COMUNICAT RELATIU AL CIBERATAC MASSIU PER RANSOMWARE "WANNACRYPT"

14 de maig de 2017

A continuació indiquem el conjunt d'IOC's, hashes i recomanacions sobre diferents mòduls de sistema de protecció perimetral i filtratge per aplicar-ho en els respectius sistemes de protecció.

En el marc de la protecció d'intent d'explotació de la vulnerabilitat de SMB (MS17-010) s'estipula que s'hauria de bloquejar qualsevol intent d'explotació en les següents firmes. També recomanem actualitzar tots els equips que disposin d'un S.O Windows per poder aplicar l'actualització corresponent a la vulnerabilitat MS17-010.

Informació d'interés sobre actualització MS17-010:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Firmes Mcafee (SMB)

CVE-2017-0143	**NETBIOS-SS: Windows SMBv1 identical MID and FID type confusion vulnerability** Attack ID: (0x43c0b800)
CVE-2017-0144	**NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability** Attack ID: (0x43c0b400)
CVE-2017-0145	**NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability** Attack ID: (0x43c0b500)
CVE-2017-0146	**NETBIOS-SS: Microsoft Windows SMB Out of bound Write Vulnerability (CVE-2017-0146)** Attack ID: (0x43c0b300)
CVE-2017-0147	**NETBIOS-SS: Windows SMBv1 information disclosure vulnerability (CVE-2017-0147)** Attack ID: (0x43c0b900)

Addicionalment recomanem que per a plataformes d'altres fabricants en els quals és disposi d'un

mòdul d'IPS habilitat, el bloqueig de la següent CVE associats a l'explotació de vulnerabilitat de SMB.

PaloAlto:

- CVE-2017-0290 ID 33376
- (MS17-010: CVE-2017-0143) ID 32393
- (MS17-010: CVE-2017-0144) ID32422
- (MS17-010: CVE-2017-0145) ID 32424
- (MS17-010: CVE-2017-0146) ID 32422 y 32427
- (MS17-010: CVE-2017-0147) ID 32427

CheckPoint:

- Microsoft Malware Protection Engine Type Confusion Remote Code Execution, CVE-2017-0290
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143)
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144)
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145)
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0146)
- Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-0147)

En l'arxiu adjunt IP's_C&C.doc trobareu el llistat total d'IP's reportades per part de Microsoft, AlienVault i tercers associats als servidors C&C del Ransomware, recomanem no obstant que a part d'incloure aquest llistat per a denegar l'accés, s'actualitzin totes les plataformes de protecció perimetral periòdicament per tal de mantenir-la el més actualitzada possible.

A continuació us indiquem d'un conjunt de hashes associats als arxius infectats per si la plataforma de protecció disposa de mòdul de detecció i bloqueig a través del hash.

File Name @WanaDecryptor@.exe
MD5 7bf2b57f2a205768755c07f238fb32cc
SHA1 45356a9dd616ed7161a3b9192e2f318d0ab5ad10
SHA256 b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
SHA512
91a39e919296cb5c6eccba710b780519d90035175aa460ec6dbe631324e5e5753bd8d87f395b5481b
cd7e1ad623b31a34382d81faae06bef60ec28b49c3122a9
CRC32 4E6C168D

File Name taskdl.exe
MD5 4fef5e34143e646dbf9907c4374276f5
SHA1 47a9ad4125b6bd7c55e4e7da251e23f089407b8f
SHA256 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
SHA512
4550dd1787deb353ebd28363dd2cdccca861f6a5d9358120fa6aa23baa478b2a9eb43cef5e3f6426f7
08a0753491710ac05483fac4a046c26bec4234122434d5
CRC32 E969EF31

File Name taskse.exe
MD5 8495400f199ac77853c53b5a3f278f3e
SHA1 be5d6279874da315e3080b06083757aad9b32c23
SHA256 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
SHA512
0669c524a295a049fa4629b26f89788b2a74e1840bcdc50e093a0bd40830dd1279c9597937301c007
2db6ece70adee4ace67c3c8a4fb2db6deafd8f1e887abe4
CRC32 BC193579

File Name mssecsvc.exe
MD5 db349b97c37d22f5ea1d1841e3c89eb4
SHA1 e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
SHA512
d6c60b8f22f89cbd1262c0aa7ae240577a82002fb149e9127d4edf775a25abcda4e585b6113e79ab4a
24bb65f4280532529c2f06f7ffe4d5db45c0caf74fea38
CRC32 9FBB1227

File Name tasksche.exe
MD5 84c82835a5d21bbcf75a61706d8ab549
SHA1 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512
90723a50c20ba3643d625595fd6be8dcf88d70ff7f4b4719a88f055d5b3149a4231018ea30d3751715
07a147e59f73478c0c27948590794554d031e7d54b7244
CRC32 4022FCAA

Llista de IPs conegudes de C&C de wannacry que cal bloquejar en el perímetre, segons diferents fonts,

Origen de les dades, Microsoft:

a. 154.35.175.225
b. 171.25.193.78
c. 178.162.194.210
d. 192.99.212.139
e. 195.154.165.112
f. 154.35.175.225
g. 171.25.193.78
h. 178.162.194.210
i. 192.99.212.139
j. 195.154.165.112
k. 91.219.236.222
l. 188.166.23.127

m. 193.23.244.244
n. 2.3.69.209
o. 146.0.32.144
p. 50.7.161.218
q. 192.42.113.102
r. 83.169.6.12
s. 158.69.92.127
t. 86.59.21.38
u. 62.138.7.171
v. 51.255.203.235
w. 51.15.36.164
x. 217.79.179.177
y. 128.31.0.39
z. 213.61.66.116
aa. 212.47.232.237
bb. 81.30.158.223
cc. 79.172.193.32
dd. 163.172.149.155
ee. 167.114.35.28
ff. 176.9.39.218
gg. 192.42.113.102
hh. 193.11.114.43
ii. 199.254.238.52
jj. 89.40.71.149

Origen de les dades, AlienVault:

a. 128.31.0.39
b. 146.0.32.144
c. 188.166.23.127
d. 193.23.244.244
e. 2.3.69.209
f. 212.47.232.237
g. 213.61.66.116
h. 217.79.179.177
i. 38.229.72.16
j. 50.7.161.218
k. 79.172.193.32
l. 81.30.158.223
m. 89.45.235.21

Origen de les dades, tercers:

IPs

202.205.99.58
144.164.229.119
182.35.47.171

176.224.108.136
205.236.19.149
25.178.43.53
102.229.120.205
21.179.145.18
88.147.146.188
101.208.25.1
107.193.178.59
56.54.252.11
75.122.73.254
46.192.71.116
163.227.70.213
110.27.193.250
207.47.161.203
55.177.207.140
22.141.227.209
214.222.65.37
96.84.87.170
158.93.156.167
162.28.242.148
18.151.16.81
129.253.239.150
36.29.206.78
210.35.248.130
50.20.29.90
151.22.37.94
132.106.5.32
30.0.40.87
4.101.18.158
168.103.36.90
216.78.159.126
137.176.178.129
37.91.98.102
6.118.20.203
200.109.165.99
166.54.62.180
149.50.190.185
57.196.23.186
152.107.95.61
131.224.163.18
184.195.16.223
185.19.196.74
68.235.43.207
116.9.28.237
211.156.37.154
102.210.143.50
193.200.201.160
175.167.45.24
172.238.16.116
168.70.38.3
44.212.112.159
58.11.107.200
205.227.105.170
162.155.130.2

19.35.172.97
131.87.77.5
116.168.27.85
171.69.83.182
201.242.119.19
139.208.16.216
5.225.123.187
136.87.154.38
13.6.119.22
13.240.101.202
99.62.95.249
183.224.202.19
142.119.113.147
210.198.199.47
167.175.118.216
61.221.0.228
209.33.250.226
136.42.250.190
68.87.85.214
206.5.112.241
110.153.23.216
116.172.113.157
164.215.181.22
33.67.210.159
36.201.150.172
37.150.230.131
19.68.174.176
182.143.156.248
99.36.189.52
122.104.98.30
174.82.205.144
212.102.133.217
150.14.112.63
139.223.66.59
204.5.220.102
57.158.114.171
156.222.183.123
150.207.190.209
198.243.125.155
199.186.193.46
138.134.102.124
90.219.232.57
81.54.18.174
205.247.164.146
121.75.147.202
205.143.222.251
144.173.4.98
214.89.183.80
60.103.182.203
65.147.36.49
123.17.112.106
126.1.232.215
140.102.61.240
102.226.234.186

99.10.236.176
74.45.18.165
217.63.97.131
4.206.60.133
43.149.104.145
18.135.4.223
184.117.30.107
176.86.155.226
134.38.23.98
143.196.106.137
221.57.241.133
223.233.88.120
88.116.154.210
120.63.98.224
143.206.202.17
79.51.239.24
77.51.87.34
37.59.164.0
170.87.84.34
18.145.99.199
31.32.225.221
99.32.34.161
80.187.153.5
53.107.176.73
43.6.83.123
105.33.233.124
152.10.114.52
65.16.27.70
100.108.81.136
215.44.123.3
33.139.54.44
54.127.0.213
135.80.218.165
185.93.145.194
157.155.117.251
4.167.199.122
22.173.221.154
134.138.43.156
95.99.29.42
122.17.252.20
14.187.50.89
93.63.105.96
215.10.227.16
192.120.114.154
38.29.234.148
121.178.76.79
64.130.249.253
138.232.177.206
22.103.120.210
3.212.84.247
49.172.59.200
41.195.65.233
105.95.167.232
139.203.35.170

15.68.6.12
135.202.47.91
145.173.9.183
157.139.120.173
172.118.10.190
139.182.47.170
170.80.158.150
43.240.97.13
188.208.205.169
196.6.12.0
210.219.217.78
198.215.171.33
88.9.223.110
7.90.97.153
215.82.175.151
13.54.209.118
34.49.188.124
209.100.238.214
195.167.30.17
107.73.92.30
156.20.77.9
68.67.67.150
187.136.34.218
26.140.154.130
130.254.220.183
47.243.238.154
115.83.25.253
182.84.195.95
108.162.169.247
216.121.18.91
91.86.43.76
28.206.185.250
99.207.121.14
195.5.252.121
106.94.72.63
85.45.27.241
128.211.17.18
215.159.208.41
210.135.66.138
1.53.154.149
34.38.80.97
144.232.91.176
203.130.167.189
187.218.76.180
152.166.53.219
208.91.90.188
195.177.37.93
111.194.23.4
114.96.80.85
141.25.94.113
129.215.80.68
15.171.52.149
194.91.36.75
173.97.50.48

13.164.179.15
217.76.232.171
15.140.173.8
200.74.132.81
133.24.91.126
85.206.8.136
174.203.168.61
86.23.31.200
217.194.40.14
80.58.176.167
190.77.78.136
92.69.40.236
83.195.175.197
48.46.65.100
207.75.174.248
102.54.236.82
132.180.230.113
69.167.62.145
188.86.42.18
121.51.226.197
160.122.115.240
155.211.199.237
149.7.183.63
122.155.29.248
48.163.14.145
135.238.140.4
39.241.147.141
59.195.43.115
155.132.47.120
180.181.119.127
11.197.176.247
75.222.136.56
34.208.117.164
26.177.225.76
192.17.185.139
2.63.191.229
132.145.3.104
112.242.5.228
110.136.47.126
77.223.157.231
73.225.217.61
6.51.134.228
25.243.131.249
88.82.36.169
135.23.1.16
137.43.2.177
8.219.139.78
122.12.121.76
68.232.17.234
49.174.116.154
129.152.174.230
206.13.122.86
5.25.169.63
150.1.120.62

113.96.229.154
71.190.57.170
209.42.120.239
85.205.88.18
119.185.34.10
42.180.31.148
153.25.242.224
110.44.23.246
135.251.223.83
207.87.38.170
214.32.219.150
217.43.119.19
20.32.100.159
186.81.208.61
100.181.96.39
14.219.85.66
223.12.254.137
21.1.83.27
190.91.134.112
210.79.8.35
16.154.253.245
126.77.209.114
107.190.54.149
212.214.162.170
12.105.6.217
28.199.248.163
6.22.176.56
114.236.156.252
180.147.161.163
149.195.190.210
156.59.160.235
5.243.252.5
201.70.158.152
64.74.139.102
87.110.183.152
210.70.38.42
19.133.209.146
67.163.71.96
6.25.1.129
95.213.143.216
178.234.84.3
65.132.74.166
42.108.24.101
63.92.234.205
164.106.11.243
180.1.226.146
211.211.208.54