“Posh” C2 IP Addresses

94.198.53.143
185.234.216.64
3.131.100.38
184.72.153.18
116.203.51.117
45.79.196.203
3.17.25.38
3.16.158.68
52.18.207.109
79.143.181.62
88.210.9.139

C2 URLs

/webhp/
/adsense/troubleshooter/1631343/
/trader-update/history&pd=/
/status/995598521343541248/query=/
/uasclient/0.1.34/modules/
/utag/lbg/main/prod/utag.15.js/
/GoPro5/black/2018/
/usersync/tradedesk/
/bootstrap/3.1.1/bootstrap.min.js/
/TOS/
/business/home.asp&ved=/
/web/20110920084728/
/vssf/wppo/site/bgroup/visitor/
/Philips/v902/
/bh/sync/aol/
/async/newtab/
/advanced_search/
/adServingData/PROD/TMClient/6/8736/
/vfe01s/1/vsopts.js/
/cisben/marketq/
/business/retail-business/insurance.asp/
/client_204/
/branch-locator/search.asp/
/work/embedded/search/
/babel-polyfill/6.3.14/polyfill.min.js=/
/cdba/
/putil/2018/0/11/po.html/
/qqzddddd/2018/load.php/
/types/translation/v1/articles/

THREAT INTEL DISCLAIMER: The information in this product is provided “as is.” It is not yet finally evaluated intelligence and should be considered raw information that is provided strictly for situational awareness, given what is known at this time.

/classroom/sharewidget/widget_stable.html/

File Hashes from Open Directory

atera_del2.bat:
3c1853831958efe2cc78ea82b4fbd565
dc14cffa48dd95157fd381cb75bae1773d510c54
512beb7dfa9fdbc8be7fbf59c7bec7911296f9e36c8a3d3b95e7aef4a88bf09c

atera_del.bat:
754e08c93369e5bfe24ca09b422affdd
591379f5d7d256e83de05207fd872acfa8e8aa5e
ea7dec8fa52d2300350367691ae2fbea13dbd5bf80d6b43b05eedf197529aa77

backup.bat:
91be6e6a8b4c2cb99db5b99d40e06978
86f599090aa2c7c1df65dccccf00e1818e72246a
beb5022543a1e12e1f8f5ffe5d520e5fc9cf623aea512cfb43ea2f8c2897420c

clearlog.bat:
f7a730acc86f1d6759249ccc579b1794
fe1fb1da6435a6d6283e993569d3fc82a67d7ac8
09f91e90a1604a633c00d6039581f552603421356cb1edb62e085b32ff01b94e

def1.bat:
1393dab192ea2e2427889839a2d8fcf7
373609c0f30ee313fd0cc6c4e572452483d87244
0e626e01d3ae7840aa486468f40138284ccbd70dfe336a6b5d4008d01eb79988

defendermalwar.bat:
1365640fc3c0e1824e348956172caed7
300c89889bbb5ef61f470174a6fcad73c4516779
5b43428452a867ad61554d763c8f19ca4cd8af8c31194304785e9e45f9258441

delbackup.bat:
a8b335886e39adf23e6aa44a00bf82dc
2de53c24663149366fca22f354aff5c0f5b348f4
6cff22a3ea7c054075b9aded5933587bf997623183539e10e426d103d604f046

disable.bat:
cc35c94e64830ff143b54783c9869ecf
4a8a4e6069ec4f6a4f24614eb885c57484bc9b79
fdc105ae79dff83f31777c6e047272c5b372251a3af49e20370e7ee9d1c70763

THREAT INTEL DISCLAIMER: The information in this product is provided “as is.” It is not yet finally evaluated intelligence and should be considered raw information that is provided strictly for situational awareness, given what is known at this time.

hyp.bat:
d1e3216cf698a58832d947d95dc4f3f8
1224f9667d7f1d3b7fba17f414d343912bec03db
08d40a402b3754e52e4e86003bffddfdccbceefd335f53591f4cf715f8d30321

LOGOFALL1.bat:
c84e1655f0ba917cc605018e32eba9f3
7dee2a38cc2ba81cc373b50f42c8946601d177cb
3691dbb1834db4eb8ef4c195d26779b87db267a56f2ebca6c146a53fb8adb9c0

LOGOFALL.bat:
9a66570b7e25035ff337fa6098f59823
a65d7caf354161798d2458cfee9e4e988f0e94af
03b3c37300bf9dcfaa4594e86841b70263324dda305484fb268b27deb09f936c

native_dropper:
444d7a27ac0327ccc0cf4e75a32025c9
8441e7b6b6b9f24439e71c6b031262bc76d73c28
039bf780ae46875945344af489a590c5b7a36d458372a3173b55b3dc3559dfff

ngrok.exe (official ngrok):
e2eadf60d8f25cae9b29decab461177b
cecc54143cc375af1b9aed0021643b179574e592
1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386

ON.bat:
8c7c782df59edd61aabbc510d7747b11
66ac6cf4bb4247daf1d09d9d4bc4e357cc39c6c8
b0056bef817408449470d3fa43e13cbc89cabdae795b1dc8cbe9905c5946f530

Posh_v2_droper_x64.exe:
a5748047ebbe34d7821a2a040e4ca54e
55126d8215b771aa2f62f16e6aad9e8832824a4c
63229da1bed0c0eafc4ed087651af3eec521e7fbd098300f7d862582d03a675d

py_dropper.sh:
679d0dab79a98da8e20351f9f887e4f2
9442647283e52c91c2e836b19749f184936cf6c2
01ec91a3145332174eef9239f7767adaa5e3dff3a436dfb7d2f978f88ea6cd93

setup_uncnow.msi (Atera Remote Admin):
c8903eb5763c670a15049d74d764188c
990f68cca516192d73ef443f51ed80813e324b0b
91d9c73b804aae60057aa93f4296d39ec32a01fe8201f9b73f979d9f9e4aea8b

THREAT INTEL DISCLAIMER: The information in this product is provided “as is.” It is not yet finally evaluated intelligence and should be considered raw information that is provided strictly for situational awareness, given what is known at this time.

shadow.bat:
4cf52cee2001cd10528f429fb6d9fd07
3cf331934996ec4338418b847b52d78d8a29d224
87ab1707a553557b10fa721a32f053fbb40d11de6f692e96e067d03316fe530b

shadowGuru.bat:
0f1290d014dfd9e66bbbed96a828f7d1
b8fc0194f6ed56e4a57c16756e506369c74c4078
2bcd5702a7565952c44075ac6fb946c7780526640d1264f692c7664c02c68465

VmManagedSetup.exe (SystemBC proxy malware):
7ee103ee99b95c07cc4a024e4d0fdc03
885fc76ba1261a1dcce87f183a2385b2b99afd96
cc4960939a41d6a281ddad307b107e16214f4aeda261c9b5037f26e60dc7bba2

WILD_PRIDE.exe (Sliver C2):
6b44d99b258c275ee7fcf230da177f3e
833a461f6d479d164b453cc9f5f51259d991b1b7
1aecadf489a6dd7a3a6e5dfda9425673a9d04d38a5cb6b0b8f961536c11237ed

z1.bat:
97dc80d3844b01587d9fd6377b9ab0a7
93b717a562f2cc3fdf2355bd9d2670ba2391cc60
a668a98e57c03decf6ea76bb32f67f3f077ef2277e57f4117d44f4342977fddf

z.bat:
fe00973fc12b3c6330abd9807dfb1d70
d2f5c890e3e1dd9b42e695586c06408b31d4ec7a
38283b775552da8981452941ea74191aa0d203edd3f61fb2dee7b0aea3514955

THREAT INTEL DISCLAIMER: The information in this product is provided “as is.” It is not yet finally evaluated intelligence and should be considered raw information that is provided strictly for situational awareness, given what is known at this time.