Aug 31 2023

NETMANAGEIT

Intelligence Report

FIN8-LINKED ACTOR TARGETS CITRIX NETSCALER SYSTEMS

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Citrix has released details of a series of attacks on its servers, following a security review by security researchers.

Confidence

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

15 / 100

Indicator

Name
01717ce6fe0f79c4dc935549c516e4a1941cb4a4e84233e8fdff447177ce556e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '01717ce6fe0f79c4dc935549c516e4a1941cb4a4e84233e8fdff447177ce556e']
Name
20b375ac4487a5955d4b0dd0a600e851d1e455a30c3f8babd0e7e1e97d11a073
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '20b375ac4487a5955d4b0dd0a600e851d1e455a30c3f8babd0e7e1e97d11a073']
Name

383df272841f9a677ee03f6f553bc6cf3197427d792dc9f86b7fb1911dc83d71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '383df272841f9a677ee03f6f553bc6cf3197427d792dc9f86b7fb1911dc83d71']

Name

85.239.53.49

Description

CC=US ASN=AS62005 BlueVPS OU

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.239.53.49']

Name

ec89ec41f0e0a7e60fa3f6267d0197c7fa8568e11a2c564f6d59855ddd9e1d64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec89ec41f0e0a7e60fa3f6267d0197c7fa8568e11a2c564f6d59855ddd9e1d64']

Name

2d53aaa2638f9a986779b9e36a7b6dfdaddf3cc06698f4aa9f558c1a0591dc9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d53aaa2638f9a986779b9e36a7b6dfdaddf3cc06698f4aa9f558c1a0591dc9a']

Name

45.66.248.189

Description

ISP: BlueVPS OU **OS:** None ---------- Hostnames: - illoumlst.transnet.pics ---------- Domains: - transnet.pics ---------- Services: **80:** ``` HTTP/1.1 404 Server: nginx/1.14.1 Content-Type: text/plain; charset=utf-8 Content-Length: 14 Connection: Close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.66.248.189']

Name

03657d8f9dcb49a690d4b07da4f49ead58000efe458ca3ba7f878233dd25e391

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '03657d8f9dcb49a690d4b07da4f49ead58000efe458ca3ba7f878233dd25e391']

Name

94f09d01e1397ca80c71b488b8775acfe2776b5ab42e9a54547d9e5f58caf11a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '94f09d01e1397ca80c71b488b8775acfe2776b5ab42e9a54547d9e5f58caf11a']

Name

bb28ba8d838c8eefdd5ae1e23d5872968d84e8cb86bf292b2c3bf4c84ad7dbd0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb28ba8d838c8eefdd5ae1e23d5872968d84e8cb86bf292b2c3bf4c84ad7dbd0']

Name

857d6f7e4b96738adb9cc023e2c504362fe8b73bdce422f8f8cb791dd6ac2449

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '857d6f7e4b96738adb9cc023e2c504362fe8b73bdce422f8f8cb791dd6ac2449']

Vulnerability

Name
CVE-2022-3236
Name
CVE-2023-3519
Name
CVE-2022-26134
Name
CVE-2018-0798
Name
CVE-2022-30190

Intrusion-Set

Name
FIN8

Description
[FIN8](https://attack.mitre.org/groups/G0061) is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Fin8 May 2016)

StixFile

Value
01717ce6fe0f79c4dc935549c516e4a1941cb4a4e84233e8fdff447177ce556e
857d6f7e4b96738adb9cc023e2c504362fe8b73bdce422f8f8cb791dd6ac2449
03657d8f9dcb49a690d4b07da4f49ead58000efe458ca3ba7f878233dd25e391
2d53aaa2638f9a986779b9e36a7b6dfdaddf3cc06698f4aa9f558c1a0591dc9a
20b375ac4487a5955d4b0dd0a600e851d1e455a30c3f8babd0e7e1e97d11a073
383df272841f9a677ee03f6f553bc6cf3197427d792dc9f86b7fb1911dc83d71
94f09d01e1397ca80c71b488b8775acfe2776b5ab42e9a54547d9e5f58caf11a
ec89ec41f0e0a7e60fa3f6267d0197c7fa8568e11a2c564f6d59855ddd9e1d64
bb28ba8d838c8eefdd5ae1e23d5872968d84e8cb86bf292b2c3bf4c84ad7dbd0

IPv4-Addr

Value
85.239.53.49
45.66.248.189

External References

- https://github.com/sophoslabs/IoCs/blob/master/2023-08-25%20Citrix%20CVE-2023-3519%20attacks.csv
- https://securityaffairs.com/150028/hacking/fin8-citrix-netscaler.html
- https://otx.alienvault.com/pulse/64edf1fe10794c40a79f86b2