botnet

SBU-PA-7080-Active : Wednesday, October 21, 2020

Confidence	Source address	Source User	Virtual System	Description
4	172.25.243.145	unknown user	vsys1	Repeatedly visited (36) the same malicious URL stats.hkjngy.me/StatisticsService.svc/V1/JSON/LogEvent
4	172.25.83.63	unknown user	vsys1	Repeatedly visited (62) the same malicious URL paumoogo.net/
4	172.24.199.87	unknown user	vsys1	Repeatedly visited (30) the same malicious URL bretterichardson.com/
4	172.24.113.227	unknown user	vsys1	Repeatedly visited (75) the same malicious URL bretterichardson.com/
4	10.1.149.97	unknown user	vsys1	Repeatedly visited (37) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=0e909f95-9ab5-5b15-a043-b7d75d6f4414&Distributer=mckodorega&Channelid=003&Barcodeid=5407900&country=US&encrypt=false&simac=true
4	172.25.55.178	unknown user	vsys1	Repeatedly visited (24) the same malicious URL ilo13ulih.com/
4	172.25.138.149	unknown user	vsys1	Repeatedly visited (33) the same malicious URL www.adamraftery.com/
4	172.25.51.25	unknown user	vsys1	Repeatedly visited (27) the same malicious URL nuszjog.com/update?os=win&arch=x86&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=63.0.3235.0&lang=en-US&acceptformat=crx2,crx3&x=id=jghljaaggimcdeopnjkfhckjnddhhck&v=15.13.25.53&installsource=notfromwebstore&uc&ap=affi-wsg_bjfpsso0w0gpy_20_01_ssg00&guid=dd4e64e5-a3da-4f6e-8b64-ee4a4c33db5d&xip_sess_guid=dd4e64e5-a3da-4f6e-8b64-ee4a4c33db5d&client=chromium&cdi=2XzuyEiNZYLYLQzuzyyC0EyCOFyEyBzz0BA0FtC0FDDAyDtN0D07zu0StBzyrBtCN1L2XzuyEiFyDzyrFiDFyDtBtN1L1Czu1ByCtN1L1G1B1YiN2YiL1Qzu2St0OCyC0E0A0DyEzzzGyEyEyBzyyBtGB0D0DtBtGyBtC0A0FtGtBtB0EtAyEtCzz0DztEyBy0zz1RtTzy2QtN0A0LzuyEtN1BZZ1Yi1T1S1NzuNi1QZZ1B1PtRzutCyDyByEzyCyDtyBzyCyDtD&cr=1343980165
4	172.25.82.207	unknown user	vsys1	Repeatedly visited (30) the same malicious URL go.eroadvertising.com/
4	172.24.129.94	unknown user	vsys1	Repeatedly visited (38) the same malicious URL bretterichardson.com/
4	172.24.84.254	unknown user	vsys1	Repeatedly visited (37) the same malicious URL bretterichardson.com/
4	172.24.193.254	unknown user	vsys1	Repeatedly visited (144) the same malicious URL ww2.fmovies.cab/
4	172.24.129.107	unknown user	vsys1	Repeatedly visited (69) the same malicious URL bretterichardson.com/
4	129.49.26.138	unknown user	vsys1	Repeatedly visited (50) the same malicious URL search.searchfff.com/
4	129.49.32.208	unknown user	vsys1	Repeatedly visited (45) the same malicious URL nuszjog.com/update?os=win&arch=x86&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=63.0.3235.0&lang=en-US&acceptformat=crx2,crx3&x=id=jghljaaggimcdeopnjkfhckjnddhhck&v=15.13.25.53&installsource=notfromwebstore&uc&ap=affi-wsg_lurprx79bdfhj2fqhjhpnt2g_19_47_ssg00&guid=e021494d-e921-48c1-b6ef-2b5c176d2e9e2&xip_sess_guid=e021494d-e921-48c1-b6ef-2b5c176d2e9e2&client=chromium&cdi=2XzuyEiNZYLYLQzuCzyyC0D0A0D0A0DtBzyE0E0D0E0D0BtN0D0Tzu0StBzzzzztBtN1L2XzuyEiFyDyBtFtDFyBtyDtN1L1Czu1BtDtN1L1G1B1YiN2YiL1Qzu2StEy0B0AyDyE0CzyyEtSyBtCyD0DyB0CBtyCtSyD0A0BtyDtDzzy0D0A0AtBy0DtEyD0AyDyDzy2QtN1MtF1BZZ1YiN2YiL1QzuZStDAtD0AyD1TtDtGtTyD1RtRGyEtBtBtyCtG1S1Q1S1SIGtGD1StD1RyEtT1QtCzyyEt1T1QtN0A0LzuyEtN1BZZ1YiN2YiL1QzuZStDAtD0AyD1TtDtGtTyD1RtRGyEtBtBtyCtG1S1Q1S1SIGtGD1StD1RyEyEyCyDzyrDtD&cr=2129661699
4	172.24.205.27	unknown user	vsys1	Repeatedly visited (94) the same malicious URL getessay.net/
4	172.25.54.109	unknown user	vsys1	Repeatedly visited (33) the same malicious URL bretterichardson.com/
4	10.245.233.205	unknown user	vsys1	Repeatedly visited (362) the same malicious URL v8p.tomuniered.club/
4	172.24.17.38	unknown user	vsys1	Repeatedly visited (28) the same malicious URL www.bulkbites.com/
4	172.24.50.106	unknown user	vsys1	Repeatedly visited (81) the same malicious URL bretterichardson.com/
4	172.25.83.127	unknown user	vsys1	Repeatedly visited (24) the same malicious URL fingahvf.top/
4	172.24.84.201	unknown user	vsys1	Repeatedly visited (30) the same malicious URL www.greedy.world/
4	172.25.87.214	unknown user	vsys1	Repeatedly visited (20) the same malicious URL on.mebtx7.com/
4	172.24.48.58	unknown user	vsys1	Repeatedly visited (51) the same malicious URL bretterichardson.com/
4	172.24.134.53	unknown user	vsys1	Repeatedly visited (24) the same malicious URL go.eroadvertising.com/
4	172.24.128.78	unknown user	vsys1	Repeatedly visited (204) the same malicious URL www.aww799.com/
4	172.24.84.8	unknown user	vsys1	Repeatedly visited (25) the same malicious URL bretterichardson.com/
4	172.25.84.86	unknown user	vsys1	Repeatedly visited (160) the same malicious URL js.wpncdn.com/
4	172.24.162.108	unknown user	vsys1	Repeatedly visited (72) the same malicious URL www.greedy.world/
4	172.25.90.231	unknown user	vsys1	Repeatedly visited (20) the same malicious URL go.eroadvertising.com/
4	172.25.245.135	unknown user	vsys1	Repeatedly visited (54) the same malicious URL bretterichardson.com/
4	10.1.227.220	asunika	vsys1	Repeatedly visited (43) the same malicious URL bretterichardson.com/
4	129.49.116.27	unknown user	vsys1	Repeatedly visited (20880) the same malicious URL shopstorys.com/
4	172.25.80.239	unknown user	vsys1	Repeatedly visited (48) the same malicious URL szreward.net/
4	172.24.17.141	unknown user	vsys1	Repeatedly visited (60) the same malicious URL i.kpzip.com/n/kuaizip/strategy_report/kb.xml
4	10.255.34.143	unknown user	vsys1	Repeatedly visited (620) the same malicious URL go.schjmp.com/
4	172.24.164.0	unknown user	vsys1	Repeatedly visited (74) the same malicious URL attachments.95zone.io/
4	172.24.53.92	unknown user	vsys1	Repeatedly visited (59) the same malicious URL down.zmshuru.com/smartcloud/srvc/cld/lsk.dat
4	129.49.57.130	unknown user	vsys1	Repeatedly visited (22) the same malicious URL work.a-poster.info:25000/
4	172.24.80.253	unknown user	vsys1	Repeatedly visited (146) the same malicious URL fingahvf.top/
4	172.25.94.226	unknown user	vsys1	Repeatedly visited (87) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=8f024f73-9621-5825-8267-816F3829C8D4&Distributer=mcmarket&Channelid=003&Barcodeid=5302700&country=US&encrypt=false&simac=true
4	172.24.171.58	unknown user	vsys1	Repeatedly visited (65) the same malicious URL delopten.com/apu.php?zoneid=1590109
4	172.25.49.79	unknown user	vsys1	Repeatedly visited (37) the same malicious URL bretterichardson.com/
4	172.24.48.130	unknown user	vsys1	Repeatedly visited (66) the same malicious URL bretterichardson.com/
4	172.24.134.111	unknown user	vsys1	Repeatedly visited (28) the same malicious URL bretterichardson.com/
4	172.24.136.243	unknown user	vsys1	Repeatedly visited (27) the same malicious URL bretterichardson.com/
4	172.24.85.146	unknown user	vsys1	Repeatedly visited (144) the same malicious URL bretterichardson.com/
4	172.25.237.165	unknown user	vsys1	Repeatedly visited (132) the same malicious URL chat2.neolive.kr/
4	172.24.52.141	unknown user	vsys1	Repeatedly visited (20) the same malicious URL ads.adsnvrk.io/
4	172.25.112.74	unknown user	vsys1	Repeatedly visited (97) the same malicious URL bretterichardson.com/
4	172.24.93.220	unknown user	vsys1	Repeatedly visited (30) the same malicious URL www.aww799.com/
4	172.24.207.150	unknown user	vsys1	Repeatedly visited (20) the same malicious URL www.aww799.com/squirrel-log
4	129.49.16.184	unknown user	vsys1	Repeatedly visited (40) the same malicious URL sync.malwareprotectionlive.com/home/postevents
4	10.1.185.156	unknown user	vsys1	Repeatedly visited (126) the same malicious URL sync.minepi.com/heartbeat
4	172.25.52.84	unknown user	vsys1	Repeatedly visited (24) the same malicious URL bretterichardson.com/

4	172.24.163.118	unknown user	vsys1	Repeatedly visited (60) the same malicious URL updates.ijnewhb.com/Update/CheckOnDemand?deviceid=0e909f95-9ab5-5b15-a043-b7d75d64f41a&Distributer=mckodioreg&ChannelId=003&BarcodeId=54079003&country=US&encrypt=false&ismac=true
4	172.24.115.36	unknown user	vsys1	Repeatedly visited (44) the same malicious URL bretterichardson.com/
4	129.49.117.127	unknown user	vsys1	Repeatedly visited (22) the same malicious URL necklace.admobe.com/
4	172.24.168.63	unknown user	vsys1	Repeatedly visited (27) the same malicious URL bretterichardson.com/
4	172.25.49.252	unknown user	vsys1	Repeatedly visited (28) the same malicious URL ofgogoatan.com/
4	172.24.202.220	unknown user	vsys1	Repeatedly visited (109) the same malicious URL stats.hkijngy.me/StatisticsService.svc/V1/JSON/LogEvent
4	172.24.165.108	unknown user	vsys1	Repeatedly visited (71) the same malicious URL ww2.fmovies.cab/
4	172.24.88.54	unknown user	vsys1	Repeatedly visited (33) the same malicious URL bretterichardson.com/
4	10.1.239.195	unknown user	vsys1	Repeatedly visited (41) the same malicious URL apimon.de/
4	10.245.236.48	unknown user	vsys1	Repeatedly visited (31) the same malicious URL 185.130.105.66:998/
4	172.25.81.56	unknown user	vsys1	Repeatedly visited (52) the same malicious URL testthehalf.top/
4	172.24.81.139	unknown user	vsys1	Repeatedly visited (60) the same malicious URL js.wpncdn.com/
4	10.1.223.37	unknown user	vsys1	Repeatedly visited (24) the same malicious URL bretterichardson.com/
4	172.24.133.242	unknown user	vsys1	Repeatedly visited (36) the same malicious URL fingahvf.top/
4	129.49.218.91	sunysb.edu\jscarola	vsys1	Repeatedly visited (1222) the same malicious URL brounelink.com/
4	10.245.235.94	unknown user	vsys1	Repeatedly visited (120) the same malicious URL apimon.de/
4	10.255.44.215	unknown user	vsys1	Repeatedly visited (213) the same malicious URL ww2.fmovies.cab/
4	172.25.88.53	unknown user	vsys1	Repeatedly visited (29) the same malicious URL www.aww799.com/squirrel-log
4	172.24.21.200	unknown user	vsys1	Repeatedly visited (30) the same malicious URL bretterichardson.com/
4	172.25.57.226	unknown user	vsys1	Repeatedly visited (54) the same malicious URL trackers.voodoo-analytics.io/
4	129.49.112.247	unknown user	vsys1	Repeatedly visited (46) the same malicious URL tawuhoju.com/update/?x=ap=&cd=2XzuyEtN2Y1L1QzuzytD0BtCtC0CyCyC0FzytDzztCzyzztAtN0D0Tzu0StBzztCyDtN1L2XzuyEtFyDyDtFtDtFtCtAtBtN1L1Czu1BtCtN1L1G1B1V1N2Y1L1Qzu2SyEtByE0E0D0CtCyDtGtDtDtDtCtG0C0AtByEtGyC0ByBtDtG0EyE0D0DyCyCtByC0FtDyDyD2QtN1M1F1B2Z1V1N2Y1L1Qzu2S1Q1OyDtB1OyC1O1RtGyBtBzy1RtGyE1P1PyBtGzz1RyEzytG1PyC1Tzy1RzytCtCtD1Q1RtA2QtN0A0LzuyEtN1B2Z1V1T1S1NzutBtAyDyBtBtN1Q2Z1B1P1RzutCyDyCzzyCyEtDyCyEtA&cr=2098573145&aflt=mnn_iouweqrlz2ontegikmoqzf783aen_19_38&os=win&arch=x86&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=63.0.3236.0&lang=en-US&acceptformat=crx2,crx3&x=id=gllihgnfnbpdmnppfjdlkciijkddfohn&v=0.0&installsource=notfromwebstore&uc
4	172.25.81.157	unknown user	vsys1	Repeatedly visited (300) the same malicious URL goverallyhandl.club/
4	172.25.53.223	unknown user	vsys1	Repeatedly visited (21) the same malicious URL bretterichardson.com/
4	172.24.162.237	unknown user	vsys1	Repeatedly visited (144) the same malicious URL ww2.fmovies.cab/
4	172.24.161.231	unknown user	vsys1	Repeatedly visited (1969) the same malicious URL testthehalf.top/
4	10.1.129.146	unknown user	vsys1	Repeatedly visited (24) the same malicious URL www.aww799.com/
4	10.1.250.89	unknown user	vsys1	Repeatedly visited (333) the same malicious URL nonblocks.com/wpad.dat?1f241d7da828d925ba2bd553b785b52417190746
4	10.1.154.176	jighuang	vsys1	Repeatedly visited (27) the same malicious URL bretterichardson.com/
4	172.24.129.106	unknown user	vsys1	Repeatedly visited (48) the same malicious URL www.greedy.world/
4	172.25.87.197	unknown user	vsys1	Repeatedly visited (20) the same malicious URL the123movies.stream/
4	172.24.48.57	unknown user	vsys1	Repeatedly visited (508) the same malicious URL attachments.f95zone.to/
4	130.245.253.21	unknown user	vsys1	Repeatedly visited (20) the same malicious URL www.partopiarental.com/
4	172.24.170.204	unknown user	vsys1	Repeatedly visited (24) the same malicious URL bretterichardson.com/
4	172.24.53.105	unknown user	vsys1	Repeatedly visited (45) the same malicious URL pv.vipwm.cc:4443/
4	172.24.207.254	unknown user	vsys1	Repeatedly visited (22) the same malicious URL www.aww799.com/squirrel-log
4	172.25.85.247	unknown user	vsys1	Repeatedly visited (432) the same malicious URL watchseries1.bypassed.icu/
4	10.1.210.127	unknown user	vsys1	Repeatedly visited (36) the same malicious URL www.aww799.com/
4	129.49.216.207	sunysb.edu\mcmaloney	vsys1	Repeatedly visited (40) the same malicious URL pumpkinblaze.org/
4	172.25.86.91	unknown user	vsys1	Repeatedly visited (75) the same malicious URL api.pdfxd.com/pdf-service/v1/report
4	10.245.205.113	unknown user	vsys1	Repeatedly visited (34) the same malicious URL go.eroadvertising.com/
4	129.49.28.249	unknown user	vsys1	Repeatedly visited (82) the same malicious URL bretterichardson.com/
4	172.24.199.174	unknown user	vsys1	Repeatedly visited (45) the same malicious URL bretterichardson.com/
4	172.25.48.161	unknown user	vsys1	Repeatedly visited (137) the same malicious URL bretterichardson.com/
4	10.255.12.236	unknown user	vsys1	Repeatedly visited (150) the same malicious URL 5nt1gx7o57.com/
4	172.24.84.253	unknown user	vsys1	Repeatedly visited (26) the same malicious URL jtuzd.rdtk.io/
2	138.118.174.125	unknown user	vsys1	Unknown UDP traffic
2	5.135.183.232	unknown user	vsys1	Unknown UDP traffic
2	205.185.123.78	unknown user	vsys1	Unknown UDP traffic
2	112.225.85.115	unknown user	vsys1	Unknown UDP traffic
2	210.0.158.192	unknown user	vsys1	Unknown UDP traffic
2	54.37.0.57	unknown user	vsys1	Unknown UDP traffic
2	142.93.8.147	unknown user	vsys1	Unknown UDP traffic
2	192.210.231.210	unknown user	vsys1	Unknown UDP traffic
2	151.80.212.46	unknown user	vsys1	Unknown UDP traffic
2	121.37.200.11	unknown user	vsys1	Unknown UDP traffic
2	183.131.231.14	unknown user	vsys1	Unknown UDP traffic
2	113.218.148.87	unknown user	vsys1	Unknown UDP traffic
2	185.142.55.36	unknown user	vsys1	Unknown UDP traffic
2	176.193.71.50	unknown user	vsys1	Unknown UDP traffic
2	200.73.131.94	unknown user	vsys1	Unknown UDP traffic
2	198.211.99.153	unknown user	vsys1	Unknown UDP traffic
2	165.227.117.43	unknown user	vsys1	Unknown UDP traffic

2	66.244.251.246	unknown user	vsys1	Unknown UDP traffic
2	51.38.16.217	unknown user	vsys1	Unknown UDP traffic
2	51.178.53.84	unknown user	vsys1	Unknown UDP traffic
2	59.6.23.142	unknown user	vsys1	Unknown UDP traffic
2	42.224.71.38	unknown user	vsys1	Unknown UDP traffic
2	151.80.212.34	unknown user	vsys1	Unknown UDP traffic
2	209.141.48.68	unknown user	vsys1	Unknown UDP traffic
2	80.253.246.118	unknown user	vsys1	Unknown UDP traffic
2	79.137.126.100	unknown user	vsys1	Unknown UDP traffic
2	125.139.50.167	unknown user	vsys1	Unknown UDP traffic
2	193.70.91.148	unknown user	vsys1	Unknown UDP traffic
2	163.172.207.18	unknown user	vsys1	Unknown UDP traffic
2	45.33.106.26	unknown user	vsys1	Unknown UDP traffic
2	167.86.114.245	unknown user	vsys1	Unknown UDP traffic
2	181.30.28.51	unknown user	vsys1	Unknown UDP traffic
2	186.235.84.34	unknown user	vsys1	Unknown UDP traffic
2	193.178.118.5	unknown user	vsys1	Unknown UDP traffic
2	54.37.64.178	unknown user	vsys1	Unknown UDP traffic
2	160.16.68.239	unknown user	vsys1	Unknown UDP traffic
2	195.89.76.159	unknown user	vsys1	Unknown UDP traffic
2	104.131.29.110	unknown user	vsys1	Unknown UDP traffic
2	107.170.254.53	unknown user	vsys1	Unknown UDP traffic
2	67.205.182.46	unknown user	vsys1	Unknown UDP traffic
2	179.96.3.248	unknown user	vsys1	Unknown UDP traffic
2	77.43.248.66	unknown user	vsys1	Unknown UDP traffic
2	64.227.106.15	unknown user	vsys1	Unknown UDP traffic
2	155.94.144.150	unknown user	vsys1	Unknown UDP traffic
2	205.185.117.4	unknown user	vsys1	Unknown UDP traffic
2	23.102.66.71	unknown user	vsys1	Unknown UDP traffic
2	206.189.76.220	unknown user	vsys1	Unknown UDP traffic
2	159.65.150.139	unknown user	vsys1	Unknown UDP traffic
2	139.162.126.103	unknown user	vsys1	Unknown UDP traffic
2	200.73.131.186	unknown user	vsys1	Unknown UDP traffic
2	103.231.146.242	unknown user	vsys1	Unknown UDP traffic
2	37.59.222.66	unknown user	vsys1	Unknown UDP traffic
2	42.235.67.206	unknown user	vsys1	Unknown UDP traffic
2	5.189.183.214	unknown user	vsys1	Unknown UDP traffic
2	165.227.181.29	unknown user	vsys1	Unknown UDP traffic
2	188.170.28.69	unknown user	vsys1	Unknown UDP traffic
2	193.188.146.25	unknown user	vsys1	Unknown UDP traffic
2	151.80.26.227	unknown user	vsys1	Unknown UDP traffic
2	95.217.162.125	unknown user	vsys1	Unknown UDP traffic
2	43.226.26.159	unknown user	vsys1	Unknown UDP traffic
2	104.233.244.229	unknown user	vsys1	Unknown UDP traffic
2	45.89.67.49	unknown user	vsys1	Unknown UDP traffic
2	199.195.254.13	unknown user	vsys1	Unknown UDP traffic
2	31.44.82.203	unknown user	vsys1	Unknown UDP traffic
2	200.71.120.82	unknown user	vsys1	Unknown UDP traffic
2	59.55.128.147	unknown user	vsys1	Unknown UDP traffic
2	5.196.117.224	unknown user	vsys1	Unknown UDP traffic
2	5.196.89.191	unknown user	vsys1	Unknown UDP traffic
2	42.236.214.29	unknown user	vsys1	Unknown UDP traffic
2	64.227.101.45	unknown user	vsys1	Unknown UDP traffic
2	124.207.138.245	unknown user	vsys1	Unknown UDP traffic
2	188.226.174.45	unknown user	vsys1	Unknown UDP traffic
2	164.90.201.56	unknown user	vsys1	Unknown UDP traffic
2	159.89.194.64	unknown user	vsys1	Unknown UDP traffic
2	5.180.79.167	unknown user	vsys1	Unknown UDP traffic
2	200.73.130.160	unknown user	vsys1	Unknown UDP traffic
2	69.51.20.152	unknown user	vsys1	Unknown UDP traffic
2	137.135.208.147	unknown user	vsys1	Unknown UDP traffic
2	209.141.51.154	unknown user	vsys1	Unknown UDP traffic

2	45.55.157.1	unknown user	vsys1	Unknown UDP traffic
2	104.168.170.80	unknown user	vsys1	Unknown UDP traffic
1	172.25.80.92	unknown user	vsys1	Visited malware URL muskegontribune.com/
1	10.1.191.220	unknown user	vsys1	Visited malware URL 221.181.72.250:443/scan
1	172.24.168.253	unknown user	vsys1	Visited malware URL wdl2.cache.wpscdn.cn/newupdate/2052/pertrial/9678/selfpatch/wpsupdate.exe
1	129.49.220.68	unknown user	vsys1	Visited malware URL downloadserv.com/inventpure/dfskbKsdGhtiskjnsl7ksfdbJHb.jsp?btR6cB78ofXD7gzHLWqYU/idwvnD99XL0FmzLlc6vhOUqnYAGYF5s7Wo1r16Y3UmL4dyfJ6vJ4cVt2S3iaMsLBwGugvlCiSG%204y/rqrej8y2C%20gGGlAZi1tz/xMZPCk7QNEv4DeGNUp50w6vIGHDCAGUX2Wr9snvRr/65auTrZEQf6IepobofoWCOjTPyqRPfb6Nh4HF3ibyRe8Dz4d3LHqamJXOStZNuRF7SDLCjVlGc7p/uK8g1N8VV4c/To4C91TjBfPNf1GrJCeegg4BRjNEFPWxinxPOsIISkmQxOdR0BUIHJsKbno4bz69F6hDazK9gUD3vMC/krp5aU3A8iTut1LAtCnxvXXcku/hsik=
1	172.24.164.111	unknown user	vsys1	Visited malware URL www.clubotaku.org/
1	10.245.197.222	unknown user	vsys1	Visited malware URL rabbitinred.com/
1	172.24.129.64	unknown user	vsys1	Visited malware URL img1.v.tmcdn.net/img/h000/h70/img20141112161304f48770.png
1	172.24.48.159	unknown user	vsys1	Visited malware URL update.helper.2345.cc/ie/index.php
1	10.1.212.78	unknown user	vsys1	Visited malware URL ads.gviworld.com/
1	172.25.83.39	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=10666&aff_sub=ms_alibaba_ios_tier1_new&aff_sub2=5f8fb8c6eeed62361191291b&aff_sub5=mobc5d193ecdab61e26&gaid=55BDFA5A-5539-4153-A5AB-E7970E5D20B7&aid=55BDFA5A-5539-4153-A5AB-E7970E5D20B7
1	172.24.193.135	unknown user	vsys1	Visited malware URL www.aww799.com/
1	129.49.220.183	unknown user	vsys1	Visited malware URL trk.brother-root-rich-of.xyz/campaign?id=582cfa64-c55c-4531-8dfa-f4dc0989d113&var1=&extcid=wvlom2flb90ls4q22vmfrkqe
1	10.1.239.134	unknown user	vsys1	Visited malware URL www.orchardcroft.ca/
1	172.24.112.175	unknown user	vsys1	Visited malware URL bretterichardson.com/
1	172.25.89.206	unknown user	vsys1	Visited malware URL m.veporns.com/theme/images/300x150.jpg
1	172.25.90.99	unknown user	vsys1	Visited malware URL hhdstreams.club/hd/ch2.php
1	172.25.88.192	unknown user	vsys1	Visited malware URL bretterichardson.com/
1	172.25.233.74	unknown user	vsys1	Visited malware URL img.cankaowang.com/
1	172.24.225.198	unknown user	vsys1	Visited malware URL wap.ylxdtww.com/encrypt/t/g
1	172.24.89.182	unknown user	vsys1	Visited malware URL popcorntime-update.xyz/?app_id=T4P_SEM&hid=6702b51cf567f2f7bd6b91184eead3fa&ver=UNKNOWN&os=OSX101505
1	172.24.132.27	unknown user	vsys1	Visited malware URL popcorntime-update.xyz/?app_id=T4P_SEM&hid=2c01cb43b519fd67eeff7d7b521fc9c3&ver=6.1.2&os=OSX101406
1	172.25.49.123	unknown user	vsys1	Visited malware URL xml.adop.co/
1	172.25.56.132	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	10.1.169.32	aresposito	vsys1	Visited malware URL pudacasa.com/update?os=mac&arch=x64&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=63.0.3230.0&lang=en-US&acceptformat=crx2,crx3&x=id=ljnfpiodfojmjfbiechgkbkhikfbknjc&v=15.13.25.53&installsource=notfromwebstore&uc&ap=aflt=mcx_me3579bdfpyzsegikmoq6vy_19_44_ssg0218&guid=2dab8a71-0625-4ee4-b529-f83ce7844a24&xlp_sess_guid=2dab8a71-0625-4ee4-b529-f83ce7844a24&client=chromium&cd=2XzuyEtN2Y1L1QzuyEzytBtD1PtByCtCyDtD1O1StCzz1PyByD1QtByEzz1TtCtCyCzzyBzz1R1OtDtDyE1T1OtDzy1TtAyBtN1L1G1B1V1N2Y1L1Qzu2SyC0AyC0A0F0E0EyBtGyCyB0CtDtGyEzztByDtG0A0CtB0DtG0Azz0FyD0F0D0AyD0CyCzytD2QtN1Q2Zzu0StBzzyCtDtN1L2XzutAtFyCtFtBtBtFtCtN1L1CzutN1T1IzuyEtN1B2Z1V1T1S1Nzu&cr=2076760599
1	172.25.52.9	unknown user	vsys1	Visited malware URL bretterichardson.com/
1	172.24.50.26	unknown user	vsys1	Visited malware URL bretterichardson.com/
1	172.25.80.151	unknown user	vsys1	Visited malware URL www.1dy.cc/
1	172.24.165.59	unknown user	vsys1	Visited malware URL ads.gviworld.com/
1	129.49.2.215	unknown user	vsys1	Visited malware URL indeki.com/
1	172.24.135.11	unknown user	vsys1	Visited malware URL creative.schjmp.com/
1	172.24.166.128	unknown user	vsys1	Visited malware URL simpleitpro.com/
1	172.25.114.146	unknown user	vsys1	Visited malware URL www.watchcartoonslive.la/
1	172.24.90.165	unknown user	vsys1	Visited malware URL www.aww799.com/lion-update
1	172.25.87.209	unknown user	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	172.25.83.158	unknown user	vsys1	Visited malware URL bretterichardson.com/
1	172.24.224.108	unknown user	vsys1	Visited malware URL js.wpncdn.com/
1	172.25.84.142	unknown user	vsys1	Visited malware URL ofgogoatan.com/
1	129.49.45.183	sunysb.edu\mingenito	vsys1	Visited malware URL houseofkleekai.com/
1	172.25.247.115	unknown user	vsys1	Visited malware URL sbrservice.cc/init/init_android.json
1	172.24.17.226	unknown user	vsys1	Visited malware URL browserr.top/
1	172.24.16.225	unknown user	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	10.1.131.241	unknown user	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	172.25.85.99	unknown user	vsys1	Visited malware URL creative.schjmp.com/
1	172.25.81.179	unknown user	vsys1	Visited malware URL popcorntimeupd.xyz/?app_id=T4P_SEM&hid=129c9727fc1c2d1a8acf70aeca17d350&ver=UNKNOWN&os=OSX101502
1	10.1.217.75	unknown user	vsys1	Visited malware URL graniteacquitcharacteristic.com/3133db3094273140d1de8027d8310778/invoke.js
1	172.25.50.171	unknown user	vsys1	Visited malware URL www.aww799.com/kitten-update
1	172.24.112.183	unknown user	vsys1	Visited malware URL netserver849.ga/
1	172.24.129.49	unknown user	vsys1	Visited malware URL guidancecorner.com/
1	10.1.243.245	unknown user	vsys1	Visited malware URL flights.opalapi.com/
1	172.24.133.86	unknown user	vsys1	Visited malware URL api.bdisl.com/redirect?s=5328614&at=4&rt=api&o=96883601&s1=648d8d2ea0774959a67042dbfa23eb71-1603299263&s2=263090_Fd52b1f8aa5e&s3=&s4=&s5=&idfa=15CC2E59-2134-4F9E-BD66-B8B8EA2CDEB3&affSub={affSub}&i=130.245.192.5&u={ua}&lang=en-us&affSub=263090_Fd52b1f8aa5e
1	172.25.87.27	unknown user	vsys1	Visited malware URL 104.192.108.136/msvquery
1	10.1.146.168	efasano	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	10.1.195.235	dbyrne	vsys1	Visited malware URL www.violation.life/lion-update
1	172.24.55.176	unknown user	vsys1	Visited malware URL 101.227.33.243/
1	172.24.129.234	unknown user	vsys1	Visited malware URL install.smokyashan.com/brand/plist
1	172.25.113.158	unknown user	vsys1	Visited malware URL popcorntime-update.xyz/?app_id=T4P_SEM&hid=45245189eb2f98328b7e6abc7af18a9d&ver=UNKNOWN&os=OSX101507
1	172.25.87.104	unknown user	vsys1	Visited malware URL www.funsunmexico.com/
1	172.25.80.179	unknown user	vsys1	Visited malware URL tygieph.com/
1	172.24.166.213	unknown user	vsys1	Visited malware URL ksjdfysu.twtrack.site/favicon.ico
1	172.25.87.131	unknown user	vsys1	Visited malware URL entrence-mpsen.games.oasgames.site/static/globalConfigs_android_2.1.4.json

1	172.25.83.187	unknown user	vsys1	Visited malware URL track.apcva.com/aff_c?offer_id=5019&aff_id=2397&aff_sub=426798&aff_sub2=v03040000803742673Sed7b0d463cb97f3286ce455eaa&aff_click_id=102dbb9f20fc482b97d0d13727c060
1	129.49.10.250	sunysb.edu/jphilogene	vsys1	Visited malware URL dynamic675.ga/
1	172.25.54.40	unknown user	vsys1	Visited malware URL stats5.retire.ly/
1	172.24.86.88	unknown user	vsys1	Visited malware URL popcorntimeupd.xyz/?app_id=T4P_SEM&hid=f7494498c4bceecfb448b2636adc8f9b&ver=5.6&os=OSX101506
1	172.25.49.178	unknown user	vsys1	Visited malware URL www.aww799.com/squirrel-log
1	172.24.49.215	unknown user	vsys1	Visited malware URL trettenchardson.com/
1	172.24.17.169	unknown user	vsys1	Visited malware URL player31.kotakhitam.casa/
1	10.245.246.6	unknown user	vsys1	Visited malware URL acs.pandasoftware.com/retail/psevents/40469psevents_suite.exe
1	172.24.86.163	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=10666&aff_sub=ms_alibaba_ios_tier1_new&aff_sub2=5f90d15bb7ab13111af3727&aff_sub5=mobc5d193eodab61e26&gaid=6A51970A-41E4-4D6D-9DF9-90AEE530BD05&aid=6A51970A-41E4-4D6D-9DF9-90AEE530BD05