NETMANAGEIT

Intelligence Report

PSA: Ongoing Webex malvertising campaign drops BatLoader

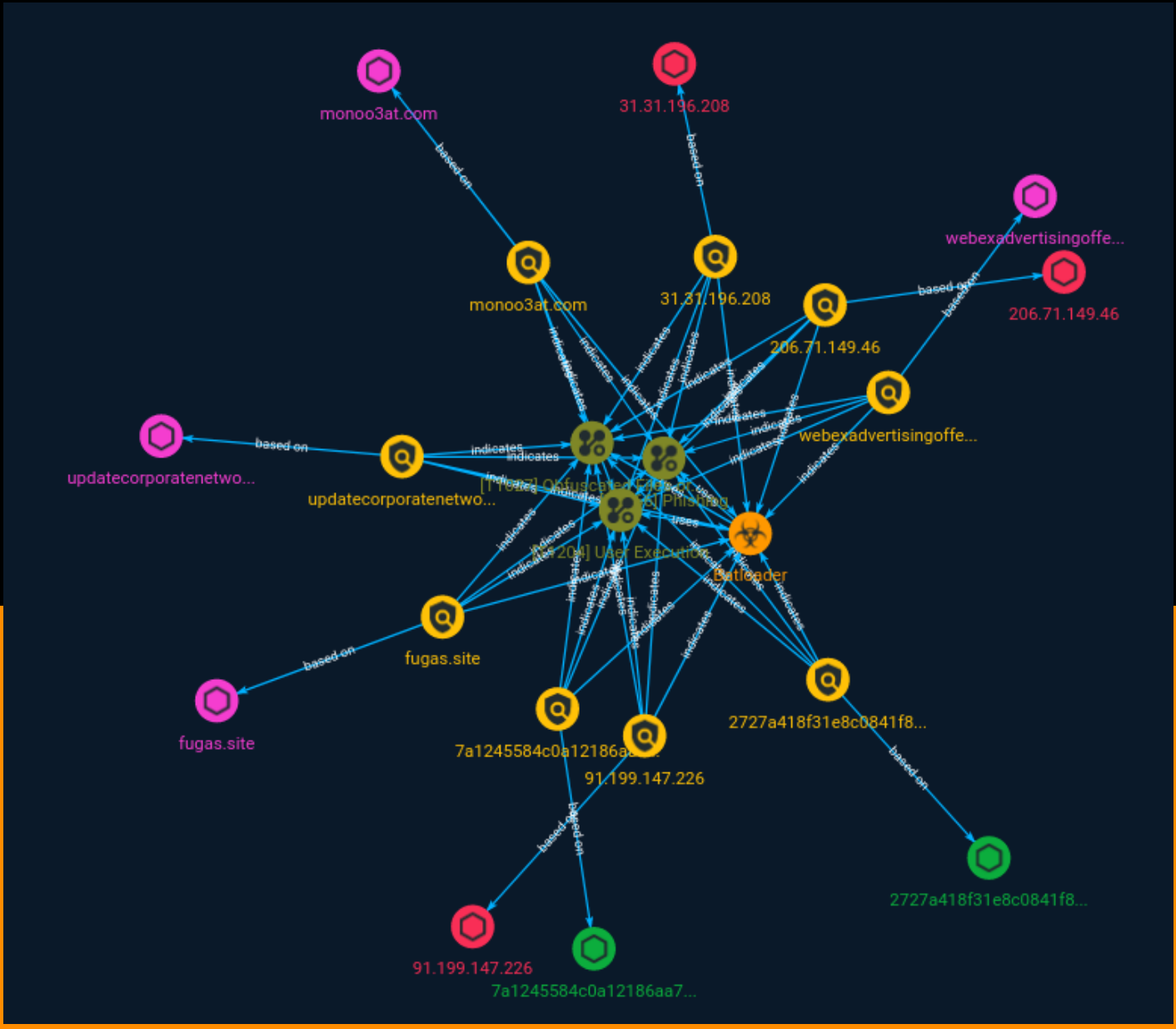

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new malvertising campaign is targeting corporate users who are downloading the popular web conferencing software Webex.

Confidence

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

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Obfuscated Files or Information

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)

Indicator

Name

206.71.149.46

Description

ISP: BL Networks **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.7 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBhKpYCya78/RsqJ9EoDuGTp FuFwOxuMr+H2dwvXs5cRx+CWUkSqYmTJ21UNF+JQmu7ds/lh3LWDsXO8gvdIGBo= Fingerprint: 1a:c5:b4:2f:ff:07:42:fd:40:f3:33:ff:25:52:8c:44 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes128-gcm@openssh.com aes128-ctr MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Sep 2023 17:13:55 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Fri, 14 Jan 2022 07:23:06 GMT Connection: keep-alive ETag: "61e124da-267" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '206.71.149.46']

Name

7a1245584c0a12186aa7228c75a319ca7f57e7b0db55c1bd9b8d7f9b397bfac8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a1245584c0a12186aa7228c75a319ca7f57e7b0db55c1bd9b8d7f9b397bfac8']

Name

monoo3at.com

Pattern Type

stix

Pattern

[domain-name:value = 'monoo3at.com']

Name

2727a418f31e8c0841f8c3e79455067798a1c11c2b83b5c74d2de4fb3476b654

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2727a418f31e8c0841f8c3e79455067798a1c11c2b83b5c74d2de4fb3476b654']

Name

fugas.site

Pattern Type

stix

Pattern

[domain-name:value = 'fugas.site']

Name

31.31.196.208

Description

ISP: "Domain names registrar REG.RU", Ltd **OS:** Linux ---------- Hostnames: - hosting.reg.ru - beloeradio.ru - beloeradio.site - server169.hosting.reg.ru - www.beloeradio.site ---------- Domains: - reg.ru - beloeradio.site - beloeradio.ru ---------- Services: **21:** ``` 220 FTP Server ready. 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 AUTH CCC* CONF* ENC* MIC* PBSZ PROT TYPE STRU MODE RETR STOR STOU APPE REST ABOR USER PASS ACCT* REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@localhost 211-Features: UTF8 LANG ja-JP;bg-BG;zh-CN;en-US*;it-IT;fr-FR;ko-KR;ru-RU;es-ES;zh-TW EPRT EPSV MDTM SSCN TVFS MFMT SIZE PROT CCC PBSZ AUTH TLS MFF modify;UNIX.group;UNIX.mode; REST STREAM MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*; 211 End ``` ---------- **22:** ``` SSH-2.0-dropbear_2022.82 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCd1GJPo30RnDjc/XUeHpe8BBOx3Wv2Sy814iqiOj6ad4B6 m7nlf9B59XRP1cdixWZK4J3ZV6b7m8BDrEs+7eQk8KSQ/

NDrsn395WSbLeGrWfTsMRrUU8sIvFpB rdA7A6ZfhJmGqgLE9EZr+UovgIeDP/ 0234ceD7AjISU5Ne6U2qjS6yCA0+VUZm0BOoAbZwhj0f5f teHjmJc/ uXF07xVTnS7Gi3nHgH2jXIW2m+eiFxYtIuoagyc7p0ZVJM/AvxfyyHZOFLDR4y/+v+hj h4hd51AWr0cRM+n4iz+ffNbazp3BIObV4AYhLdjE6Ae8HQ6syPWEKs5W9C7Srsb9Z8Id Fingerprint: 3b:62:43:fa:70:17:3d:55:27:f2:62:1e:4b:dc:8e:eb Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 kexguess2@matt.ucc.asn.au Server Host Key Algorithms: ecdsa-sha2-nistp256 rsa-sha2-256 ssh-rsa ssh-dss Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes256-ctr MAC Algorithms: hmac-sha1 hmac-sha2-256 Compression Algorithms: none ``` ---------- **25:** ``` 220 server169.hosting.reg.ru ESMTP Exim 4.96 Wed, 13 Sep 2023 15:14:18 +0300 250-server169.hosting.reg.ru Hello 224.0.239.232 [224.0.239.232] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH LOGIN PLAIN 250-STARTTLS 250 HELP ``` ---------- **53:** ``` none Resolver name: server169.hosting.reg.ru ``` ---------- **53:** ``` none Resolver name: server169.hosting.reg.ru ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 15 Sep 2023 14:11:40 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN . ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS 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. ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 15 Sep 2023 02:08:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/7.4.33 Link: ; rel="https://api.w.org/", ; rel="alternate"; type="application/json", ; rel=shortlink Strict-Transport-Security: max-age=31536000; ``` HEARTBLEED: 2023/09/15 02:09:22 31.31.196.208:443 - SAFE ---------- **465:** ``` 220 server169.hosting.reg.ru ESMTP Exim 4.96 Mon, 04 Sep 2023 14:29:55 +0300 250-server169.hosting.reg.ru Hello rhxv1cvk6ad.org [224.88.176.66] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH LOGIN PLAIN 250 HELP ``` HEARTBLEED: 2023/09/04 11:30:03 31.31.196.208:465 - SAFE ---------- **587:** ``` 220 server169.hosting.reg.ru ESMTP Exim 4.96 Thu, 07 Sep 2023 10:16:45 +0300 250-server169.hosting.reg.ru Hello hb65s5wcvog0.org [224.28.10.231] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH LOGIN PLAIN 250-STARTTLS 250 HELP ``` ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * 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: 2023/09/11 14:57:43

31.31.196.208:993 - SAFE ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/09/14 12:23:22 31.31.196.208:995 - SAFE ---------- **3306:** ``` MySQL: Protocol Version: 10 Version: 5.7.27-30 Capabilities: 65535 Server Language: 8 Server Status: 2 Extended Server Capabilities: 49663 Authentication Plugin: mysql_native_password ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.31.196.208']

Name

91.199.147.226

Description

ISP: SmartApe OU **OS:** None ---------- Hostnames: - www.updatecorporatenetworks.ru - s710873.srvape.com - updatecorporatenetworks.ru ---------- Domains: - updatecorporatenetworks.ru - srvape.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDGxSdVCgym2CDL54bOXZ3cpVKHwbmoFEcmZu01NltNscUY 9/7/tI3D9TKkDLElaXkJWDliU84NJUjw82gi5aRz01RtFav+UqTY/GXuke6aJ6ppqPLb0qTnpxmJ AQcULadZ8m5Es+S4XIxsNOrS82Kea0EssIX7PBTEnhA7S9nYsTGP6ix1gQTjSpeP97ppjgVyq0lY r2F3FzOBZPtAREtMQ4vGmQuxA3JV8tMH0kXlWWa7rePo45eeqXeF+qeTfgPTaI8Z5ZRlDKv3ARYv FM6R969gGdRvIlhHanOXcH7F6djNKBUMEJTGEuBYILU5335mrP5X3NwHm+MQmM5I6tGR Fingerprint: d9:8f:07:83:8e:a1:9c:1d:8f:26:4f:48:1d:d9:f9:e5 Kex Algorithms: 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 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa 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 ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Server: nginx/1.14.2 Date: Fri, 15 Sep 2023 11:34:46 GMT Content-Type: text/html Content-Length: 571 Connection: keep-alive ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 2 leap: 0 precision: -24 rootdelay: 0.0306701660156 rootdisp: 0.0363922119141 refid: 3557228932 reftime: 3903763731.94 poll: 3 ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Tue, 12 Sep 2023 23:21:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding ``` HEARTBLEED: 2023/09/12 23:22:31 91.199.147.226:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.199.147.226']

Name

updatecorporatenetworks.ru

Pattern Type

stix

Pattern

[domain-name:value = 'updatecorporatenetworks.ru']

Name

webexadvertisingoffer.com

Pattern Type

stix

Pattern

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

Malware

Name
Batloader

Domain-Name

Value
monoo3at.com
fugas.site
updatecorporatenetworks.ru
webexadvertisingoffer.com

StixFile

Value
7a1245584c0a12186aa7228c75a319ca7f57e7b0db55c1bd9b8d7f9b397bfac8
2727a418f31e8c0841f8c3e79455067798a1c11c2b83b5c74d2de4fb3476b654

IPv4-Addr

Value
31.31.196.208
206.71.149.46
91.199.147.226

External References

- https://otx.alienvault.com/pulse/6504b1daa3ab2929aab9745a
- https://www.malwarebytes.com/blog/threat-intelligence/2023/09/ongoing-webex-malvertising-drops-batloader