cybereason

Darkside Ransomware | Indicators of Compromise

April 1st, 2021

IOC	Type	Description
243dff06fc80a049f4fb37292f8b8def0fce29768f345c88ee10699e22b0ae60 12ee27f56ec8a2a3eb2fe69179be3f7a7193ce2b92963ad33356ed299f7ed975 9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297 5860f2415aa9a30c045099e3071f099313f653ae1806d6bcdb5f47d5da96c6d7 78782fd324bc98a57274bd3fff8f756217c011484ebf6b614060115a699ee134 dc4b8dfff72ff08ec4daa8db4c096a350a9a1bf5434ba7796ab10ec1322ac38c 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193c3cfc4bde4d3bc 4edb883d1ac97824ee42d9f92917cc84b52995abcd17b2852a7e3d5bb567ffbe e9417cb1baec2826e3f5a6f64ade26c1374d74d8aa41bfabd29ea20ea5894b14 fb76b4a667c6d790c39fcc93a3aac8cd2a224f0eb9ece4ecfd7825f606c2a8b6 4d9432e8a0ceb64c34b13d550251b8d9478ca784e50105dc0d729490fb861d1a 508dd6f7ed6c143cf5e1ed6a4051dd8ee7b5bf4b7f55e0704d21ba785f2d5add cc54647e8c3fe7b701d78a6fa072c52641ac11d395a6d2ffaf05f38f53112556 68872cc22fbdf0c2f69c32ac878ba9a7b7cf61fe5dd0e3da200131b8b23438e7 1ef8db7e8bd3aaba8b1cef96cd52fde587871571b1719c5d40f9a9c98dd26f84 43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa ec153c3cb67f742b12a35a498d93cd80f47b19ea7b7eb0de217139f136ea0073 533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d 1cc7c198a8a2c935fd6f07970479e544f5b35a8eb3173de0305ebdf76a0988cb 151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5 ac092962654b46a670b030026d07f5b8161cecd2abd6eece52b7892965aa521b 06cfe7f5d88e82f7adda6d8333ca8b302debb22904c68a942188be5730e9b3c8 afb22b1ff281c085b60052831ead0a0ed300fac0160f87851dacc67d4e158178 17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61 0839aabe5fd63b16844a27b3c586c02a044d119010a1a40ee4035501c34eae0d f42bcc81c05e8944649958f8b9296c5523d1eb8ab00842d66530702e476561ef adcb912694b1abcdf9c467b5d47abe7590b590777b88045d10992d34a27aa06e 6228f75f52fd69488419c0e0eb3617b5b894a566a93e52b99a9addced7364cff bac2149254f5ce314bab830f574e16c9d67e8198532961984143103 4c31646e0 f764c49daffdacafa94aaece1d5094e0fac794639758e673440329b02c0fda39 691515a485b0b3989fb71c6807e640eeec1a0e30d90500db6414035d942f70a5 6d656f110246990d10fe0b0132704b1323859d4003f2b1d5d03f665c710b8fd3 e0c0cbc50a9ed4d01a176497c8dba913cbbba515ea701a67ef00dcb7c8a84368 48a848bc9e0f126b41e5ca196707412c7c40087404c0c8ed70e5cee4a418203a	SHA256	DarkSide binaries
temisleyes[.]com catsdegree[.]com	Domains	C2
198.54.117[.]200 198.54.117[.]198	IP	C2

198.54.117[.]199
198.54.117[.]197
185.117.119[.]87