Jul 27 2023

NETMANAGEIT

Intelligence Report

Into the tank with Nitrogen

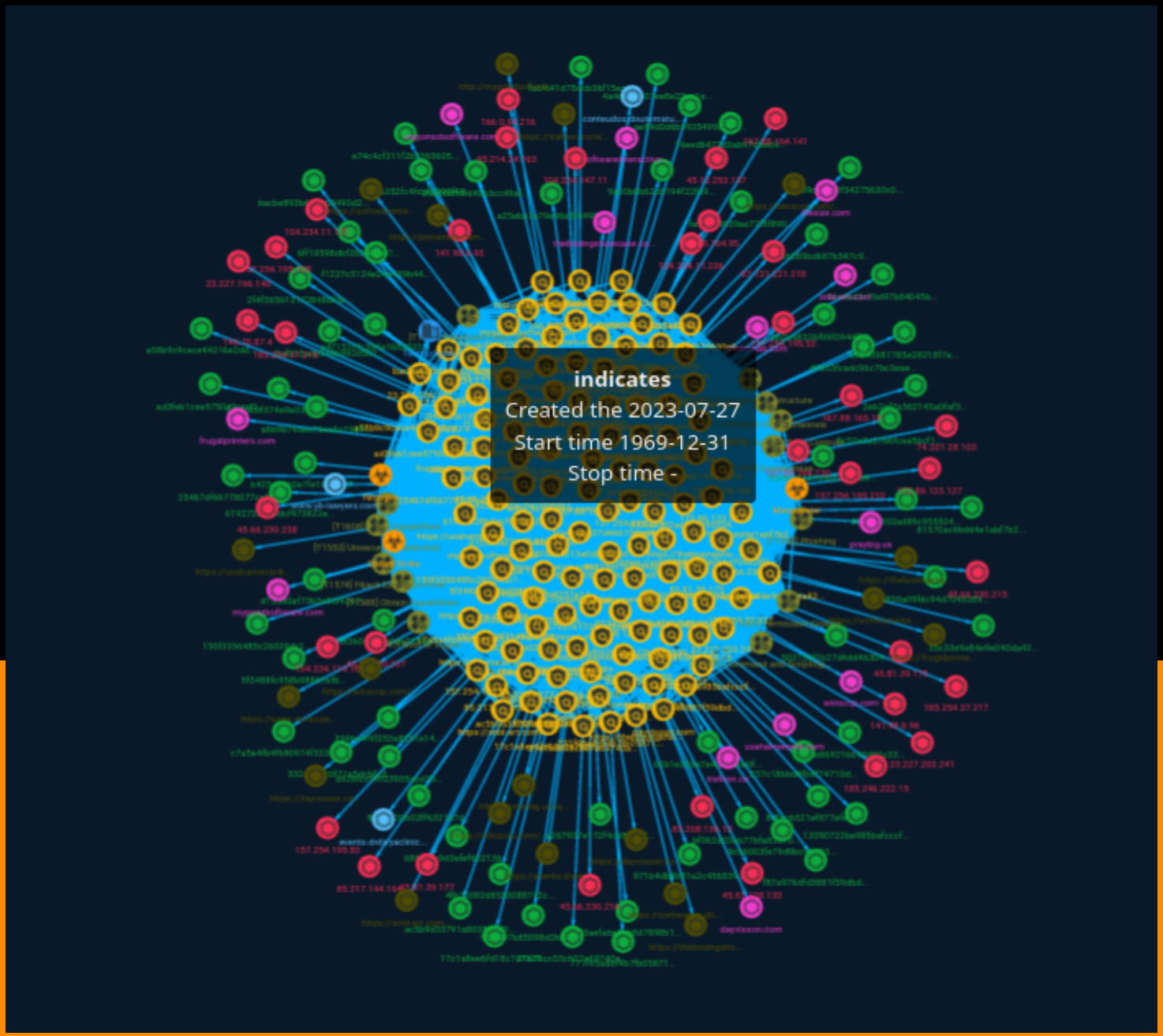

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A previously unreported initial-access malware family, known as Nitrogen, has been identified by researchers and is likely to use this infection chain to stage compromised environments for ransomware.

Confidence

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

15 / 100

Indicator

Name
503156f1b27d4dd463048f85924a2bbbeb3d0e09de2574395a51f77b48e9639d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '503156f1b27d4dd463048f85924a2bbbeb3d0e09de2574395a51f77b48e9639d']
Name
a267937e172f4cd8ce873e4fcfceeddf07ae03db68f64e047f940e2e7a2a136a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a267937e172f4cd8ce873e4fcfceeddf07ae03db68f64e047f940e2e7a2a136a']
Name

d155d0af73b3e86f42672714caa4391ab615c426a3e3fc44a41e4d125a06172a

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd155d0af73b3e86f42672714caa4391ab615c426a3e3fc44a41e4d125a06172a']

Name

e47151f7c394e1b530314cc15d482b5ce797c803c251a61e45efb0316115c677

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e47151f7c394e1b530314cc15d482b5ce797c803c251a61e45efb0316115c677']

Name

0af013ad0548b992d50287e3b11963cad9aa0af1f1e47e254637d28ee05208d8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0af013ad0548b992d50287e3b11963cad9aa0af1f1e47e254637d28ee05208d8']

Name

62b1e355a7e4c850bb0f03c7f182f48f0ebaafa07ddae1fee599a78772d149f2

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '62b1e355a7e4c850bb0f03c7f182f48f0ebaafa07ddae1fee599a78772d149f2']

Name

https://winsccp.com/eng/download.php

Pattern Type

stix

Pattern

[url:value = 'https://winsccp.com/eng/download.php']

Name

https://protemaq.com/wp-content/update/iso/6.1/tusto/WinSCP-6.1-Setup.iso

Pattern Type

stix

Pattern

[url:value = 'https://protemaq.com/wp-content/update/iso/6.1/tusto/WinSCP-6.1-Setup.iso']

Name

85.208.136.13

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.208.136.13']

Name

trafcon.co

Pattern Type

stix

Pattern

[domain-name:value = 'trafcon.co']

Name

https://winsccp.com/HPVrxkWv?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE

Pattern Type

stix

Pattern

[url:value = 'https://winsccp.com/HPVrxkWv?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE']

Name

a25f3604213a0db2375ddc2af800faa3833dc5597ca20b3138462c1d77faf952

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a25f3604213a0db2375ddc2af800faa3833dc5597ca20b3138462c1d77faf952']

Name

theboxingshowcase.com

Pattern Type
stix
Pattern
[domain-name:value = 'theboxingshowcase.com']
Name
157.254.195.53
Description
CC=US ASN=AS14956 -Reserved AS
Pattern Type
stix
Pattern
[ipv4-addr:value = '157.254.195.53']
Name
a8b9b74dee76ea6a19845b80498d91e002133d20741b6707744fb345a3581abe
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'a8b9b74dee76ea6a19845b80498d91e002133d20741b6707744fb345a3581abe']

Name

www.yb-lawyers.com

Pattern Type

stix

Pattern

[hostname:value = 'www.yb-lawyers.com']

Name

237c18bbd8fb8f74710dacaf7795c473a988b66fce667facc6f17b2c6e071745

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '237c18bbd8fb8f74710dacaf7795c473a988b66fce667facc6f17b2c6e071745']

Name

45.66.230.237

Description

CC=BG ASN=AS211252 Delis LLC

Pattern Type
stix
Pattern
[ipv4-addr:value = '45.66.230.237']
Name
167.88.164.130
Description
CC=US ASN=AS14956 -Reserved AS
Pattern Type
stix
Pattern
[ipv4-addr:value = '167.88.164.130']
Name
45.66.230.216
Description
CC=BG ASN=AS211252 Delis LLC
Pattern Type
stix

Pattern

[ipv4-addr:value = '45.66.230.216']

Name

a25eba7a79e46e5f6498ccb82fb4ef0eb3abe784fa0d061fe9e1adce9d39caa7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a25eba7a79e46e5f6498ccb82fb4ef0eb3abe784fa0d061fe9e1adce9d39caa7']

Name

https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE

Pattern Type

stix

Pattern

[url:value = 'https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE']

Name

61927228b3dcf973822eb5fff44ca7940d950af7116aefe957cc31287c5283d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61927228b3dcf973822eb5fff44ca7940d950af7116aefe957cc31287c5283d5']

Name

87.121.221.218

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '87.121.221.218']

Name

https://dayvisson.com/Cisco-Mobility-Client-v4.iso

Pattern Type

stix

Pattern

[url:value = 'https://dayvisson.com/Cisco-Mobility-Client-v4.iso']

Name

104.234.119.16

Description

ISP: RouterHosting LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **8880:** ``` HTTP/1.1 200 OK Connection: close Server: Apache Content-Length: 44


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

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '104.234.119.16']

**Name**

9c57a2a27b6fcea5bcf1eda791ccdaa0eb3fdbf93781b37283d956332f4d2ceb
```

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c57a2a27b6fcea5bcf1eda791ccdaa0eb3fdbf93781b37283d956332f4d2ceb']

Name

fce4ca6e37d466154ed49871ac31116473b1c72cf36a9653af80e9cc83edb358

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fce4ca6e37d466154ed49871ac31116473b1c72cf36a9653af80e9cc83edb358']

Name

protemaq.com

Pattern Type

stix

Pattern

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

Name

157.254.195.210

Description

ISP: RouterHosting LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAQCI2I4FHp0Y2UovBi8sy8++UwNBtNlNzBnKrEszEL/q7JqfvWf8GkS+e0CoQIWzv8puKkZuPjQJGFT1nrWzkc= Fingerprint: 50:35:36:8e:6a:cd:7c:01:af:93:38:a7:7f:c0:87:d2 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 ``` ---------- **8880:** ``` HTTP/1.1 200 OK Connection: close Server: Apache Content-Length: 44

It works!

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

## Pattern Type

stix

## Pattern
```

[ipv4-addr:value = '157.254.195.210']

Name

150f3356485c26039dc145d0bedda265d3e9626fd1f3a180455f8b911c53c260

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '150f3356485c26039dc145d0bedda265d3e9626fd1f3a180455f8b911c53c260']

Name

d9d53fcadc96c7bc3eae0a84a574b6222f0c906ee4916a9e68e0322b5c694d49

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd9d53fcadc96c7bc3eae0a84a574b6222f0c906ee4916a9e68e0322b5c694d49']

Name

971b4db8b81a2c456839d4609364bb6cd7800c9ce980379bb5a11d1d4689d504

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '971b4db8b81a2c456839d4609364bb6cd7800c9ce980379bb5a11d1d4689d504']

Name

141.98.6.95

Description

CC=BG ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '141.98.6.95']

Name

104.234.11.236

Description

CC=CA ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.234.11.236']

Name

8f02fa20b02ff6321a7db6dae478c2215bb463ebec6de4db73f247873aca1315

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8f02fa20b02ff6321a7db6dae478c2215bb463ebec6de4db73f247873aca1315']

Name

167.88.165.18

Description

ISP: RouterHosting LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHM3qqnhRwooeG579yxNrR0U tDz0pV47ROki3AO17pygQ50UyeISFzDlXkiPnXWru24lFeQQl2pfdZ9n7w52W3Y= Fingerprint: d7:de:b6:bc:91:36:e7:c0:6a:d9:1e:0a:5c:b1:ef:b9 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 ``` ---------- **8880:** ``` HTTP/1.1 200 OK Connection: close Server: Apache Content-Length: 44

It works!

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

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [ipv4-addr:value = '167.88.165.18'] |
| **Name** |
| 9c66003fe79d9bc9570373c465e69dd5db56f24c51ad4bb16c83efde5b966510 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '9c66003fe79d9bc9570373c465e69dd5db56f24c51ad4bb16c83efde5b966510'] |
| **Name** |
| b425de9b0e7fe10b89b730339bbcda2d0d4668f5b9226be633409cfb89b3dacd |
```

Description

SUSP_XORed_URL_in_EXE

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b425de9b0e7fe10b89b730339bbcda2d0d4668f5b9226be633409cfb89b3dacd']

Name

fa911a3639ae77f8f890fb76ba1ab78c2ab17ab80bdfec381ab6a9ba8fef32fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa911a3639ae77f8f890fb76ba1ab78c2ab17ab80bdfec381ab6a9ba8fef32fe']

Name

https://events.drdivyaclinic.com/wp-content/task/update/WinSCP-6.1-Setup.iso

Description

ISO 9660 CD-ROM filesystem data '05_23_2023'
25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c

Pattern Type
stix
Pattern
[url:value = 'https://events.drdivyaclinic.com/wp-content/task/update/WinSCP-6.1-Setup.iso']
Name
26a68bfc0d40b3cc49af1958f2004f404c960663b140fd612a2a53ccaf99f004
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '26a68bfc0d40b3cc49af1958f2004f404c960663b140fd612a2a53ccaf99f004']
Name
81570ac9bdd4e1abf7b296b528c7507e7df773a7c3cf05ef01a874ba9af1b36f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '81570ac9bdd4e1abf7b296b528c7507e7df773a7c3cf05ef01a874ba9af1b36f']

Name

b926fcc98f23905abd76b7ed9fa50fb84cc66aa9fb7994064ada715702e80722

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b926fcc98f23905abd76b7ed9fa50fb84cc66aa9fb7994064ada715702e80722']

Name

167.88.164.95

Description

ISP: RouterHosting LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMwRUZG6+QQGqS0SH3RBOd32 EKJ0q0SUn9SX3JHuZ8EvZ4xXly2Acw8sL+tFyFQvqaWWXrMgXmNYLA0eU4L9BCg= Fingerprint: 66:a0:78:a7:df:91:40:06:9b:12:58:f2:41:43:73:be Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 = '167.88.164.95']

Name

usahamenarik.com

Pattern Type

stix

Pattern

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

Name

185.254.37.216

Description

CC=BG ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.254.37.216']

Name

8000af302ad89c9555241366edc65b9b9b24828c8ea74bde658984b92e8c8ec6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8000af302ad89c9555241366edc65b9b9b24828c8ea74bde658984b92e8c8ec6']

Name

686c7fc9d3efef602136cde2716d20ca13d1e3de3c57f787fa74e28cc8b743cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '686c7fc9d3efef602136cde2716d20ca13d1e3de3c57f787fa74e28cc8b743cd']

Name

9a00b8b62d5194f22f690127084f626b1abbf88777b5b8474799bca1576e5fbd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a00b8b62d5194f22f690127084f626b1abbf88777b5b8474799bca1576e5fbd']

Name

ccd5e869216640460c3329e41ec30fa22ee729f0b4fc2e61781026c4defea6e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ccd5e869216640460c3329e41ec30fa22ee729f0b4fc2e61781026c4defea6e6']

Name

mypondsoftware.com

Pattern Type

stix

Pattern

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

Name

45.12.253.137

Description

ISP: Delis LLC **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-

OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDUZC5jMdDBbg94DvSSPekqk2J5ZPCYKNmk7iQqmlhO79cs dMTMm+nGjwoxjIkHVbGZ7dFIMRz9YVaV7rdrlG2iBZDAzw4SSpso245f3YaDLhiylGh0kHdYAhHwmqUDXRJA5+Syq9937erOO6iuLfVzlDaEkaE7LH3Trr1K6pNQDUgbPWZJxtZ/s3fJFdk1FYiaOa2405BsM0NitfxDWyyFbY+79fHRC+pIrMOIekQ++NlPjYmj36CNN12Dw06cHkuFI7KRsEy8z+5zSuZHcSQC//lStlfROmSC9zb++uU2DPoyxJ3e6fn0QtGvFfSOZTw7qiNOocOZu1jZXM94Mzpa8/WwA8YhdqfeVUxgqt2eXZsZ84g11MvLkOGLGQnHLnTtXus6Ru5e5m6+e5+eWElo/O6HC8U9V5/UZsm/f2ZZ iC8Vl1Roq62QhzrLVpWT2hyXoksV/zlVAeOODhOJLD5l8qT545z7ociyI0Jp2/MOWiXysHtNd6ID DQ3gIWurm5k= Fingerprint: e4:59:62:ca:0d:dd:5f:5a:c4:d3:42:7c:5c:e9:ef: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-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: Fri, 21 Jul 2023 05:02:10 GMT Server: Apache/2.4.56 (Debian) Last-Modified: Mon, 15 May 2023 21:37:11 GMT ETag: "29cd-5fbc241e1b2f9" Accept-Ranges: bytes Content-Length: 10701 Vary: Accept-Encoding Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.12.253.137']

Name

535aefaba2eb8d7898b176b0dcdd23fcef984994e609db222c33ece2d1c081b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '535aefaba2eb8d7898b176b0dcdd23fcef984994e609db222c33ece2d1c081b3']

Name

f1227c5124e24e439b44083369d7fa7a719e076f5839629d2ef10aa5e19e6afc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1227c5124e24e439b44083369d7fa7a719e076f5839629d2ef10aa5e19e6afc']

Name

2eb2ef7a562145a0faf3c82f439221908adfcc784022a64e5bb17a432f4a8a91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2eb2ef7a562145a0faf3c82f439221908adfcc784022a64e5bb17a432f4a8a91']

Name

3346a4f9f253a8251e14f0d42138e5b4420dd3c1b46afcd9f688d4e26c98c561

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3346a4f9f253a8251e14f0d42138e5b4420dd3c1b46afcd9f688d4e26c98c561']

Name

95.214.24.163

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **8880:** ``` HTTP/1.1 200 OK Connection: close Server: Apache Content-Length: 44


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

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '95.214.24.163']
```

Name

bf062d03ab77bfa835700f7131e6f95f19e2c5015ff65e47614b736ea9817dd6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf062d03ab77bfa835700f7131e6f95f19e2c5015ff65e47614b736ea9817dd6']

Name

2f4f365613172848df3e91d43514b9da34b8c84eded8fae683f94586d22f86cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f4f365613172848df3e91d43514b9da34b8c84eded8fae683f94586d22f86cf']

Name

db2a48326f99f0944f50800539817cfb6562f2bfbbcc2f2409901319eb3592ec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db2a48326f99f0944f50800539817cfb6562f2bfbbcc2f2409901319eb3592ec']

Name

4fb70092d8533088742ca23788f29e0802b223eada1748ce82731162d25920c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fb70092d8533088742ca23788f29e0802b223eada1748ce82731162d25920c7']

Name

104.234.147.11

Description

CC=CA ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.234.147.11']

Name

praybig.us

Pattern Type

stix

Pattern

[domain-name:value = 'praybig.us']

Name

332e19cc0f71a5dcbfc3d24fb08564589d0cb884d21d1fddbbf9c0230d678ec0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '332e19cc0f71a5dcbfc3d24fb08564589d0cb884d21d1fddbbf9c0230d678ec0']

Name

ae84d0d6b9935499a5e0e18052ce7ea64378eba1e9579ca98fdd925d8e6f8639

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ae84d0d6b9935499a5e0e18052ce7ea64378eba1e9579ca98fdd925d8e6f8639']

Name

f87a976dfd3881f59dbd2ea53fbfa3a663e1fff83a333b548b4fdc4651d5b8f7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f87a976dfd3881f59dbd2ea53fbfa3a663e1fff83a333b548b4fdc4651d5b8f7']

Name

a58b9c9cece44216e2dd3304fd4825db3c324393607574f87bec00be505a0d93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a58b9c9cece44216e2dd3304fd4825db3c324393607574f87bec00be505a0d93']

Name

6c340981785e28218f7ef5ee991e1888fadce9a3c29bc31316359562386124bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c340981785e28218f7ef5ee991e1888fadce9a3c29bc31316359562386124bd']

Name

https://praybig.us/wp-content/smb/srs/24/5333/WinSCP-6.1-Setup.iso

Pattern Type

stix

Pattern

[url:value = 'https://praybig.us/wp-content/smb/srs/24/5333/WinSCP-6.1-Setup.iso']

Name

166.0.94.216

Description

ISP: RouterHosting LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGmEWYOQVzK8IHQo9CWT7CeA V47c7y3bn3fjPRMZukK3f1HC8BFl9+G8ljDQSQHixcabqLFPjYKXtHafiATtTqA= Fingerprint: 60:a9:1c:b2:be:44:c6:b6:de:05:c8:25:3e:26:58:37 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 ``` ---------- **8880:** ``` HTTP/1.1 200 OK Connection: close Server: Apache Content-Length: 44

It works!

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

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [ipv4-addr:value = '166.0.94.216'] |
| **Name** |
| 8dfac6521ef877efede0a82bf46d94f590127e2607b78d08321953796fddbba9 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '8dfac6521ef877efede0a82bf46d94f590127e2607b78d08321953796fddbba9'] |
| **Name** |
| frugalprinters.com |
```

Pattern Type
stix
Pattern
[domain-name:value = 'frugalprinters.com']
Name
tresize.com
Pattern Type
stix
Pattern
[domain-name:value = 'tresize.com']
Name
17c1a8ee6fd18c7a75270c31b6602c12592242affdd6608f5297a8bb88376923
Description
stack_string
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '17c1a8ee6fd18c7a75270c31b6602c12592242affdd6608f5297a8bb88376923']

Name

104.234.11.121

Description

CC=CA ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.234.11.121']

Name

winsccp.com

Pattern Type

stix

Pattern

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

Name

events.drdivyaclinic.com

Pattern Type

stix

Pattern

[hostname:value = 'events.drdivyaclinic.com']

Name

https://trafcon.co/wp-content/plug/des/sus/cisco/anyconnect/cisco-anyconnect-4.iso

Pattern Type

stix

Pattern

[url:value = 'https://trafcon.co/wp-content/plug/des/sus/cisco/anyconnect/cisco-anyconnect-4.iso']

Name

185.246.222.15

Description

ISP: Sukhoi Su-57 LLC **OS:** Windows Server 2012 R2 (build 6.3.9600) -------------------------- Hostnames: -------------------------- Domains: -------------------------- Services: **3389:** ``` \x0b\x12\x7f\x15\x00@\x10\x05H\x9e\x9a\x03\x04\xd0\x04\xd0\x00\x01\x00\x02\x00\

x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\

x00\x00 ``` ------------------ **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 07 Jul 2023 07:14:09 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.246.222.15']

Name

146.70.87.4

Description

CC=US ASN=AS9009 M247 Europe SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.70.87.4']

Name

snbl-art.com

Pattern Type

stix

Pattern

[domain-name:value = 'snbl-art.com']

Name

ac5b9d33791a80387e99ddc1cb63346f975982741c6275be7ff03ce4b0459b4f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ac5b9d33791a80387e99ddc1cb63346f975982741c6275be7ff03ce4b0459b4f']

Name

myponsdsoftware.com

Pattern Type

stix

Pattern

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

Name

45.81.39.175

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.81.39.175']

Name

https://usahamenarik.com/wp-content/WinSCPSetup.iso

Pattern Type

stix

Pattern

[url:value = 'https://usahamenarik.com/wp-content/WinSCPSetup.iso']

Name

a9fc36389bd687b547c9fbadaf75f1d27036c08385f4976acb8689ad79d83310

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a9fc36389bd687b547c9fbadaf75f1d27036c08385f4976acb8689ad79d83310']

Name

45.61.128.133

Description

CC=US ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.61.128.133']

Name

6ff18598dbf26038faa16773f277808cd9d39710ec6c9ec6109fec8550d1d53f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ff18598dbf26038faa16773f277808cd9d39710ec6c9ec6109fec8550d1d53f']

Name

45.66.230.215

Description

CC=BG ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.66.230.215']

Name

85.217.144.164

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFC7JWycXIgq0aQFrB8egzwPygcsmegypa4WX6xE60l8CURji0tQm5/IzinWHvfjb7+90Wewml5dvGmK7JL3AQ4= Fingerprint: 7b:b2:b6:e3:69:7a:c8:07:22:19:fe:be:f4:ad:ff:65 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 ``` ---------- **81:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.217.144.164']

Name

fa6f641d78dcb36f15ea26b0a05a8a29b9761c7838c30a9b3bb09074bb4fc7c9

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa6f641d78dcb36f15ea26b0a05a8a29b9761c7838c30a9b3bb09074bb4fc7c9']

Name

23.227.203.241

Description
CC=US ASN=AS29802 HVC-AS
Pattern Type
stix
Pattern
[ipv4-addr:value = '23.227.203.241']
Name
0daf5c0f374e9a03fbe24dbcb4f0a24837a35bc2f0ca76ca35bb705f8c079486
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0daf5c0f374e9a03fbe24dbcb4f0a24837a35bc2f0ca76ca35bb705f8c079486']
Name
b39c5fb42f54275630c05925a1c8f0d92373560b4a735b8d9a63e6498b25ecfb
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'b39c5fb42f54275630c05925a1c8f0d92373560b4a735b8d9a63e6498b25ecfb']

Name

ff32997b85098d2bb0f1adccc5dc4e608a869dd54fc8539482788855d53d43b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff32997b85098d2bb0f1adccc5dc4e608a869dd54fc8539482788855d53d43b7']

Name

e74c4cf311f2b3365605b6648d96baf5674990c3f181f01f462e1ba665bf1f7f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e74c4cf311f2b3365605b6648d96baf5674990c3f181f01f462e1ba665bf1f7f']

Name

141.98.6.96

Description

CC=BG ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '141.98.6.96']

Name

5f3488fc958b98867ef661c6697b5c2cd920199f7209086591a5e87e691891f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f3488fc958b98867ef661c6697b5c2cd920199f7209086591a5e87e691891f4']

Name

167.88.164.141

Description

ISP: RouterHosting LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP5irw/v8bGOiU4l6a48BV9HgVu2KngIDzVtf4ASNrWDN7k7O0zyWndiP1S/CwRGMmNKo/1rDjQ2lefylB4N5J8= Fingerprint: 96:e3:62:09:3e:22:fa:67:80:de:c0:32:82:7a:ab:44 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Fri, 14 Jul 2023 06:23:50 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Thu, 23 Mar 2023 13:17:06 GMT ETag: "3f-5f79117d97880" Accept-Ranges: bytes Content-Length: 63 Content-Type: text/html ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x01\x08\x00\x00\x00\x00\x00 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.88.164.141']

Name

https://theboxingshowcase.com/wp-content/sdrg/sdhr/dftjft/zsge/TreeSizeFreeSetup.iso

Pattern Type

stix

Pattern

[url:value = 'https://theboxingshowcase.com/wp-content/sdrg/sdhr/dftjft/zsge/TreeSizeFreeSetup.iso']

Name

https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/[gclid

Pattern Type

stix

Pattern

[url:value = 'https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/[gclid']

Name

74.201.28.103

Description

CC=US ASN=AS35913 DEDIPATH-LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '74.201.28.103']

Name

45.81.39.177

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.81.39.177']

Name

8c6352fc4fdaf2990f48e44ce1dce9ed375cdb75222f3dc2fc3b061d5bfa6acf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c6352fc4fdaf2990f48e44ce1dce9ed375cdb75222f3dc2fc3b061d5bfa6acf']

Name

185.254.37.217

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: - clark-jackson.prospectsw.com ---------- Domains: - prospectsw.com ---------- Services: **25:** ``` 220 circulationfactory.org.uk ESMTP service ready 250-circulationfactory.org.uk says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **80:** ``` HTTP/1.0 404 Not Found Date: Tue, 17 Jan 2023 07:16:39 GMT Server: Apache Content-Length: 162 Connection: close Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.254.37.217']

Name

ad3feb1cee5750d9acd0119fbfa6af56c07e9387d3ed24633afa48b2d031aaf3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ad3feb1cee5750d9acd0119fbfa6af56c07e9387d3ed24633afa48b2d031aaf3']

Name

76eed6472d3ab97d3e69328cea84e6aa322791f5d3cc74007b929842c425820d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '76eed6472d3ab97d3e69328cea84e6aa322791f5d3cc74007b929842c425820d']

Name

https://conteudos.doutornature.com/wp-content/upt/upgrade/scp/v7/WinSCP-6.1-Setup.iso

Pattern Type

stix

Pattern

[url:value = 'https://conteudos.doutornature.com/wp-content/upt/upgrade/scp/v7/WinSCP-6.1-Setup.iso']

Name

23.227.196.140

Description

ISP: HIVELOCITY, Inc. **OS:** None ---------- Hostnames: - 23-227-196-140.static.hvvc.us ---------- Domains: - hvvc.us ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDfojyxMnzLanZ9fhKrtSyutUbbe47sVUo7cYivIAub3ImcatQW75ClLdveTdYFHP9472JsO4JFNPv2nW3gDzkm6RZIjt6KTJJo3UPxHF0/lRqxdmvwPktNtWtIwuOUWZnEdw1MfTC5HunbXS1FFiZXzxzmrv8gFYUQ7T3v5A4NG2T60OmmY/6kubWy73/oTRW69048 ZXjXQafjRLjkuKqowJls5r+mh+OaX7VN7328ur9RqjcKs46/+vBfUlAYsH3eOXSkqSlZEig4Ii/rpbHkgGKw2PEs+GZfDu0Mz6ndVgPsRsSyiZE1OeLKhBEYBblswEmD83eqwd1KYPncaSTx Fingerprint: 32:43:5a:be:39:58:0d:c0:35:ce:c3:2b:a4:20:94:cf 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 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 ``` ---------- **443:** ``` ``` ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Content-Type:

text/html; charset=utf-8 Content-Length: 9 ETag: W/"9-0gXL1ngzMqISxa6S1zx3F4wtLyg" Date: Thu, 06 Jul 2023 18:59:21 GMT Connection: keep-alive Keep-Alive: timeout=5 ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.227.196.140']

Name

https://theboxingshowcase.com/wp-content/dht/asxdfj/gkgy/cvgkjc/WinSCP-6.1-Setup.iso

Pattern Type

stix

Pattern

[url:value = 'https://theboxingshowcase.com/wp-content/dht/asxdfj/gkgy/cvgkjc/WinSCP-6.1-Setup.iso']

Name

https://dayvisson.com/WinSCPSetup.iso

Pattern Type

stix

Pattern

[url:value = 'https://dayvisson.com/WinSCPSetup.iso']

Name
softwareinteractivo.com
Pattern Type
stix
Pattern
[domain-name:value = 'softwareinteractivo.com']
Name
dayvisson.com
Pattern Type
stix
Pattern
[domain-name:value = 'dayvisson.com']
Name
45.66.230.238
Description
CC=BG ASN=AS211252 Delis LLC
Pattern Type
stix

Pattern

[ipv4-addr:value = '45.66.230.238']

Name

172.86.123.127

Description

CC=US ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.86.123.127']

Name

https://snbl-art.com/wp-content/wp-content/WinSCPSetup.iso

Pattern Type

stix

Pattern

[url:value = 'https://snbl-art.com/wp-content/wp-content/WinSCPSetup.iso']

Name

http://mypondsoftware.com/cisco

Pattern Type

stix

Pattern

[url:value = 'http://mypondsoftware.com/cisco']

Name

https://frugalprinters.com/wp-includes/WinSCP_setup.iso

Pattern Type

stix

Pattern

[url:value = 'https://frugalprinters.com/wp-includes/WinSCP_setup.iso']

Name

https://www.yb-lawyers.com/wp-content/ter/anyconnect/AnyDesk.iso

Description

Simple indicator of observable {https://www.yb-lawyers.com/wp-content/ter/anyconnect/AnyDesk.iso}

Pattern Type

stix

Pattern

[url:value = 'https://www.yb-lawyers.com/wp-content/ter/anyconnect/AnyDesk.iso']

Name

https://winsccp.com/HPVrxkWv?[gclid

Pattern Type

stix

Pattern

[url:value = 'https://winsccp.com/HPVrxkWv?[gclid']

Name

771f95a8df4b7fb058712e43bbf2549a97075518523f0cc409f3869181457b86

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '771f95a8df4b7fb058712e43bbf2549a97075518523f0cc409f3869181457b86']

Name

157.254.195.108

Description

CC=US ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.254.195.108']

Name

35c33e9e84e9e040da42b3d6e9c3c00e8f0dff2e7ee8bb59625c7378d89f3b37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35c33e9e84e9e040da42b3d6e9c3c00e8f0dff2e7ee8bb59625c7378d89f3b37']

Name

157.254.195.83

Description

CC=US ASN=AS14956 -Reserved AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.254.195.83']

Name

conteudos.doutornature.com

Pattern Type

stix

Pattern

[hostname:value = 'conteudos.doutornature.com']

Name

13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe']

Name

25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c']

Name

3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce']

Name

21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839']

Name

bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef']

Name

8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5']

Name

c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe']

Name

4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a']

Malware

Name
Nitrogen
Name
Meterpreter
Name
Cobalt Strike
Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Attack-Pattern

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)

Name

Compromise Infrastructure

ID

T1584

Description

Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle. (Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage. Use of compromised infrastructure allows adversaries to stage, launch, and execute operations. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may also compromise infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) By using compromised infrastructure, adversaries may make it difficult to tie their actions back to them. Prior to targeting, adversaries may compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

Name

Obtain Capabilities

ID

T1588

Description

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle. In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab) In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

Permission Groups Discovery

ID

T1069

Description

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions. Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.(Citation: CrowdStrike BloodHound April 2018)

Name

Unsecured Credentials

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg

Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

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

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be

intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Command and Scripting Interpreter

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)

Sector

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Domain-Name

Value
winsccp.com
myponsdsoftware.com
dayvisson.com
mypondsoftware.com
theboxingshowcase.com
softwareinteractivo.com
frugalprinters.com
trafcon.co
tresize.com
snbl-art.com
protemaq.com
praybig.us
usahamenarik.com

StixFile

Value
9c66003fe79d9bc9570373c465e69dd5db56f24c51ad4bb16c83efde5b966510
0af013ad0548b992d50287e3b11963cad9aa0af1f1e47e254637d28ee05208d8
0daf5c0f374e9a03fbe24dbcb4f0a24837a35bc2f0ca76ca35bb705f8c079486
8000af302ad89c9555241366edc65b9b9b24828c8ea74bde658984b92e8c8ec6
a25f3604213a0db2375ddc2af800faa3833dc5597ca20b3138462c1d77faf952
503156f1b27d4dd463048f85924a2bbbeb3d0e09de2574395a51f77b48e9639d
ae84d0d6b9935499a5e0e18052ce7ea64378eba1e9579ca98fdd925d8e6f8639
b39c5fb42f54275630c05925a1c8f0d92373560b4a735b8d9a63e6498b25ecfb
d9d53fcadc96c7bc3eae0a84a574b6222f0c906ee4916a9e68e0322b5c694d49
a9fc36389bd687b547c9fbadaf75f1d27036c08385f4976acb8689ad79d83310
f1227c5124e24e439b44083369d7fa7a719e076f5839629d2ef10aa5e19e6afc
62b1e355a7e4c850bb0f03c7f182f48f0ebaafa07ddae1fee599a78772d149f2
2f4f365613172848df3e91d43514b9da34b8c84eded8fae683f94586d22f86cf

a267937e172f4cd8ce873e4fcfceeddf07ae03db68f64e047f940e2e7a2a136a

61927228b3dcf973822eb5fff44ca7940d950af7116aefe957cc31287c5283d5

9a00b8b62d5194f22f690127084f626b1abbf88777b5b8474799bca1576e5fbd

ac5b9d33791a80387e99ddc1cb63346f975982741c6275be7ff03ce4b0459b4f

332e19cc0f71a5dcbfc3d24fb08564589d0cb884d21d1fddbbf9c0230d678ec0

2eb2ef7a562145a0faf3c82f439221908adfcc784022a64e5bb17a432f4a8a91

ccd5e869216640460c3329e41ec30fa22ee729f0b4fc2e61781026c4defea6e6

3346a4f9f253a8251e14f0d42138e5b4420dd3c1b46afcd9f688d4e26c98c561

b425de9b0e7fe10b89b730339bbcda2d0d4668f5b9226be633409cfb89b3dacd

150f3356485c26039dc145d0bedda265d3e9626fd1f3a180455f8b911c53c260

f87a976dfd3881f59dbd2ea53fbfa3a663e1fff83a333b548b4fdc4651d5b8f7

d155d0af73b3e86f42672714caa4391ab615c426a3e3fc44a41e4d125a06172a

5f3488fc958b98867ef661c6697b5c2cd920199f7209086591a5e87e691891f4

535aefaba2eb8d7898b176b0dcdd23fcef984994e609db222c33ece2d1c081b3

a58b9c9cece44216e2dd3304fd4825db3c324393607574f87bec00be505a0d93

ad3feb1cee5750d9acd0119fbfa6af56c07e9387d3ed24633afa48b2d031aaf3

bf062d03ab77bfa835700f7131e6f95f19e2c5015ff65e47614b736ea9817dd6

4fb70092d8533088742ca23788f29e0802b223eada1748ce82731162d25920c7

237c18bbd8fb8f74710dacaf7795c473a988b66fce667facc6f17b2c6e071745

db2a48326f99f0944f50800539817cfb6562f2bfbbcc2f2409901319eb3592ec

81570ac9bdd4e1abf7b296b528c7507e7df773a7c3cf05ef01a874ba9af1b36f

9c57a2a27b6fcea5bcf1eda791ccdaa0eb3fdbf93781b37283d956332f4d2ceb

e74c4cf311f2b3365605b6648d96baf5674990c3f181f01f462e1ba665bf1f7f

26a68bfc0d40b3cc49af1958f2004f404c960663b140fd612a2a53ccaf99f004

b926fcc98f23905abd76b7ed9fa50fb84cc66aa9fb7994064ada715702e80722

a8b9b74dee76ea6a19845b80498d91e002133d20741b6707744fb345a3581abe

17c1a8ee6fd18c7a75270c31b6602c12592242affdd6608f5297a8bb88376923

fa6f641d78dcb36f15ea26b0a05a8a29b9761c7838c30a9b3bb09074bb4fc7c9

686c7fc9d3efef602136cde2716d20ca13d1e3de3c57f787fa74e28cc8b743cd

971b4db8b81a2c456839d4609364bb6cd7800c9ce980379bb5a11d1d4689d504

a25eba7a79e46e5f6498ccb82fb4ef0eb3abe784fa0d061fe9e1adce9d39caa7

fa911a3639ae77f8f890fb76ba1ab78c2ab17ab80bdfec381ab6a9ba8fef32fe

8dfac6521ef877efede0a82bf46d94f590127e2607b78d08321953796fddbba9

6c340981785e28218f7ef5ee991e1888fadce9a3c29bc31316359562386124bd

771f95a8df4b7fb058712e43bbf2549a97075518523f0cc409f3869181457b86

76eed6472d3ab97d3e69328cea84e6aa322791f5d3cc74007b929842c425820d

fce4ca6e37d466154ed49871ac31116473b1c72cf36a9653af80e9cc83edb358

8c6352fc4fdaf2990f48e44ce1dce9ed375cdb75222f3dc2fc3b061d5bfa6acf

e47151f7c394e1b530314cc15d482b5ce797c803c251a61e45efb0316115c677

35c33e9e84e9e040da42b3d6e9c3c00e8f0dff2e7ee8bb59625c7378d89f3b37

8f02fa20b02ff6321a7db6dae478c2215bb463ebec6de4db73f247873aca1315

ff32997b85098d2bb0f1adccc5dc4e608a869dd54fc8539482788855d53d43b7

6ff18598dbf26038faa16773f277808cd9d39710ec6c9ec6109fec8550d1d53f

3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce

c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe

8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5

25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c

bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef

13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe

21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839

4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a

Hostname

Value
www.yb-lawyers.com
events.drdivyaclinic.com
conteudos.doutornature.com

IPv4-Addr

Value
185.254.37.216
45.61.128.133
167.88.165.18
157.254.195.53
45.66.230.215
95.214.24.163
45.81.39.177
167.88.164.141
104.234.11.236
45.81.39.175
23.227.196.140
167.88.164.95
45.66.230.237

166.0.94.216

157.254.195.210

141.98.6.96

157.254.195.83

74.201.28.103

85.217.144.164

104.234.11.121

45.66.230.216

146.70.87.4

185.246.222.15

157.254.195.108

45.12.253.137

141.98.6.95

172.86.123.127

87.121.221.218

104.234.119.16

185.254.37.217

104.234.147.11

167.88.164.130
23.227.203.241
45.66.230.238
85.208.136.13

Url

Value
https://praybig.us/wp-content/smb/srs/24/5333/WinSCP-6.1-Setup.iso
https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE
https://protemaq.com/wp-content/update/iso/6.1/tusto/WinSCP-6.1-Setup.iso
https://events.drdivyaclinic.com/wp-content/task/update/WinSCP-6.1-Setup.iso
https://dayvisson.com/Cisco-Mobility-Client-v4.iso
https://frugalprinters.com/wp-includes/WinSCP_setup.iso
https://winsccp.com/HPVrxkWv?[gclid
https://winsccp.com/eng/download.php
https://softwareinteractivo.com/streamlining-team-collaboration-the-power-of-for-seamless-file-sharing/[gclid
https://trafcon.co/wp-content/plug/des/sus/cisco/anyconnect/cisco-anyconnect-4.iso
https://usahamenarik.com/wp-content/WinSCPSetup.iso

https://www.yb-lawyers.com/wp-content/ter/anyconnect/AnyDesk.iso

https://snbl-art.com/wp-content/wp-content/WinSCPSetup.iso

https://dayvisson.com/WinSCPSetup.iso

https://theboxingshowcase.com/wp-content/dht/asxdfj/gkgy/cvgkjc/WinSCP-6.1-Setup.iso

http://mypondsoftware.com/cisco

https://theboxingshowcase.com/wp-content/sdrg/sdhr/dftjft/zsge/TreeSizeFreeSetup.iso

https://winsccp.com/HPVrxkWv?gclid=EAIaIQobChMI3aXW7fjA_wIViN3ICh1NKQW6EAAYASAAEgLEZfD_BwE

https://conteudos.doutornature.com/wp-content/upt/upgrade/scp/v7/WinSCP-6.1-Setup.iso

External References

- https://otx.alienvault.com/pulse/64c285ca0a63ae2110040830
- https://news.sophos.com/en-us/2023/07/26/into-the-tank-with-nitrogen/
- https://github.com/sophoslabs/IoCs/blob/master/Nitrogen%202023-07.csv