name

73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a']

Intrusion-Set

Name
Agenda

Country

Name
Australia
Name
Thailand
Name
United States of America
Name
Argentina

Region

Name
Australia and New Zealand
Name
Oceania
Name
South-eastern Asia
Name
Asia
Name
Northern America
Name
Latin America and the Caribbean
Name
Americas

StixFile

Value
e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70
dd50d1f39c851a3c1fce8abdf4ed84d7dca2b7bc19c1bc3c483c7fc3b8e9ab79
afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38
73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a

External References

- https://documents.trendmicro.com/assets/txt/ioc-agenda-ransomwareJwTLz0J.txt
- https://otx.alienvault.com/pulse/6602eacf4b33429afac7e45d