Analysis of Fox Kitten Infrastructure Reveals Unique Host Patterns and Potentially New IOCs

: 9/17/2024

censys
Analysis of Fox Kitten Infrastructure Reveals Unique Host Patterns and Potentially New IOCs

Executive Summary

Background

On August 28, 2024, the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center (DC3) published a joint Cybersecurity Advisory (CSA) "to warn network defenders that, as of August 2024, a group of Iran-based cyber actors" (aka "Fox Kitten") continues to exploit U.S. and foreign organizations."[1] The CSA included a list of 17 IOCs (12 IP addresses/hosts, five domain names) with "First Seen" and "Most Recently Observed" dates but added, defenders should "investigate or vet these IP addresses prior to taking action…." and "[T]he FBI and CISA do not recommend blocking of the indicators in Table 11 based solely on their inclusion in this CSA."

Censys' Perspective

Censys assisted defenders in these tasks of investigation and vetting by leveraging its historical, global internet perspective to analyze the IOCs' profiles during the timeframe of nefarious activity outlined in the CSA. This allows defenders to compare those historical profiles against the hosts' current dispositions and determine if enough similarities exist to recommend blocking the IOCs in question.

Censys' Findings

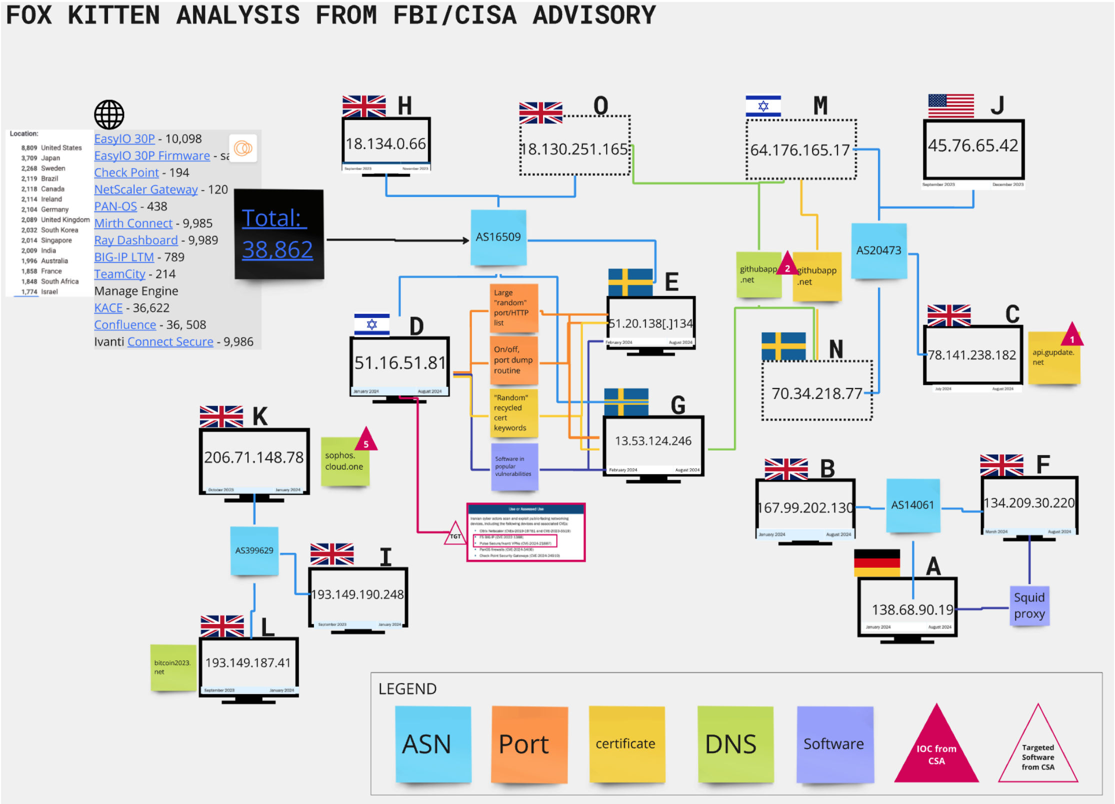
By investigating the hosts connected to the IOC IPs as well as the hosts and certificates connected to the domain IOCs listed in the FBI/CISA Advisory for Fox Kitten, Censys was able to uncover extremely unique patterns amongst these hosts over time. These patterns were then used in searches to:

- Find **active hosts not mentioned in the Advisory that have**:
  - **Matching patterns and Autonomous Systems (ASs) as Hosts D, E, & G** from the report, and could be part of the **same infrastructure** to possibly be used in future attacks
  - **Matching domain IOCs** to Host G and matching ASs to Hosts J & C from the report and could be part of the same infrastructure to possibly be used in future attacks
- Identify timeframes outside of those specified in the Advisory where IOC hosts appear similar or identical to the timeframes of nefarious activities, possibly indicating previously unknown durations of threat activity

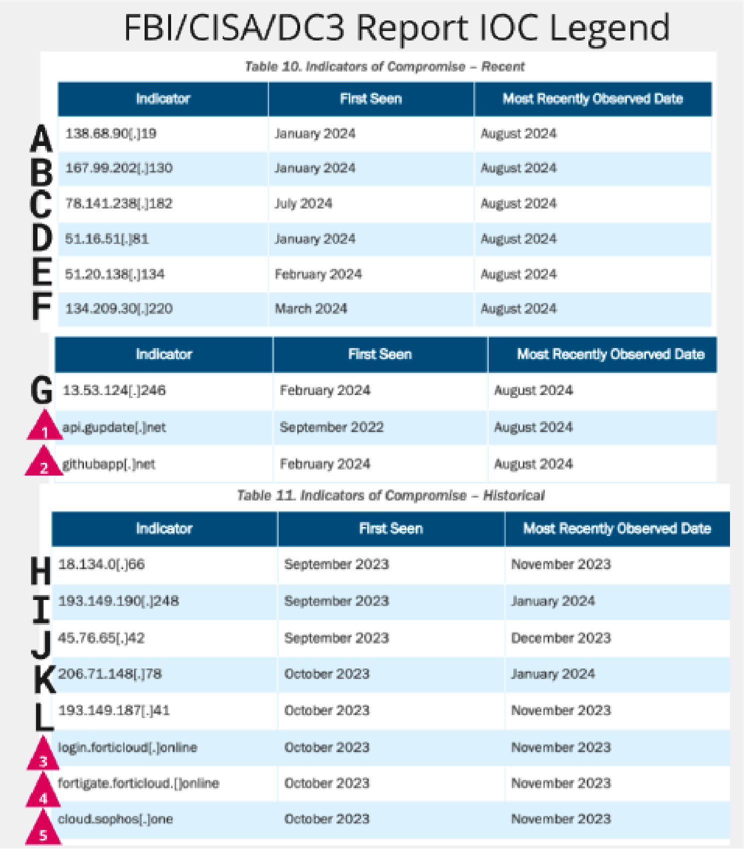
- Find **current certificates with matching domain IOCs** that could be used on future hosts.

Analysis

Censys uncovered unique and unusual patterns observed historically on the IOC hosts that seem to have no known, legitimate use. Therefore, the active hosts that match these patterns, discovered via Censys Search are, at worst, part of the Fox Kitten infrastructure and at best, still worth consideration for cyber defenders to guard against as they seem to have no legitimate business function. The same can be said for the two active hosts that have matching domain IOCs.



Link analysis diagram of Indicators of Compromise (IOCs) listed in Joint CSA AA24-241A



FBI/CISA/DC3 Report IOC Legend

Table 10. Indicators of Compromise – Recent

	Indicator	First Seen	Most Recently Observed Date
A	138.68.90[.]19	January 2024	August 2024
B	167.99.202[.]130	January 2024	August 2024
C	78.141.238[.]182	July 2024	August 2024
D	51.16.51[.]81	January 2024	August 2024
E	51.20.138[.]134	February 2024	August 2024
F	134.209.30[.]220	March 2024	August 2024

	Indicator	First Seen	Most Recently Observed Date
G	13.53.124[.]246	February 2024	August 2024
1	api.gupdate[.]net	September 2022	August 2024
2	githubapp[.]net	February 2024	August 2024

Table 11. Indicators of Compromise – Historical

	Indicator	First Seen	Most Recently Observed Date
H	18.134.0[.]66	September 2023	November 2023
I	193.149.190[.]248	September 2023	January 2024
J	45.76.65[.]42	September 2023	December 2023
K	206.71.148[.]78	October 2023	January 2024
L	193.149.187[.]41	October 2023	November 2023
3	login.forticloud[.]online	October 2023	November 2023
4	fortigate.forticloud.[]online	October 2023	November 2023
5	cloud.sophos[.]one	October 2023	November 2023

Consolidated list of IOCs from Joint CSA AA24-241A

Key Findings

Commonalities Amongst IP IOCs from Report

- 9 of the 12 hosts share geolocations
  - 7 hosts = London, UK (Hosts B, C, F,H,I, K, L)
  - 2 hosts = Stockholm, SWE (Hosts E, G)
  - 1 host each= Frankfurt, DE (Host A) Los Angeles, US (Host J) Tel Aviv, IS (Host D)
- All of the hosts have an Autonomous System Number in common with at least one other host from the group
  - AS 14061 (DIGITALOCEAN-ASN) = Hosts A, B, F
  - AS 16509 (AMAZON-02) = Hosts D, E, G, H
  - AS 399629 (BLNWX) = Hosts I, K, L
  - AS 20473 (AS-CHOOPA) = Hosts C, J
- Hosts D, E & G are not “identical” but share nearly identical patterns of ports, certificate names, and software/HTTP Titles; these patterns match findings from a Censys Mirth Connect blog from May 2024. An assessment from the blog stated that hosts with these characteristics indicated “a particular variety of honeypot-like entities that seem designed to catch internet scanners.”
- Patterns during times of interest from the report include:
  - A long list (20+) of open services/ports, the vast majority of which are HTTP
  - HTTP ports with HTML Titles and/or software fingerprints for
  - Mirth Connect (also covered in Censys Rapid Response (RR) blog)
  - Ivanti Connect Secure (covered in RR blog, RR 08APR24 Advisory)
  - Ray Dashboard (covered in RR 28MAR24 Advisory)
  - F5 BIG-IP (covered in RR blog)
  - Confluence
  - KACE
  - JetBrains Team City (only Host G)
  - ManageEngine (only Host G)
- Certificates presented on HTTP ports that are seemingly random, but reuse a list of names to appear part of legitimate organizations, including “futureenergy.us,” next-finance.mil,” “schneider-electric.oil-bright.mil” etc.

The subdomains listed in some of the certificates include some of the same software types listed above including “kace”, “bigip” and “fortinet.”

Note: Using the ‘tarpit’ label in Censys Search (especially on the same AS as Hosts D, E, & G) will help analysts find more of these same hosts with certificates matching the same pattern as the ones mentioned above.

Analysis: It appears that the owners/operators of the IOC hosts may have been attempting to obfuscate relations between the hosts by choosing various ASs, locations, certificates and port configurations among other techniques; however, by viewing the profiles of these IOC hosts in totality, patterns emerge that link the hosts. These links, coupled with their identification as IOCs by the FBI/CISA/DC3, further the claim that they are related to nefarious activity.

Commonalities in Initial Hosts Used to Uncover Possible Additional Infrastructure Not Mentioned in FBI/CISA Report

- A search conducted for the “tarpit” label (indicating hosts with an unusually high number of ports open on a host) on Censys Search within the same ASN as Hosts D, E, & G reveals a total of 38,862 hosts globally that seem to match the same patterns of Hosts D, E, & G of:
  - A long list (20+) of open services/ports, the vast majority of which are HTTP
  - Those HTTP ports with running software that includes the list above but also includes Easy IO 30P, Check Point (Check Point Security Gateways was also listed as a targeted software product in the FBI/CISA Advisory), and PanOS (again, listed in the FBI/CISA Advisory as targeted).
  - Certificates on the HTTP ports follow the same pattern as those on Hosts D, E, & G

Note: Host G exhibited these patterns in SEP & NOV23

Analysis: While further confirmation will be needed, it is logical that these hosts may be part of the same infrastructure owned by the Fox Kitten group due to the amount of similarities between the hosts found through these searches and the known bad actor Hosts D, E, & G listed in the FBI/CISA Advisory. *This information can be used by organizations to add to watchlists or blacklists, especially if those hosts match the AS, country of origin, or have similar octets to the IPs uncovered via this search.*

Censys Observed 3 Domain IOCs on IOC IPs

- IOC 1 (api.gupdate[.]net) was observed by Censys in the Forward DNS records of Host C as early as 14APR24 which is outside the activity time frame of July – August 2024 in the Advisory. The domain IOC was also in name fields of certificates on the same host as early as 27MAY24.
- IOC 2 (githubapp[.]net) was observed first by Censys in the Forward DNS records of Host G on 24FEB24 which coincides with the first active timeframe for this host in the Advisory. The IOC is still active on this host and others as of the time of this report.
- IOCs 3 & 4 (login.forticloud[.]online & fortigate.forticloud[.]online) were not observed historically on any hosts nor on any current hosts. However, the words “fortios,” “fortiproxy,” and “fortinet” have appeared on certificates of Hosts D, G and other hosts mentioned in this report that match their patterns.
- IOC 5 (cloud.sophos[.]one) was observed by Censys in the Forward DNS records of Host K on 03OCT23. This corresponds to the first active timeframe for this host as a part of Fox Kitten in the FBI/CISA Advisory of October 2023. IOC 5 is not currently observed on any active hosts.

Censys Observed Domain IOC 2 on Three Current/Active IPs Not Mentioned in the Advisory

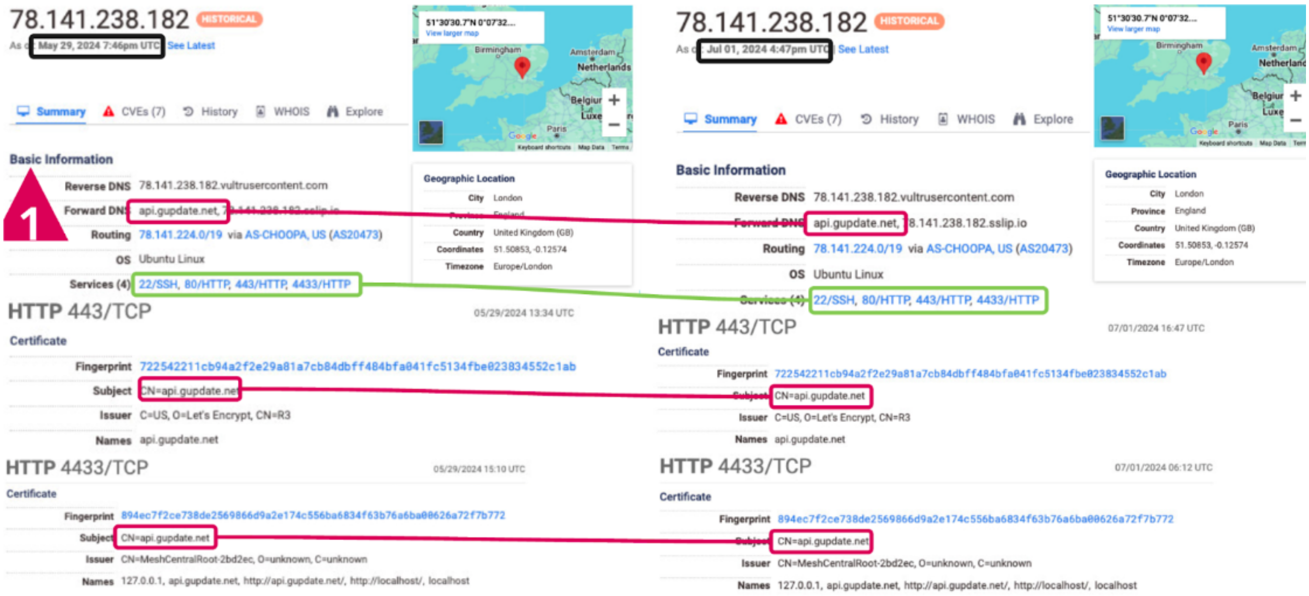
A search for IOC 2 on active hosts in Censys Search indicates that IOC 2 is currently in the forward DNS records of Host O as well as in certificates on Hosts M & N, none of which were not mentioned in the Advisory. Host O shares an AS with Hosts D, E, G, and H and Hosts M & N share an AS with Hosts C & J.

Recommendation: Defenders should consider adding these host IPs (M= 64.176.165[.]17; N= 70.34.218[.]77; O = 18.130.251[.]165) to their watchlists or blocklists.”

IOC IP Host Profiles Appear Similar or Identical Beyond the Timeframes Listed in the Report

Censys investigated the profiles of hosts tied to the IP IOCs from the CSA and noticed that some host profiles looked very similar or identical before or after the “First Seen” and “Most Recently Observed Date[s]” identified in the CSA. These observations may indicate previous or unreported attacks/activity.

Host C: First seen JUL24; most recent AUG24. Censys observed an identical host profile of Host C as early as MAY24 which is before the first seen date in the CSA, during which IOC 1 can be seen on the host. Commonalities are depicted below.



78.141.238.182

As of May 29, 2024 7:46pm UTC

Basic Information

Reverse DNS	78.141.238.182.vultrusercontent.com
Forward DNS	api.gupdate.net, 78.141.238.182.sslip.io
Routing	78.141.224.0/19 via AS-CHOOPA, US (AS20473)
OS	Ubuntu Linux
Services (4)	22/SSH, 80/HTTP, 443/HTTP, 4433/HTTP

Geographic Location

City	London
Province	England
Country	United Kingdom (GB)
Coordinates	51.50853, -0.12574
Timezone	Europe/London

HTTP 443/TCP 05/29/2024 13:34 UTC

Certificate

Fingerprint	722542211cb94a2f2e29a81a7cb84dbff484bfa041fc5134fbe023834552c1ab
Subject	CN=api.gupdate.net
Issuer	C=US, O=Let's Encrypt, CN=R3
Names	api.gupdate.net

HTTP 4433/TCP 05/29/2024 15:10 UTC

Certificate

Fingerprint	894ec7f2ce738de2569866d9a2e174c556ba6834f63b76a6ba00626a72f7b772
Subject	CN=api.gupdate.net
Issuer	CN=MeshCentralRoot-2bd2ec, O=unknown, C=unknown
Names	127.0.0.1, api.gupdate.net, http://api.gupdate.net/, http://localhost/, localhost

78.141.238.182

As of Jul 01, 2024 4:47pm UTC

Basic Information

Reverse DNS	78.141.238.182.vultrusercontent.com
Forward DNS	api.gupdate.net, 78.141.238.182.sslip.io
Routing	78.141.224.0/19 via AS-CHOOPA, US (AS20473)
OS	Ubuntu Linux
Services (4)	22/SSH, 80/HTTP, 443/HTTP, 4433/HTTP

Geographic Location

City	London
Province	England
Country	United Kingdom (GB)
Coordinates	51.50853, -0.12574
Timezone	Europe/London

HTTP 443/TCP 07/01/2024 16:47 UTC

Certificate

Fingerprint	722542211cb94a2f2e29a81a7cb84dbff484bfa041fc5134fbe023834552c1ab
Subject	CN=api.gupdate.net
Issuer	C=US, O=Let's Encrypt, CN=R3
Names	api.gupdate.net

HTTP 4433/TCP 07/01/2024 06:12 UTC

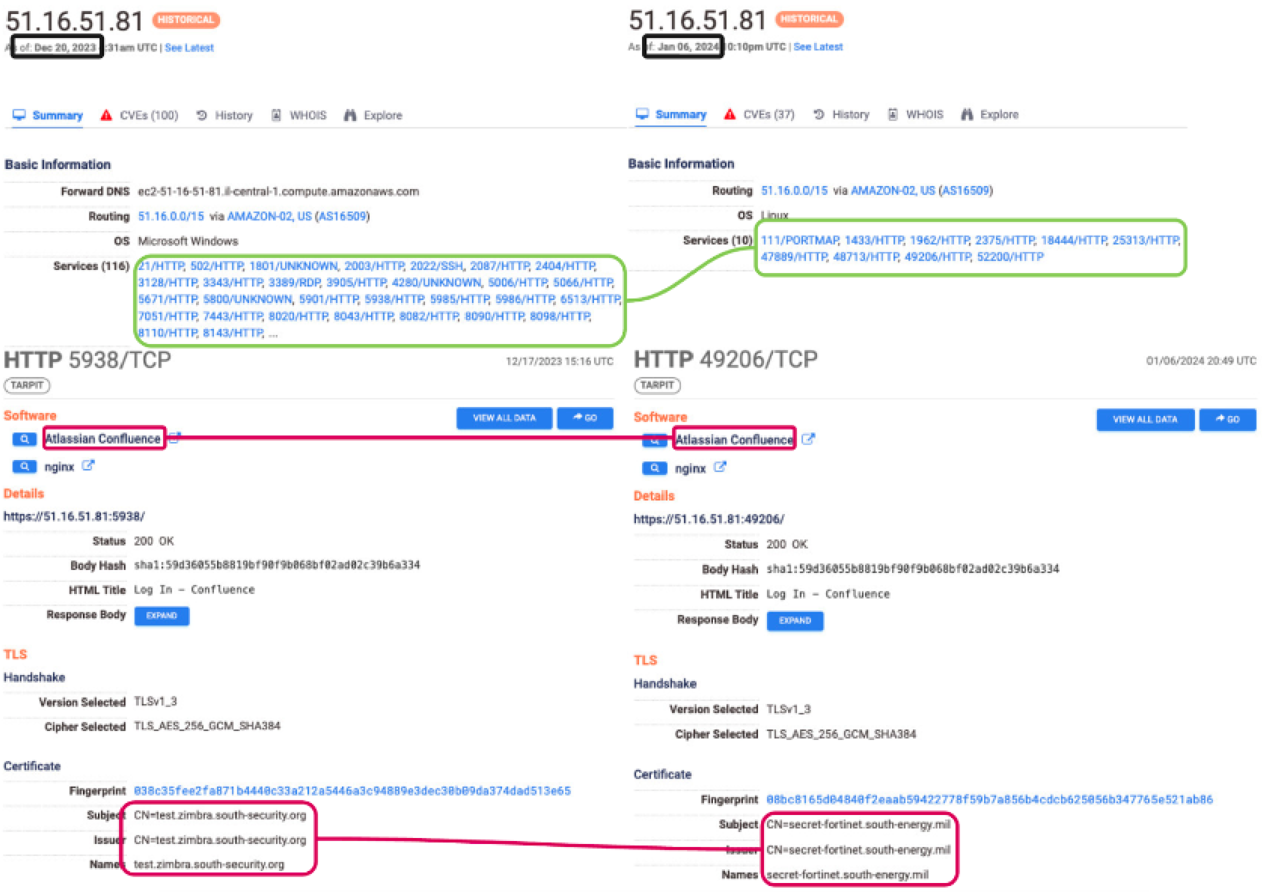
Certificate

Fingerprint	894ec7f2ce738de2569866d9a2e174c556ba6834f63b76a6ba00626a72f7b772
Subject	CN=api.gupdate.net
Issuer	CN=MeshCentralRoot-2bd2ec, O=unknown, C=unknown
Names	127.0.0.1, api.gupdate.net, http://api.gupdate.net/, http://localhost/, localhost

Host C: MAY24 (left), JUL24 (right)

Host D: First seen JAN24; most recent AUG24. Censys observed a host profile of Host D in DEC23 similar to Host D's profile in JAN24, which is one month prior to the first seen date in the CSA. Commonalities, depicted below, include a seemingly random, large number of HTTP ports open, software such as Confluence that match other hosts connected to Host D, as well as seemingly random certificate names that use the same set of keywords.

Host D: First seen JAN24; most recent AUG24. Censys observed a host profile of Host D in DEC24 similar to Host D's profile in JAN24, which is one month prior to the first seen date in the CSA. Commonalities, depicted below, include a seemingly random, large number of HTTP ports open, software such as Confluence that match other hosts connected to Host D, as well as seemingly random certificate names that use the same set of keywords.



51.16.51.81 HISTORICAL

As of: Dec 20, 2023 :31am UTC | See Latest

Basic Information

Forward DNS ec2-51-16-51-81.il-central-1.compute.amazonaws.com

Routing 51.16.0.0/15 via AMAZON-02, US (AS16509)

OS Microsoft Windows

Services (116) 21/HTTP, 502/HTTP, 1801/UNKNOWN, 2003/HTTP, 2022/SSH, 2087/HTTP, 2404/HTTP, 3128/HTTP, 3343/HTTP, 3389/RDP, 3905/HTTP, 4280/UNKNOWN, 5006/HTTP, 5066/HTTP, 5671/HTTP, 5800/UNKNOWN, 5901/HTTP, 5938/HTTP, 5985/HTTP, 5986/HTTP, 6513/HTTP, 7051/HTTP, 7443/HTTP, 8020/HTTP, 8043/HTTP, 8082/HTTP, 8090/HTTP, 8098/HTTP, 8110/HTTP, 8143/HTTP, ...

HTTP 5938/TCP 12/17/2023 15:16 UTC

TARPIT

Software

Atlassian Confluence

nginx

Details

https://51.16.51.81:5938/

Status 200 OK

Body Hash sha1:59d36055b8819bf90f9b068bf02ad02c39b6a334

HTML Title Log In - Confluence

Response Body EXPAND

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_AES_256_GCM_SHA384

Certificate

Fingerprint 038c35fee2fa871b4440c33a212a5446a3c94889e3dec38b09da374dad513e65

Subject CN=test.zimbra.south-security.org

Issuer CN=test.zimbra.south-security.org

Names test.zimbra.south-security.org

51.16.51.81 HISTORICAL

As of: Jan 06, 2024 0:10pm UTC | See Latest

Basic Information

Routing 51.16.0.0/15 via AMAZON-02, US (AS16509)

OS Linux

Services (10) 111/PORTMAP, 1433/HTTP, 1962/HTTP, 2375/HTTP, 18444/HTTP, 25313/HTTP, 47889/HTTP, 48713/HTTP, 49206/HTTP, 52200/HTTP

HTTP 49206/TCP 01/06/2024 20:49 UTC

TARPIT

Software

Atlassian Confluence

nginx

Details

https://51.16.51.81:49206/

Status 200 OK

Body Hash sha1:59d36055b8819bf90f9b068bf02ad02c39b6a334

HTML Title Log In - Confluence

Response Body EXPAND

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_AES_256_GCM_SHA384

Certificate

Fingerprint 08bc8165d04840f2eaab59422778f59b7a856b4cdcb625056b347765e521ab86

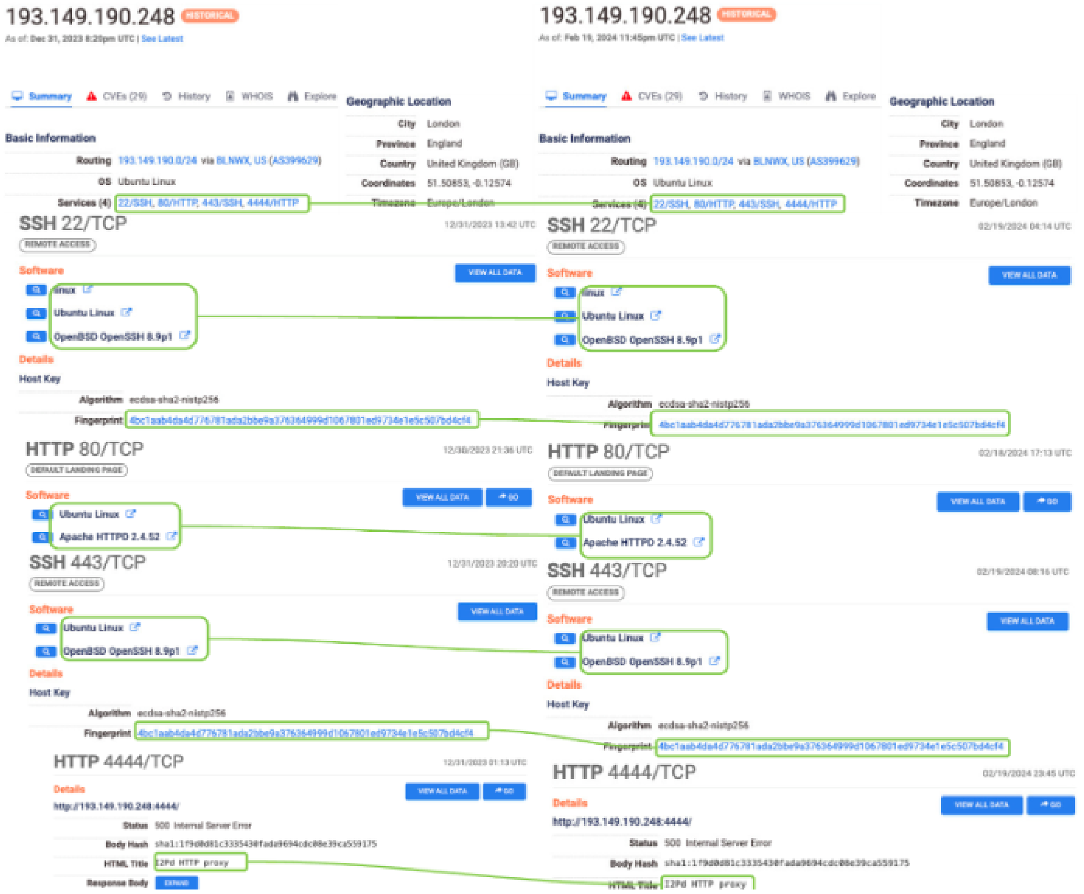
Subject CN=secret-fortinet.south-energy.mil

Issuer CN=secret-fortinet.south-energy.mil

Names secret-fortinet.south-energy.mil

Host D: DEC23 (left), JAN24 (right)

Host I: 1st seen SEP23; most recent JAN24. Censys observed a host profile of Host I in DEC23, identical to Host I's profile in FEB24, which is one month following the most recent date in the CSA. All details are the same, including the SSH key fingerprints, depicted below.



193.149.190.248 HISTORICAL

As of: Dec 31, 2023 8:20pm UTC | See Latest

Basic Information

Routing 193.149.190.0/24 via BLNWX, US (AS399629)

OS Ubuntu Linux

Services (4) 22/SSH, 80/HTTP, 443/SSH, 4444/HTTP

Geographic Location

City London

Province England

Country United Kingdom (GB)

Coordinates 51.50853, -0.12574

Timezone Europe/London

SSH 22/TCP 12/31/2023 13:42 UTC

REMOTE ACCESS

Software

linux

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

Details

Host Key

Algorithm ecdsa-sha2-nistp256

Fingerprint 4bc1aab4da4d776781ada2bbe9a376364999d1067801ed9734e1e5c507bd4cf4

HTTP 80/TCP 12/30/2023 21:36 UTC

DEFAULT LANDING PAGE

Software

Ubuntu Linux

Apache HTTPD 2.4.52

SSH 443/TCP 12/31/2023 20:20 UTC

REMOTE ACCESS

Software

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

Details

Host Key

Algorithm ecdsa-sha2-nistp256

Fingerprint 4bc1aab4da4d776781ada2bbe9a376364999d1067801ed9734e1e5c507bd4cf4

HTTP 4444/TCP 12/31/2023 01:13 UTC

Details

http://193.149.190.248:4444/

Status 500 Internal Server Error

Body Hash sha1:1f9d0d81c3335430fada9694cdc08e39ca559175

HTML Title I2Pd HTTP proxy

Response Body

193.149.190.248 HISTORICAL

As of: Feb 19, 2024 11:45pm UTC | See Latest

Basic Information

Routing 193.149.190.0/24 via BLNWX, US (AS399629)

OS Ubuntu Linux

Services (4) 22/SSH, 80/HTTP, 443/SSH, 4444/HTTP

Geographic Location

City London

Province England

Country United Kingdom (GB)

Coordinates 51.50853, -0.12574

Timezone Europe/London

SSH 22/TCP 02/19/2024 04:14 UTC

REMOTE ACCESS

Software

linux

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

Details

Host Key

Algorithm ecdsa-sha2-nistp256

Fingerprint 4bc1aab4da4d776781ada2bbe9a376364999d1067801ed9734e1e5c507bd4cf4

HTTP 80/TCP 02/18/2024 17:13 UTC

DEFAULT LANDING PAGE

Software

Ubuntu Linux

Apache HTTPD 2.4.52

SSH 443/TCP 02/19/2024 08:16 UTC

REMOTE ACCESS

Software

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

Details

Host Key

Algorithm ecdsa-sha2-nistp256

Fingerprint 4bc1aab4da4d776781ada2bbe9a376364999d1067801ed9734e1e5c507bd4cf4

HTTP 4444/TCP 02/19/2024 23:45 UTC

Details

http://193.149.190.248:4444/

Status 500 Internal Server Error

Body Hash sha1:1f9d0d81c3335430fada9694cdc08e39ca559175

HTML Title I2Pd HTTP proxy

Host I: DEC23 (left), FEB24 (right)

Censys Observed All Domain IOCs from the Advisory on 64 Currently Valid, Self-Signed Certificates

- IOC 1 (api.gupdate[.]net) = 3 valid certificates, 3 expired certificates; all issuers are Let's Encrypt except for one active certificate with issuer "unknown" with an expiration date in 2049. This certificate was also the first generated with this domain, in 2018.
- IOC 2 (githubapp[.]net) = 11 valid certificates, 12 expired certificates; all issuers are Let's Encrypt except for one expired certificate with issuer "unknown" and one active certificate with issuer "unknown" with an expiration date in 2049. Like IOC 1, this certificate was also the first generated with this domain, in 2018.
- IOC 3 (login.forticloud[.]online) = 19 valid certificates, 11 expired certificates; all issuers are Let's Encrypt. The first certificate for this domain was generated in 2023.
- IOC 4 (fortigate.forticloud[.]online) = 5 valid certificates, 11 expired certificates; all issuers are Let's Encrypt. The first certificate for this domain was generated in 2023.
- IOC 5 (cloud.sophos[.]com) = 26 valid certificates, 4 expired certificates; all issuers are Let's Encrypt. The first certificate for this domain was generated in 2023.

Analysis: Defenders should continue monitoring for these IOCs within certificates since some host IP IOCs are still active and there are 64 valid certificates that can be used on these hosts or others.

Conclusion

By studying the profiles of the hosts tied to the IOCs from the CSA over time, Censys uncovered patterns and commonalities amongst those hosts, and then used those patterns and commonalities to identify other, currently active hosts and certificates that may be part of the same Fox Kitten infrastructure. In the future, defenders can leverage IOCs, along with known periods of nefarious activity, to study host and certificate profiles before, during and after reported attacks to identify linkages, patterns, and common indicators. They can then leverage those factors to conduct dynamic searches across public scan datasets like Censys' to observe how those threats may stand up new infrastructure, leveraging the same techniques as previously observed.

Despite attempts at obfuscation, diversion, and randomness, humans still must instantiate, operate, and decommission digital infrastructure. Those humans, even if they rely upon technology to create randomization, almost always will follow some sort of pattern whether it be similar Autonomous Systems, geolocations, hosting providers, software, port distributions or certificate characteristics. If defenders can pick up on these patterns, much the same way that Soldiers in World War 2 picked up on Morse code operators' "fists" or communication personalities, they have a chance at staying one step ahead of threat actors.

Methodology

Censys used parsed fields to accurately search for the IOCs, trends, patterns, and other indicators mentioned in the Advisory or found over the course of investigation. Censys used historical profiles of hosts to investigate Censys' perspective at points in time to corroborate IOCs with timeframes listed in the Advisory as well as observations that seemed to match the profiles of IOC hosts, yet were outside of the timeframe listed in the Advisory, possibly indicating a timeframe of staging or nefarious activity not observed previously.

Censys used a link diagram analysis to identify similarities, patterns, and trends across IOCs, hosts, certificates, Autonomous Systems, and various other parsed fields from Censys' scan dataset.

[1] https://www.cisa.gov/sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations_0.pdf