Aug 21 2023

NETMANAGEIT

Intelligence Report

Catching up with WoofLocker, the most elaborate traffic redirection scheme to tech support scams

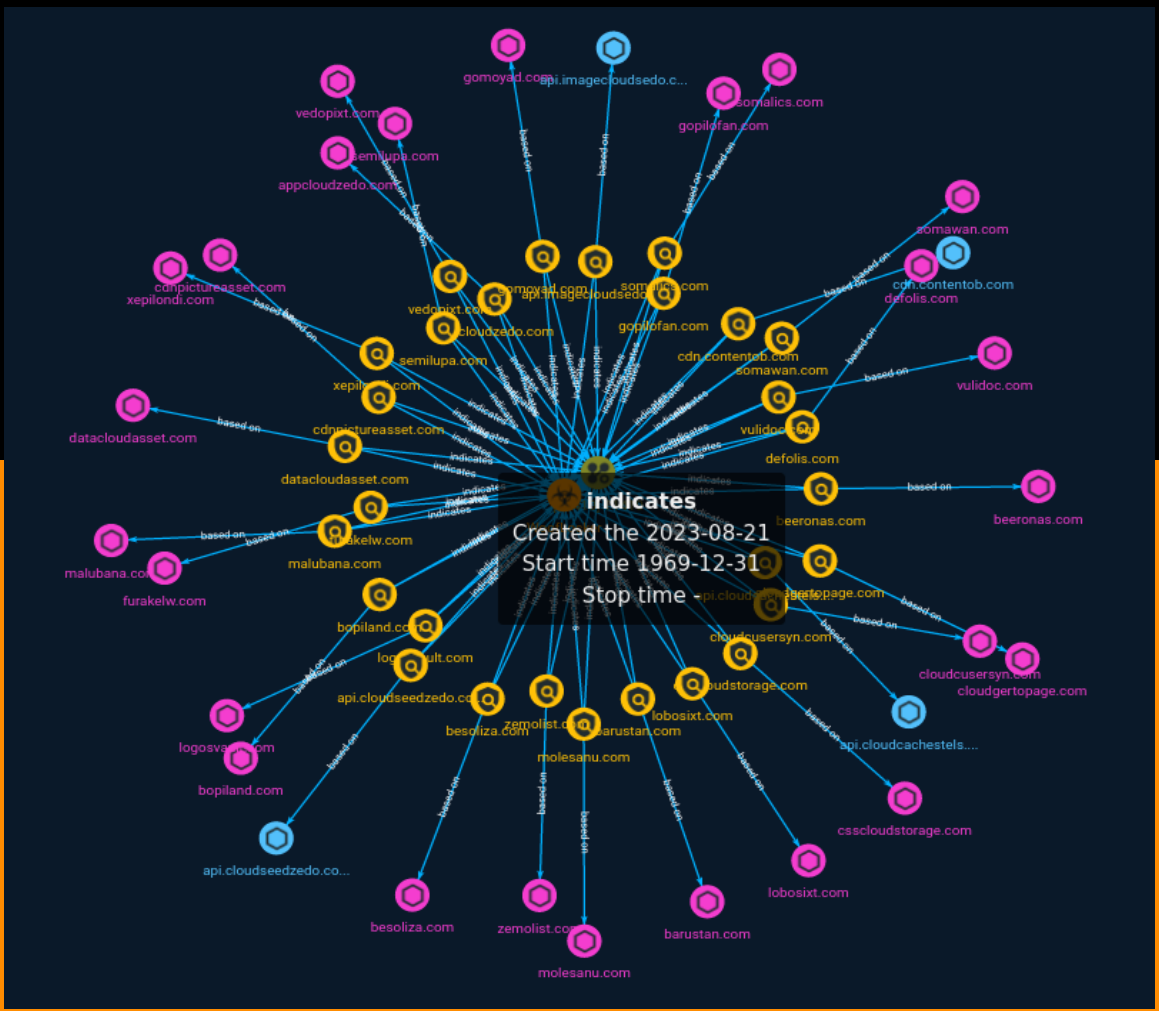

Table of contents

Overview

Entities

Observables

External References

Overview

Description

WoofLocker is being distributed via a limited number of compromised websites. The threat actor appears to have gained access to two categories: non adult traffic and adult traffic. That distinction can be seen in the unique redirection URL created for each victim with a parameter called "nad" and "ad" respectively.

Confidence

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

15 / 100

Attack-Pattern

Name
T1410
ID
T1410

Indicator

Name
besoliza.com
Pattern Type
stix
Pattern
[domain-name:value = 'besoliza.com']
Name
cdn.contentob.com
Pattern Type
stix
Pattern
[hostname:value = 'cdn.contentob.com']
Name
csscloudstorage.com

Pattern Type
stix
Pattern
[domain-name:value = 'csscloudstorage.com']
Name
api.imagecloudsedo.com
Pattern Type
stix
Pattern
[hostname:value = 'api.imagecloudsedo.com']
Name
appcloudzedo.com
Pattern Type
stix
Pattern
[domain-name:value = 'appcloudzedo.com']
Name
cloudcusersyn.com

Pattern Type
stix
Pattern
[domain-name:value = 'cloudcusersyn.com']
Name
xepilondi.com
Pattern Type
stix
Pattern
[domain-name:value = 'xepilondi.com']
Name
defolis.com
Pattern Type
stix
Pattern
[domain-name:value = 'defolis.com']
Name
malubana.com

Pattern Type

stix

Pattern

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

Name

vulidoc.com

Pattern Type

stix

Pattern

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

Name

molesanu.com

Pattern Type

stix

Pattern

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

Name

furakelw.com

Pattern Type
stix
Pattern
[domain-name:value = 'furakelw.com']
Name
beeronas.com
Pattern Type
stix
Pattern
[domain-name:value = 'beeronas.com']
Name
zemolist.com
Pattern Type
stix
Pattern
[domain-name:value = 'zemolist.com']
Name
datacloudasset.com

Pattern Type
stix
Pattern
[domain-name:value = 'datacloudasset.com']
Name
cloudgertopage.com
Pattern Type
stix
Pattern
[domain-name:value = 'cloudgertopage.com']
Name
semilupa.com
Pattern Type
stix
Pattern
[domain-name:value = 'semilupa.com']
Name
gopilofan.com

Pattern Type
stix
Pattern
[domain-name:value = 'gopilofan.com']
Name
logosvault.com
Pattern Type
stix
Pattern
[domain-name:value = 'logosvault.com']
Name
gomoyad.com
Pattern Type
stix
Pattern
[domain-name:value = 'gomoyad.com']
Name
lobosixt.com

Pattern Type
stix
Pattern
[domain-name:value = 'lobosixt.com']
Name
bopiland.com
Pattern Type
stix
Pattern
[domain-name:value = 'bopiland.com']
Name
vedopixt.com
Pattern Type
stix
Pattern
[domain-name:value = 'vedopixt.com']
Name
barustan.com

Pattern Type
stix
Pattern
[domain-name:value = 'barustan.com']
Name
cdnpictureasset.com
Pattern Type
stix
Pattern
[domain-name:value = 'cdnpictureasset.com']
Name
somawan.com
Pattern Type
stix
Pattern
[domain-name:value = 'somawan.com']
Name
api.cloudseedzedo.com

Pattern Type
stix
Pattern
[hostname:value = 'api.cloudseedzedo.com']
Name
somalics.com
Pattern Type
stix
Pattern
[domain-name:value = 'somalics.com']
Name
api.cloudcachestels.com
Pattern Type
stix
Pattern
[hostname:value = 'api.cloudcachestels.com']

Malware

Name
WoofLocker

Domain-Name

Value
zemolist.com
molesanu.com
malubana.com
semilupa.com
lobosixt.com
gomoyad.com
vulidoc.com
appcloudzedo.com
cloudcusersyn.com
furakelw.com
defolis.com
cloudgertopage.com
datacloudasset.com

cdnpictureasset.com

barustan.com

xepilondi.com

somalics.com

bopiland.com

gopilofan.com

csscloudstorage.com

vedopixt.com

somawan.com

besoliza.com

logosvault.com

beeronas.com

Hostname

Value
api.cloudseedzedo.com
api.imagecloudsedo.com
cdn.contentob.com
api.cloudcachestels.com

External References

- https://otx.alienvault.com/pulse/64e374c89862f3f419b51037
- https://www.malwarebytes.com/blog/threat-intelligence/2023/08/wooflocker2