IOCs

Reference: https://www.recordedfuture.com/houdini-paste-sites/

Domains

022121563.ddns.net
02google.ddns.net
0930077842.ddns.net
09300778421996.linkpc.net
777777722.zapto.org
ahmad00.linkpc.net
ahmad100.linkpc.net
ahmedftw50.no-ip.biz
ajlmntsd.myftp.biz
alaa2.no-ip.biz
anime-online.myftp.org
anin288.ddns.net
anonogu.ddns.net
atwa.ddns.net
bhz1.ddns.net
black31.no-ip.biz
calva77.linkpc.net
camifer39.ddns.net
charifo1313.no-ip.biz
chrome11.ddns.net
dark4444.hopto.org
dephh.sytes.net
desertfox2038.ddns.net
ebf.myq-see.com
elaspany.ddns.net
elaspany1.myftp.biz
elhacker313.ddns.net
film2plugins.hopto.org
flhjflhjflhjflhjflhkjfdhlksjhglkdjhgls.no-ip.biz
force-ss.noip.me
geant80hd.linkpc.net
ghf.no-ip.biz
googelcom.ddns.net
googledd.sytes.net
gusmarijon.ddns.net
gx0654.ddns.net
hackerorhackerfokar.ddns.net
hisokadev.no-ip.biz
hiurle.crabdance.com
hsdvhgyvhl.ddns.net

ilyes555.ddns.net
ines0049.ddns.net
italf.hopto.org
java.no-ip.info
kalislax99.ddns.net
kameles09.ddns.net
karasqlee91.no-ip.org
killer-204.sytes.net
king999.ddns.net
lego8.ddns.net
maistro.linkpc.net
majroo7.no-ip.info
microsofit.net
mohamedsaeed.ddns.net
mohammadx47.ddns.net
mohpipa.no-ip.piz
moradoffis.sytes.net
mouni1983.ddns.net
mozilee.gotdns.ch
mrshadow.hopto.org
mrshadowsx.hopto.org
mustafanjrat111.myftp.biz
mustafanjrat111111.myftp.biz
mustafanjratkjkjkjkjkj111.myftp.biz
nasr23200000.no-ip.org
nemo-2015@hopto.org
nj8.ddns.net
nonono30.sytes.net
notepad11.myq-see.com
noura13.ddns.net
omomom.ddns.net
postventa-vodafone.duckdns.org
postventa-vodafone.myq-see.com
rida1999.ddns.net
saefnaje.ddns.net
sandboxupdate.myq-see.com
scream.hopto.org
serviceupport.ddns.net
sex69.ddns.net
sks2020.noip.me
skwem.servehttp.com
sniper110.ddns.net
sonylive.linkpc.net
svchosttt.ddns.net
swwity.ddns.net
system.ilovecollege.info
tcp.linkpc.net

test212.dynu.net
th3kin9.no-ip.biz
tigano0724.myq-see.com
tosson.ddns.net
toutou.dynu.net
valerianactor.ddns.net
viviban.no-ip.org
winddns.hopto.org
windows.servehalflife.com
windowsdwm.ddns.net
x-diler.no-ip.biz
xhostvw55.ddns.net
xxxxx1.myq-see.com
yeswecan.duckdns.org
you3939.ddnsking.com
youben.ddns.net
zikadanger.duckdns.net
zikadanger.duckdns.org
zoomzoom.3utilities.com

Paste Sources

http://pastebin.com/0Cr2F8ZW
http://pastebin.com/0CxxQk5p
http://pastebin.com/0d8BAgGG
http://pastebin.com/0TCFZ4Qu
http://pastebin.com/0Yck7UB4
http://pastebin.com/15zh8LqD
http://pastebin.com/1aS9dJxE
http://pastebin.com/1w1YBdtD
http://pastebin.com/24VKTMwK
http://pastebin.com/2sN9wifS
http://pastebin.com/2UrcMsyQ
http://pastebin.com/36pEjDmf
http://pastebin.com/39G4j3ag
http://pastebin.com/3CQj3sUQ
http://pastebin.com/3LPiTPGS
http://pastebin.com/3XF2n8Le
http://pastebin.com/4R0f42RD
http://pastebin.com/5FSzXCwi
http://pastebin.com/6WkqdmDK
http://pastebin.com/6ZuH4ZvV
http://pastebin.com/7DpTiUGt
http://pastebin.com/7n0iyhHD
http://pastebin.com/7v7cSbWy
http://pastebin.com/825rudu1
http://pastebin.com/82vt1Fcm

http://pastebin.com/84nm2RHe
http://pastebin.com/8RKF59ZD
http://pastebin.com/8xjCV9gq
http://pastebin.com/9TaMLTvt
http://pastebin.com/A68ZVuKL
http://pastebin.com/a74gjPK0
http://pastebin.com/A7bVjdYT
http://pastebin.com/a8zfeLg0
http://pastebin.com/AB5KJ7kc
http://pastebin.com/aDmaaYm0
http://pastebin.com/AnY7YJHQ
http://pastebin.com/ASsxW0G8
http://pastebin.com/aVcXy2wF
http://pastebin.com/axfrG3MB
http://pastebin.com/b6RSW05K
http://pastebin.com/b8BWwkUm
http://pastebin.com/bafEGnWf
http://pastebin.com/beqniW6T
http://pastebin.com/BExhPePw
http://pastebin.com/BmiDjNXg
http://pastebin.com/bynE7apU
http://pastebin.com/c18Eh16Z
http://pastebin.com/cEa3BcLJ
http://pastebin.com/cJWqvQ6i
http://pastebin.com/cuZvs7ec
http://pastebin.com/cy8ypp4S
http://pastebin.com/D2XRUhgs
http://pastebin.com/DAq5aWn3
http://pastebin.com/DbXzwtfD
http://pastebin.com/DcFgrMiz
http://pastebin.com/DgSi6QFj
http://pastebin.com/DHYHbLb7
http://pastebin.com/DTM4hFqE
http://pastebin.com/dUsqGMxA
http://pastebin.com/dwVPHWjW
http://pastebin.com/dYXSMf31
http://pastebin.com/E3WpWji1
http://pastebin.com/e91eX47e
http://pastebin.com/Ea9kpKa2
http://pastebin.com/EdBPXCkw
http://pastebin.com/ekw6KtSu
http://pastebin.com/eLCPWSzT
http://pastebin.com/ESRYeB5q
http://pastebin.com/Eu2c4meY
http://pastebin.com/EwJt0VmM
http://pastebin.com/EWzE3dwr
http://pastebin.com/EyGN0cVZ

http://pastebin.com/FJqcU1d0
http://pastebin.com/fpgh0uDP
http://pastebin.com/FtYgVH9E
http://pastebin.com/Ggb0R4WK
http://pastebin.com/GyTiGsfp
http://pastebin.com/h6AC8M2D
http://pastebin.com/h9PEz0xS
http://pastebin.com/hrCiLLgy
http://pastebin.com/hVcU94x7
http://pastebin.com/HXMentf2
http://pastebin.com/i5peKgmJ
http://pastebin.com/iEUCQ8p0
http://pastebin.com/iPzQsNti
http://pastebin.com/iuaNRh6a
http://pastebin.com/iWkx4c7f
http://pastebin.com/J62VynH0
http://pastebin.com/jFLwJw6s
http://pastebin.com/jH7TrdwV
http://pastebin.com/jHDk6mN7
http://pastebin.com/JiNtnpN2
http://pastebin.com/JJBm2QGY
http://pastebin.com/JQQsc620
http://pastebin.com/jqwcLyai
http://pastebin.com/JW2UESkE
http://pastebin.com/k0ZG1aTs
http://pastebin.com/KAmTyKrR
http://pastebin.com/KdWRxR05
http://pastebin.com/Kf4xK7YR
http://pastebin.com/KMTy9kZT
http://pastebin.com/KPAZSGUH
http://pastebin.com/KTCPXDiD
http://pastebin.com/KUVQiTyi
http://pastebin.com/L16d1iyi
http://pastebin.com/Lear1hVs
http://pastebin.com/LZhQCcqx
http://pastebin.com/MCGG1ccd
http://pastebin.com/mdzsfYuv
http://pastebin.com/mE2qGSm8
http://pastebin.com/mEqzF53y
http://pastebin.com/mguQ5kzB
http://pastebin.com/mN44j66Y
http://pastebin.com/mNJUuDL4
http://pastebin.com/MPEqHHj7
http://pastebin.com/mrDGq6Hv
http://pastebin.com/MXJyqbhZ
http://pastebin.com/n3idvqZz
http://pastebin.com/nabsjYMp

http://pastebin.com/nHsiEKTQ
http://pastebin.com/nShRdWyJ
http://pastebin.com/ntHswc0R
http://pastebin.com/NW8DNxAT
http://pastebin.com/pgai1jyC
http://pastebin.com/pGrFwYnF
http://pastebin.com/PhwF7c63
http://pastebin.com/Pik8rDsY
http://pastebin.com/PKcgQbBz
http://pastebin.com/pMezwY4X
http://pastebin.com/PmQLPCcL
http://pastebin.com/q2HCxC3N
http://pastebin.com/Q431wbmr
http://pastebin.com/q6JSnNNF
http://pastebin.com/QgRLbavP
http://pastebin.com/qHnhxLbe
http://pastebin.com/qzEc6UFz
http://pastebin.com/R1kNZU5c
http://pastebin.com/r9TLqVsX
http://pastebin.com/rcisPR7F
http://pastebin.com/RJiYReSC
http://pastebin.com/rpdzTJTe
http://pastebin.com/RUHLXZZC
http://pastebin.com/S56D5rew
http://pastebin.com/s5wQ2xL6
http://pastebin.com/S7W9d0pt
http://pastebin.com/SARPbsJc
http://pastebin.com/SFefsdG1
http://pastebin.com/sfMeJFND
http://pastebin.com/sh8rjFC3
http://pastebin.com/sHSyv8ZF
http://pastebin.com/sLykn106
http://pastebin.com/SNVSnwZT
http://pastebin.com/SpwZ7Mxj
http://pastebin.com/SyVqz8Gg
http://pastebin.com/T5tfH1Sm
http://pastebin.com/TaUEkfkL
http://pastebin.com/twwJbhMS
http://pastebin.com/tXT2uc3h
http://pastebin.com/U2GCke1v
http://pastebin.com/u2t7QXix
http://pastebin.com/UbNGbuuZ
http://pastebin.com/uGLsBLvE
http://pastebin.com/uGnSC0dE
http://pastebin.com/UkQekWDV
http://pastebin.com/uPnfLgTM
http://pastebin.com/uvDGUdTj

http://pastebin.com/vaBrbZ3W
http://pastebin.com/vHKeBHCP
http://pastebin.com/vhstSCV0
http://pastebin.com/VqdKnidc
http://pastebin.com/VvULDxfc
http://pastebin.com/vXQuuZSq
http://pastebin.com/W2UTrwxV
http://pastebin.com/wM7C2c7B
http://pastebin.com/WMfVgWj1
http://pastebin.com/WPKbeLmr
http://pastebin.com/wRdfJ5Wd
http://pastebin.com/x1dsBi9e
http://pastebin.com/X3x4sf98
http://pastebin.com/X6uuDFWM
http://pastebin.com/x7NmfJme
http://pastebin.com/X80JQJtP
http://pastebin.com/xisX4bbE
http://pastebin.com/XJ48vqCB
http://pastebin.com/xqvfw3XG
http://pastebin.com/xUdGy9YH
http://pastebin.com/XX3dJeY3
http://pastebin.com/XxmUhKXj
http://pastebin.com/YF0nFa5r
http://pastebin.com/YGtWgXcB
http://pastebin.com/YHcttpGf
http://pastebin.com/yJ4Vv02C
http://pastebin.com/YJ5CAUMV
http://pastebin.com/ykX4Pagr
http://pastebin.com/YnuGvivd
http://pastebin.com/yXDsRkTj
http://pastebin.com/zd0WmtBe
http://pastebin.com/zdwEz6af
http://pastebin.com/zfFgwzJ2
http://pastebin.com/zFvnB9K8
http://pastebin.com/zqR2s47i
http://pastebin.com/zRmYz7Df
http://pastebin.com/zVBVKTb4
http://pastebin.com/ZwAvWVa9
http://pastebin.com/Zwjcf4wv
https://pastebin.com/9ibrtSVp
https://pastebin.com/CTZU5Egs
https://pastebin.com/KEw7MeFb
https://pastebin.com/NnwP0SsL
https://pastebin.com/tAGtWMLG
https://pastebin.com/VDhVvZET
https://pastebin.com/Vr6feRMS
https://pastebin.com/wjA92m03

Hashes

0221af4ccbe93e10d9b5a6eace261a66fa2e8f229a2a6102788855d804351f23
03609ae94a5cb522670bb6e3ad3559a7417eb8b302ab8ec84c5f2d1a99be1c0d
03693c2dcfe67ac8b1f7c58ab6e0e25652643e8a7ad28978461a204583d4344d
047c5cca9c834a6ca7e9fc8fa60d5b57c0a532a00d608faecdfa5dc9e38bf55e
05113fc0ff72b0e62d11f72bd50f4662e844f8ce788421c483870cc93bb3e3b5
051b50f88565468fa16f52a84a18e698e62de3ce1c2a372b85b63208ab4fb651
0759628d2fa5d76c811cee5dc14a08fb15c02054ef34efe0e2d0f925b0cd213f
07de71da7e596456f7098228209d18e5b19c5af27dce5724e7cbe7c3e275a5e6
08031b41a9dfaca06f96da6ba1a442ccbccfa0874d56ee63ed10ecc1d59479b7
092b5b1252f345d9aa80769ab01ffac51899dacd2566e08b8ce92e44d7482a19
09a7b8c5b7c208173b5393a33163426c9f34850f7b1a8c9ab68ac33d74fbbc4c
0a8a379060483ae04581ef63dc8455593bbf9c90193d238b5c8f397ab17d419d
0d7dd0372e925c6d3bc7ad9915f82b6166cc732759518439d4d696d3de88b616
10179d9da0c975489d5c7bb08fb493f3d93a2fd48053578ea2b216c360a6dfb7
105b77dc45ea08b5f56de4f40fb99bf72214d6de74c27f188fbbc4daedbe179d
118ec6f7fd2928a186e02b994734f5ebff03db8871f1020ede673eec92657b0c
13df2b2cfb2d6508092a1c6d1bde6c0050141dd1679f66f4fb2550c6cbf3a1d2
1456d6fe3ce838f65bf45c6a1ba89b445a471e728f0f708e8afc2276bffe0f23
14745238539ec8ceca8062cd84ad89ff2fce9271a16d00c2b30d08b47e4e3c00
1841d51bd0f33c895ce59cd60c9434b98eed7cc06ac39ddb5be562868925a6b5
1950021c0360a2d5398e91535cef2631e86114bb980fd2545f433974de22b4d6
1a5e13069d6672c2f0bfef721115cfcc852a0598ec4955b994ca7c69ea539a68
1c3ce5248afd357231ca9001f1340b3f6d3a44ff807996ad67aa09a232368787
1d63f5f934a2b1107d7b0dc2dc44fb4592d38464a197d8bbeeed4af33e68cdc9
1d6a5515cb81af88a58380e7b41ab9950b448540708f83e0c565d50f9a230d71
1e33b89d3e3147560e54d0a27bfac1b856bebed058d45d8c91840fc3bf8f5990
1e5c4802a49bb0490fa4a76f14cd29eb76a1def02ecf05645cd7073a15e8e654
1f64f7f14ffaafec380ffce5657afa77a43af623cef1e3d8f3274a749d733cc5
21d54dcfc4a50424b018ee76244b1d74f0dcca212dd409b5464ab1fdb634aba0
23228890518cc2eff9d3628f81ab9442f52dd4d563227ecbd72594aab200b501
241d44d7741c5229a66067b7f5fe57c3024a25064ed989e9b25b4d0dcb9044a6
25aa2e8d5ed40bcb3aab00d8df0f5fe4ba4fa6d3a0d7b75acfc7a1c2e5d7fa9d
289dd183a01d409c73bd526f063f93349b5c9b71b45e7222a3a2f8d24058f3ac
2ab4e5228428231c2461c6ad56894d42ca4e8da2d1e4305cf1edc02a4c1dbcf4
2c49d45d0739c161c2593e74de516f073e8dedfec869ce978f7f6711dc8034fb
2d3bb3781bdfac62b57ab4490999c7e5dec9cf08255f8beca189fe25d543254d
2e033532fcbdebd0c38c0f950d3da5334b6ddf8ea279e479bc8df982eb500022
2f0988baac35d0335e7dd8645637a64c7af34a551b2df70199243d837456bd0a
30019a0efbcc66e415601f4827773689771c9c1135257d7357710eb2ce780e50
302999f092a0d2b712008b12b33a458eac97a8a412eec0742520d194f37a31e8

30480441df5a29501dbd9c956306a0bf9bd4e5f9f166f0bd1e9bd0f3ad00a4fe
32e278f6b0a7849b47bd610d1c3abdd93826e61b452ffaa05c794b2bf5078a7b
330e8eb03cf8d0ab2dcec09fb8f41a7fa5100564a3fde5e44ac542c02233cd01
34a659e40e7f5e9aa64f75a2de10ce82432e60a3e02844f0677c44de687232d7
35064c2da32af314dece89e0dac5b0d6e3e96bbc402b1fcd78ec5a5b8fa85f9f
352ff5d55a67fa6a25f0bdf09af6e45eb89f449c5840ef14fe641be045e24686
38087864d3f2a2b6910d5a0115a006b3ea1d72cfebf7ad73a0cc4141ec991dc8
3965ff4939e2026b5a8e012f3adfe4efb0cc6691da57422856163911aabee4a4
3ae7eb446d4ae7b12f40002634c6003a4a17f2187577b7a2fae3642a75804353
3b11b600146877f60d77eabeee46336075d4d5e9c9b678d559da52bd25e78bc1
3f0aa7aedaf3d9bc24fd46a126725b77404b3420538169c25ed9f0e37cae4d20
431061d0b617c5cf3342d1382a69f5a857fe923958f640243190f1885774a760
462f2dd9f83760917623707ed90b22cd38e826c4c58703236676cab15fd3d809
467e5cb8c86a5f7ec4e94a3b39fca9097d08935003f6c4cb7293ce78f608241f
474d25873630cd904a0baaed21af80304d3efb406efbd7bad0add58e14818038
47c6d49477418665cfcd73126d3c717541d44a7f1aa35dbd33cefee847e95784
4a72f00ce46ecf9b8d502a3a35954d08c1a91d9003af49ddc3ce490ed3cc71ec
4b9c112ca96501f6f67d6f0408493298dae5e5805eb9fa737399be985b3a5593
4e227d02bf5735ec5934a5ddb6b9c1a0a8ffffebf3305f0540761a3e8e4a15eb
4f30b86e88e685ba0619ad18cb41cac318de558b9d16b6622456ac653b37a288
4f32ca1dc42011b6435759468f201c23a2fcd219fb6e447c17faf75f96810b5a
4f35a0714cf4bc3411f1a98c7ada8bd95b837c852a16937d55a3ca3c9f7d4b00
51971af04fccff6aa565bfc5f8f1e507db85dd10b3fbddf93aeca66773c3533c
51e287e5589314200f66b7ef9b4b351c2208e89f2718f2a27d4d14020c6a0e11
520d099d4f043782604e5885cafce5de15e1a77683cbdbd5fd1b8dfd22aaf19b
52bffcc9caeb7e9a9e50dd952bc359f93e9df751fa8c87b67ec0b7ca3681153c
54a0c12454b91cae36b9545aa3787882312d32d9ee5abf36f1b37128934d44c2
56e0ebb83548a038b87392367a03f91a720ce22ee745b4ef3dae51f7fac756aa
58705a68fda7866e93e5c68ec20fa175b83a18ded01beee38b7d904c855ea68d
58f844ce92252279b35cc425b828a7615ddc03a9c5a86eee0fe3f0a6eea2c8fd
5a55680b0a2dd3e0de2025d733d4d01bacd08058cbe92a1ab31de54f75197c46
5c34171922971c47a9df1192d6a216098996e7304febb3232ef9739dc25c1a93
5f937f0b11051c0e9524c033e912389941ce5d1f86b35957419529d15101ce27
5fe0815219153f1a77e8d049b4bef5c480cc86f363f6b4173cecb6e055a8892d
6185e315932ea30d59b472e255fdfa29fc1d1b831afb110348bfbfb2ce2d6490
61f2c19b04ba6e704aaac02ec68d27d7f1fc8f71fdcbee3b7faaf52e1c04c687
631f5206ec55266cdb7ff5791201a59d881e97fb76db0ef45cb50b9cb174ad62
6410fccf3e3f96266dad1cd1ce4d654c425d9a4e55d22b1807edaf7f45c49c89
643997707370990ff109f5865bfb632a88c2b64b28cd03c5e46ee5237c1cca5f
66dd988050ca2a093830cc630b6d5c97007b5610eb6d1d5af246727cfeabd5bc
68c43b122d27a7c9aa20c7c484f93505ea057434312755f3ac8f6bdd27219341
68ec80ae54d2f6eedb15f6caabfbbf97ed70ad9a727e869461a66bbddde4399d

6f3f21c63874a14586cda4e5643ae0794c28e243e93b63956ebc6be22202c210
707b5a5107259b665c5344cc9e10e786838f858605c7804215d17565e326afa4
70f25a64d04c80529ab910ba5e2e18fef33229d7fde8603057ea60648af51259
715be802d3303e85207a4822f90d40c867f7cbcfb1e3acafa7794e2abc17410a
73addeb97f5dd3339c923a110d795774f6032e0c79667d4d0f4fb4a00ac7595b
747cebfb8c156857b299d6b78222375ef190b5728ae651fe068eb766ec8dc766
752e9ccacb6e43405bc703c720cd55e2c96e91d2ef0416d474323f94b364d86d
75829afb2c900677266ca14bfb0ec738aea82e1e18c55ffd12f7f946d7ba74af
7702734c9d5d9ca1254f14825454d0cf15757050d6594de8bfba1a10b3c196e1
771dcc401819dcd3be5b4ab500afdbf3e536be54d442e865590c2bc22fee1bef
7e8612486246ed21924b91e506354b75058e8caad0eedb0e206913d401678b4e
7e999fcc207a529517d59609f8f6e3519a3557fe37d2f8b7f61ba20959a2ea7f
8179ece968e4792141db0747afabd15175e87d6ce082b0eba08b80ed95756a13
81b2623c86bdb2735727779bc1c4fc238ed8bc67b40f7dd474fc47dbdb7d9997
83b3151c1aac6e4f3a59f154d602327b1f683d1b5c0351146ff132bae58d2135
8442a8e9a0c8adc3bda7ad166b947de994c6f88a59fcc8d07cc300138dffa3ce
84f738e7432625d9ef98169450cc8841db4555c0e14622c8f083fc8c738e17dd
86bd4c6f2d3381bb08ecffeae4da6f011d1cba1a759aeb86cb34140b4ccaea66
882d46db0f4c43a687fe385326130647fc6d55cd59aeae521d1f70d88a8c6f8f
884edd3725629b468a37c1615f7d5e554916408b535a604447f9b530750631fd
884ff1f2fb6a37c8ee11147a956bd031a7226e6d843cd27c5f33fe2f83141466
887c4f9bcc886d1814a2ea6d6f3301f3163074f22d59124f90511d0d9f2001ca
89b6803bc6f8b134a9eb7a7b3a172a74336a105e898c6d305a0203757d66295d
8c7231d9a7ed451a260b1b67a6870d23f71a16c478913133dcccf483e60e9cda
8cf9f5338b2ad271aca23964fc5f57a29d3f89463195834f01dac727d9664f47
8da598b116bad8f5cf280a8729e463aa5de07d46b666027439e799d28f2e3277
8daf4280ca6f44a46b37c5b17dc7a47d571165c08befadc21752a7f822581297
916054de82dcd4f8e0f43e37231d6b20de7a009a27ca0acd18550ea6809a0a6d
9354830dcb4f2bd0dee5966b374199c066938b7f30eb028e436a9e926bd65047
956232816a7841885ea68b0f1fee49edec254044f412416ed78a69a29ff30ba2
9967485408aaf1319521d7c68d1fcc9de54076b91858587a4309b3b767ae30fb
9c009927aa7163a265313b251bef37a389b63da17a54bcc770559f36b144cefc
9c75bcdb38477517d5db30771ee232e6c8109a41cdbc1c1f1e4a5c71b3f3916c
9e8dcb3aa58e439beab68f35f77714e2118a16a710256f5dae3ec432f4bb2336
a0ee74a3faac2a626218a21242c8a84138a85b861c58b39db4bc4b7ee8badb5b
a39c21b83c25acb26503bbdba96200fb56c5accd5047dd61f17f2330ab60074a
a813c72c124268238538dfeadfb4c356dffe553711979000dee99ec24b72b54a
a84b648cd968472e540be8f2819a343ed40529b3109d0802d0eb30b2ca86ed14
a883ffae728f8474e638175aeeb58120b7de8d55c2c26e7b4a373ef92a88cb1b
aa32bb9addbb871a4edd3b911cd96bed3d60d47ce97713f29cf62dcb21b916cd
ab1d79358162a9d8fb2b46375efa9af725c2ac15b6d571acc3403b931e515d83
ac678b0804773a08d8abe0d8c71b653386e00d646e5892d659ca1cae71170231

b17a07840a5abdc8cf06b33d087347f095af113ad029bc78467bdab88bb63b38
b1947fbcc9bc64ec13fd76cdd27a3f379f9eea9599bc7b06483922cc3ec1d2f0
b51619a26fe55040761ffb248c1a5c9b54ff43b6c415cba63ea400d9685de9e6
b7caaf2f44ae79f46121be8124460ed9c24116f8f1571563cb85017ff6b6b7c7
b7db53d3dc5279b038c9f83c4813324d0fc0178df9650bfb6abfd145bdabfd5a
b8897cc2d8c88f92e464b9dfc77483e1f0749d69c8d78d1e3ee1622800e31b0c
b8d18b0d5dca9a3b54ba92dcc52b63610d4309d1c9de02f1cbf40288f10f4254
b8d400f3796ac47b8671913bf92afb444c753eb4b8104c75a53cafdd9d435097
ba26781b019bec5808c59659eecdd25cd3fbe7eacb4c318e662a78b0967ed409
ba71710233c81410cd7ccab7d822345a242305f2b44225efd45915f71ed54ca0
bb5c01fefa38ef5356c0e0216d5d0a73958e2a84adeb55040fbb9f6cbe1d630d
bce1e67035e5c6a6204d5a246f057f6f3bf6e2d7f984db33a122a64edd6be975
bcf82f6cc651bea2b6cdc548d2d7ef21719ed56b1375da55cc7d0ee84206ab39
be4589914ff331f966e55595329c4996699c76ff04b93d0013ba4145c1e76942
bf4c3739f1c39da35b29bb8d5491e598cf64bd842457fc4fac416c3147858ab8
c07b909401a9644bcf2802aca6913982c8a3b15d3b5886dd1669da3ea40fd73d
c1a47c9cd4d7efd9cf451dd731b7ae616e9d386e98459cc6c3c585118bcfd5c3
c30ce39385171f94144c4588a112977932b79dca5b6cdb9100efec6ea7f6ca06
c78503496493a4608ff8ff17ab80f5f2e836b7e7392152570eab1b228de000af
c92e05aed343349ec02b83a0b234f181787bffca627459e98b3ce3102807be32
c9ca904f905f14f4ab8049d71c4516b1b21c6d6b7da5c8c29f19cc1df6682326
ca0d4cd161339206fa90881a10670e33251bd2674d4f4cd58c0711ed61491c34
cb4df314c03dcf93cc9770dd0be2c00aa849f4b6b9f816bee46e73d202e1a748
cc626b0be2424eb18e159b84d641227b3acab89d873cf1e160d8a08c0331f218
cc882eb967bc5a6b2f04c88eec42f301a39b583af34571d10d512a4384bb58ce
cc972d32308c50d0b0cb2d5a57db6fdb2936c4026dd271efa7dbed7bd334e611
ccc730e8abb3b3b0d48abf959bd651c533bd7aa5deea8ef19bcc1d513b71e640
cd0f882b0e57657ede7793ef577ee1f2cc81f78d2416d9d7eafbfad174ebf010
cd20e783b256655b47c83a159fe26bf12fa7c68e8bd8cfa91f890ff851830982
d0dc608188ed861b44364549f8c8f300731e8cac060f83a1bc1378bc9237d694
d1aae23bef3b0a4fb0831ebb989c3e894585c2e6b5f0b1e28a9b354cd90a0ff1
d2ee6bec91ef02bd0b8698835bab650798abfe813e5af6c65cc632b785c12d4a
d551a8430a988c83d17f4b95a9126bdffdd12e6c40c9d7061c998f27bc2475d9
d561cd0092eba7aff87d999a597dbff04d9e4642b6c8b0457a29fcca0f1db98b
d6cbf1bcd8eb2faf954655dae0e5a5ebba40f8ebcadc8fe3b548cda7f2e61fe6
da8f5e0afc084727b83e243c1c9e9bbc2bbd4e4e4f885c76177f11a0643f8c0c
daffad3dd4e16fdce79adc19df04160cc4c3f091c1710dc1123a93150885b32b
dc964f415157dbe082f3ec91d7dd57c927c3a359cc35bedeeda38b61262e4c18
dc980e2b4975c34ddae6c3c7d791790e58632e6fc7f21ec5401c30f9ad6bd90a
deaa219063925053555f374293fb48c6fc9614991e0f130b73a5914e3f85dc2c
def9d5046d78e54ece5a2f301088b3c9f2ed7b320eb67cd10688e02661f15a5d
e00cde820dff0f36a43ae1f337e0a04f4418268a1ec2750876243cc7927fd136

e095217e76e2b81343b151670e4e6e0437aeaebb8fdee7b12bc7fced82703699
e349953f21eff139738d7a836aae69325677cd7abdcefe6cb3912d3dcdee4067
e4a6c56989bdde542ca1fb9fbd5c8972c5ef7176869044a33417cedcef86caf1
e4eaf18918cdbba3ae8f032d9c1183af1a045739480285b3970430d4975908f0
e66d91331b3eaae4f0508124ebf66510046bb44746e66fd709922affabf241ec
e78a8e7c5a82fdf1958730c528a5ecc2087f9b81b3af7161c79d568b9482f51b
e84d8e7e4b782fec1b478f83fe68849ba17e7f38ac309f69281ca93b5a1227fe
eaa82a2f11eb49787ab96223cbfce7c3e4ae5cb150685c267268449b249dd73b
ebf7a760fde6ba974d1c811602cbd38d1cad39b85f324e5721502390a7978265
edf75b18fa10854da14c4be54d785fb8ca6712b72a1daa2da9b6327f4d9dd498
ee4d3ebcaa71a47ef08c68552f15ae782b97b101555e15cb5d15b03ce24269c1
f3e044796f89d969551b6f288b43b512bce1c57bb9c3efae2dd7b4c692a22c05
f3f1f7448952b53ca8a2241fc54f1ea86f8dabe94e94d10f35ebca66e24a643e
f431d06ffe2babcfe534e5ac542c05a3c4beb8d6664f1b5f27c268ca321b8390
f431d06ffe2babcfe534e5ac542c05a3c4beb8d6664f1b5f27c268ca321b8390
f583183444bfd40d3d4ddc251a8e928ec479f0fc982e7d52137a990c5635e3ff
f6ddab5cc79b0a9d8e011435bc022ce50c270e241f4090b4d633f8e9a4eb02c7
f7ac077a5f262dbd02a8f0aff362b380b0468dfb06747ec4c9f0fd5fb1d474c7
f90461220a54fa3bd8b6e65fec8ee01205f52ec818a67cefc4ac3845ade11c85
f9b945758b2d318550f5dd3382fc9144c0f056761375dd71a73ab446d8caa0e6
fa9059eccb9921fd47b8da7204ec3a98e76e486e8ff205f15ba29832e755abfc
fabc2d865216b9919e0551545891d6167e65111047ac53490df1b120296fba33
fb9d25043e17d32355cea92e054c3e18faf5f991db76fe4344e94c3739b333d1
fd7b3a06e55ccdf0475ea6fd4409fbe448619b6ed6cf9b098e9e588faf2e5c54

Script

Below is a copy of the script used to pull the domains form from paste sites based on our search.

```
#!/usr/bin/python3

# Imports
from rfapi import ApiClient     # pip install rfapi
import datetime
import argparse
import requests
import hashlib
import os
import re

# Read arguments
parser = argparse.ArgumentParser()
```

```
parser.add_argument('--days', '-d', default=30, type=int, help='Number of
days to search Recorded Future')
args = parser.parse_args()

# Global variables
dir_path = os.path.dirname(os.path.realpath(__file__))  # Get working dir
API = ApiClient('API_KEY_HERE')                         # Insert API key
here
timeout_value = 10                                      # Timeout value for
downloads
search_days = ('-{}d to +{}d'.format(args.days, args.days))

# Process input form user to get the date object to search
def get_days_to_search():
  # Get the date formated for RF API
  today = datetime.datetime.now()
  delta = today - datetime.timedelta(days=args.days)
  today = today.strftime('%Y-%m-%d')
  delta = delta.strftime('%Y-%m-%d')
  formated_search_range = ('{}--{}'.format(delta, today))
  search_date_options = {'formated_search_range': formated_search_range,
'today': today, 'delta': delta}
  return search_date_options

# Search paste sites with Recorded Future
def get_rf_documents():
  # The Actual Search
  return API.paged_query({"reference": {"searchtype": "scan", "time_range":
search_days, "attributes": [{"string": ["houdini"], "name":
"Event.event_fragment"},{"string": ["recoder"], "name":
"Event.event_fragment"},{"string": ["skype"], "name":
"Event.event_fragment"},{"name": [["Event.document_source",
"Source.media_type"]],"entity": {"id": ["KDS1Zp", "POdRlc"]}}]}},
batch_size=1000, limit=10000)

# Looks up the sub document
def lookup_rf_documents(url):
  return API.paged_query({"instance": {"searchtype": "scan", "time_range":
search_days, "document": {"url": url}}}, batch_size=1000, limit=10000)

def main():
  # List To Save URLs to
```

```
  documents_list = []
  remove_errors = ['save', 'adodb.stream', 'objhttpdownload.open',
'httpobj.open', 'shellobj.run', 'wscript.shell', 'wscript.shell', 'open',
'file.name', 'name', 'stream', 'run', 'objitem.name', 'lnkobj.save',
'shell', 'folder.name']
  whitelist = ['nopaste.me', 'pastebin.com', 'virustotal.com',
'linkpc.net', 'ddns.net', 'hopto.org', 'myftp.biz', 'publicvm.com',
'no-ip.org', 'zapto.org', 'duckdns.org', 'myq-see.com', 'dynu.net',
'duckdns.net', 'myftp.org', 'dds.net', 'sytes.net', 'no-ip.biz',
'no-ip.info', 'noip.me', 'gotdns.ch', 'ilovecollege.info', 'ssl443.org',
'crabdance.com']
  final_domain_list = []

  # Get today's date and time
  today = datetime.datetime.today()
  date_output = today.utcnow().strftime('%Y-%m-%d %H:%M:%S')
  # Output to user
  print('Starting Hunt on {} for {} days...\n'.format(date_output,
args.days))

  # Query RF to get a list of source URLs. This is needed for the 2nd level
search to get the IOCs from the source URL.
  instances = list(get_rf_documents())
  # Save The Results To Data
  rf_documents_all = instances[0]['instances']

  # Output To User
  results_total = len(rf_documents_all)
  if results_total is 0:
      print('No Results Within The Date Range.')
  else:
      print('Processing {} Results'.format(results_total))

  # Iterate through the results and append the ID and URL to id_list.
  for document in rf_documents_all:
      item = {'id': document['id'], 'url': document['document']['url']}
      documents_list.append(item)

  # Iterate over the list of all document URLs and IDs.
  for document in documents_list:
      # Search Recorded Future for the document URL.
      document_data = list(lookup_rf_documents(document['url']))
```

```
      document_data = document_data[0]['entities']
      # Iterate over the output from the specific document.
      for data in document_data:
          # Look for only data that contains a domain aka "idn:".
          if 'idn:' in data:
              # Remove the idn: from the string
                  # Create dictionary
                  item = {'source_url': document['url'],
'suspicious_domain': data}
                  # Add item to the final list
                  final_domain_list.append(item)
  # Iterate over the final list and print the output
  for item in final_domain_list:
      print('{},{}'.format(item['source_url'], item['suspicious_domain']))

if __name__ == '__main__':
  main()
```