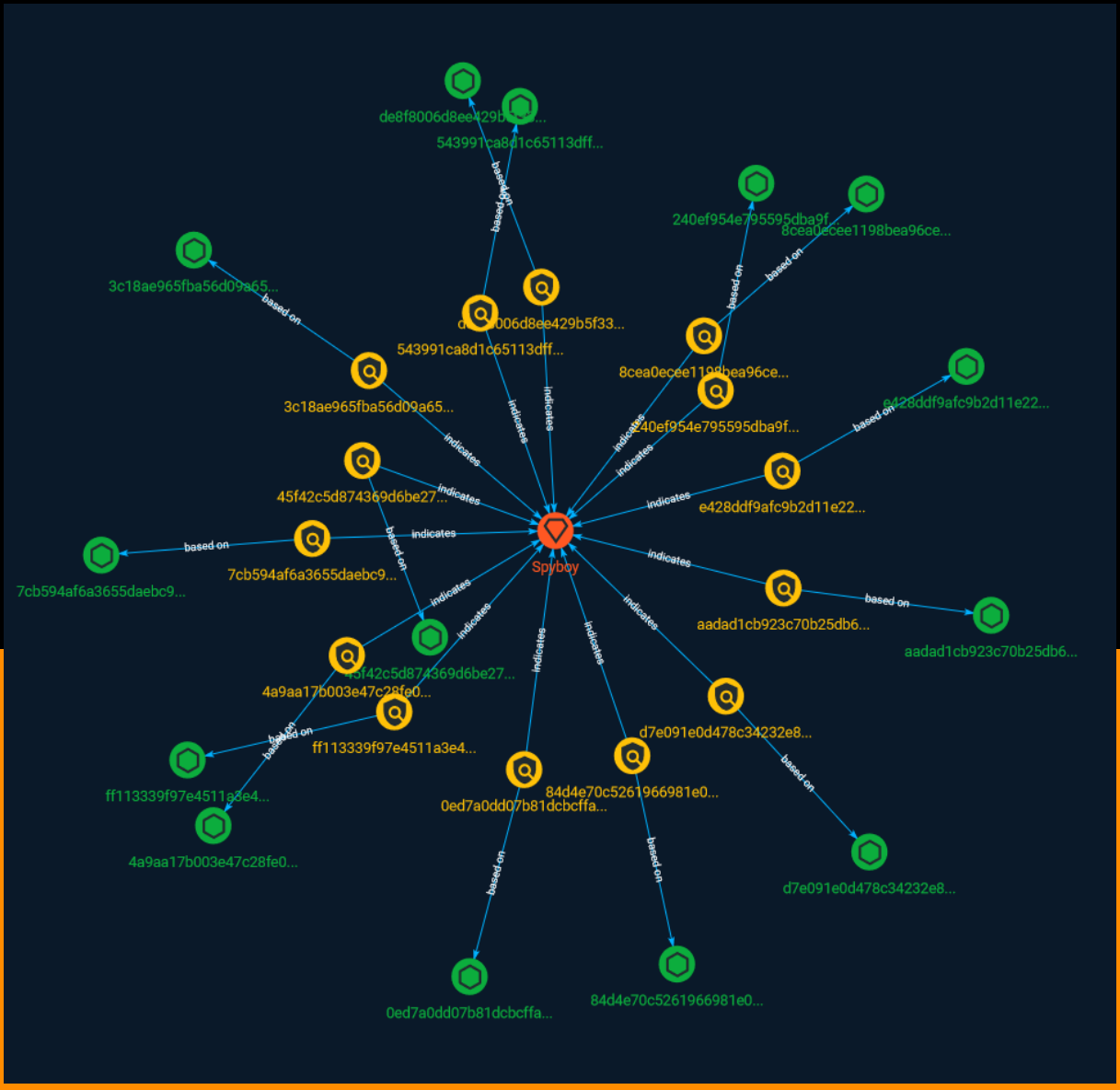
Jun 10 2023

NETMANAGEIT

# Intelligence Report

# Terminator antivirus killer is a vulnerable Windows driver in disguise



# Table of contents

## Overview



## Entities



## Observables



## External References

# Overview

## Description

Terminator is allegedly capable of bypassing 24 different antivirus (AV), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) security solutions, including Windows Defender, on devices running Windows 7 and later. Terminator just drops the legitimate, signed Zemana anti-malware kernel driver named zamguard64.sys or zam64.sys. Hashes for this driver are in Virustotal link.

## Confidence

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

15 / 100

# Indicator

| Name |
| --- |
| de8f8006d8ee429b5f333503defa54b25447f4ed6aeade5e4219e23f3473ef1c |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'de8f8006d8ee429b5f333503defa54b25447f4ed6aeade5e4219e23f3473ef1c'] |
| **Name** |
| d7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'd7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0'] |
| **Name** |

4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338

**Pattern Type**

stix

**Pattern**

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

**Name**

240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22

**Pattern Type**

stix

**Pattern**

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

**Name**

0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5

**Pattern Type**

stix

**Pattern**

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

**Name**

3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b

**Pattern Type**

stix

**Pattern**

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

**Name**

aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64

**Pattern Type**

stix

**Pattern**

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

**Name**

7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21

**Pattern Type**

stix

**Pattern**

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

**Name**

8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4

**Pattern Type**

stix

**Pattern**

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

**Name**

84d4e70c5261966981e014e294cfc004300db97d4f742aab489ded37585b0dfb

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '84d4e70c5261966981e014e294cfc004300db97d4f742aab489ded37585b0dfb']

**Name**

45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef

**Pattern Type**

stix

**Pattern**

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

**Name**

e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f

**Pattern Type**

stix

**Pattern**

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

**Name**

ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408

**Pattern Type**

stix

**Pattern**

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

**Name**

543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

**Pattern Type**

stix

**Pattern**

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

# Intrusion-Set

| Name |
| --- |
| Spyboy |

# StixFile

| Value |
| --- |
| 0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5 |
| ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408 |
| 4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338 |
| 45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef |
| aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64 |
| 84d4e70c5261966981e014e294cfc004300db97d4f742aab489ded37585b0dfb |
| e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f |
| 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91 |
| 7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21 |
| de8f8006d8ee429b5f333503defa54b25447f4ed6aeade5e4219e23f3473ef1c |
| d7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0 |
| 3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b |
| 8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4 |

240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22

# External References

- https://otx.alienvault.com/pulse/6478bbf77d8fa4b93726d95d
- https://www.virustotal.com/gui/file/543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91/details
- https://www.virustotal.com/gui/file/aadad1cb923c70b25db6eadc81c9d46fdf0f8ad02338762d138b81a4f19c4c64
- https://www.virustotal.com/gui/file/de8f8006d8ee429b5f333503defa54b25447f4ed6aeade5e4219e23f3473ef1c
- https://www.virustotal.com/gui/file/240ef954e795595dba9fb969b63eab040b849b975936e42c34983076178d5f22
- https://www.virustotal.com/gui/file/0ed7a0dd07b81dcbcffa49ce1e19ccdd4820be9f184483dbab6772bc9e1ebac5
- https://www.virustotal.com/gui/file/3c18ae965fba56d09a65770b4d8da54ccd7801f979d3ebd283397bc99646004b
- https://www.virustotal.com/gui/file/ff113339f97e4511a3e49fd2cc4bc1a80f69a9e57e090644271fafb803f25408
- https://www.virustotal.com/gui/file/8cea0ecee1198bea96ce838f637b6e35f679d4eab5e18170e74a58d920e47fa4
- https://www.virustotal.com/gui/file/d7e091e0d478c34232e8479b950c5513077b3a69309885cee4c61063e5f74ac0
- https://www.virustotal.com/gui/file/7cb594af6a3655daebc9fad9c8abf2417b00ba31dcd118707824e5316fc0cc21
- https://www.virustotal.com/gui/file/45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef

- https://www.virustotal.com/gui/file/84d4e70c5261966981e014e294cfc004300db97d4f742aab489ded37585b0dfb
- https://www.virustotal.com/gui/file/4a9aa17b003e47c28fe04fb3b18bdca0dcf97eef0a1dae4e30664274eced0338
- https://www.virustotal.com/gui/file/e428ddf9afc9b2d11e2271f0a67a2d6638b860c2c12d4b8cc63d33f3349ee93f
- https://www.bleepingcomputer.com/news/security/terminator-antivirus-killer-is-a-vulnerable-windows-driver-in-disguise/