Apr 15 2024

Intelligence Report

Connect:fun: New exploit campaign in the wild targets media company

NETMANAGEIT

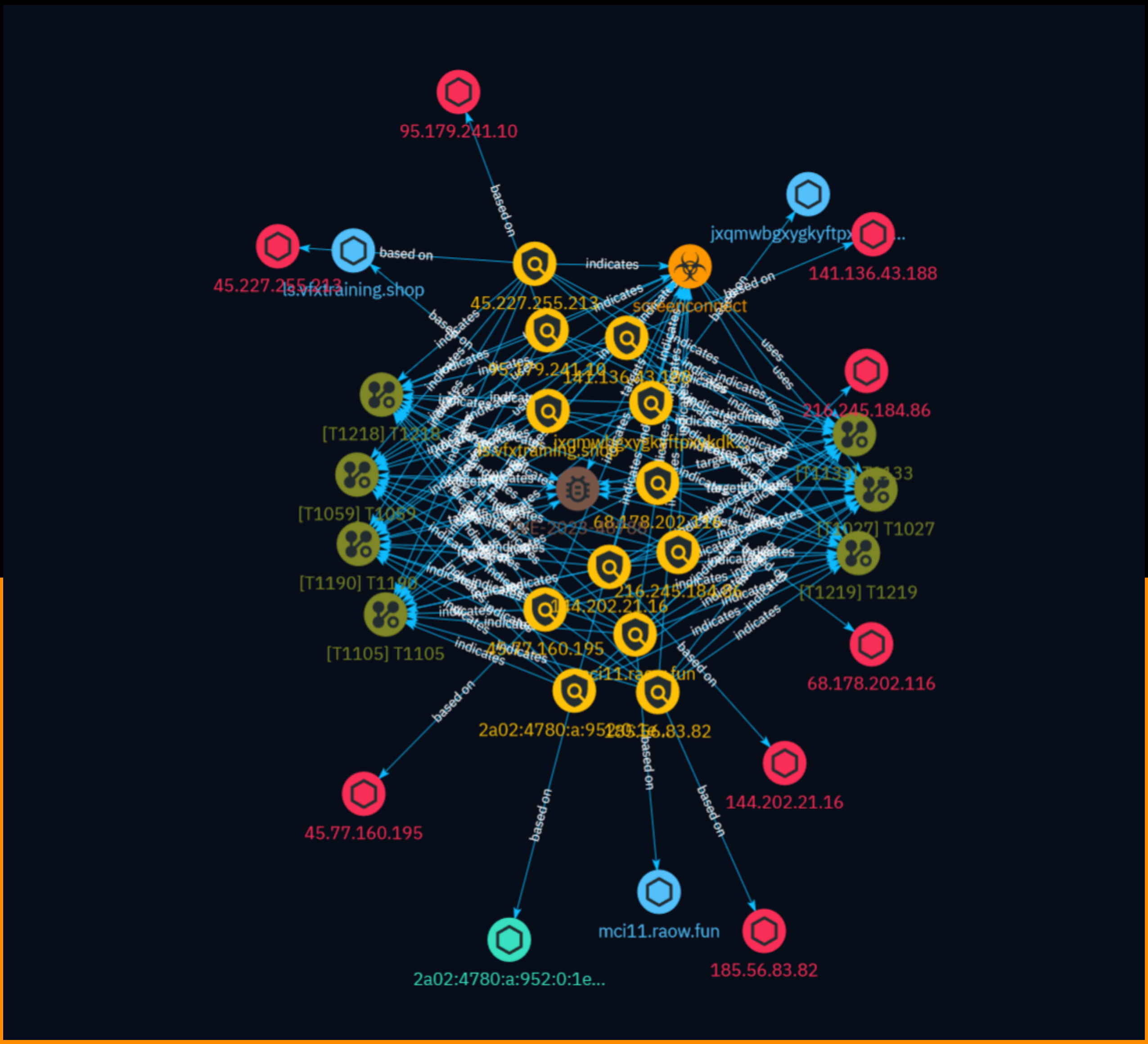

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details an ongoing exploitation campaign utilizing the recently disclosed CVE-2023-48788 vulnerability in Fortinet's FortiClient EMS solution. The actors behind this campaign are actively scanning for vulnerable systems and attempting to gain initial access by exploiting this vulnerability. Once successful, they deploy remote management tools like ScreenConnect and malicious scripts to maintain persistence and execute further malicious activities within the compromised networks. Evidence suggests a potential threat actor has been active since at least 2022, targeting Fortinet appliances and leveraging infrastructure with Vietnamese and German language elements. The report provides technical details, indicators of compromise (IoCs), and mitigation recommendations related to this ongoing campaign.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
mci11.raow.fun
Pattern Type
stix
Pattern
[hostname:value = 'mci11.raow.fun']
Name
ls.vfxtraining.shop
Pattern Type
stix
Pattern
[hostname:value = 'ls.vfxtraining.shop']
Name
jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast.fun

Pattern Type
stix
Pattern
[hostname:value = 'jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast.fun']
Name
2a02:4780:a:952:0:1e10:e79b:1
Description
CC=GB ASN=AS47583 Hostinger International Limited
Pattern Type
stix
Pattern
[ipv6-addr:value = '2a02:4780:a:952:0:1e10:e79b:1']
Name
95.179.241.10
Description
ISP: The Constant Company, LLC **OS:** - -------------------------- Services: **2083:** ``` HTTP/1.1 400 Bad Request Server: cloudflare Date: Thu, 28 Mar 2024 10:19:37 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: - ``` ------------------ **2087:** ``` HTTP/1.1 400 Bad Request Server: cloudflare Date: Wed, 27 Mar 2024 12:45:27 GMT Content-Type: text/html Content-Length: 155 Connection: close CF-RAY: -

400 Bad Request

---

cloudflare

``` ------------------ **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 21 Mar 2024 22:34:57 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ------------------ **8443:** ``` HTTP/1.1 400 Bad Request Server: cloudflare Date: Tue, 26 Mar 2024 22:06:27 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: - ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.179.241.10']

Name

68.178.202.116

Description

ISP: GoDaddy.com, LLC **OS:** - ------------------------- Services: **21:** ``` 220 ProFTPD Server (Debian) [68.178.202.116] 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD XRMD MKD XMKD PWD XPWD SIZE SYST HELP NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF* ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR STOR STOU APPE REST ABOR RANG USER PASS ACCT* REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@116.202.178.68.host.secureserver.net 211-Features: CLNT EPRT EPSV HOST LANG ja-JP;es-ES;it-IT;zh-CN;ko-KR;zh-TW;bg-BG;fr-FR;ru-RU;en-US MDTM MFF modify;UNIX.group;UNIX.mode; MFMT MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.groupname*;UNIX.mode*;UNIX.owner*;

UNIX.ownername*; RANG STREAM REST STREAM SITE COPY SITE MKDIR SITE RMDIR SITE SYMLINK SITE UTIME SIZE TVFS UTF8 211 End ``` ------------------ **25:** ``` 220 116.202.178.68.host.secureserver.net ESMTP Postfix (Debian/GNU) 250-116.202.178.68.host.secureserver.net 250-PIPELINING 250-SIZE 10240000 250-VRFY 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING ``` ------------------ **8443:** ``` HTTP/1.1 200 OK Server: nginx Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Cache-Control: max-age=0, must-revalidate, private Date: Tue, 09 Apr 2024 07:13:05 GMT Expires: Tue, 09 Apr 2024 07:13:05 GMT Set-Cookie: locale=en; path=/; secure; httponly; samesite=lax Set-Cookie: cloudpanel=4pbmonte6rlglpgk5bu1rmqrj2; path=/; secure; httponly; samesite=lax ``` HEARTBLEED: 2024/04/09 07:13:14 68.178.202.116:8443 - ERROR: heartbleed: timeout ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '68.178.202.116']

Name

45.77.160.195

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 45.77.160.195.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.81189919 - **Longitude:** -80.23179626

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.77.160.195']

Name

45.227.255.213

Description

ISP: NForce Entertainment B.V. **OS:** Linux ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLnMjQHHOYwpbAhp5w/bAt7Z vZZZMDWso6dXBbOA2+k3uA2dnjUHXxno43Dwh80KEDzG4rM6TW1UTjIP7UZqHyc= Fingerprint: c2:97:3b:e1:06:c8:82:66:24:b6:48:ae:4a:48:6d:69 Kex Algorithms: sntrup761x25519-sha512@openssh.com 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 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 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 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.227.255.213']

Name

216.245.184.86

Description

- **Zip Code:** N/A - **ISP:** BLNWX - **ASN:** 399629 - **Organization:** BLNWX - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 216.245.184.86 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Illinois - **City:** Chicago - **Latitude:** 41.84999847 - **Longitude:** -87.65000153

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.245.184.86']

Name

144.202.21.16

Description

ISP: The Constant Company, LLC **OS:** Windows (build 10.0.17763) -------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ------------------ **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 11 Apr 2024 02:13:09 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ------------------ **8443:** ``` HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Date: Sun, 17 Mar 2024 21:06:08 GMT Transfer-Encoding: chunked 800 0 ``` ------------------

Pattern Type
stix
Pattern
[ipv4-addr:value = '144.202.21.16']
Name
141.136.43.188
Description
- **Zip Code:** N/A - **ISP:** Hostinger International - **ASN:** 47583 - **Organization:** Hostinger International - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** cpl90.hosting24.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** Manchester - **Latitude:** 53.5 - **Longitude:** -2.22000003
Pattern Type
stix
Pattern
[ipv4-addr:value = '141.136.43.188']
Name
185.56.83.82
Description

CC=SC ASN=AS211720 Datashield, Inc.
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.56.83.82']

Vulnerability

Name
CVE-2023-48788
Description
Fortinet FortiClient EMS contains a SQL injection vulnerability that allows an unauthenticated attacker to execute commands as SYSTEM via specifically crafted requests.

Malware

Name
screenconnect

Attack-Pattern

Name
T1059
ID
T1059
Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1218

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS

Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)).

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

Name

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn’t require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Hostname

Value
mci11.raow.fun
ls.vfxtraining.shop
jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast.fun

IPv6-Addr

Value
2a02:4780:a:952:0:1e10:e79b:1

IPv4-Addr

Value
95.179.241.10
68.178.202.116
45.77.160.195
144.202.21.16
45.227.255.213
216.245.184.86
141.136.43.188
185.56.83.82

External References

- https://www.forescout.com/blog/connectfun-new-exploit-campaign-in-the-wild-targets-media-company/
- https://otx.alienvault.com/pulse/661ced406a4dfb51ce9084e6