BEAST Ransomware: IOCs

🚨Beast Ransomware making waves as new samples are detected out in the Wild!🔥

MD5 Hashes
==========
059ac4569026c1b74e541d98b6240574
7fe11977d078da0c3c7ace54ab47f04e
19ad2f04f5f5972a7824e8683a3045a4
f68013f5189a198b16f6dabac3b64721
2a976f4af95e9275056cd534d55e4011
d5b88355c3bc65b8b9471201e35597e4
74fd302390dc8e8b5f49d2da186e3e8c
7dd96ccc46eca19b03244159483e2230
5679c70050aac4050018f9899cf6e230

BEAST Ransomware
=============
📌Beast Ransomware came to spotlight in May 2024, but have been active since October 2023.
📌.BEAST extension appended after victim file encryption
📌Unlike other groups, this group did not yet launched their DLS on Dark Web. We may expect it in the coming days!
💡Might be the spin off of LockBit Ransomware Builder, as some of the samples are labelled as Black LockBit.
📌LockBit builder was leaked in Sept. 2022
💡Memory Pattern Domains detected with Popular Cities with respective country TLDs such as: astrakhan.ru, kiev.ua
⚠️There are many samples out there with Beast Identification, but do not fall for it, as encrypted extension needs to be double checked before labeling.

Quick Sample Analysis
===============
📌Adds the extension: .BEAST
📌Mutex: BEAST HERE?

📌srvsvc pipe used for data transfer by Beast, which is previously used by notable ransomwares like BlackByte, BlackMatter, Lockbit.
📌The Server service allows a remote machine to create, configure, query, and delete shares through RPC over a named pipe (\\pipe\srvsvc).

IP Addresses
=========
104.18.38.233
104.21.82.93
142.251.179.94
150.171.27.10
152.199.19.161
172.217.14.227
172.67.167.249
192.229.221.95
199.232.210.172
20.223.35.26
20.99.133.109
204.79.197.203
23.216.81.152
23.32.238.178
23.32.238.201
40.126.32.68
40.126.32.72
142.251.111.94
142.251.215.227
20.99.186.246
23.192.210.9
74.125.131.94
74.125.132.94
142.251.211.227
172.253.115.94
104.21.76.57
13.64.180.106
13.85.23.86
142.251.33.67
172.67.188.178
192.229.211.108
20.114.59.183

23.32.238.226
23.32.238.232
23.39.2.183
23.73.129.93
40.126.7.32
51.124.78.146
104.110.191.133
104.110.191.140
104.18.4.5
104.18.5.5
104.71.213.90
104.97.45.70
114.114.114.114
13.107.4.50
131.107.255.255
152.199.19.74
188.234.145.154
184.31.197.9
218.85.157.99
23.198.171.50
23.207.202.79
23.220.169.74
23.39.185.73
23.50.34.78
23.59.198.43
148.251.234.93
178.79.225.0
178.79.225.128
142.250.179.195
142.250.217.99
2.19.192.112
20.223.36.55
20.74.47.205
20.99.184.37
204.79.197.200
216.239.32.29
23.216.147.64
23.216.147.76
51.145.123.29

93.184.221.240

142.250.69.195

172.253.62.94

20.103.156.88

204.79.197.237

92.123.180.184

Follow me on Twitter for more: @RakeshKrish12

#ransomware #beast #infosec #security #cybersecurity