cybereason

Prometei Botnet | Indicators of Compromise

April 15th, 2021

Domains	IPs	Hashes - SHA256
P1.feefreepool.net xmr.feefreepool.net gb7ni5rgeexdcncj.onion rongo.prohash.org bk1.bitspiritfun2.net mkhkjxgchtfgu7uhofxzgoawntfzrkd ccymveektqgpxrpjb72oq.zero dummy.zero cp22.umbrellapool.club 193.160.102.91.in-addr.arpa 102.72.239.193.in-addr.arpa 183.247.34.37.in-addr.arpa cp23.umbrellapool.club bk2.bitspiritfun2.net	217.165.8.218 77.92.138.51 91.102.160.193 103.11.244.221 121.200.54.85 112.109.89.53 178.21.164.68 69.84.240.57 208.66.132.3	Sqhost.exe / zsvc.exe: f0a5b257f16c4ccff520365ebc143f09ccf23 3e642bf540b5b90a2bbdb43d5b4 ExchDefender.exe D8e3e22997533300c097b47d71feeda51d ca183c35a0d818faa12ee903e969d5 SearchIndexer.exe: b0e743517e7abf75a80b81bb7aadc9c166a c47ba89c0654ba855dda1e4d96c3e Netwalker.7z: 55fc69a7e1b2371d8762be0b4f403d32db2 4902891fdbfb8b7d2b7fd1963f1b4
P1.feefreepool.net xmr.feefreepool.net gb7ni5rgeexdcncj.onion rongo.prohash.org bk1.bitspiritfun2.net mkhkjxgchtfgu7uhofxzgoawntfzrkd ccymveektqgpxrpjb72oq.zero dummy.zero cp22.umbrellapool.club 193.160.102.91.in-addr.arpa 102.72.239.193.in-addr.arpa 183.247.34.37.in-addr.arpa cp23.umbrellapool.club bk2.bitspiritfun2.net	217.165.8.218 77.92.138.51 91.102.160.193 103.11.244.221 121.200.54.85 112.109.89.53 178.21.164.68 69.84.240.57 208.66.132.3	Rdpclip.exe: e4bd40643f64ac5e8d4093bddee0e26fcc7 4d2c15ba98b505098d13da22015f5 Miwalk: fb8f100e646dec8f19cb439d4020b5f5f43af dc2414279296e13469f13a018ca Bklocal2.exe / Bklocal4.exe f86f9d0d3ea06bd4be6ee84c09bd13e43ecf cc71653d15994a39e55c2d6bd664 e961c07d534bc1cb96f159fce573fc671bd1 88cef8756ef32acd9afb49528331
P1.feefreepool.net xmr.feefreepool.net gb7ni5rgeexdcncj.onion rongo.prohash.org	217.165.8.218 77.92.138.51 91.102.160.193 103.11.244.221	Nethelper2.exe / Nethelper4.exe: 2f114862bd999c38b69b633488bcbb6c74c 9a11e28b7ef335f6c77bba32ed2d6

bk1.bitspiritfun2.net mkhkjxgchtfgu7uhofxzgoawntfzrkd ccymveektqgpxrpjb72oq.zero dummy.zero cp22.umbrellapool.club 193.160.102.91.in-addr.arpa 102.72.239.193.in-addr.arpa 183.247.34.37.in-addr.arpa cp23.umbrellapool.club bk2.bitspiritfun2.net	121.200.54.85 112.109.89.53 178.21.164.68 69.84.240.57 208.66.132.3	5de7afdde08f7b8ba705c8332c693747d53 7fd5b1bb0e7b0c757c0f364a60eb8 Windrlver.exe: dc73a88f544efc943da73c9f6535facdb618 00f6205ad3dddb9adb7c6ab229ab