Dec 06 2023

NETMANAGEIT

Intelligence Report

AA23-339A Threat Actors Exploit Adobe ColdFusion CVE- 2023-26360 for Initial Access to Government Servers

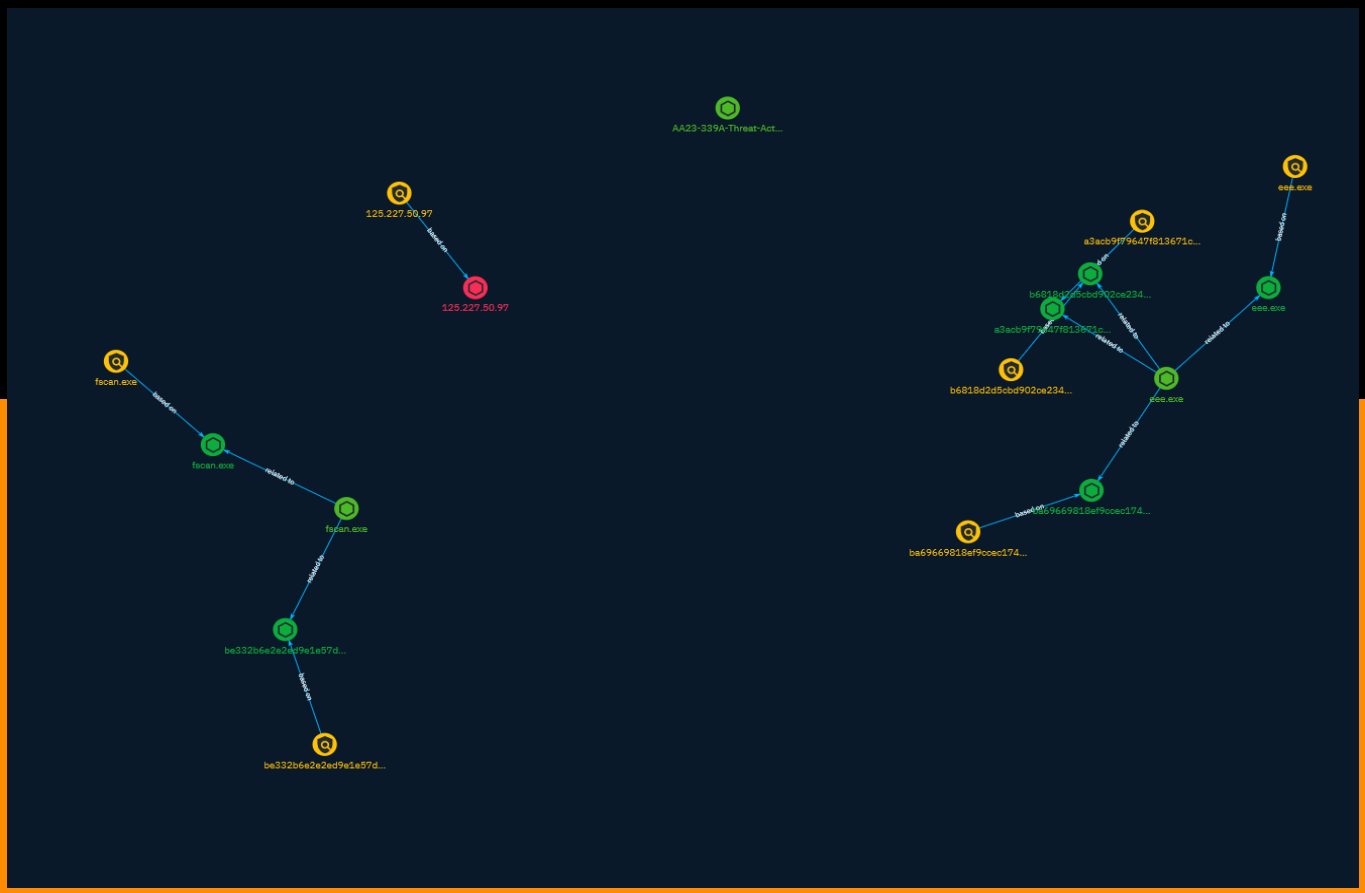

Table of contents

Overview

Entities

Observables

Overview

Description

AA23-339A Threat Actors Exploit Adobe ColdFusion CVE- 2023-26360 for Initial Access to Government Servers

Confidence

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

20 / 100

Content

N/A

Indicator

Name
be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656
Pattern Type
stix
Pattern
[file:hashes.'SHA-1' = 'be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656']
Name
eee.exe
Pattern Type
stix
Pattern
[file:name = 'eee.exe']
Name
a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864

Description

ConventionEngine_Term_Users SHA256 of b6818d2d5cbd902ce23461f24fc47e24937250e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864']

Name

125.227.50.97

Description

ISP: Data Communication Business Group **OS:** None ---------- Hostnames: - ms.chengkuo.com ---------- Domains: - chengkuo.com ---------- Services: **25:** ``` 220 ESMTP MAIL Server 250-ms.chengkuo.com 250-PIPELINING 250-SIZE 102400000 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` ---------- **81:** ``` HTTP/1.1 200 OK Date: Wed, 06 Dec 2023 17:30:18 GMT Date: Wed, 06 Dec 2023 17:30:18 GMT Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate Set-Cookie: JSESSIONID=1sx176e2rrnwy1phljsgrg52k8;Path=/ Expires: Thu, 01 Jan 1970 00:00:00 GMT Content-Type: text/html;charset=UTF-8 Content-Language: en-US Content-Length: 9358 ``` ---------- **88:** ``` HTTP/1.1 400 Bad Request Date: Wed, 29 Nov 2023 00:32:28 GMT Server: Apache Content-Length: 481 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **110:** ``` +OK MS OK +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN . ``` ---------- **465:** ``` 220 ESMTP MAIL Server 250-ms.chengkuo.com 250-PIPELINING 250-SIZE 102400000 250-VRFY 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` HEARTBLEED: 2023/11/10 04:09:38 125.227.50.97:465 - SAFE ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] MS OK * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed.

A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` HEARTBLEED: 2023/11/24 01:59:16 125.227.50.97:993 - SAFE ---------- **995:** ``` +OK MS OK +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/12/05 18:35:51 125.227.50.97:995 - SAFE ---------- **1723:** ``` PPTP: Firmware: 1 Hostname: local Vendor: linux ``` ---------- **1900:** ``` HTTP/1.1 200 OK CACHE-CONTROL: max-age=120 ST: upnp:rootdevice USN: uuid:6b19faef-7d0e-4cb9-a5be-ef45a15baefa::upnp:rootdevice EXT: SERVER: ASUSTeK UPnP/1.0 MiniUPnPd/1.4 LOCATION: http://172.16.5.1:50574/rootDesc.xml ``` ---------- **8888:** ``` HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=9A4D1EA0E72370017F1BD67743AB3AE0; Path=/ Content-Type: text/html Content-Length: 1073 Date: Tue, 05 Dec 2023 03:59:44 GMT ``` ---------- **55000:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Wed, 18 Mar 2015 06:10:36 GMT Content-Type: text/html Content-Length: 166 Connection: close

400 Bad Request

---

nginx

``` ----------

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [ipv4-addr:value = '125.227.50.97'] |
| **Name** |
| ba69669818ef9ccec174d647a8021a7b |
| **Pattern Type** |
```

stix

Pattern

[file:hashes.MD5 = 'ba69669818ef9ccec174d647a8021a7b']

Name

b6818d2d5cbd902ce23461f24fc47e24937250e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-1' = 'b6818d2d5cbd902ce23461f24fc47e24937250e6']

Name

fscan.exe

Pattern Type

stix

Pattern

[file:name = 'fscan.exe']

StixFile

Value
be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656
fscan.exe
b6818d2d5cbd902ce23461f24fc47e24937250e6
ba69669818ef9ccec174d647a8021a7b
a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864
eee.exe

IPv4-Addr

Value
125.227.50.97

Text

Value
fscan.exe
AA23-339A-Threat-Actors-Exploit-Adobe-ColdFusion-CVE-2023-26360-for-Initial-Access-to-Government-Servers.stix_.json
eee.exe

External References