Jul 05 2023

NETMANAGEIT

Intelligence Report

Chinese Threat Actors Targeting Europe in SmugX Campaign

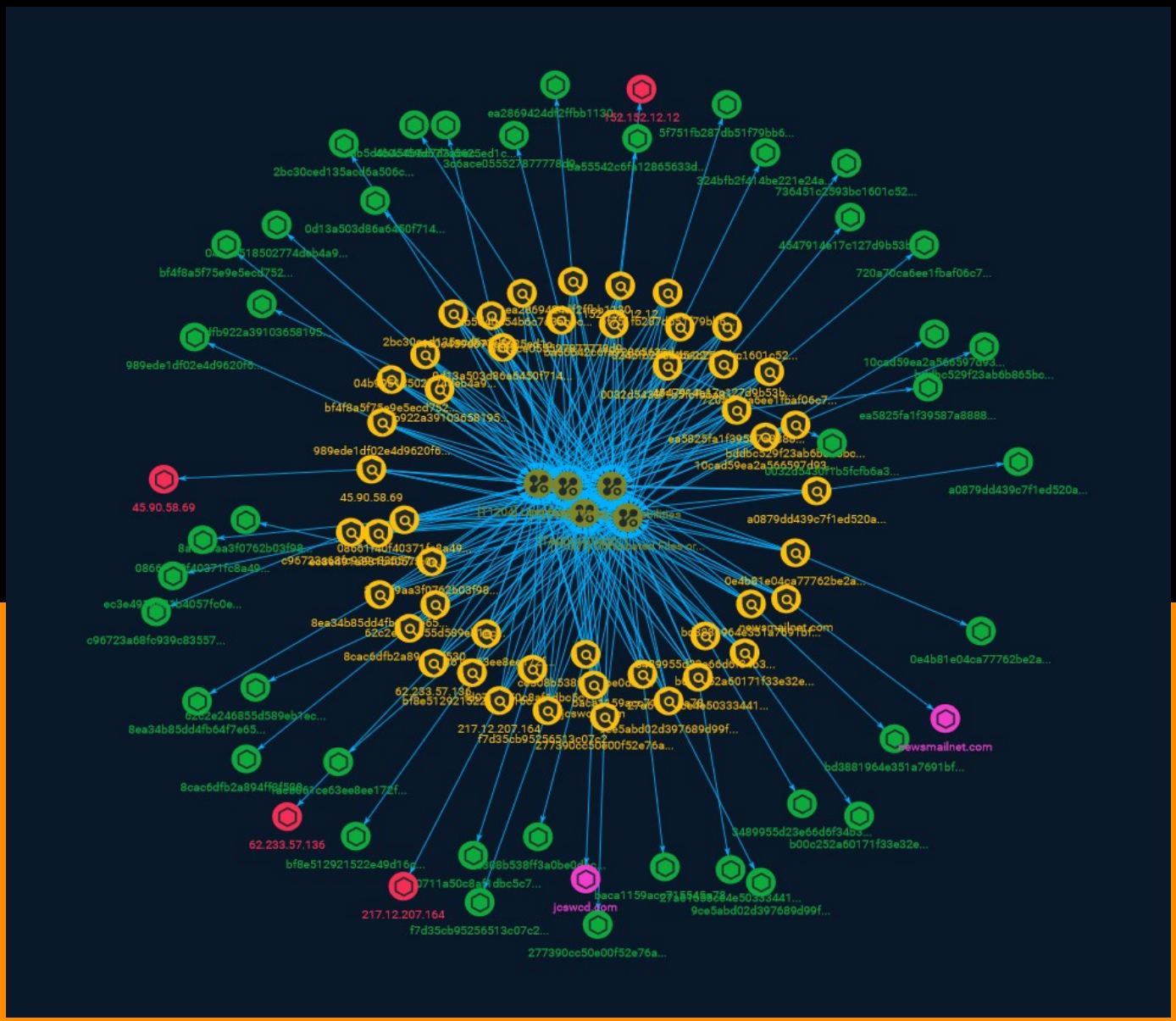

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In the last couple of months, Check Point Research (CPR) has been tracking the activity of a Chinese threat actor targeting Foreign Affairs ministries and embassies in Europe. Combined with other Chinese activity previously reported by Check Point Research, this represents a larger trend within the Chinese ecosystem, pointing to a shift to targeting European entities, with a focus on their foreign policy.

Confidence

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

15 / 100

Indicator

Name
08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12']
Name
0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0']
Name

ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2

Description

SUSP_obfuscated_JS_obfuscatorio

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2']

Name

b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405']

Name

bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5']

Name

736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af']

Name

fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429']

Name

1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885']
Name
8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8']
Name
ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659']

Name

0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0']

Name

27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c

Description

SUSP_obfuscated_JS_obfuscatorio

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c']

Name

8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32']

Name

3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee']

Name

62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c']

Name

324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b']

Name

f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42']

Name

c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1']

Name

152.152.12.12

Description

CC=BE

Pattern Type

stix

Pattern

[ipv4-addr:value = '152.152.12.12']

Name

baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3']

Name

0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1']

Name

3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb']

Name

04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61']

Name

ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a']

Name

newsmailnet.com

Pattern Type

stix

Pattern

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

Name

460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76']

Name

bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880']

Name

bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1']

Name

10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee']

Name

jcswcd.com

Pattern Type

stix

Pattern

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

Name

8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3']

Name

720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05']

Name

217.12.207.164

Description

ISP: GREEN FLOID LLC **OS:** None ---------- Hostnames: - vds1147307.hosted-by-itldc.com ---------- Domains: - hosted-by-itldc.com ---------- Services: **443:** ``` HTTP/1.1 200 OK Content-Length: 0 ``` HEARTBLEED: 2023/06/19 16:06:02 217.12.207.164:443 - SAFE ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 30 Jun 2023 11:27:39 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.12.207.164']

Name

45.90.58.69

Description

ISP: GREEN FLOID LLC **OS:** None ---------- Hostnames: - steenbock.store ---------- Domains: - steenbock.store ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDE8+lParWBXXe6TnWE93VgvvDp9Y9pfw8pEM5xChwUjhXx 9D/nA5uruzg7Nckut2qDyHOu5fcj0oOPLiwsB14a7LVOGg8dlm/mz0SRrNyPSLR5wmZRftSFbc6o 6N4cCPW3n1DOeYdIrPG+0mYHnL2yaDauurHyjqZLG6V7yQYU0p97ejlYcuSxGZ6iKpNftnQUXMWpeQUQn+pd0th2JBvEDckq+31HKFJIVjA4JDGplnP+qDXz7KhIEfSMBViQC8mnpvcQh/sLSOVyooiNA/ZGdISYLTP99BORFuikZGTDlRis3mCBEclNIOKX71PYZXgyVION63WACoSYpe0pJP65 Fingerprint: 8a:b7:57:23:5a:9b:eb:11:26:af:46:59:67:6c:0c:09 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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: Sat, 01 Jul 2023 09:36:00 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 X-Powered-By: PHP/7.1.33 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 28 Jun 2023 00:08:08 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 Content-Length: 481 Content-Type: text/html;charset=ISO-8859-1 ``` HEARTBLEED: 2023/06/28 00:08:26 45.90.58.69:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.90.58.69']

Name

0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1

Description

UPX

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1']

Name

ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4']

Name

5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db']

Name

a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7']

Name

989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05']

Name

ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d']

Name

9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a']

Name

4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838']

Name

bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6']

Name

62.233.57.136

Description

ISP: GREEN FLOID LLC **OS:** Ubuntu ---------- Hostnames: - hokanssonlinda1990.pserver.space ---------- Domains: - pserver.space ---------- Services: **80:** ``` HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Wed, 28 Jun 2023 09:22:47 GMT Content-Type: text/html Content-Length: 580 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.233.57.136']

Name

edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd']

Name

277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347']

Name

2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e']

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)

Domain-Name

Value
jcswcd.com
newsmailnet.com

StixFile

Value
ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2
04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61
720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05
8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3
ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659
f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42
bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6
5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db
edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd
736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af
0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1
3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee
0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0

ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d

ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a

baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3

c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1

62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c

fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429

8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8

324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b

3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb

a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7

4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838

277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347

9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a

0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1

bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5

10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee

bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1

2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e

27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c

08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12

bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880

8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32

ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4

b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405

0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0

460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76

1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885

989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05

IPv4-Addr

Value
45.90.58.69
152.152.12.12
62.233.57.136
217.12.207.164

External References

- https://otx.alienvault.com/pulse/64a5960b230e2e9a1bf9ec66
- https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/