Jul 21 2023

NETMANAGEIT

Intelligence Report

Analysis of Storm-0558 techniques for unauthorized email access

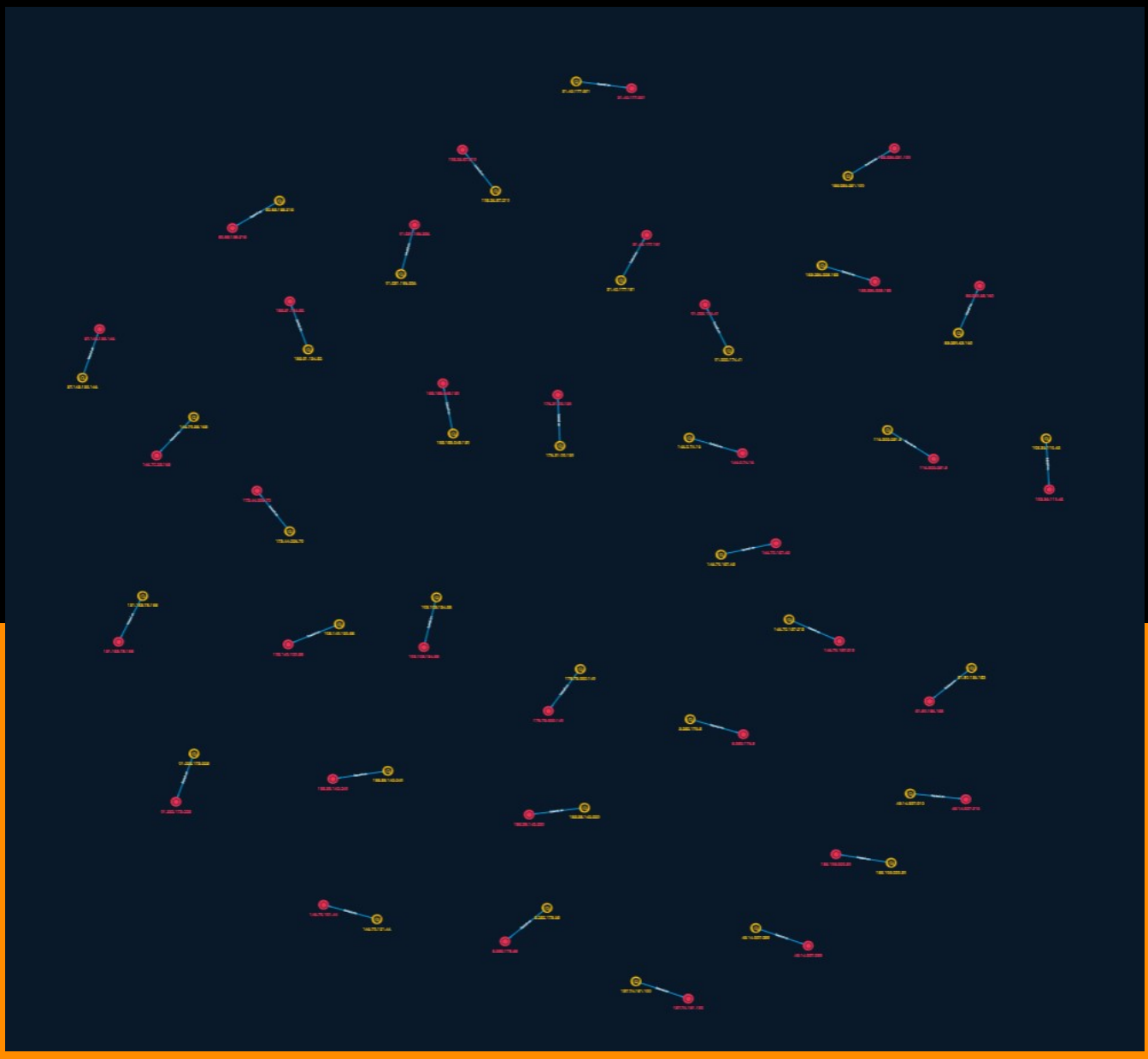

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4

Observables

- IPv4-Addr 18

External References

- External References 21

Overview

Description

Analysis of the techniques used by the threat actor tracked as Storm-0558 for obtaining unauthorized access to email data, tools, and unique infrastructure characteristics.

Confidence

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

15 / 100

Indicator

Name
195.26.87.219
Pattern Type
stix
Pattern
[ipv4-addr:value = '195.26.87.219']
Name
31.42.177.181
Pattern Type
stix
Pattern
[ipv4-addr:value = '31.42.177.181']
Name
116.202.251.8

Pattern Type
stix
Pattern
[ipv4-addr:value = '116.202.251.8']
Name
5.252.178.68
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.178.68']
Name
185.51.134.52
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.51.134.52']
Name
85.239.63.160

Pattern Type
stix
Pattern
[ipv4-addr:value = '85.239.63.160']
Name
173.44.226.70
Pattern Type
stix
Pattern
[ipv4-addr:value = '173.44.226.70']
Name
185.236.228.183
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.236.228.183']
Name
185.158.248.159

Pattern Type
stix
Pattern
[ipv4-addr:value = '185.158.248.159']
Name
91.222.173.225
Pattern Type
stix
Pattern
[ipv4-addr:value = '91.222.173.225']
Name
146.70.157.213
Pattern Type
stix
Pattern
[ipv4-addr:value = '146.70.157.213']
Name
193.149.129.88

Pattern Type
stix
Pattern
[ipv4-addr:value = '193.149.129.88']
Name
131.153.78.188
Pattern Type
stix
Pattern
[ipv4-addr:value = '131.153.78.188']
Name
178.73.220.149
Pattern Type
stix
Pattern
[ipv4-addr:value = '178.73.220.149']
Name
137.74.181.100

Pattern Type
stix
Pattern
[ipv4-addr:value = '137.74.181.100']
Name
146.70.35.168
Pattern Type
stix
Pattern
[ipv4-addr:value = '146.70.35.168']
Name
185.38.142.249
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.38.142.249']
Name
91.231.186.226

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.231.186.226']

Name

185.236.231.109

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.236.231.109']

Name

146.70.121.44

Description

ISP: M247 Europe SRL **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCxyUjNw4blpcmTpOA8L+oKvgr4aE9Uf4fTCkGUs0PBMU Ro ZsWYo/ Hfh8hBlyUX1Z1fnIdP7dB9o5ZU4NpXMTjxOy9iy6BvuJNK9H8jTfFrpyRD5+yyndcUbQHa w7ZsFC9ni+SHS4Cz5oZ+G0pQEaHtJNb4oQemqjw5YtlTjwhBm6uQeAmSF6TMZ+CT/Un57jJyrMee +bJqdxVU2ltwXa9ganB86aIplZpvorYYkQpVktgLsJNmCMtORvuS3r5wzkJcadqbTDRuj5T7/4nS O5crNBB5PCXS6G7Fdsz9pDvEMwAzCERf9GUY3KVT9HDFXDGf/s8mr4q116cQc0xI8jmb Fingerprint: c1:1f:a7:30:d5:3f:2e:29:ce:42:6c:98:c8:af:ad:87 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.70.121.44']

Name

31.42.177.201

Description

ISP: SOLLUTIUM EU Sp z.o.o. **OS:** None ---------- Hostnames: - server18.magerslpfact.com ---------- Domains: - magerslpfact.com ---------- Services: **1194:** ```
@\x98\x9e\x9aF\xadj\xfb\x94\x01\x00\x00\x00\x00\xd9\xce:
\xbe\xf6\x98\xa5m\x00\x00\x00\x00 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.42.177.201']

Name
185.195.200.39
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.195.200.39']
Name
5.252.176.8
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.176.8']
Name
80.85.158.215
Pattern Type
stix
Pattern
[ipv4-addr:value = '80.85.158.215']

Name
45.14.227.212
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.14.227.212']
Name
37.143.130.146
Pattern Type
stix
Pattern
[ipv4-addr:value = '37.143.130.146']
Name
51.89.156.153
Pattern Type
stix
Pattern
[ipv4-addr:value = '51.89.156.153']

Name
176.31.90.129
Pattern Type
stix
Pattern
[ipv4-addr:value = '176.31.90.129']
Name
193.105.134.58
Pattern Type
stix
Pattern
[ipv4-addr:value = '193.105.134.58']
Name
91.222.174.41
Pattern Type
stix
Pattern
[ipv4-addr:value = '91.222.174.41']

Name

146.70.157.45

Description

ISP: M247 Europe SRL **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCx/K/RDhC81ryv1WFFet6QZ6bHvA2DS1/GcxCS0bC1lNa5 q2Zy/dOIBW9Rh0ZEcwAP0kPUrmjX0Yvr25jERyjesrVL3rHU/Q9Wnol27h0Ig0dBUE9nnEWmGLNeDLJwkmkw6dO2iZshVMq5o2jAvD48I1Ncke9AQ5tVq6JHlwdXZbxgM7144t5smUrxDnLF59pFwaWlxYjrHdlW3+r8blRSr6054EirBMA7mk1KqkqGnEPMPei8pialJRO1C1FbaALirmLCDQkmTGrN+K/huER9pGCNIC2MriKr3rkSzMxuhV1bb97ihvMmzE4lcixWj91uGbr2niMiaXbS9PWhKOd7 Fingerprint: e7:a1:4a:98:58:c6:7a:75:28:d2:78:2d:fd:bb:06:76 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 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 = '146.70.157.45']

Name

193.36.119.45

Pattern Type
stix
Pattern
[ipv4-addr:value = '193.36.119.45']
Name
45.14.227.233
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.14.227.233']
Name
146.0.74.16
Pattern Type
stix
Pattern
[ipv4-addr:value = '146.0.74.16']
Name
185.38.142.229

Description

ISP: Net Solutions - Consultoria Em Tecnologias De Informacao, Sociedade Unipessoal LDA **OS:** None ---------- Hostnames: - woueywoueywouey7whatever.com ---------- Domains: - woueywoueywouey7whatever.com ---------- Services: **21:** ``` 220 (vsFTPd 3.0.2) 530 Login incorrect. 530 Please login with USER and PASS. 211-Features: EPRT EPSV MDTM PASV REST STREAM SIZE TVFS UTF8 211 End ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Date: Thu, 19 Jan 2023 09:25:28 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 X-Powered-By: PHP/7.4.33 Set-Cookie: PHPSESSID=6o71i4lhnddf39plgt2hvaarvk; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.38.142.229']

IPv4-Addr

Value
146.70.121.44
91.231.186.226
45.14.227.233
193.149.129.88
85.239.63.160
193.105.134.58
185.51.134.52
193.36.119.45
131.153.78.188
31.42.177.181
146.70.157.213
173.44.226.70
116.202.251.8

178.73.220.149

91.222.174.41

45.14.227.212

146.70.35.168

185.236.231.109

185.195.200.39

185.158.248.159

146.0.74.16

91.222.173.225

176.31.90.129

137.74.181.100

80.85.158.215

185.236.228.183

5.252.178.68

195.26.87.219

5.252.176.8

185.38.142.249

31.42.177.201

51.89.156.153
37.143.130.146
146.70.157.45
185.38.142.229

External References

- https://otx.alienvault.com/pulse/64ba6031d2051c26d794df02
- https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/