cybereason

MoleRATS: Indicators of Compromise

February 10, 2020

Indicators of Compromise

DOMAINS

nts[.]comnmaherheles[.]egnyte[.]com
csaasd.egnyte[.]com
Webtutorialz[.]com
Nysura[.]com
Laceibagrafica[.]com
Motoqu[.]com
itkeve

URLs

hxxps://uc66abb2815bc75067758741b381.dl.dropboxusercontent[.]com/cd/0/get/Asbu4F1tHfvTjpwbuTeQp1jA8Bkux2hCqodrleSwjOFtB3gVSZZ5rdWNGEaH9UJ9Jl_ElmIbblQNqhUKDdBjTEH5F2BjwsBVZarqItw_9HRgn-PsD-MYoEXYJtaXhOUISbU/file?dl=1
hxxps://www.dropbox[.]com/s/zvjyhigsx39zawx/Details%20Ceasefire%20with%20Israel.zip?dl=1
hXXs://nmaherheles[.]egnyte[.]com/dd/iY4MakFkq4
hxxps://csaasd.egnyte[.]com/dd/h5s7YHzOy5

IPs

78.128.114[.]76

SHA-256 hashes

PDF Downloader:
5b476e05aacea9edc14f7e4bab1b724ef54915f30c39ac87503ed395feae611e

Decoy Document:
2c50eedc260c82dc176447aa4116ad37112864f4e1e3e95c4817499d9f18a90d

Archives:

31b08c139b6fc3bdde0734d1b2c609550a03ca97ec941eaf24224bb449e17e26

E8d73a94d8ff18c7791bf4547bc4ee2d3f62082c594d3c3cf7d640f7bbd15614
0293e43cb22c1ee2bfde4c74c7b818073adaf83590285d95d36d3c2638e661a4
A6e0297777ba29e21e5d1acca6210d436eee5c2b93d2dec27910ffd6e2266559
f9e9bca91b3ebd3921b3299128da5622114f79c27a2475af6fb2b1012dbcd348

Spark Backdoor:

6e896099a3ceb563f43f49a255672cfd14d88799f29617aa362ecd2128446a47
2268101c32989e7cfcb8b2ef47163f741850e7619edf0c0e8f365cfceb1b1e82
7bb719f1c64d627ecb1f13c97dc050a7bb1441497f26578f7b2a9302adbbb128
Cf32479ed30ae959c4ec8a286bb039425d174062b26054c80572b4625646c551
b08b8fddb9dd940a8ab91c9cb29db9bb611a5c533c9489fb99e36c43b4df1eca
6e60f5c65299ee7f7b257f5c83d3bb36154654b26e721136f7184514fcf6b296
c2bb3a70fc86ded19f03d81d9b051f5afa7e3c2591a9250ef950055a56b9e296
7bb719f1c64d627ecb1f13c97dc050a7bb1441497f26578f7b2a9302adbbb128
89acce7cdd354a04f2edd4a2226caf5c47246a8196ec1d9b98159da38ec20c24
5139a334d5629c598325787fc43a2924d38d3c005bffd93afb7258a4a9a8d8b3
92d0c5f5ecffd3d3cfda6355817f4410b0daa3095f2445a8574e43d67cdca0b7
1fedd4c7b2dbe95533a276405d2250cca0d638e74560593957a25b456a12ef23
ab4e247dd0c784cd5d1377b4ff41e2e338f1d83cb41866fdcfc246a87a49b5e7
f19276efbbd02fc58dd9bc60210f8d7a7037251e5c695a3bad50566f98dbece7
2268101c32989e7cfcb8b2ef47163f741850e7619edf0c0e8f365cfceb1b1e82
92d0c5f5ecffd3d3cfda6355817f4410b0daa3095f2445a8574e43d67cdca0b7
7774b9f930a4b290fb6925f6a1b944c8c6f9151870df74bff6fefc6901d0d6f6
4bddf57ffea80569e91c3c62bcbe8ad4fe7a3955b8cdfa9a10003b4fe3882f6c
1706fd05f02f13aca66f36785c2d8dae42eaf5142bffd3931c96228a35ee98de
1d8c54c9af1b05b9679f1c67850a7e2eb6db95343a44d9aa882896c6d4f9c490
5139a334d5629c598325787fc43a2924d38d3c005bffd93afb7258a4a9a8d8b3
40b7a1e8c00deb6d26f28bbdd3e9abe0a483873a4a530742bb65faace89ffd11
4bddf57ffea80569e91c3c62bcbe8ad4fe7a3955b8cdfa9a10003b4fe3882f6c
7774b9f930a4b290fb6925f6a1b944c8c6f9151870df74bff6fefc6901d0d6f6
1d8c54c9af1b05b9679f1c67850a7e2eb6db95343a44d9aa882896c6d4f9c490
1706fd05f02f13aca66f36785c2d8dae42eaf5142bffd3931c96228a35ee98de
01887df1febdf6fdf85e870e8d87f4397a4854ffedeaffd2f8d21310306e50b0
04fa6aaea5e3a26c1c46ab9a30102fca3a2e0360542f5e8bf3331d74ef1aa918