Oct 15 2023

NETMANAGEIT

Intelligence Report

Dark Angels | ESXi Ransomware Borrows Code & Victimology From RagnarLocker

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 7
- Intrusion-Set 10

Observables

- Domain-Name 11
- StixFile 12

External References

- External References 13

Overview

Description

In September 2023, automation and manufacturing company Johnson Controls was targeted in a ransomware attack where threat actors used Dark Angels ransomware to lock the company's VMWare ESXi servers. SentinelOne has analyzed the binary related to this attack and found that it has considerable overlap with RagnarLocker's ESXi version.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Data Encrypted for Impact
ID
T1471
Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Indicator

Name

f668f74d8808f5658153ff3e6aee8653b6324ada70a4aa2034dfa20d96875836

Description

is__elf SHA256 of 5411d7905bef69cb16d44f52fc46aa32fd922c80

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f668f74d8808f5658153ff3e6aee8653b6324ada70a4aa2034dfa20d96875836']

Name

fe8b6b7c3c86df0ee47a3cb04a68891fd5e91f3bfb13482112dd9042e8baebdf

Description

is__elf SHA256 of 06187023d399f3f57ca16a3a8fb9bb1bdb721603

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe8b6b7c3c86df0ee47a3cb04a68891fd5e91f3bfb13482112dd9042e8baebdf']

Name

p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd.onion']

Name

lyoevnzm3ewiq6jeyyuob2wfou7gh47yotuucsrwlf6ju3xrw43wacad.onion

Pattern Type

stix

Pattern

[domain-name:value = 'lyoevnzm3ewiq6jeyyuob2wfou7gh47yotuucsrwlf6ju3xrw43wacad.onion']

Name

qspjx67hi3heumrubqotn26cwimb6vjegiwgvrnpa6zefae2nqs6xqad.onion

Pattern Type

stix

Pattern

[domain-name:value = 'qspjx67hi3heumrubqotn26cwimb6vjegiwgvrnpa6zefae2nqs6xqad.onion']

Intrusion-Set

Name
RagnarLocker

Domain-Name

Value
qspjx67hi3heumrubqotn26cwimb6vjegiwgvrnpa6zefae2nqs6xqad.onion
lyoevnzm3ewiq6jeyyuob2wfou7gh47yotuucsrwlf6ju3xrw43wacad.onion
p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd.onion

StixFile

Value
fe8b6b7c3c86df0ee47a3cb04a68891fd5e91f3bfb13482112dd9042e8baebdf
f668f74d8808f5658153ff3e6aee8653b6324ada70a4aa2034dfa20d96875836

External References

- https://otx.alienvault.com/pulse/6528501905a1f9a70a132b7c
- https://www.sentinelone.com/blog/dark-angels-esxi-ransomware-borrows-code-victimology-from-ragnarlocker/