Oct 10 2023

NETMANAGEIT

Intelligence Report

Threat Actors Actively Exploiting Progress WS_FTP via Multiple Attack Chains

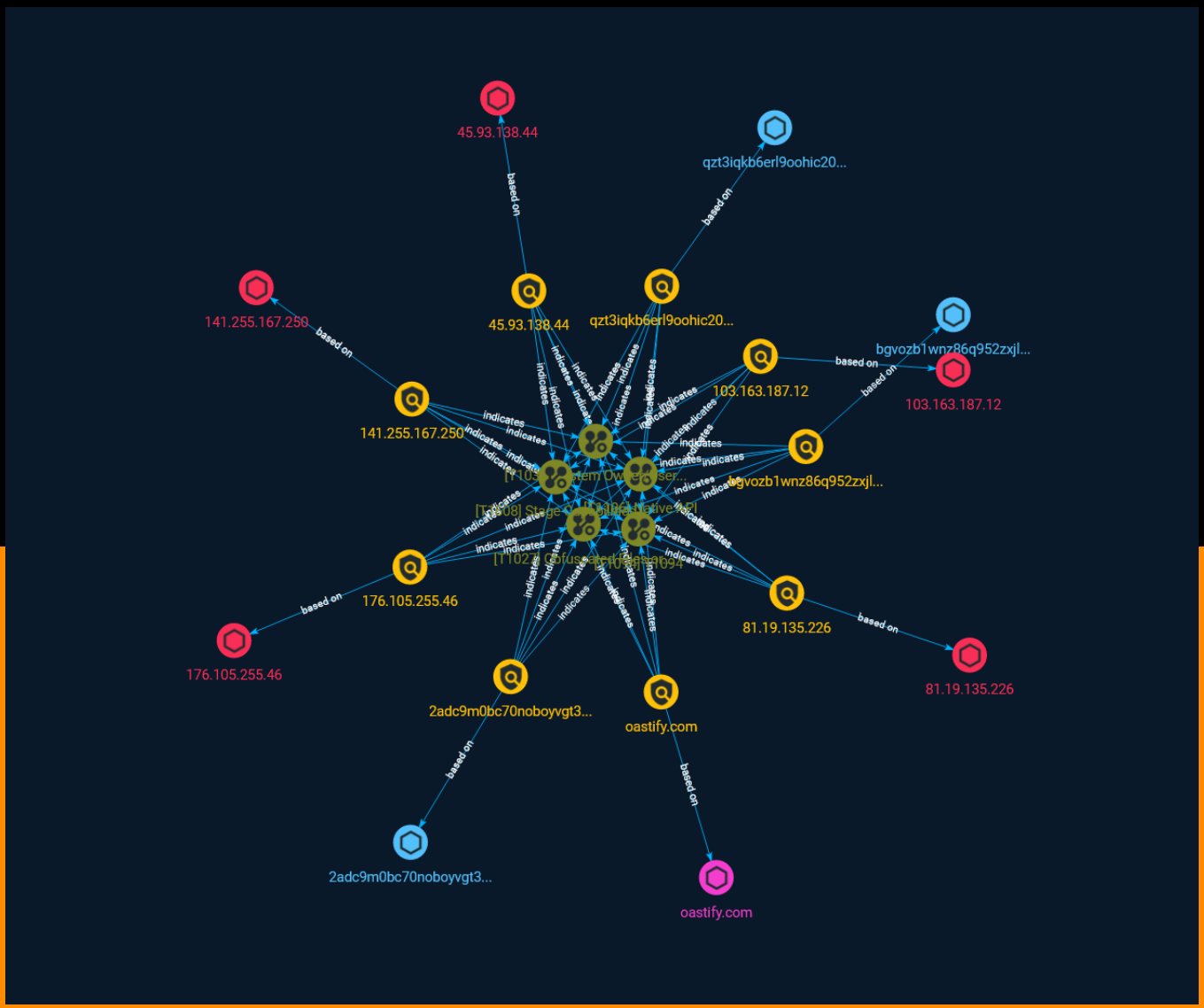

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Starting on September 30, 2023, SentinelOne has observed actors exploiting the recently disclosed flaws in Progress' WS_FTP against Windows servers running a vulnerable version of the software. The two highest severity vulnerabilities–CVE-2023-40044 and CVE-2023-42657–were assigned a CVSS score of 10 and 9.9, respectively. We observed at least three types of multi-stage attack chains, which begin with exploitation, and then commands to download a payload from a remote server, often via an IP-literal URL.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Native API
ID
T1106
Description
Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize

various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

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)

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

T1094

ID

T1094

Name

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Indicator

Name

103.163.187.12

Description

ISP: SpeedyPage Ltd **OS:** Ubuntu ---------- Hostnames: - 12.187.163.103.speedyvps.uk ---------- Domains: - speedyvps.uk ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCmsh00Ma4dLEmPBwV8OynGvIAzXvcJPHxaZaXyesaiFxu+ bxQM1ycZrByIiUUG1AjGvxi11Y5jN8wQnenDnyLLllou882i1CZkDUg0W6xBk4FUSSwVklt0E4GEeIf9/yZyKF+z9tsHwnVqNWU/CpXgspEc9mkG4EGkBZIfM8cVP8JP/a6nNK9+JLWg1tlvc6kZ5bcNF2QAcVtXjRri7NtOZjWA/XN8X75YxBCnjJYqNBIWNSA8+qAv7SvaT6jW69++M6cUii+3gCq5zKBwKDphgt4Bj7SCAy8eKCpwCsTvruY87Fk0Fbed9Rvj0u+TeSQDgfx4EUwELOxujALOh0bz Fingerprint: 31:a0:f0:89:64:0b:54:57:e7:84:22:a0:92:96:2e:db 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: ssh-rsa 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 ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Wed, 13 Sep 2023 21:53:19 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 13 Connection: keep-alive Cache-Control: no-cache, no-store, must-revalidate Expires: 0 Pragma: no-cache Vary: Accept-Encoding ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Wed, 06 Sep 2023 11:56:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 13 Connection: keep-alive Cache-Control: no-

cache, no-store, must-revalidate Expires: 0 Pragma: no-cache Vary: Accept-Encoding ```
HEARTBLEED: 2023/09/06 11:57:04 103.163.187.12:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.163.187.12']

Name

2adc9m0bc70noboyvgt357r5gwmnady2.oastify.com

Pattern Type

stix

Pattern

[hostname:value = '2adc9m0bc70noboyvgt357r5gwmnady2.oastify.com']

Name

45.93.138.44

Description

CC=LT ASN=AS47583 Hostinger International Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.93.138.44']

Name

81.19.135.226

Description

CC=RU ASN=AS209588 Flyservers S.A.

Pattern Type

stix

Pattern

[ipv4-addr:value = '81.19.135.226']

Name

176.105.255.46

Description

ISP: BREEZLE LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDDOF5eKQrIJ6M7n8nkrj6n3wsfCZXeQwe2XK9T9Jts2xqdlYKTu7BxOST1RP2HWSiL4/23jUGBo2pjU0mQcC9Hj9cOoawO4kKHwtRxNrS4QIYqGOhJ69nSemL4 XRG1xW1J3GE8cwvCV9WHIgvKS4SEnh0vIpM07ytC0jAj949lHk+kr1czAWOBVerv3jvJT+9577A4agyMwZwSkDWNjBG8PcJbyOXaxLo+YUF57eq5xnwEuUj24D2lxRC2PFampID6SIqOzf984B/Es/DhrsOxr25ZdOfWx5bQ11XZ46Fvn7a70sUt8UyeFDowQQ1zQHhOLcP9xZjcNaZMOmLEl2Fizi9TluGr8utwwrtBCOu8RFWfF66WZ+22pLu6WWIc6IUaKa/QHYpJkxVCRxacfvmHIPWxw+YeOIYdYZ9uX7IaWljY9TrfWtn+b2oC3KAtFyEkcRQtcnvp4gT9r/4keYaUoqYlf2KNheVQaCY3+9dE2eFXwHWmVw5E03/kWBbkxrc= Fingerprint: bd:aa:9b:69:b9:1c:34:eb:89:75:85:93:0e:da:73:fc 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: ssh-rsa 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 10 Oct 2023 07:28:43 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Tue, 26 Sep 2023 06:01:11 GMT ETag: "2aa6-6063ccd4482fb" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **4000:** ```` ```` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.105.255.46']

Name

qzt3iqkb6erl9oohic20f9bal1rsfh.oastify.com

Pattern Type

stix

Pattern

[hostname:value = 'qzt3iqkb6erl9oohic20f9bal1rsfh.oastify.com']

Name

oastify.com

Pattern Type

stix

Pattern

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

Name

141.255.167.250

Description

ISP: Private Layer INC **OS:** None ---------- Hostnames: - hostedby.privatelayer.com ---------- Domains: - privatelayer.com ---------- Services: **21:** ``` 220 pyftpdlib 1.5.8 ready. 230 Login successful. 214-The following commands are recognized: ABOR ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MFMT MKD MLSD MLST MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR RNTO SITE SIZE STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD XPWD XRMD 214 Help command successful. 211-Features supported: EPRT EPSV MDTM MFMT MLST type*;perm*;size*;modify*;unique*;unix.mode;unix.uid;unix.gid; REST STREAM SIZE TVFS UTF8 211 End FEAT. ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC1BBYE3Ac9YvICE/UWH2G2KpKRHmB74+jCSvW9bYXd2wWC RwX6NSbvSPGokj4sH0xgBTRM6hYfNsqSC0F4LOS0x29LIzbQ7Z60BIrGISnsV0FatmBD4+2E64Uv IG7gtyp48+f0yIAQTS85CKRBwc+nqKIadM9EVjompiKKB9GpZCmcoiFWCsJacma/GO5HKNiktfQx qhE6zSV5xbeSGxKhjDeI33ndgSe/LjcOjJcuR1oIalM4jZA0kGtmAjkzXAUygwBB0MqQGXjp07tH azPAmwnd5lvcsTAqEFB75In+ywW4l2dbuqgCwG+mTstmn9ZHBxV7A5LHrBAhK66AsN+QsM1/ cvjd XiGXmJ/ZYJj9tp79I5onp2j+Ry6zYWBzUtwgsDG7k2mtkzM8Z0QZczdaJdkr/4Mfz9kG3n0FCciN GxzxBmnpFsAgXf6bv6iLXpG/QIS0960MbglDXP54Ye3DCX2QILxn45APWuxRs6iZBrGSUeOS/JxI 5FMn4nMzw9k= Fingerprint: ad:97:73:91:47:fa:88:22:a6:eb:27:79:9d:e3:65:ce 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 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/1.1 200 OK Date: Tue, 10 Oct 2023 06:32:05 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Fri, 22 Sep 2023 13:21:00 GMT ETag: "2aa6-605f27ac219ed" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` SSL Error: TLSV1_ALERT_PROTOCOL_VERSION ``` HEARTBLEED: 2023/10/10 09:55:33 141.255.167.250:443 - ERROR: remote error: protocol version not supported ---------- **8080:** ``` ``` ---------- **8081:** ``` ``` ---------- **31337:** ``` SSL Error: TLSV1_ALERT_PROTOCOL_VERSION ``` HEARTBLEED: 2023/10/10 10:04:44 141.255.167.250:31337 - ERROR: remote error: protocol version not supported ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '141.255.167.250']

Name

bgvozb1wnz86q952zxjlwusv2m8gw5.oastify.com

Pattern Type

stix

Pattern

[hostname:value = 'bgvozb1wnz86q952zxjlwusv2m8gw5.oastify.com']

Domain-Name

Value
oastify.com

Hostname

Value
bgvozb1wnz86q952zxjlwusv2m8gw5.oastify.com
qzt3iqkb6erl9oohic20f9bal1rsfh.oastify.com
2adc9m0bc70noboyvgt357r5gwmnady2.oastify.com

IPv4-Addr

Value
81.19.135.226
103.163.187.12
141.255.167.250
45.93.138.44
176.105.255.46

External References

- https://otx.alienvault.com/pulse/6525605d7e0da326e806369b
- https://www.sentinelone.com/blog/threat-actors-actively-exploiting-progress-ws_ftp-via-multiple-attack-chains/