cybereason

Pierogi: Indicators of Compromise

February 13, 2020

Indicators of Compromise

URLs

hxxp://linda-callaghan[.]icu/Minkowski/microsoft/utilities
hxxp://linda-callaghan[.]icu/Minkowski/brown
hxxp://nicoledotson[.]icu/debby/weatherford/Ekspertyza
hxxp://nicoledotson[.]icu/debby/weatherford/Zavantazhyty
hxxp://nicoledotson[.]icu/debby/weatherford/Vydalyty
hxxp://nicoledotson[.]icu/debby/weatherford/Yortysnr

Domains

Nicoledotson[.]icu
Linda-callaghan[.]icu

IPs

68.65.122[.]210
198.54.115[.]49

Weaponized Word Documents
4a6d1b686873158a1eb088a2756daf2882bef4f5ffc7af370859b6f87c08840f
b33f22b967a5be0e886d479d47d6c9d35c6639d2ba2e14ffe42e7d2e5b11ad80

Decoy documents (SHA-256)

7b4c736b92ce702fb584845380e237aa55ddb4ef693ea65a766c9d9890b3852c
50a597aa557084e938e2a987ec5db99187428091e8141e616cced72e6a39de1b
9e4464d8dc8a3984561a104a93a7b8d6eb3d622d5187ae1d3fa6f6dafa2231a8
65c8b9e9017ac84d90553a252c836c38b6a3902e5ab24d3a4b8a584e2d615fcc
d3771d58051cb0f4435232769ed11c0c0e6457505962ddb6eeb46d900de55428
9e4464d8dc8a3984561a104a93a7b8d6eb3d622d5187ae1d3fa6f6dafa2231a8
f6876fd68fdb9c964a573ad04e4e0d3cfd328304659156efc9866844a28c7427

932ecbc5112abd0ed30231896752ca471ecd0c600b85134631c1d5ffcf5469fb
4583b49086c7b88cf9d074597b1d65ff33730e1337aee2a87b8745e94539d964

Backdoor hashes (SHA-256):

Eab20d4c0eeff48e7e1b6b59d79cd169cac277aeb5f91f462f838fcd6835e0ac
0de10ec9ec327818002281b4cdd399d6cf330146d47ac00cf47b571a6f0a4eaa
83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b
094e318d14493a9f56d56b44b30fd396af8b296119ff5b82aca01db9af83fd48
707e27d94b0d37dc55d7ca12d833ebaec80b50decb218a2eb79565561a807fe6
80fb33854bf54ceac731aed91c677d8fb933d1593eb95447b06bd9b80f562ed2
23aa2347bf83127d40e05742d7c521245e51886f38b285be7227ddb96d765337
D08e7464fa8650e669012056548383fbadcd29a093a28eb7d0c2ba4e9036eb07
4e77963ba7f70d6777a77c158fab61024f384877d78282d31ba7bbac06724b68
050a45680d5f344034be13d4fc3a7e389ceb096bd01c36c680d8e7a75d3dbae2
4be7b1c2d862348ee00bcd36d7a6543f1ebb7d81f9c48f5dd05e19d6ccdfaeb5
d8dc553fbb4569045a298759af75a3a108f82cf883ae986214d3075cc738836e