Aug 09 2023

NETMANAGEIT

Intelligence Report

Rhysida ransomware

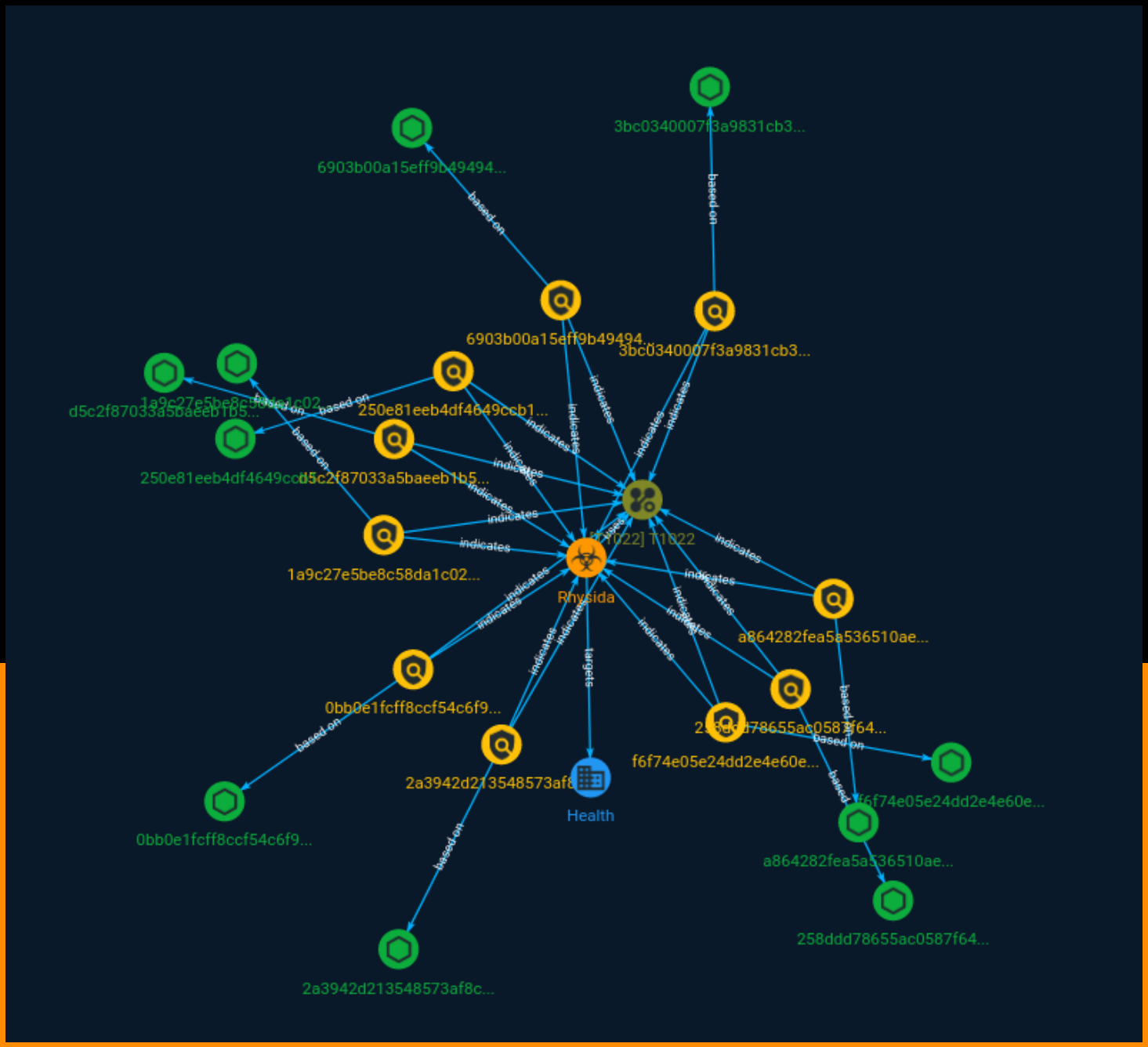

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Malware 10
- Attack-Pattern 11
- Sector 12

Observables

- StixFile 13

External References

- External References 14

Overview

Description

Cisco Talos is aware of the recent advisory published by the U.S. Department of Health and Human Services (HHS) warning the healthcare industry about Rhysida ransomware activity.

Confidence

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

15 / 100

Indicator

Name
3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96']
Name
1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd']
Name

6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de']

Name

f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab']

Name

0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f']

Name

2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2']

Name

258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595']

Name

250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1

Description

stack_string SHA256 of b07f6a5f61834a57304ad4d885bd37d8e1badba8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1']

Name

a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6

Description

stack_string SHA256 of 69b3d913a3967153d1e91ba1a31ebed839b297ed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6']

Name

d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

Description

RareEquities_LibTomCrypt SHA256 of 338d4f4ec714359d589918cee1adad12ef231907

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'd5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee']

Malware

Name
Rhysida

Attack-Pattern

Name
T1022
ID
T1022

Sector

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

StixFile

Value
3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96
2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2
6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de
f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab
0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f
1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd
258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595
250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

External References

- https://otx.alienvault.com/pulse/64d33784ed2c382401a39070
- https://blog.talosintelligence.com/rhysida-ransomware/