Oct 28 2023

NETMANAGEIT

Intelligence Report

Peculiarities of destructive cyber attacks against Ukrainian providers

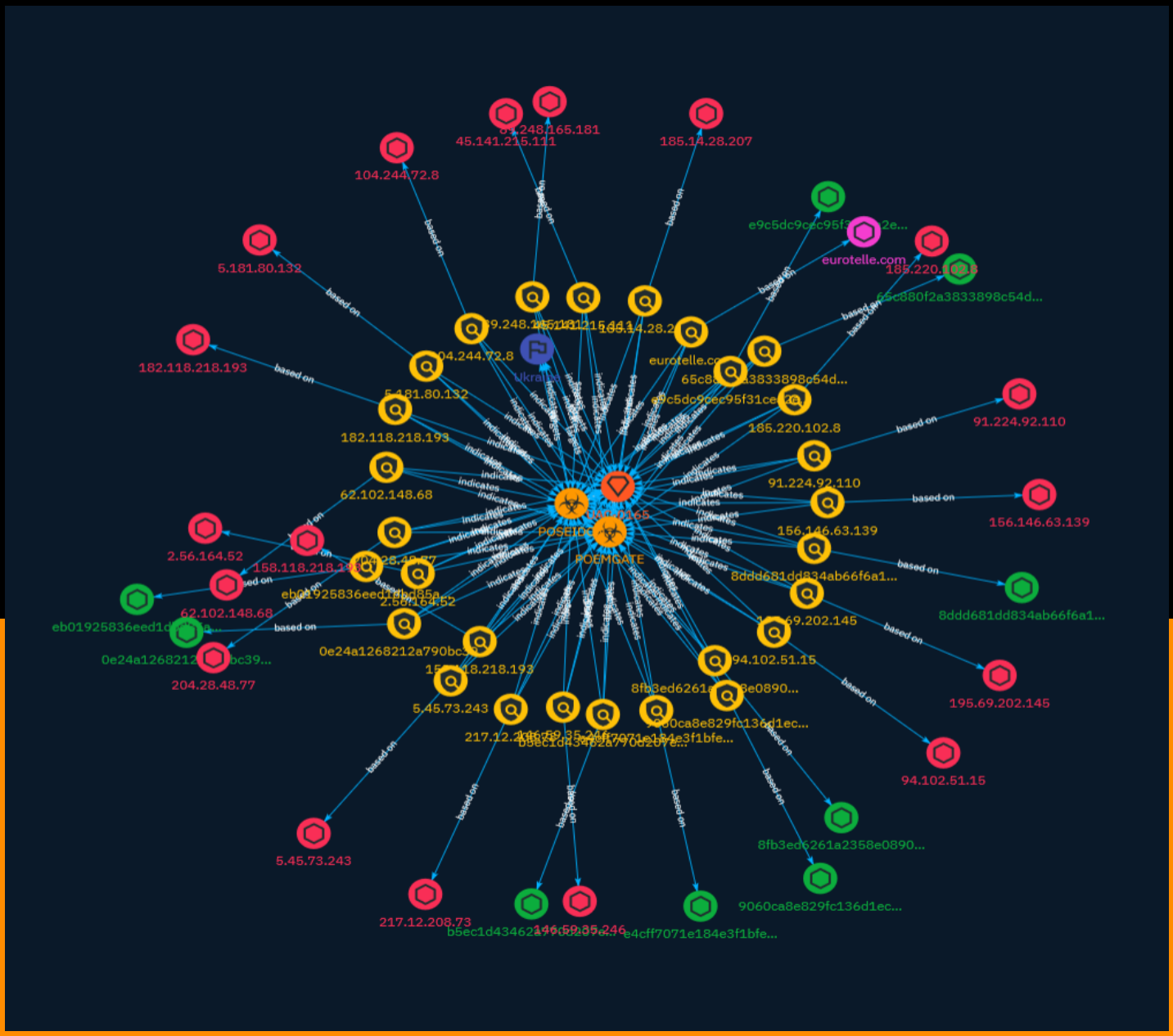

Table of contents

Overview

Entities

Observables

External References

Overview

Description

According to public sources, for the period from 11.05.2023 to 27.09.2023, an organized group of criminals tracked by the identifier UAC-0165 interfered with the information and communication systems (ICS) of no less than 11 telecommunications providers of Ukraine, which, among other things, led to to interruptions in the provision of services to consumers.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
2.56.164.52
Description
Agressive IP known malicious on AbuseIPDB - countryCode: GB - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-25T17:32:57+00:00
Pattern Type
stix
Pattern
[ipv4-addr:value = '2.56.164.52']
Name
158.118.218.193
Description
CC=US
Pattern Type

stix

Pattern

[ipv4-addr:value = '158.118.218.193']

Name

5.45.73.243

Description

CC=NL ASN=AS58061 Scalaxy B.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.45.73.243']

Name

146.59.35.246

Description

CC=FR ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.59.35.246']

Name

8ddd681dd834ab66f6a1c00ba2830717bf845de5639708eb8e8ab795ffd1df5a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ddd681dd834ab66f6a1c00ba2830717bf845de5639708eb8e8ab795ffd1df5a']

Name

0e24a1268212a790bc3993750f194ac1e0996a6770b32b498341f06abac45d81

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e24a1268212a790bc3993750f194ac1e0996a6770b32b498341f06abac45d81']

Name

89.248.165.181

Description

CC=NL ASN=AS202425 IP Volume inc

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.248.165.181']

Name

185.220.102.8

Description

Agressive IP known malicious on AbuseIPDB - countryCode: NL - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-28T17:44:10+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.220.102.8']

Name

62.102.148.68

Description

CC=SE ASN=AS51815 GlobalConnect AB

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.102.148.68']

Name

91.224.92.110

Description

400 BAD REQUEST

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.224.92.110']

Name

8fb3ed6261a2358e0890bfd544e515af232f87d3aef947e09f640da7cc1b89d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8fb3ed6261a2358e0890bfd544e515af232f87d3aef947e09f640da7cc1b89d9']

Name
185.14.28.207
Description
CC=NL ASN=AS21100 ITL LLC
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.14.28.207']
Name
195.69.202.145
Description
CC=RU ASN=AS29031 Lugansk Telephone Company
Pattern Type
stix
Pattern
[ipv4-addr:value = '195.69.202.145']
Name
eb01925836eed1dbd85a8ab9aa05c5c45dc051abaae9e67db3a53489d776b6c2

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'eb01925836eed1dbd85a8ab9aa05c5c45dc051abaae9e67db3a53489d776b6c2']
Name
65c880f2a3833898c54d7f48ee0709a13887376b2ea5bc933b2e70f29614e728
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '65c880f2a3833898c54d7f48ee0709a13887376b2ea5bc933b2e70f29614e728']
Name
b5ec1d43462a770d207eefb906516631e4d80eea55779509616b58b39a764455
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b5ec1d43462a770d207eefb906516631e4d80eea55779509616b58b39a764455']

Name
204.28.48.77
Description
CC=US
Pattern Type
stix
Pattern
[ipv4-addr:value = '204.28.48.77']
Name
156.146.63.139
Description
CC=FR ASN=AS212238 Datacamp Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '156.146.63.139']
Name
e4cff7071e184e3f1bfedfe30afa52ddd2cac1a00983508d142e51ecebfcba14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e4cff7071e184e3f1bfedfe30afa52ddd2cac1a00983508d142e51ecebfcba14']

Name

eurotelle.com

Pattern Type

stix

Pattern

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

Name

e9c5dc9cec95f31cea2eb88cc26a35d29c5f89f23bff6a7cfa1250dec6d5701a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9c5dc9cec95f31cea2eb88cc26a35d29c5f89f23bff6a7cfa1250dec6d5701a']

Name

182.118.218.193

Description

CC=CN ASN=AS4837 CHINA UNICOM China169 Backbone

Pattern Type

stix

Pattern

[ipv4-addr:value = '182.118.218.193']

Name

45.141.215.111

Description

Agressive IP known malicious on AbuseIPDB - countryCode: DE - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-25T17:36:24+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.141.215.111']

Name

9060ca8e829fc136d1ecd95a5204abb48f3ce5b7339619c5668c7e176dcbb235

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9060ca8e829fc136d1ecd95a5204abb48f3ce5b7339619c5668c7e176dcbb235']

Name

104.244.72.8

Description

ISP: FranTech Solutions **OS:** None ------------------------- Hostnames: - 4.tor-exit.neelc.org ------------------------- Domains: - neelc.org ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_9.4 Key type: ssh-ed25519 Key: AAAAC3NzaC1lZDI1NTE5AAAAIHvFtCkvqrtJqSfKQompeFEGu34BU4396JfrqpWodaUc Fingerprint: 90:b6:4c:0b:bc:d2:55:66:fc:4d:63:c8:62:f5:27:53 Kex Algorithms: sntrup761x25519-sha512@openssh.com curve25519-sha256 curve25519-sha256@libssh.org diffie-hellman-group-exchange-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-gcm@openssh.com aes256-ctr aes192-ctr aes128-ctr MAC Algorithms: hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com umac-128-etm@openssh.com Compression Algorithms: none zlib@openssh.com ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.244.72.8']

Name

94.102.51.15

Description

SSH intrusion attempt from 94.102.51.15

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.102.51.15']

Name

217.12.208.73

Description

CC=NL ASN=AS21100 ITL LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.12.208.73']

Name

5.181.80.132

Description

CC=BG ASN=AS50360 Tamatiya EOOD

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.80.132']

Intrusion-Set

Name
UAC-0165

Country

Name
Ukraine

Malware

Name
POEMGATE

Name
POSEIDON

Domain-Name

Value
eurotelle.com

StixFile

Value
e4cff7071e184e3f1bfedfe30afa52ddd2cac1a00983508d142e51ecebfcba14
9060ca8e829fc136d1ecd95a5204abb48f3ce5b7339619c5668c7e176dcbb235
8fb3ed6261a2358e0890bfd544e515af232f87d3aef947e09f640da7cc1b89d9
8ddd681dd834ab66f6a1c00ba2830717bf845de5639708eb8e8ab795ffd1df5a
0e24a1268212a790bc3993750f194ac1e0996a6770b32b498341f06abac45d81
e9c5dc9cec95f31cea2eb88cc26a35d29c5f89f23bff6a7cfa1250dec6d5701a
b5ec1d43462a770d207eefb906516631e4d80eea55779509616b58b39a764455
eb01925836eed1dbd85a8ab9aa05c5c45dc051abaae9e67db3a53489d776b6c2
65c880f2a3833898c54d7f48ee0709a13887376b2ea5bc933b2e70f29614e728

IPv4-Addr

Value
104.244.72.8
94.102.51.15
2.56.164.52
91.224.92.110
204.28.48.77
182.118.218.193
156.146.63.139
62.102.148.68
217.12.208.73
146.59.35.246
89.248.165.181
195.69.202.145
5.45.73.243

185.220.102.8
5.181.80.132
45.141.215.111
185.14.28.207
158.118.218.193

External References

- https://otx.alienvault.com/pulse/652e95bde547f6e590a6fad2
- https://cert.gov.ua/article/6123309