Dec 22 2023

NETMANAGEIT

Intelligence Report

OSINT - BattleRoyal, DarkGate Cluster Spreads via Email and Fake Browser Updates

Table of contents

Overview

Entities

Observables

Overview

Description

OSINT - BattleRoyal, DarkGate Cluster Spreads via Email and Fake Browser Updates

Confidence

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

20 / 100

Content

N/A

Indicator

Name
http://79.110.62.96:80/Downloads/bye.zip/bye.vbs
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[url:value = 'http://79.110.62.96:80/Downloads/bye.zip/bye.vbs']
Name
searcherbigdealk.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix

Pattern

[domain-name:value = 'searcherbigdealk.com']

Name

http://searcherbigdealk.com:2351/msizjbicvmd

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://searcherbigdealk.com:2351/msizjbicvmd']

Name

kairoscounselingmi.com

Pattern Type

stix

Pattern

[domain-name:value = 'kairoscounselingmi.com']

Name

79.110.62.96

Description
DarkGate botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '79.110.62.96']
Name
79.110.62.96
Pattern Type
stix
Pattern
[hostname:value = '79.110.62.96']
Name
96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77']

Name

2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084']

Name

7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f']

Name

ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f']

Name

http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe

Pattern Type

stix

Pattern

[url:value = 'http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe']

Name

heilee.com

Pattern Type

stix

Pattern

[hostname:value = 'heilee.com']

Name

http://searcherbigdealk.com:2351/zjbicvmd

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://searcherbigdealk.com:2351/zjbicvmd']

Name

https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url

Pattern Type

stix

Pattern

[url:value = 'https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url']

Name

zxcdota2huysasi.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'zxcdota2huysasi.com']

Name

searcherbigdealk.com

Pattern Type

stix

Pattern

[hostname:value = 'searcherbigdealk.com']

Name

79.110.62.96

Pattern Type

stix

Pattern

[domain-name:value = '79.110.62.96']

Name

kairoscounselingmi.com

Pattern Type

stix

Pattern

[hostname:value = 'kairoscounselingmi.com']

Name

fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4']

Name

e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243']

Name

http://5.181.159.29:80/Downloads/12.url

Pattern Type

stix

Pattern

[url:value = 'http://5.181.159.29:80/Downloads/12.url']

Name

https://heilee.com/qxz3l

Pattern Type

stix

Pattern

[url:value = 'https://heilee.com/qxz3l']

Name

5.181.159.29

Pattern Type

stix

Pattern

[hostname:value = '5.181.159.29']

Name

heilee.com

Pattern Type

stix

Pattern

[domain-name:value = 'heilee.com']

Name

5.181.159.29

Description

ISP: MivoCloud SRL **OS:** None ---------- Hostnames: - no-rdns.mivocloud.com ---------- Domains: - mivocloud.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.10 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDjvOKuLYUfCYIS3NI9ijRWp0K1F5tJt1sz3qxNfidIlQwu T9w0Uiz2Q145NZwHvh9UHFKrZ/7tZaUgAHQ4v1EkpkiH4zn4DluRRcrFN0WulPkY+zXZR/CiJqh6 9AwWRIMkmN23juw9ZT12jaoGIPMH5yhbFnCXf/dgSKK9DbG03UDDoGRHi5VR8U9/ DuNI+GIpLZa/ jn0rZjpuuk94IvpaemFnJ6I/ F+5YNRSJdmTl+4XUQrj5eg4GoLiJLFKGU4E2nMtatFOH03b6JQSK GPeJrbwAi+96tnHh1iJNuhh9HmgZLG12dRj/NWplt6avtau71vVNApYLe/0SEEBV9MGH6ArYTKAC 18m1eFvckzVSFV+JY2I015L3w43PzeVz4ciBeuLMG4MBN08HXKvydNxyQ5cH4a9g/hFD0rmbOPpN HJuAEk3Wi7pR8qPMBMLFOmZwlGt6zZVsITWNQ00dN+9LJla5rVcs4B9WBC/ ECLwuO542MKqEgJEq bqQB9AjVxxs= Fingerprint: 0f:29:7b:f2:4e:8d:2b:0e:bf:f1:13:02:58:90:1e:47 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256

ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 207 Multi-Status Content-Type: text/xml; charset=utf-8 Date: Fri, 22 Dec 2023 04:41:40 GT Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.159.29']

Name

5.181.159.29

Pattern Type

stix

Pattern

[domain-name:value = '5.181.159.29']

Name

nathumvida.org

Pattern Type

stix
Pattern
[domain-name:value = 'nathumvida.org']

Domain-Name

Value
5.181.159.29
79.110.62.96
zxcdota2huysasi.com
kairoscounselingmi.com
heilee.com
searcherbigdealk.com
nathumvida.org

StixFile

Value
2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084
96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77
fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4
e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243
7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f
ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f

Hostname

Value
5.181.159.29
79.110.62.96
kairoscounselingmi.com
heilee.com
searcherbigdealk.com

IPv4-Addr

Value
5.181.159.29
79.110.62.96

Text

Value
96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77
ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f
CVE-2023-36025
fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4
7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f
https://www.proofpoint.com/us/blog/threat-insight/battleroyal-darkgate-cluster-spreads-email-and-fake-browser-updates
http://searcherbigdealk.com:2351/zjbicvmd
http://79.110.62.96:80/Downloads/bye.zip/bye.vbs
http://searcherbigdealk.com:2351/msizjbicvmd
https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url
2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084
e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe
http://5.181.159.29:80/Downloads/12.url
https://heilee.com/qxz3l

Url

Value
http://searcherbigdealk.com:2351/zjbicvmd
http://79.110.62.96:80/Downloads/bye.zip/bye.vbs
http://searcherbigdealk.com:2351/msizjbicvmd
https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url
http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe
http://5.181.159.29:80/Downloads/12.url
https://heilee.com/qxz3l

External References