Jun 21 2023

NETMANAGEIT

Intelligence Report

Terminator EDR Killer (Spyboy) | Detecting and Preventing a Windows BYOVD Attack

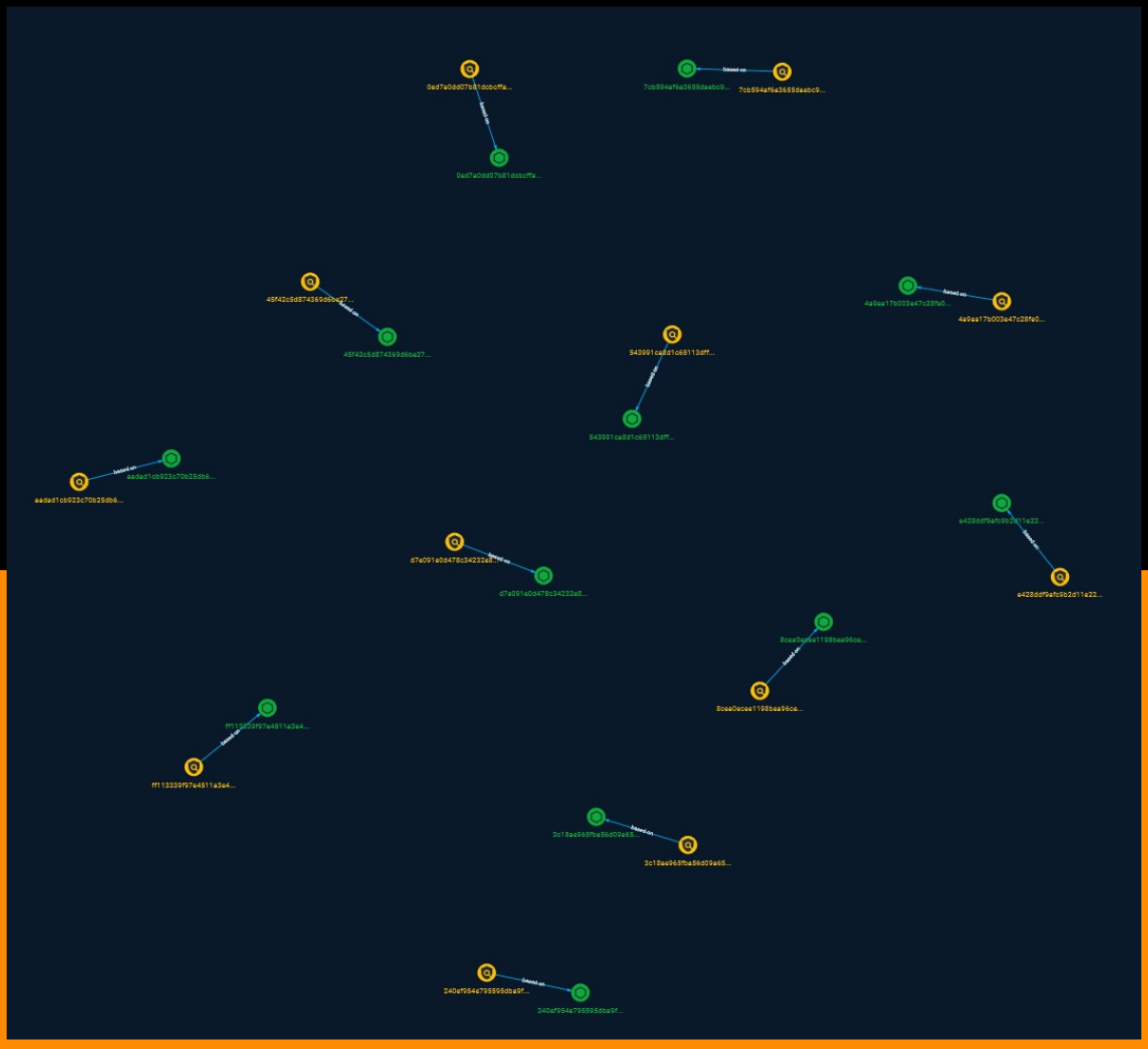

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A Russian-speaking hacker has been making headlines recently after promoting a tool that the threat actor claims can bypass EDR and AV tools. The so-called 'Terminator' tool is said to be able to kill processes belonging to "all AVs/EDRs/XDRs", which if used in conjunction with other malware, could allow threat actors to breach defenses.

Confidence

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

15 / 100

Indicator

Name

d7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0

Description

ConventionEngine_Keyword_Malware SHA256 of 628e63caf72c29042e162f5f7570105d2108e3c2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0']

Name

4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338

Description

ConventionEngine_Keyword_Malware SHA256 of ce42d6114fef0a42aee5866c68d0a31170bb8fa7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338']

Name

240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22

Description

ConventionEngine_Keyword_Malware SHA256 of c0d19461eb48b2bb66c0d2835370f491b35d24d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22']

Name

0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5

Description

ConventionEngine_Keyword_Malware SHA256 of adc5510dd775a4e846aba9fde84b5984d33768b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5']

Name

3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b

Description

ConventionEngine_Keyword_Malware SHA256 of 8f4b79b8026da7f966d38a8ba494c113c5e3894b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b']

Name

aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64

Description

ConventionEngine_Keyword_Malware SHA256 of 8dd52bfea92cbd91a042939a9cad69fdb666dfa3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64']

Name

7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21

Description

ConventionEngine_Keyword_Malware SHA256 of b99a5396094b6b20cea72fbf0c0083030155f74e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21']

Name

8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4

Description

ConventionEngine_Keyword_Malware SHA256 of a42018caa7243c54ecec35982790d96f38af90ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4']

Name

45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef

Description

ConventionEngine_Keyword_Malware SHA256 of 3b8ddf860861cc4040dea2d2d09f80582547d105

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef']

Name

e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f

Description

ConventionEngine_Keyword_Malware SHA256 of dd4cd182192b43d4105786ba87f55a036ec45ef2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f']

Name

ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408

Description

ConventionEngine_Keyword_Malware SHA256 of c83075a691401c015566eff8b0d06c42410a9cbb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408']

Name

543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

Description

ConventionEngine_Keyword_Malware SHA256 of 16d7ecf09fc98798a6170e4cef2745e0bee3f5c7

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91']

StixFile

Value
0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5
ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408
4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338
45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef
aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64
e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f
543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91
7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21
d7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0
3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b
8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4
240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22

External References

- https://www.sentinelone.com/blog/terminator-edr-killer-spyboy-detecting-and-preventing-a-windows-byovd-attack/
- https://otx.alienvault.com/pulse/6492f6198e6ee33b986b19ef