Hashes:

LNKs:
8a10797ac7f84d09cfb4cb3a6a1e75473dc81dab757c0000036a861575216e5c
124677d655b829892bfe73877ca2a2289bbf623cf404ae50f73f255866205adc
df542d57b80c6bb0cdfff0e009ed410e4241d91624cb7b38c1b806bd6df103d8
49796c18a09c100118b7d678dc76bea283a70d6ba695224db9364ff740597103
54759951089f44a3918e164b8bf29c8f388cfd41f9930f81b8103852947fed93
e16153ee38bc971c4fd94f4d35996d0ef41a33bb53d5028170da48712904a3e7
a55d19aabd1b56c5d583311da142314df09400b7a1eea4dcd49474524a8f879b
df47ca45bdf2f910a0ebae49d29549240066f77d0abb735cf1afe41368cb0d85
b74e20c912e5c1529ec73bcd89776d4f81e56663edcfaccc82ecac50e34d5284
ee58d8ecc5dce13f4eee1e6164654f82a5eb339dc3c6e023b69ea7d6df5b930f
75033494867c133e7470c348cc36da13b18aa20d13612619540a9a909aa29f48
16e153921beabc0bc5bc1b161e19afb14e39cfe9991dcd04f20a923ed1d27989
1a2cf862d210f6d0b85fbf71974f3e1fbe1d637e2ef81f511ea64b55ed2423c7
5e804c0a24a5f471635bed760fee8bba15a3d69fc6ddac306ef0da364b58aa34
4d6488a7db35e0447f6fe44e94f26773cf8666c7071ec27257daeca7bd72bab1
de6d22103f4d655614d5c8cb7fa6350486edc08a80da48b20a3c83ec45bb7aba
7f800784b00354dd15eee129317a63bd3f7bb25622e898c873603e5b142cbb09
24469a7f1f33cdecf507824a773814b5f3190c81acaf04d06c168ccbf71b2ee8
b220804279422bd5e6150e93bea68ead6648f92fc192fe26df9ff77efda1b319
91cbd850c6ac25ad762eb256ab432c45af78737cb3fb042f6fd8b3ece9a96dfb
bb5733aaea12b3d0f38eccb5725fc0fa5e56d0a6462f0eb4228c3d34a177e1d6
907f594f49e498f0526684e03afd76e953b46b2c4947dd260f90f2665b7ff875
c54cde89abbc781c3c435b2bc2a71189a78f34cd4dfa3a0e804eea407d14c944

HTAs:
caed359105265eac5e9628548c95a898c3f8d0e427354eaa6ec3a2acb3515c83
a8c75aaf566c230b2e006e36209bda758864ef990b5e324c338f12ec3b1e9d3d
d11fdc8146e3ed7669601b5a787843542711f6f4d0a728aecbf855a787e1b148
c073355b2b6b41fa7bba206e872df1439f63c8bb4bcd85dd4e5e076e4e466f0a
772dd3668bb5449a6e83b94103335f890423e1f7206963f79f4b3b77ea9d4bcd
f0431adfc5921c02cfdcd4b86a1f5b56fe476355622768 6ffff41e2a602af93a
74ce70dd77d6f8a8c22ec4ce9af76c2a9d2c39f858a3b0610b6d1598aea38548
fb48d1a60ad9dd2325ea161cacf84355185fc33aed8b08a415d0098cb1c4560a
660427971b04313c2ebf2410f9ba4f67c5f1d8ecc472be6c709546a12dc97f7d
f034db8f1e05edaa8b5c9fcd6f2987cb8cbb480a3793b9d67c3ff1d3c25f2b68

a00813028306c519829ca3b2f16357124aa77b998c9c6cc6f16c00c24503eace
0b68637be6ecc8f66bd68dd5a4b669f15aeeeb66a873e7b8caaad575b4215aca
0409094e0075f146a84cae1df4404262cb0de371863d1b3dde45b0b69f8c354c
3534eec1bcc94e717060c4fd4ed249cff77b6ce20c3be45061c8d9717c53da44
e2428029a07f6964fb945acda1f3f72852f5fc9c85924420fa0bee63d2370659
4749dc156be23be1e49dc2e48bfd370048c3d46e2be08b8b108088c5ea695fdb
931f50af89987aaf7f4e85516e42ccdd7d3c9bba2d51b13324fef184b14d96ef
d96014c5357a338aa2659822bea02d1901985a84a0bee8dce11686993df015c7
6ed9dc3f18d676b66cf4bb583c31137267ea6b8652f14eb44df47a49b45da3d8
f927d3aec7a84b45d8b6e4f871cf4d4c462143079b31f7d07214754cfb04cb0a
0a52ba42fae2876b014c5343935df94de0659272df2ec9a018a3015fbaa7f5d2
f0bbc9b2ae7ad32636c6c0ca2b95eab4b3e0498daac5175b44cb42b369fc7366
72b0004a0d4551a43d5ce30a6cc733806ac0fa2220cb42857cb40f183eec31ef
6e7cb476f8ad98f64ec4b3633aa600aeb0dfe20d964b22c2dba35b7e3fe6d944
3972fe894765a9262e401d7e5e9a23d042655265bf8f4944b91ddbfcbbdba45a
65ae52ac448a011701c4f077449112329b79f23f758524dd753dfe757c52f508
05c129e088486b1b9c8f8728fdd8081363f6c58f2db5fe2e34cf01913bdf08dc
f889d2358eec85212659b0d273e5e892e610e114c990bfde93c9d607d85f58b0
234defc7e28089ce81141907ceb16f3c80b12b6c19a4516d97f049ec66af633d
bb1e62f812c67a049d7148e609f9abc4047e07ba942446628cc7149f517afd34
18f53a353621376c9ddc610a8c916e582c69aa799fc6ab2ff5bd146e9ecefbe1
1e36dc2d6ca94e14dc7acc7c183d1cca3e05d6f01813c9a1918ef99f9caae693
4ad90c52ef1ee513305a50f0247a44bdec8edb2d80c8042a4139e6e5a69a8c83
a80fd4681d2c55e65ab0417288bed5985576da3723b4f4116caaa742f42ad3a1

Loader DLLs:
fd2f6e33ab19446828dc73771e2696220f4f3a03a2cd73037bae1b77db548385
98dce6975b7b771746b7442395393d8c8bc717320dca87a900020fba68f63b99
e3be76c52c08653d3188461f1bc2ff5fbaaed2a5c667ee11c05c66b6344fc00c
9117930194e292e17520e5719c5cb0a5258ea6b59eb94b727270b996b70479b5
c43028136118dc1aeed2d47bbb0c6822297f65c9fd411b4de19824f52dafa01f
743376f1673d84721dd9348160accf180c534a2ea1959fb9f484ebd225cddc5b
8156a453e69bfda734b79d87617b957fbecc40b563aca55b266b709bd8b50b3b
494b16a94ecf464ac0a821d8d2652d3a19784ae2827eb83b5fc7e2dc970e1858
5312c8090fa56746f27a9947b3277f437bcdb18b220dea712a97308c06eea001
a3c7f182ccea96f557e423fb57ec699a1902f1ef51cc766cdd0c690a38f88010
be7cd33506a63919e0f01487dc672563263af618822ce54150fb5f14839003dc
58f7edd094daac8e11832a4bb57fb4df4aad991b1499af827ac56b951ac7cdbb
353b9177483c499c806a604299ef28e655f5647e039a408e4226bec650bea2d2
6afbb8029cb52890b4d8893029b789dcbcd86aace059e50c4c6ed12dc4364a4a
62124b7d418a3defd0b33e3c15c4cee7c88808d2c7712768c25c304011652d4c

3da037462cda8dd0e32999798c70bbc699d2d6fff34d9dbc20066c4aa2c67543

DUser dlls:
9d7edfa9834f4c5b5b35c04c7906993c330fc0a29382a69f9601793211ccf253
cf16c7ece034eca4d6489f77d87a7100ba3b4721678bde3bf2e54a01dd4ecc51
f08fdfc993072272f4b3945800d50558e03ae532af7099b8d86e467cb522f0bf
01f14a8749b2022fb72334b9d10a06a5ef8921f3f38fe4a3f78ca78cf23d3e5e
5b3f238fa7392e6e5a35d41f0b3f2eff7fce70547d0572df7ef8bf46e07d9a9a
3dfa7180dcd674b26539687313e2e80d705f52dbe74163c40ae050e60488382a

njRAT Droppers:
1afb690159f041ce4f0af3618ebd1cef4597d3d94bd249c4644b8e359f46199d
f17fd9ff93d1b3db6c3e4463d5ca5c11b99827890c58721d2860df75d4323705
84609f9e443225a23cca8ab6be910c207d220bb430fd543d0724eaae8f7df592
c79ab21cf7fc23b9a096c4d9aa5b7cd02d968b8dfc58b137c2df44b1e55307b6

njRAT VBS:
a90605c2c755558778d3200d52496229951c0cbb7d13b2ce8f75d9ea7d738bf1
6d4f18ec7564d4e1abcd0c6e4697f9cd029fba5fb4889d647dacd938d9aabb65
2545fcbee4cdb94cac171f8242bcfe1b2cdd048864c6f47ce0386d701918104e
e7b6c91784817e63ff897405b43eac864320a6b645ec56af28556f44636f433b
eedbd29387319cc474fa3e09d5d5e7af5ca6e6034872cc6617414b45899379a6

njRAT:
a8768e632a5c8fbb7c7b201f1e6df6362ed48d77efa74c62eaa900e0e73eebee
5d52f58a75bbe7519bbcae8333e91b5dbcc8459bb23bb01d077d5c51954c0ef8
1dab360111d8a0f59674bc5c725b88edac598dd7e0171ab7c3bc5416d45e6e89
8e3f04d34dfb35e685f6785c406ab5ffdad15ba376c8ac584bf25c7a7b3b547a
eb688e9d721c561fe334147c66679bbd988da10c06704a15f048b97a9f6b0f7f
7d6822107e82ad3fee7b901e4e74bc9f885892da1a1378e63f8cdeaf651b4f49
7bf2d1167b4cd57a72aa1c34b2c3f978ed42569ff0494411af164b1ead715466

CetaRAT:
2bcd8fd2292b57cb0e093bd723d70560aa49c50bc3f34e9f1ff9ba66ac3f5cee
b0942f024982da62053fa5c469b02ccdc2ceb16290a07bb2eae01d9a42b55452
3f34c61025b5cf46075d79e68efb5da0f4ac01c113d8c1aaff3903ccd9a0fa3e
fa02de1f2dbd29f19e8ab0ff2931b063bd8f8ccadf0d7e321f0a02d2e2f86419
73a2df93ded57d1ddcdc9091eeded169668d8abbe7e8e35b7a737c01fceffa59

1e488c21314be1a976218e39c90ee17902636508e6e97754152b3bb14f5af062
c5b93a7a94b80d1548f09bce173ef20b5675cf39f479d923e670ba0112b3ef13
59fcc32fc7f64db71b868cd5bb674da5604cb5da032c8329e7183437c2d3936f
19e680eaa52c0ad14274b04141a8e172d2ec1a01a3f429263090a990120ad9df

MargulasRAT:
864dc421ddda3032938a5f1753ebc4d24c6250cd201204c4024012fe2b8a460a
ee2cc931d5b4bad780abb0e5cee7d9bb51916035e4cce0e8239fe0a444ed523d
259e0acea693e80af641925c2f881842e8aa979d770cc34a1769065028dd9d74
31564bd50713e63a6d4cb749048f7908b5f7629d2ef950b7240f85d734a32ceb
b7ce2df21b8a9e8cba08e86700f435d42937b07d2103d9191767737de67ea82b

DetaRAT:
35770d80cd1d8ef8047799148b03f8f749b63a6d9d4f2c771bef143b78fd3785
38924cc5c2cd098460dc4d7105411fb5ef041a9948e77bdcbbcfc4ce47dd4ad0

ReverseRAT:
f769315cfdeeff46fdea93da13ec4592cc6d63ff0eddc0537611fafad3bbfd01 (USB)
85cde5af2b728d3a99948169caa0aaf4aa3a85483b52b3f5744c933327dfd1ca
a40a5b308253a683b706885327fd8445600451bfd410778126b309ea8bb54236
a13211600feea651bdff217cb7a3f630eaceb08fbaf213df79b2d115beae7612

ActionRAT:
e53a25c5ee5de4c9dc4ca531293270d1aa921b9fc110ecb2a0afb57872c51324
33533dadcc92631727eaf4bfb9df640fd29aa68f6914aafe12597ef3404d0082
57466da1095f6c28d5d7c56d171417bb796b153f1c545e846fee1743cacc15fc
38a5e825577b51eefe4c571d29b34713b4fd2a2b09a013df4803110d5ce553e8
3cf3c7a9e9958a41a23ca6f47a8c92d9dc027fa1f09fcb3059be228b7918f74d
63464b22186b090c4c9d6db615756b96348d6a8f0438fd2900be600f3b71cdaf
45918acc04ad790445fd423b348aa88855570d57ebed870741603a7e5473d456
1ac0288aaebbe07b6145f20dc3ba2c0107ab00b47a4fe90215a784c887bad35d
120d1835df79b464dce91fd4151a69bae5ef5603e6eb4821a79f8a84767f7724 (C# based)
149b121b8f5755bc841ddd38f8dbcb6f857b00c8943b446ab85e1706e2216bde
3a435ad1c01335d31c05ca77a125d0162c223c135363c120071b7bac284a64e3
41727c5a33c42edb3754670fd43db95ff8e0bfb06e57b28e0fe97f5054a2c0dc
433a3e3023179959f8d99d29a645f0c29ed86beb172c23b22ca311a767cfbb74
149b121b8f5755bc841ddd38f8dbcb6f857b00c8943b446ab85e1706e2216bde
3dfa7180dcd674b26539687313e2e80d705f52dbe74163c40ae050e60488382a

Lilith RAT:
132870a1ae6a0bdecaa52c03cfe97a47df8786f148fa8ca113ac2a8d59e3624a

EpicenterRAT
01601be48e0eef098ae1650c178df0152f13c270c5375d22bdc047824887df65
e30732b7502ad3658af5e1cb9ad371e38e688c85b23090adb5694f53476437b8
c20cb6983369182c93d5877a8839d58fc91d054888286daa2d4e3d8539308f4f
66ba8ea89be5737240d1ba5143a10d4df64e3e4a9290e53a137df18764d7d33d

Allakore MSI
465b98cb9bb3aed725184628e3e99d481775c336068852044e66070e0805bc33

Allakore Loader EXE and BAT
1b6ff871d57285453cd7227844bf70191ff25f1c19e4512d973fda123ce202eb - Setup Allakore persistence and run -> MSI based attack.
d1cb43c940de0e7367db51462d9b2277eb7b8ebad802f05036f409b2fa80c7ff

Allakore exe
35c0e8f7818a105cda52ead6bc01e13053f03ee7827daad3ce22dd693f7faa91

Allakore:
2bab9140682074a58393845420211fdb78a1b9d5697948ba68301f71e1a84d73
ac5400b5471e3c67fe6d721f1d8d78d55ae549bfd956d1776d39e55058592bab
5a4616da2511ae67e0892a043d3079977e9b57c73f2c21031284ce473f84e071
1e446a01f147efe9f7471290a21921cd1af3d310c0d09a28b670252323c200fa
f63c9c67ef1cc74f3936d637217b1812e04794316cc3895665688068cb31b50e
e355e3927b72656191ffc8269d6aad49d7b3cb73e73beaf565683e13e9d33ce3
16ea88868cae6eff24f19693b7d18f84023947c3c46569d4e437225ac6396149
bf1586e0b7a41d7ae1931b1eedcfd33131e2075763b5458497db4b43d5bcbd08
247446c1e49f6613c4cffb072bd8f9d8153045c0c0106285151cd4f0fb0a48d2
f6da10e03aa705e8f87a08804f396d3188a57526e1fea98c5c2022856cff97bb
bfa9d84b96352a4c8a2a96f3a0011902d33466c7f5594b7420d45746690a31aa
1b07cd6d39ad74eee46c9de794445ff0be75517abc0b01052e4aff6843e21f5b
7f3ce9fd0863bf591f360e163dc7d3aee6d3810a89863fed3cbad980fef72430
d36dd9c94384c8e8f9b2229ef01dfb9fc799f0420428af8e3d04b06c324a6b59
5fc7b0db661dd144390f4358d638b1cc26429d0db5ec0226f1051a9c4ccbccd0
0996fd9884f51a95486138010d6457d4e6482f56747ff47b57dd6511b77193d6
f0439ab8d77fa02fca3b148ec55c971a482043025d10ad198baa463bb694777d
2c3849f3555085ea3d019ada508eeff203b75464710eec42cf362601ef329c83
8b11db3a20f447b31cfc6a6af626c037b8f77ed0f96f7210f9d58a21f83e6eda
66ccccd43e925d2107c3e8c13561ec80885a77b32d34f9208718d84bc540c16c
8a72a70e4a1ac0285e205a8ce72155f6707f3e3e55317c6444fb098444d9491d
413d6f350e633bcb05b896f7e35f9adad3a205bee5d49882876e8a576ac429f3
d6f9926beb1845a783fb0954218f21721edd190dba6ab87601836f49a84d91e0

b5fdbdcd669e20fdc43814e0495ab75537ec598d85361849ba5c4e80faf64e5f
4e110011e8467c77c2de3a335d291b45b24633b2d22169552c200a1095355111
35c0e8f7818a105cda52ead6bc01e13053f03ee7827daad3ce22dd693f7faa91
db24325b3bfc666a6f52f70199833da33f33d6c1ae9ba76f30e642361018285f
43d469f38545b63389712eba636e87ad483308eb6ce609c1117a2fdddcefe1a2
e97c2c1ce6243327eecf6ca9a827c80650745bdbdb47c1cb72801b67cf21d9dc
705d392207444a86774796785a461ae5429a1c6bd77d5d13b0059e6ace65611e
88337372097e9fb18358ec5f4d8ea87022b4f2f23c19e52143aec2bf0a56f96b
fa0212dd679037fa795373e9cb63de12a76686fbb931ee908d77c3f85f960005
a882160ba5e1029787f6c508e5410185b4ec9be67abb0b119a9c69bd576fac0c
23d8fc6a21750f5d37cb1771383b0c07c2f9c064fe2d6c5630862a8547d60d51

Plugins:

Files Manager:
dfaf8898350e60c766aadd438a16694ad4078b6b01a46463734cb01cdd3e4241
04f98059541ed7c84e5a99472338af950a6bd523c2e9846ecfa8043233cde28f
ac81e2924421ea896cc19799b883bc9f6a2142e9611a341036f34aad4fd6a1e8
af95f2f7ff76cc70a7e14334f12184b2dbff440acd5267b1d4fe197ab33f3051

UPirate USB document copier
7250b90480bb3d3528e5cd0317e51d8324f947721d968a68ca2f8d5beec16072
04992584371c0664760e23f42b6c86e2e168738c809122c3491860bf5748d9e1

Browser Credentials stealer:
dbf2fdb7115059af98acce595c1fa6e00c10a301c02a324aff259c77696b14ca
7af894af3b36d1397fc75aa2ebe434787d0b137b6400a069a70fab96ada9f211
f6394588dc632acd4d0298e422066ffc1420e98c3fec0ff74db3d3f1d53e2d36

Keyloggers
Lavao
e30a9e450a64204f830f99f5e2015e3eedea955a1ff6986586a0e3bd59bae360
a18d0c51009c77d947384823bd3f4d2d4d777bd18f417698be51c71b06fe0d82

Xeytan
13c73303cae3d79f525ec1a37ac233450deb003196d948010a38db0b90116a46
58ee5b7f6eb75161f39a47b4637716db097e40ddfd6513782d419af43c858045
3aaca3ddbf641cc511685436e9d510459716e5419d4be93bf99edc48502ae43a

Golang malware - nodachi
6871bf94e788cce0176c475ed20e3c3e816f10a6b2df0c0d11ce181daead0a02
d1a9d1149782824503e574c329a342fb3c069fe8d5b33d2cc335d951bdfb863b
6d11f055e438353f9a4cf3875ad0a343b3b5193c4762fe327394d169b86cbb53
365681a960f277357346c1217fede4b1140300e08e78b9978e085d2919c73e23
7b93d0d7270e7abec053b61f601b8f3ebc1460815fe78c5f6e28a099107fe9c1
5993ff30ebea87a28a674aa7739869ab9229c3ec13299bbd4ac0d7c835da8418
8e91cc7928662c9d0e69d944fae3f0d2611498ca7f508f3deef20050a6144977

Misc:
Meterpreter shells
71bbf2394fe4909a6ce0f7085ca41f21cf5e05e3d761620e4d7f307183fb1e1b
852612666095aec2e9f3456ec4f8a9566be2c690c8583aff6055d180507d5476
a3ca5131a8cf34cfb03a5d9a4e9bddbbf8ee5b3f605dc6d31dc5c1294328d26a

Custom Revershell :
956f0f369082068ef24b76ec162cfc2119adbffda94e33e41b40f39d2f192ffe
76604e165cc020479f9a2e461e052c7bd0d0aabd6e8e9afcc587b5aedf70b6e0
f24e1040e8ababf91480b92554996c3cb0be68139a914d24a3da02618d557915
2e938219f769e828ace8d98969764064914373e616aca9097cecd33b742fdf33
093d12272c70006dac89a9009406ebd0a41df1c615482a49fd84248758c48060
616b2c7f168b8e9cd5182f273c395bb6c2fc0605763a4e4351b333369b87fe7d

Decoy docs:
52c0c1d258ca8c4d03d8b1bce5c4560d8ca1c48cc7c94d677730dd7dd3c263b9
df90ebaf8b756ec736249d31dc3d27833bee84bd2df99ef22080764d237ad221
1dc5aeb9a7dcbe8f3c214869713f007808f728f50c1bc1ca94cb22ecccee64c0
08160e19045d1b7ee4d70855ba1afceb6c9a120d15afcb4c347397fbd0a5d73e
dd25f9251dbd296caa26246e91bd3fb2e0e7583c378bf67fdfd8d1cdb54a9ed6
835d2b8215a77aff04d0f16b125e81ae10ebf3217ab00a7057cdd0d8102ed896
b413a833227c7df8e47f57e331c049147719c4fe7e80f37c448222feb1a62836
38f5ddfb3318684fbcff0b2a5f75a921c4fd2ce7735aa9596f89318b4ed503d4
100cbb8c5ae1f77fece6eb9bcea4fab5830474cd4d1eafdb1e87c9d38f3d5225

honeytrap decoy JPGs:
65c462a0a04f7748e0aa67c7897323896e4be80a847bfa0966a2035e2ff1f288

173652906ab8a90cdfaa04ea8fbe481c060479b33a61631458f154e0fcd5b1b0
427d714d35813a3b2ce4f0a2357b0de964c00178444808af6db6ab870ce644b6
70227dcd0600f1651514751945eab782193480054dd7c5be2051dc7ec00e7baf
d96295805f1396490d6eaabed42a13c3bc70e2b3c05a0c73c107757374e5d81b
ebfc2483abf15086c0415809a5b9307856501943c83e9fece0606da26a9466d5
9f70697cbc58ae5a3f67a2b98613daa970677907f938f2a684be769a46c6c984