

TYPE	INDICATOR	DESCRIPTION
IP ADDRESS	139.224.17.182	C&C server
IP ADDRESS	123.56.225.31	C&C server
IP ADDRESS	192.229.211.108	C&C server
IP ADDRESS	120.79.47.9	C&C server
IP ADDRESS	1.92.84.147	C&C server
IP ADDRESS	101.133.168.75	C&C server
IP ADDRESS	107.173.248.41	C&C server
IP ADDRESS	112.126.85.225	C&C server
IP ADDRESS	114.55.86.183	C&C server
IP ADDRESS	116.205.246.230	C&C server
IP ADDRESS	120.77.201.255	C&C server
IP ADDRESS	121.41.130.38	C&C server
IP ADDRESS	122.51.216.39	C&C server
IP ADDRESS	123.56.106.203	C&C server
IP ADDRESS	123.56.141.243	C&C server
IP ADDRESS	123.57.248.191	C&C server
IP ADDRESS	123.57.50.228	C&C server
IP ADDRESS	123.57.51.44	C&C server
IP ADDRESS	182.92.123.99	C&C server
IP ADDRESS	182.92.20.52	C&C server
IP ADDRESS	182.92.21.95	C&C server
IP ADDRESS	39.105.204.46	C&C server
IP ADDRESS	39.105.52.147	C&C server
IP ADDRESS	39.106.19.143	C&C server

IP ADDRESS	39.99.39.116	C&C server
IP ADDRESS	47.103.80.176	C&C server
IP ADDRESS	47.106.165.142	C&C server
IP ADDRESS	47.116.177.101	C&C server
IP ADDRESS	47.93.174.98	C&C server
IP ADDRESS	47.94.104.161	C&C server
IP ADDRESS	47.94.107.105	C&C server
IP ADDRESS	47.94.227.173	C&C server
IP ADDRESS	47.94.234.19	C&C server
IP ADDRESS	47.94.237.26	C&C server
IP ADDRESS	47.94.43.118	C&C server
IP ADDRESS	60.205.176.230	C&C server
IP ADDRESS	60.205.232.221	C&C server
IP ADDRESS	8.134.48.101	C&C server
IP ADDRESS	8.138.118.56	C&C server
IP ADDRESS	8.138.147.209	C&C server
IP ADDRESS	8.141.83.102	C&C server
IP ADDRESS	8.147.116.134	C&C server
IP ADDRESS	82.156.184.108	C&C server
URL	https://123.56.225.31/flag.jpg	Payload download URL
URL	https://139.224.17.182/api/v1/endpoints	C&C endpoint
SHA256	914b1b3180e7ec1980d0baf6fa36daade752bb26aec572399d2f59436eaa635	SquidLoader
SHA256	01c5b2be71a64b6bbd2029a774f63ed8afc0d122e269e2340c9ab5ec9303318e	SquidLoader
SHA256	08f78a98770666da78416b034559a99a325de6732400ab4e6d357f9748f1d4cb	SquidLoader
SHA256	0f04bdf76617081f33b86896d2fdb1c0ca741ee6ffe40602a04db0dbac975fa4	SquidLoader

SHA256	23a041fd6c1f9ac20bc189f3c74e3ad96a2353c0ac3b917b27966497f40d4d85	Loaded payload
SHA256	2838813ddc32db0cdfdc87176665929a1a9846b346c91fbf44ccfb7d4d99db16	SquidLoader
SHA256	2c497cd09bb4a108b4f29bb96e89d140ba7a04a9ff33f7cd642b9ac6598ecb09	SquidLoader
SHA256	2cd9936fbdd2b98d1abfe9396341501223d35aa43b88a8ca1337dca36f4553ed	SquidLoader
SHA256	35b8ddc1e1f632e70dc20387951f06e664d0969c3ede6eb21c353ac021981da0	SquidLoader
SHA256	396a0b467b9067cfc5a005b728e2c4a782502895fdc27ab4988bca975f58a961	SquidLoader
SHA256	41523349ade62c5d2e9a3274043970ea43ce7c7e5fb2153497979f4b4df1479b	SquidLoader
SHA256	46caddb7dc5598817cac3c325bd434f1d1cc7e476523fa5eaf4649f5edc7fbc2	SquidLoader
SHA256	47bdd9282889be2bcf0c70bf52c2da7730a39c4f5a56d93d17793c91381f0db0	SquidLoader
SHA256	54bc0e62f154f3c86687b8e2c845619b071d374b2970edc055b293c2226c5d64	SquidLoader
SHA256	565fc225391c1d37c15eb8f852819902d801092fdd93eb1da596a97b42cce0c	SquidLoader
SHA256	597b7e9962b42c4568492aaa44c7164fbf2c1a81d627bc2262a82b05b1e19534	SquidLoader
SHA256	663d4a7f6224db2718b015dca7b739a0538ccf0c8176c1f84ed6030ac3e7e2d0	SquidLoader
SHA256	6d41e0e197b9635f27252dba94293ad714eadcfc39d1627288cb88900ef6e3af	SquidLoader
SHA256	6e67cfa4cbd2b35c584f47bd9ab08e355266c4cd1b59d7a958c3d16c11bfaa57	SquidLoader
SHA256	75d73e41be593a9990c9357e6ed407c05193de6e8d424c56747ad0063f1374b2	SquidLoader
SHA256	7638c944f39ce58230dfd97e171777d9aa333737ead9baddf8534196f3790a91	SquidLoader
SHA256	8004c68e2ac21bfed82747f11105f202776593f980d7dc90af782cf7649d0fe6	SquidLoader
SHA256	8ab8a80ffb64145a30231d9097852b5a1008ab20665feb6bb9c3caf98b1e479b	SquidLoader
SHA256	8f66d46fb02a13ccd993ed04dcdf0324a3345bb41a1329092c7d6634b412ba2d	SquidLoader
SHA256	914b1b3180e7ec1980d0baf6fa36daade752bb26aec572399d2f59436eaa635	SquidLoader
SHA256	a851fab94f89315bc305cd7fe6bc308ffc6e912e793552e7757a7f6bea13965	SquidLoader
SHA256	aa9f4f876a332f4ce53aa629c3548c79c62d9b540130198c64e00b251ee94171	SquidLoader
SHA256	b247fad2f1361e0e10fd3ad31d9485ee1b6af722c8caaff2d2643e67bbe2e6a2	SquidLoader
SHA256	b2c2b31e042879ac75c7a4a3d4a475256bca0658bb1ec5c291febaee44d31bef	SquidLoader

SHA256	b4701b91af131597ec887646f066fb6c6c968a74f35e3bb64a20ad93d5ccf0b8	SquidLoader
SHA256	bdc2cd4ce434e57bfa6aa1c6e8f4a62114a581eb4cdb4ad57cf36a1fad3c06db	SquidLoader
SHA256	cc94f49acdd8741c94263ec4d79b3cf929ae811cd12802c960e4eedb74581bc8	SquidLoader
SHA256	cd7759b3075e0d4ed8ce787e52a8130faecf6535676a33739b3242305102a26c	SquidLoader
SHA256	d73f823a09ab7820dabadb9b32041e3839551c4b8fdc291a0196233aba24c942	SquidLoader
SHA256	d81dc8d657477014a3d2a5fdeb507b0573e35f7484e8d0a57eb030211ad89505	SquidLoader
SHA256	dcb8ddcdf89e0896340b253a4008118f9b40000484f7ab41a359805e9d9f7fd3	SquidLoader
SHA256	e4294bdd8927952c9cca75792ca29a8c0d51bd59034272944e203313160f6e2a	SquidLoader
SHA256	e65208bc0a0302e55755d47628e89cc80a788512f40252083078f931c4e6d239	SquidLoader
SHA256	f303fac65e7487e1fa7a229516fc493a48dc6d5b54544b4820298aef785b9429	SquidLoader
SHA256	f3ed0548e08c1032a81f483f3453cc0837b405603b24f158d99cc587c354edcc	SquidLoader