Jul 25 2023

NETMANAGEIT

Intelligence Report

Sliver C2 in circulation through domestic program developers

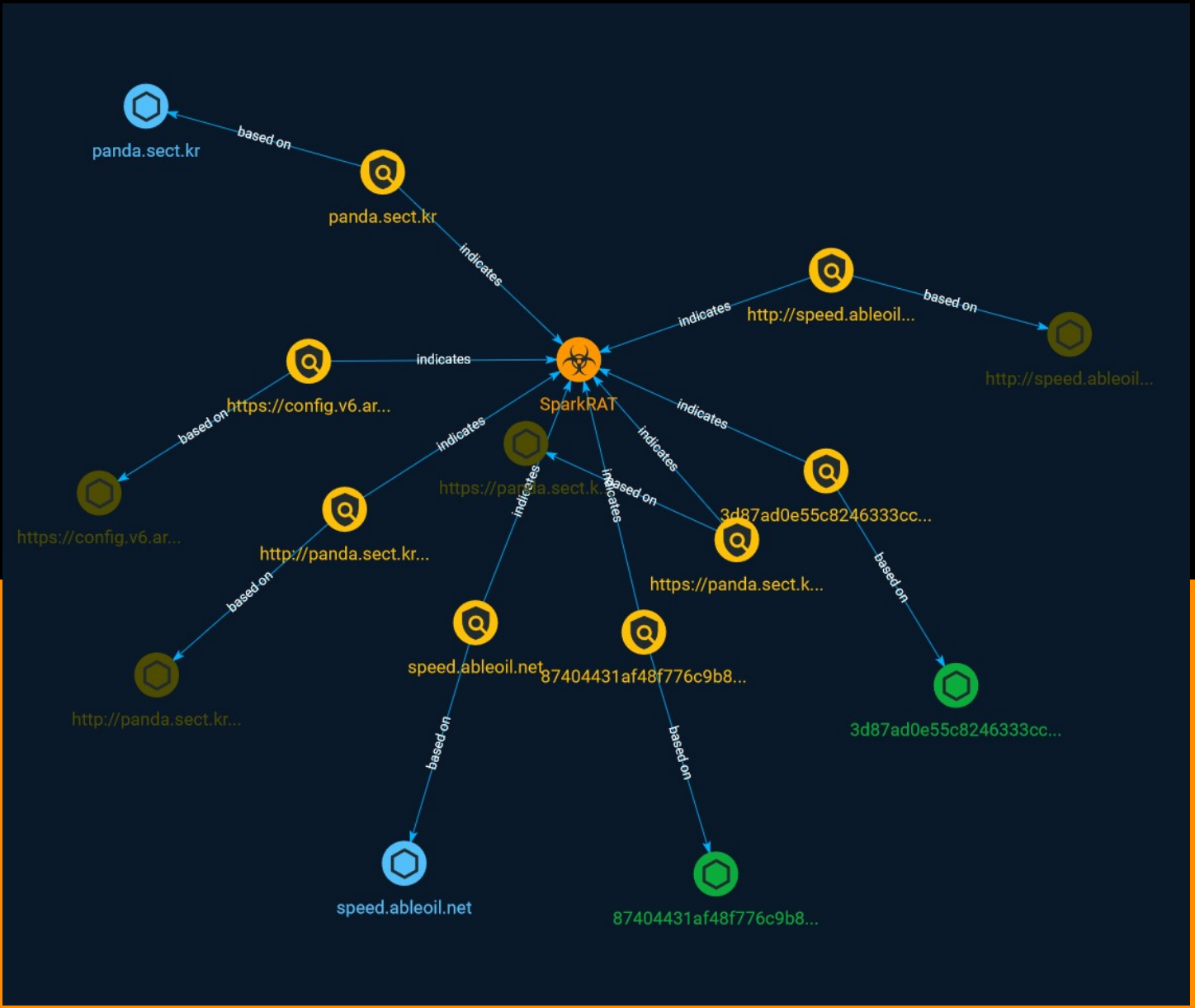

Table of contents

Overview

Entities

Observables

External References

Overview

Description

SparkRAT malware was distributed in the installation files of domestic VPN companies through posting “ SparkRAT being distributed and included in domestic VPN installation files ” [1] and “ Analysis of attack cases leading to MeshAgent infection in domestic VPN installation ”

Confidence

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

15 / 100

Indicator

Name
http://speed.ableoil.net:443
Pattern Type
stix
Pattern
[url:value = 'http://speed.ableoil.net:443']
Name
speed.ableoil.net
Pattern Type
stix
Pattern
[hostname:value = 'speed.ableoil.net']
Name
http://panda.sect.kr:443

Pattern Type

stix

Pattern

[url:value = 'http://panda.sect.kr:443']

Name

https://panda.sect.kr

Pattern Type

stix

Pattern

[url:value = 'https://panda.sect.kr']

Name

https://config.v6.army/sans.woff2

Description

data 3d87ad0e55c8246333ccaf8fc96f67b5e4fc63b0ef705cc3ec125e4d101c9a03

Pattern Type

stix

Pattern

[url:value = 'https://config.v6.army/sans.woff2']

Name

3d87ad0e55c8246333ccaf8fc96f67b5e4fc63b0ef705cc3ec125e4d101c9a03

Description

SHA256 of 73f83322fce3ef38b816bef8fa28d37b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d87ad0e55c8246333ccaf8fc96f67b5e4fc63b0ef705cc3ec125e4d101c9a03']

Name

87404431af48f776c9b83b5b57c1ddf43b05c7e986460b1a97473caf3c85f567

Description

SHA256 of 5eb6821057c28fd53b277bc7c6a17465

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87404431af48f776c9b83b5b57c1ddf43b05c7e986460b1a97473caf3c85f567']

Name

panda.sect.kr
Pattern Type
stix
Pattern
[hostname:value = 'panda.sect.kr']

Malware

Name
SparkRAT

StixFile

Value
87404431af48f776c9b83b5b57c1ddf43b05c7e986460b1a97473caf3c85f567
3d87ad0e55c8246333ccaf8fc96f67b5e4fc63b0ef705cc3ec125e4d101c9a03

Hostname

Value
speed.ableoil.net
panda.sect.kr

Url

Value
http://speed.ableoil.net:443
http://panda.sect.kr:443
https://panda.sect.kr
https://config.v6.army/sans.woff2

External References

- https://otx.alienvault.com/pulse/64bfcbe57ed2870842264e97
- https://asec.ahnlab.com/ko/55524/