

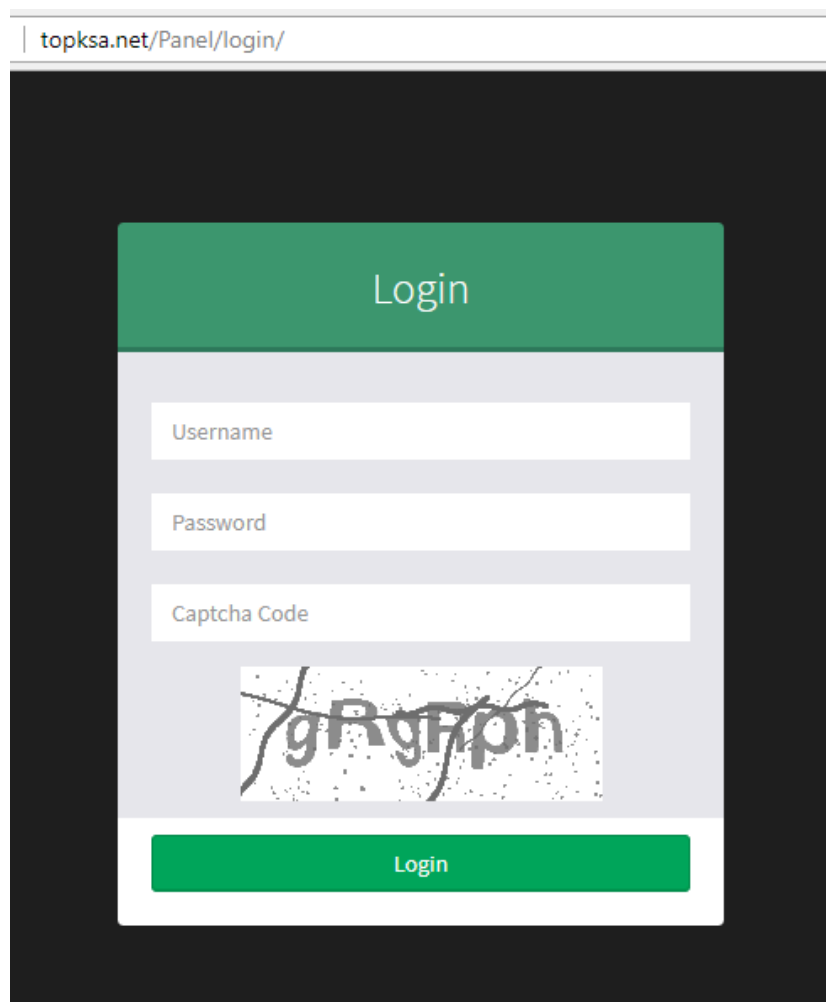
Recent LiteHTTP activities and IOCs - Malware Analysis - Malware Analysis, News and Indicators

Published: 2018-06-29 · Archived: 2026-04-10 03:15:41 UTC

This post serves as a dump of IOCs seen in the last 90 days related to LiteHTTP malware. The interest into LiteHTTP came from a bump in sighting in the month of may 2018.

One particular instance of a control panel was seen repeatedly in my research on virustotal. Multiple samples were seen for the first time in May on the platform. They were calling out to : `hxxp://topksa[.]net/Panel/page[.]php`

The panel of those samples was : `hxxp://topksa[.]net/Panel/login/`



A total of 106 LiteHTTP malware samples were seen from May 2nd, 2018 to May 20th, 2018. The panel is still live at moment of writing this but sightings of new samples on VT has stopped since May 20th, 2018.

I also saw some other LiteHTTP panels that have been active since the 1st of April 2018, which the IOCs will be listed below:

http://topksa.net/Panel/login/
topksa.net
212.237.55.178
79dae4a5b199281f924722be1f3ca1ce
67615ff09fb36efbdb2b37bb7a594d88
7747340fe0465e80910abdaa202abfe5
a39733bbaf88069e793f3f6b4937b545
5268dfbcc1b98498480cf648d52cf5c6
042b604594887802b08e4d79f29d1eb6
0523a8c5c9e3e31a2ad32f6c77b1447b
067abd137f315170fee9c1a1ece78df7
0975201adbdc0331e24b43b9d40ea520
520e7563015cf54d0b8bf003025bb56b
589e9608e2ee2852e145e3470fd0d7e6
643f27afbddb0ee532720c54cc0abd18
64f2d05dfe9a5760594a6c6439b63100
6c1d8b229bb02ee9ab3562fa8c268534
733be540fd11365c3b2b8bd38914f8a0
741d1f46b2b2d253b3dcd66f9f39485a
7f0909ead4bd5d8f471e9f4f5b5d89c1
9720c546cd771d3440aa14cb2c17df84
99d0c5262e99cd6b43eb33438399e016
bb293f81679dcbd098102fe707902377
ccbd0192a391ec97bbaa6778285a22b4
ce8e383c7c315ee27a4a2c53d494ff33
ecc9511440e1cadb2864f4b757eb52bf
eee5d8ba1c06afaaa5a0d1563cf9e2db
49f56083538e4f0aa43873781132bd61
500d9aaaa485b73610c3aec1fa686a3b
63fe05d7b1951fd4660dd1857430796b
768a0e0e27749d94ea4675abe4de1a8d
bbf5f31d7a41d45cc68e667471c63871
c2a5ab21a6e2a349fd173337cd1e0a48
d3d83a8a744cb862ec67eb771d9d984a
dfe58df1e543c014ac1b166402fd0e2a
23f4c86f255d2cd1c85962d6552520fc
306c76bb087b95ceae7a7399a2e41f4e
3c84d0927a75e75b28ff4553a192b5e2
418e32f2188ce2a38d1dbbf1ef05efeb
490e10e390ae6995e83d4e49cb10cea4
4e50a38741609c418ef2884f62e0d4af
4f901b87e938ba01516313c71e6dc8a5

7c86374250574fc13eaa2efb3fd9a786
aa1cbbf73b761585ee0353bf8f40461b
e8084007d595879f52f05f9083175d3f
f398d68d59cfc3a1a3415649f8324e6b
1696e4b5342fa4f1721767ec5e7f5cdc
1a1fcd0e1b661b4ecc160a7772b4f46a
2361397d688312d862efad87d1c0a525
50de216e6a3f99abc33b025a2d8acb41
65964e1d3841ea26e9552a57f0a8d37d
65d808967ca7b7ba87d2d1ae9b268f77
67d85a9af46ac0e4052f647561e45012
70eedafb7494b27ff94781c2245d7624
834e5453349b71d21783e475509f46e3
881618effece7fea5bba2fc3e589cca
b5803930438bd2578b0983cca7dcb08b
bd7098ecac3678c98e9907086576292d
c30afb3577826654aea95810a0e87dec
dccecbd3baf3fc2e451b54bb392b01eb
dd94c70d4a53ee04a7a1c25c48ac2f70
e1f2104ea54aed9a7eedc954d24c2b6d
e256c4d3b44c55b040e7576121b15ee3
fac365dc7c1588ff054094481e33633d
48f9633d03cbe781f65c76087844e2e9
19b5c9f833ed1dd0b68df970a765d0f5
2d4f85618adb4b1576a6414cb37db449
45e5864c3a69fbb9ee3a11b6b3c26f7c
977cbdd6b7e8623465e35176085dc17d
9aa3bd406b254181d1a16d6d280d7490
a2d955231b610626fc68510722cb27fc
de80e2b7f87438e4f39414a94083c954
e47313dbfac4934a866069d2c2c1a305
21c7805d4227866332fc25425981b360
6ebff77cfc1ab21e02d604a12ab416b4
063b7db270c03c58316d6d1f17be55e6
0be1d348eececff5817fe5c513e9172
1989abbcef413c2473d71c5d868b649f
3f54cc5d47fff7cf7735b0f30afa5707
423fd2489703f155640ce488cc776e8f
43db1aa9e2574c84f09d087efec21bc2
4fcf013cda3586e3dda973cab9b5eff4
629ae5236ebaec9452ff4ad47daa2d10
634a92c9b1c2beb584965d15222f01aa

666819caa468e2fa24f0107a3d076700
6da563bef78ba94647915ae795278b42
6fa88e08a3055282fd4e78a483821a0b
7ebf7da0d048ce95514359644bbf1db8
9b92e55cba936c390a62ff8b00b57326
9c84f43ff72aff262a0fd34e26e5c811
9d523a63c28d34afdbe80b7f0e080d08
a3508b09f61b15d86e6a1659f3e4f05c
a5eb787d733fc39a0375bf176f11a9a4
a723f616e0ae03c4a9e198d04b4d8bd6
b0358707ddfde044c4944396d2c7c29b
c5bae65408bf00f89428fc2d200d9c48
cfd77b5405814fa9022affc48c76a420
da8976c966de36eb1b177a41093406c5
e110d1db461441607c21c18cd42ba82c
e1c375876659407ed7452504839ad6c0
f27f3222353280e52793a7130e41f5c5
fe1759f0600e3221d6323ee2ac5c9ace
38b789e9fba006ead95c9d8a9def44bb
b3a6ec4f4a4889ecd245a75458268646
ec03d66b68304502b36aa765497cbd18
26d95659c646f88d2b14dc71e2bc07b2
5f8b7d6cae04ff17bcf7186bbf8b30d7
dc3fa09bc67a9ca0f2aae55e0af4184a
ed1b204cd1e6850c43b814bb96e94097

http://103.194.170.51/Panel/login/
adeaada185fa73cd8b779869e10cbe91

http://172.81.133.27//lite/login/
d91ad16e2e3c57dba48dfffe315e715c
cff1ab09d5d582086588882e5fdf1696

http://176.223.131.228/Panel/login/
18ada7caf0478dda9ca3b62dcef66c6b
775cdac7ee3daa4fa462431b7f51998b
b49e2dcb3aef79d61a9832d1903d101e
cf992f2fc1c2ad4b8f5ad5a9410cc50f

http://62.77.155.65/Panel/login/
5691ab6b01e9092578d4f3e0199a1583

http://babycute.thats.im/sociu/login/
0c163243ba933d4b14a7673a9c561795

http://bananaloop.ru/Panel/login/
987d46def142dc455f32e3c8ea052edb
f3e02148b8f4dccf131fd24667e2f8dd

http://k9stock.com/Panel/login/
671d6ad1db0e32d2626f1de297f08471

http://partnerwithuss.ru//Panel/login/
39c5fb2236aac6d5a672155ba174a028

http://posalive.su/login/
2615eabfac63bc5ff0418ca7edf10092

http://razilov06.hldns.ru/panel/login/
543f8a019a3f886afdf3b3b4efc7a312

http://sketchie.ru/HTTP/ZzZz/login/
a3e211615cddff693f73bfab8317fcdc

http://tik-media.info//login/
bc9f581a808576eabe09c19a09737ff1

http://x420.me/latte/login/
7f170a002757bd3c1f6fcdd61e750944
7c0176ede8e8920b559eb7c7a7cd72d5
d3ab4462ace2bd0ad62a9adec5b47516
789388866ccb7b45d79d5e1b827211ac

http://xanull.phy.sx/Panel/login/
f5549ac23c7e934efe149cd63c3ed7b5
6e3050622a038866506890c1c94224eb
5d1ebb7a2a459467cfcfb87acfd3c4ca

http://yylisah0.beget.tech/images/thumbs/about/informio/login/
0494ef09f44c8646a3ebf79baad93417

Article Link: [Recent LiteHTTP activities and IOCs – ViriBack Blog](https://malware.news/t/recent-litehttp-activities-and-iocs/21053)

Source: <https://malware.news/t/recent-litehttp-activities-and-iocs/21053>