Jun 11 2023

NETMANAGEIT

Intelligence Report

Hypervisor Ransomware | Multiple Threat Actor Groups Hop on Leaked Babuk Code to Build ESXi Lockers

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Due to the prevalence of ESXi in on-prem and hybrid enterprise networks, these hypervisors are valuable targets for ransomware. Over the past two years, organized ransomware groups adopted Linux lockers, including ALPHV, Black Basta, Conti, Lockbit, and REvil. These groups focus on ESXi before other Linux variants, leveraging built-in tools for the ESXi hypervisor to kill guest machines, then encrypt crucial hypervisor files.

Confidence

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

15 / 100

Attack-Pattern

Name
Hypervisor
ID
T1062
Description
This technique has been deprecated and should no longer be used. A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware. (Citation: Wikipedia Hypervisor) It presents a virtual running environment to an operating system. An example of a common hypervisor is Xen. (Citation: Wikipedia Xen) A type-1 hypervisor operates at a level below the operating system and could be designed with [Rootkit](https://attack.mitre.org/techniques/T1014) functionality to hide its existence from the guest operating system. (Citation: Myers 2007) A malicious hypervisor of this nature could be used to persist on systems through interruption.
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.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Pharmacy and drugs manufacturing
Description
Public and private entities involved in producing and selling medicinal products and drugs.
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name

83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00

Description

ELF:Filecoder-DI\ [Trj] SHA256 of 76fb0d08fd5b9c52cb9da118ce5561cc0462555f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00']

Name

dc90560d7198bf824b65ba2cfbe403d84d38113f41a1aa2f37f8d827fd9e0ceb

Description

is__elf SHA256 of 885a734c7869b52aa125674cb430199b2645cda0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dc90560d7198bf824b65ba2cfbe403d84d38113f41a1aa2f37f8d827fd9e0ceb']

Name

ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4

Description

is__elf SHA256 of 29f16c046a344e0d0adfea80d5d7958d6b6b8cfa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4']

Name

930760c00de1b9a4bc2eefcd96173f1e9a906b11a9566c517fcb87a13acaa327

Description

is__elf SHA256 of cd19c2741261de97e91943148ba8c0863567b461

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '930760c00de1b9a4bc2eefcd96173f1e9a906b11a9566c517fcb87a13acaa327']

Name

11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6b66

Description

is__elf SHA256 of f25846f8cda8b0460e1db02ba6d3836ad3721f62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6b66']

Name

87db70368910dbf29c3dac5f39466c59631087120add02c405338706dfc369ca

Description

ELF:Filecoder-DI\ [Trj] SHA256 of e8bb26f62983055cfb602aa39a89998e8f512466

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87db70368910dbf29c3dac5f39466c59631087120add02c405338706dfc369ca']

Name

2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e

Description

ELF:Filecoder-BO\ [Trj] SHA256 of 048b3942c715c6bff15c94cdc0bb4414dbab9e07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e']

Name

95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7

Description

is__elf SHA256 of ee827023780964574f28c6ba333d800b73eae5c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7']

Name

f0f0279eb38391e25a6cac9c903da0bd23d418ed8100194295ea69130acc5e3f

Description

ELF:Filecoder-DI\ [Trj] SHA256 of 71ed640ebd8377f52bda4968398c62c97ae1c3ed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0f0279eb38391e25a6cac9c903da0bd23d418ed8100194295ea69130acc5e3f']

Name

d1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c

Description

ELF:Filecoder-DI\ [Trj] SHA256 of 933ad0a7d9db57b92144840d838f7b10356c7e51

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'd1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c']
```

Malware

Name
Conti

Description
[Conti](https://attack.mitre.org/software/S0575) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://attack.mitre.org/software/S0575) has been deployed via [TrickBot](https://attack.mitre.org/software/S0266) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://attack.mitre.org/software/S0575) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.(Citation: Cybereason Conti Jan 2021)(Citation: CarbonBlack Conti July 2020)(Citation: Cybleinc Conti January 2020)

Name
Mario

Name
Babuk-Locker

StixFile

Value
83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00
87db70368910dbf29c3dac5f39466c59631087120add02c405338706dfc369ca
ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
930760c00de1b9a4bc2eefcd96173f1e9a906b11a9566c517fcb87a13acaa327
d1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c
95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7
2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e
f0f0279eb38391e25a6cac9c903da0bd23d418ed8100194295ea69130acc5e3f
dc90560d7198bf824b65ba2cfbe403d84d38113f41a1aa2f37f8d827fd9e0ceb
11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6b66

External References

- https://otx.alienvault.com/pulse/645d0a843536d3878d95d18d
- https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/