botnet

SBU-PA-7080-Active : Tuesday, September 08, 2020

Confidence	Source address	Source User	Virtual System	Description
4	172.24.54.37	unknown user	vsys1	Repeatedly visited (20) the same malicious URL pudacasa.com/update?os=mac&arch=x64&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=57.0.2987.110&lang=en-US&x=id=ljnfpiodfojmjfbiechgkbkhikfbknjc&v=15.13.25.53&installsource=notfromwebstore&uc&ap=aflt=mcx_me3579bdfpyzsegikmoq6vy_19_17_ssg0311&guid=16f32239-88b1-44fb-a677-493ad800802d&xlp_sess_guid=16f32239-88b1-44fb-a677-493ad800802d&client=chromium&cd=2XzuyEtN2Y1L1QzuyDyBtC1R1PtBzyzzzy1RzyyCyBtDtDtDyD1RtB1Q1OtD1PtB1S1S1OtA1T1O1P1QtA1TtBtAzy1StBtAtN1L1G1B1V1N2Y1L1Qzu2StByCtA0D0DzytDyBtGyC0AzytBtGyEtCyB0EtG0BtCtDyCtGzy0B0FyEtCtD0E0CtAtB0CtA2QtN1Q2Zzu0StByCyBtAtN1L2XzutAtFyCtFtCtBtFtCtN1L1CzutN1T1IzuyEtN1B2Z1V1T1S1Nzu&cr=266120674
4	172.24.197.126	unknown user	vsys1	Repeatedly visited (21) the same malicious URL webcompanion.com/nano_download.php?partner=BT170603
4	172.25.51.25	unknown user	vsys1	Repeatedly visited (44) the same malicious URL rokuq.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=ncjbeingokdeimlmolagjaddccfdlkbd&v=1.0.7.50&installsource=notfromwebstore&uc&ap=aflt=wsg_bjfpsso0w0qpy_20_01_ssg00&guid=2f1766be-bc43-4962-a90d-2d601894a16c&cd=2XzuyEtN2Y1L1QzuzyyC0EyC0FyByBzz0BtA0FtC0F0DtAyDtN0D0Tzu0StBzytBtCtN1L2XzuyEtFyDzytFtDtFyDtBtN1L1Czu1ByCtN1L1G1B1V1N2Y1L1Qzu2StD0CyC0E0AtDyEzztGyEyBzyyBtGtB0D0DtBtGyBtC0A0FtGtBtB0EtAyEtCzz0DzztDyByC2QtN1M1F1B2Z1V1N2Y1L1Qzu2S1RzztDzyztCtD1StGtCyCyE1RtGyE1P1R1PtG1TyC1S1StGyE1O1RtA1PtAyByCzz1R1Tzy2QtN0A0LzuyEtN1B2Z1V1T1S1NzutN1Q2Z1B1P1RzutCyDyByBzzyDtAyCyDtD&cr=1343980165
4	172.24.83.140	unknown user	vsys1	Repeatedly visited (28) the same malicious URL necklace.admobe.com/
4	172.25.88.149	unknown user	vsys1	Repeatedly visited (92) the same malicious URL conkac.com/
4	172.24.20.26	unknown user	vsys1	Repeatedly visited (47) the same malicious URL i.kpzip.com/n/kuaizip/strategy_report/kb.xml
4	172.25.89.166	unknown user	vsys1	Repeatedly visited (48) the same malicious URL dogsamily.net/
4	172.25.88.53	unknown user	vsys1	Repeatedly visited (27) the same malicious URL www.aww799.com/
4	172.24.167.179	unknown user	vsys1	Repeatedly visited (27) the same malicious URL socalledsteadilyeducated.com/
4	129.49.26.138	unknown user	vsys1	Repeatedly visited (26) the same malicious URL imp.myquickconverter.com/
4	10.1.235.228	unknown user	vsys1	Repeatedly visited (2219) the same malicious URL yammupiro.top/
4	172.25.53.234	unknown user	vsys1	Repeatedly visited (90) the same malicious URL joyglasses.net/
4	172.25.236.185	unknown user	vsys1	Repeatedly visited (60) the same malicious URL conkac.com/
4	172.24.161.31	unknown user	vsys1	Repeatedly visited (27) the same malicious URL childrencdn.qupeiyin.com/
4	172.24.53.180	unknown user	vsys1	Repeatedly visited (132) the same malicious URL ssoextension.com/
4	172.25.48.195	unknown user	vsys1	Repeatedly visited (48) the same malicious URL socalledsteadilyeducated.com/
4	172.25.56.11	unknown user	vsys1	Repeatedly visited (23) the same malicious URL download.mycouponsmartmac.com/crx/update_extension.php?guid=56464991277290790&source=upd-2020&os=mac&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.83&lang=en-US&acceptformat=crx3&x=id=lfbenaabfliihodeianphjhhhcjgddlh&v=0.0.0.0&installsource=notfromwebstore&installedby=policy&uc
4	172.25.89.194	unknown user	vsys1	Repeatedly visited (21) the same malicious URL go.schjmp.com/
4	172.25.86.91	unknown user	vsys1	Repeatedly visited (64) the same malicious URL api.pdfxd.com/pdf-service/v1/report
4	129.49.218.91	sunysb.edu\jscarola	vsys1	Repeatedly visited (763) the same malicious URL brounelink.com/
4	129.49.218.209	sunysb.edu\adwyer	vsys1	Repeatedly visited (120) the same malicious URL www.cheaterboard.com/
4	172.24.88.132	unknown user	vsys1	Repeatedly visited (54) the same malicious URL www.greedy.world/
4	172.24.49.246	unknown user	vsys1	Repeatedly visited (20) the same malicious URL rowelking.com/
4	10.1.212.124	fkhatun	vsys1	Repeatedly visited (20) the same malicious URL igfap.com/
4	172.25.242.155	unknown user	vsys1	Repeatedly visited (162) the same malicious URL ww1.seehd.uno/
4	129.49.45.251	sunysb.edu\animarino	vsys1	Repeatedly visited (588) the same malicious URL proudflex.org/
4	172.24.162.237	unknown user	vsys1	Repeatedly visited (144) the same malicious URL ww1.seehd.uno/
4	172.25.84.15	unknown user	vsys1	Repeatedly visited (30) the same malicious URL www.aww799.com/
4	172.24.224.199	unknown user	vsys1	Repeatedly visited (22) the same malicious URL js.wpncdn.com/
4	10.255.9.86	unknown user	vsys1	Repeatedly visited (54) the same malicious URL ww1.seehd.uno/
4	10.1.148.40	unknown user	vsys1	Repeatedly visited (23) 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	172.24.128.78	unknown user	vsys1	Repeatedly visited (192) the same malicious URL www.aww799.com/
4	172.24.162.108	unknown user	vsys1	Repeatedly visited (66) the same malicious URL www.greedy.world/
4	172.24.80.108	unknown user	vsys1	Repeatedly visited (21) the same malicious URL socalledsteadilyeducated.com/
4	129.49.93.121	unknown user	vsys1	Repeatedly visited (20) the same malicious URL pt-static1.awepsi.com/
4	172.24.138.196	unknown user	vsys1	Repeatedly visited (104) the same malicious URL www.jlzebszkilcz.ru/
4	172.25.56.174	unknown user	vsys1	Repeatedly visited (45) the same malicious URL socalledsteadilyeducated.com/
4	172.25.91.205	unknown user	vsys1	Repeatedly visited (48) the same malicious URL goverallyhandl.club/
4	172.25.80.239	unknown user	vsys1	Repeatedly visited (50) the same malicious URL ezreward.net/
4	172.25.240.88	unknown user	vsys1	Repeatedly visited (112) the same malicious URL pt-static3.awepsi.com/
4	10.1.146.212	unknown user	vsys1	Repeatedly visited (23) the same malicious URL updates.ijnewhb.com/Update/CheckOnDemand?deviceid=60a474c5-04c1-5aea-bd4f-1490295db15b&Distributer=mctarrev&ChannelId=195&BarcodeId=54319195&country=US&encrypt=false&ismac=true
4	172.24.88.117	unknown user	vsys1	Repeatedly visited (20) the same malicious URL webcf.innovanathinklabs.com/
4	129.49.116.27	unknown user	vsys1	Repeatedly visited (11337) the same malicious URL shopstorys.com/
4	172.24.199.205	unknown user	vsys1	Repeatedly visited (26) the same malicious URL the123movies.stream/
4	172.24.53.92	unknown user	vsys1	Repeatedly visited (77) the same malicious URL down.znshuru.com/smartcloud/svc/cld/tsk.dat
4	172.24.92.125	unknown user	vsys1	Repeatedly visited (66) the same malicious URL www.greedy.world/
4	172.24.20.89	unknown user	vsys1	Repeatedly visited (627) the same malicious URL un-stop.info/wpad.dat?7f62d316717f37a5c4ed6dd10d72322911570884
4	172.25.82.105	unknown user	vsys1	Repeatedly visited (25) the same malicious URL bgtc.mac-autofixer.com/maf/prefs/mafgset.plist
4	10.245.246.6	unknown user	vsys1	Repeatedly visited (22) the same malicious URL acs.pandasoftware.com/retail/psevents/4046/psevents_suite.exe
4	172.24.167.50	unknown user	vsys1	Repeatedly visited (1443) the same malicious URL yammupiro.top/
4	172.24.199.150	unknown user	vsys1	Repeatedly visited (72) the same malicious URL stats.hkijngy.me/StatisticsService.svc/V1/JSON/LogEvent
4	10.255.12.236	unknown user	vsys1	Repeatedly visited (553) the same malicious URL pt-static4.awepsi.com/
4	10.1.218.230	unknown user	vsys1	Repeatedly visited (33) the same malicious URL stats.hkijngy.me/StatisticsService.svc/V1/JSON/LogEvent
4	172.25.87.34	unknown user	vsys1	Repeatedly visited (60) the same malicious URL ssoextension.com/
4	172.24.171.58	unknown user	vsys1	Repeatedly visited (54) the same malicious URL deloplen.com/apu.php?zoneid=1590109

4	10.1.131.132	unknown user	vsys1	Repeatedly visited (22) the same malicious URL secure.electblackdemocrats.org/
4	172.25.94.226	unknown user	vsys1	Repeatedly visited (111) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=8B224F73-9621-5B25-B267-B16F3829C8D4&Distributer=mcmarket&Channelid=003&Barcodeid=53027003&country=US&encrypt=false&ismac=true
4	172.24.128.119	unknown user	vsys1	Repeatedly visited (40) the same malicious URL protectourcoastline.org/
4	172.24.49.160	unknown user	vsys1	Repeatedly visited (30) the same malicious URL browserr.top/
4	172.24.224.164	unknown user	vsys1	Repeatedly visited (64) the same malicious URL dogsamily.net/
4	129.49.16.184	unknown user	vsys1	Repeatedly visited (37) the same malicious URL sync.malwareprotectionlive.com/home/postevents
4	172.25.236.97	unknown user	vsys1	Repeatedly visited (164) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=F32CB536-9A35-5728-A420-EA3DF9CC48A9&Distributer=mcwnet2&Channelid=003&Barcodeid=56043003&country=US&encrypt=false&ismac=true
4	10.1.241.88	ehonisch	vsys1	Repeatedly visited (30) the same malicious URL necklace.admobe.com/
4	172.24.133.192	unknown user	vsys1	Repeatedly visited (104) the same malicious URL socalledsteadilyeducated.com/
4	172.24.160.52	unknown user	vsys1	Repeatedly visited (74) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=0e909f95-9ab5-5b15-a043-b7d75d64f141a&Distributer=mckodioreg&Channelid=003&Barcodeid=54079003&country=US&encrypt=false&ismac=true
4	172.25.92.165	unknown user	vsys1	Repeatedly visited (441) the same malicious URL socalledsteadilyeducated.com/
4	129.49.45.251	unknown user	vsys1	Repeatedly visited (499) the same malicious URL proudflex.org/
4	172.25.139.66	unknown user	vsys1	Repeatedly visited (60) the same malicious URL ww1.seehd.uno/
4	172.24.162.35	unknown user	vsys1	Repeatedly visited (36) the same malicious URL ssoextension.com/
4	172.25.235.35	unknown user	vsys1	Repeatedly visited (21) the same malicious URL go.schjmp.com/
4	172.24.113.88	unknown user	vsys1	Repeatedly visited (21) the same malicious URL www.aww799.com/
4	172.24.161.200	unknown user	vsys1	Repeatedly visited (85) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=E26F37A4-9D3F-5AB1-8032-0E1CB84DDCBC&Distributer=mctarev&Channelid=198&Barcodeid=54319198&country=US&encrypt=false&ismac=true
4	129.49.112.247	unknown user	vsys1	Repeatedly visited (387) the same malicious URL ssoextension.com/
4	172.24.50.221	unknown user	vsys1	Repeatedly visited (78) the same malicious URL browserr.top/
4	172.24.48.242	unknown user	vsys1	Repeatedly visited (36) the same malicious URL new.edu/
4	172.25.113.79	unknown user	vsys1	Repeatedly visited (92) the same malicious URL schoolofgamedesign.com/
4	10.245.201.243	unknown user	vsys1	Repeatedly visited (46) the same malicious URL runnewlevel.com/
4	172.25.50.133	unknown user	vsys1	Repeatedly visited (89) the same malicious URL updates.jnewhb.com/Update/CheckOnDemand?deviceid=002D073E-420C-5E93-A0C6-CDE365165A0F&Distributer=mctarev&Channelid=195&Barcodeid=54319195&country=US&encrypt=false&ismac=true
4	172.24.224.183	unknown user	vsys1	Repeatedly visited (40) the same malicious URL www.aww799.com/lion-update
4	172.24.17.52	unknown user	vsys1	Repeatedly visited (29) the same malicious URL un-stop.info/wpad.dat?7f62d31671737a5c4ed6dd10d72322911570884
4	172.25.85.247	unknown user	vsys1	Repeatedly visited (535) the same malicious URL watchseries1.bypassed.eu/
4	10.245.215.208	unknown user	vsys1	Repeatedly visited (26) the same malicious URL necklace.admobe.com/
4	172.24.134.231	unknown user	vsys1	Repeatedly visited (48) the same malicious URL www.greedy.world/
4	172.24.56.1	unknown user	vsys1	Repeatedly visited (28) the same malicious URL www.truyen-hentai.com/
4	172.25.86.47	unknown user	vsys1	Repeatedly visited (108) the same malicious URL ssoextension.com/
4	129.49.32.208	unknown user	vsys1	Repeatedly visited (45) the same malicious URL rokug.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=ncjbeingokdeimlmolajjaddccfdkbdk&v=1.0.7.50&installsource=notfromwebstore&uc&ap=aflt=wsg_iuqrpx79bdfh2f8qhjnpt2g_19_47_ssg00&guid=2def0055-452c-4762-9725-44d108c533af&cdr=2KzuyEiNZY1L1QzuICzzyCyC0D0AiDA0DtByE0EtD0EtD0BtN0D0Tzu0StBzzzzzBtN1L2KzuyEiFyDyBtFiDFyByDtN1L1Czu1BtOiN1L1G1B1V1N2Y1L1QzuJSyE0B0AyDyE0CzyyEtGyByCyOtDiDy60CtByCtGy00AtByDtDyEtD0AyDzy2QtN1M1FtB2Z1Y1N2Y1L1QzuJSyE0B0AyDyE0CzyyEtGyByCyOtDiDy60CtByCtGy00AtByDtDyEtD0AyDzy2QtN1M1FtB2Z1Y1N2Y1L1QzuJStDAtiDtDAyD1TtDtG1Ty01R1RtGyEtBtByCtG1S1Q1S1StG1D1StD1RyE1T1tQzyyE1T1Q2QtN0A0LzuyEtN1B2Z1Y1T1S1NztuttN1Q2Z1B1P1RzuiCyDyByEyCyCyDzytDtD&cr=2129661699
2	80.82.77.193	unknown user	vsys1	Unknown UDP traffic
2	103.231.146.242	unknown user	vsys1	Unknown UDP traffic
2	203.171.245.119	unknown user	vsys1	Unknown UDP traffic
2	218.241.82.20	unknown user	vsys1	Unknown UDP traffic
2	202.142.102.195	unknown user	vsys1	Unknown UDP traffic
2	58.216.139.181	unknown user	vsys1	Unknown UDP traffic
2	80.82.78.100	unknown user	vsys1	Unknown UDP traffic
2	89.248.168.217	unknown user	vsys1	Unknown UDP traffic
2	106.75.7.109	unknown user	vsys1	Unknown UDP traffic
2	139.162.126.103	unknown user	vsys1	Unknown UDP traffic
1	172.24.115.71	unknown user	vsys1	Visited malware URL www.syxo.ga/
1	172.25.85.220	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=-3473429
1	10.1.183.200	unknown user	vsys1	Visited malware URL arloreed.com/
1	10.1.252.102	kmuff	vsys1	Visited malware URL www.celebritieswith.com/wp-content/uploads/2017/10/Joe-Biden-Plastic-Surgery.jpg
1	172.24.131.169	unknown user	vsys1	Visited malware URL www.rtbdem.com/redirect.php?aff=3355448&incent=0&gaid=&aff_sub=C_ODBhMDMyOnJ0YjpyNzMzMDM1MzoyNTAwOjYwNDg6dXM=_C&idfa=&id=27330353&type=CPI&adult=0&aff_sub2=a6XeeHocQlaJb7gWz_ILtA&demand=129&s1=[sourceapp]
1	172.24.49.163	unknown user	vsys1	Visited malware URL necklace.admobe.com/
1	172.24.88.89	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=92694&aff_sub2=ir_i58LWX1v1maOPnoQHoDYZP4UsjNFP&aff_sub5=82&gaid=&aid=&app_id=
1	172.25.87.27	unknown user	vsys1	Visited malware URL africanwritershq.com/
1	172.25.236.201	unknown user	vsys1	Visited malware URL 110.43.81.34/jquery/754558096
1	172.24.48.58	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=92694&aff_sub2=ir_ZZvVYnyAWAocSm6_f-lbbQrauzUwvM7N&aff_sub5=82&gaid=&aid=&app_id=
1	172.24.161.30	unknown user	vsys1	Visited malware URL pt-static3.awepsi.com/
1	172.24.16.104	unknown user	vsys1	Visited malware URL dolohen.com/afu.php?zoneid=2627325
1	172.24.168.136	unknown user	vsys1	Visited malware URL www.boesten.com/?type=iaf&pub_id=4101&sub_id=5f5704c43579c80001f961a1&srcid=331_2129699-2614096103-0
1	129.49.37.116	unknown user	vsys1	Visited malware URL svblqg.info/
1	172.24.81.119	unknown user	vsys1	Visited malware URL menu.admobe.com/
1	172.24.85.30	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	172.24.82.37	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=92694&aff_sub2=ir_ZaSOjlk3zrtK1T6mp9k4ft5asrmmr8h&aff_sub5=82&gaid=&aid=&app_id=
1	172.25.247.238	unknown user	vsys1	Visited malware URL pcacceleratepro.com/clamav.php
1	172.24.225.153	unknown user	vsys1	Visited malware URL m.bsjuge.info/82_62245/
1	172.25.232.57	unknown user	vsys1	Visited malware URL vc.airdropanalytics.com/
1	172.24.166.20	unknown user	vsys1	Visited malware URL js.wpncdn.com/

1	172.24.21.106	unknown user	vsys1	Visited malware URL smart.maroolatrack.com/
1	172.24.20.178	unknown user	vsys1	Visited malware URL guay.labtrffc.com/
1	10.1.227.150	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=9269&aff_sub2=tr_33EjzOMOjwFiuQOMjiHRed6f_3XqPNjZ&aff_sub5=82&gaid=&aid=&app_id=
1	172.24.225.198	unknown user	vsys1	Visited malware URL wap.ylxdtww.com/encrypt/t/g
1	10.1.185.103	unknown user	vsys1	Visited malware URL bgtc.mac-autofixer.com/maf/db/db_adw_mac.db
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	172.24.160.224	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=9269&aff_sub2=tr_jlgFHpbaH4DNyrfhoGd9NawQIwlD5t7U&aff_sub5=82&gaid=&aid=&app_id=
1	172.25.89.144	unknown user	vsys1	Visited malware URL xml.hueadsxml.com/click?i=rx*OA2AEFGM_0
1	172.24.18.244	unknown user	vsys1	Visited malware URL js.wpncdn.com/
1	172.24.82.243	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=9269&aff_sub2=tr_UVEm27udt6HVMb_Hq4aGsS7fJVmB6uFI&aff_sub5=82&gaid=&aid=&app_id=
1	172.24.21.148	unknown user	vsys1	Visited malware URL pt-static3.awepsi.com/
1	172.24.193.45	unknown user	vsys1	Visited malware URL socalledsteadilyeducated.com/
1	10.1.195.172	rsamulyak	vsys1	Visited malware URL xml.hueadsxml.com/click?i=7nWOy*FAqQ8_0
1	10.1.245.87	unknown user	vsys1	Visited malware URL errors.newdatastatsserv.com/mac-error.gif?msg=Safari%20version%2013.1.2%20is%20not%20supported&funcName=WebSocketServerApp::main&errtype=WSSException&os=mac_10_14_6&ibic=E3A67785CAB8422FB2C8F8C7740A489A&rnd=1599578609048864
1	172.24.202.30	unknown user	vsys1	Visited malware URL popcorntimeupd.xyz/?app_id=T4P_SEM&hid=3d1c0ed5bca3c8a234f558afe80229b2&ver=UNKNOWN&os=OSX101506
1	172.25.245.151	unknown user	vsys1	Visited malware URL pt-static3.awepsi.com/
1	172.25.57.176	unknown user	vsys1	Visited malware URL cdn2121.advancedmaccleaner.com/amc/prefs/webSettings_us.plist
1	129.49.12.10	sunysb.edu\jjmaher	vsys1	Visited malware URL bullseye-electric.nuresponse.com/wp-content/uploads/2009/12/ar120674869004739.jpg
1	172.25.85.235	unknown user	vsys1	Visited malware URL go.eroadvertising.com/eactrl.go
1	172.25.88.35	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	129.49.83.137	unknown user	vsys1	Visited malware URL 180.163.222.153/cloudquery.php
1	172.25.91.75	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	185.177.126.181	unknown user	vsys1	Visited malware URL check2.zennolab.com/proxy.php
1	172.24.164.227	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=165879947&affiliate_id=11023&aid={idfa}&device_id={device_id}&aff_sub2=5f576cfdd6efcf0001642270&aff_sub5=108&{gaid}=&{aid}=&{app_id}=countdown+%20ios%20lite
1	10.245.236.48	unknown user	vsys1	Visited malware URL 185.130.105.66:998/
1	172.25.113.34	unknown user	vsys1	Visited malware URL popcorntimeupd.xyz/?app_id=T4P_SEM&hid=5d99114b739c4cfd2ba4e81ce6f76512&ver=5.6&os=OSX101506
1	172.25.84.26	unknown user	vsys1	Visited malware URL cloneclicks.com/
1	172.25.151.162	unknown user	vsys1	Visited malware URL img.vim-cn.com/
1	172.24.113.129	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=9269&aff_sub2=tr_HoF2bD5eCayc5baaoxuUGLb0c3VEObVy&aff_sub5=82&gaid=&aid=&app_id=
1	172.25.82.100	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	172.24.16.77	unknown user	vsys1	Visited malware URL ouslayer.co/c/Dq9b6Gbj2t5qlxSdWbQR9HMojagL1/NYT/QtyyN/Ss0jyZOiDHUP1-NbDsYp5q
1	172.25.52.40	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	172.25.243.159	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=165879947&affiliate_id=9269&aff_sub2=tr_o0uXETxKzC0xkMP2zSTr71RNkwbsejQP&aff_sub5=82&gaid=&aid=&app_id=FFC9F125-1937-4F2D-9DBE-196BF8DFC56C
1	10.1.171.82	unknown user	vsys1	Visited malware URL www.greedy.world/
1	10.1.230.73	alcchan	vsys1	Visited malware URL socalledsteadilyeducated.com/
1	172.25.89.212	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=165879947&affiliate_id=11023&aid={idfa}&device_id={device_id}&aff_sub2=5f57040b26106300019fef19&aff_sub5=108&{gaid}=&{aid}=&{app_id}=scan%20and%20print_cfl_ios_1017261655
1	172.25.49.54	unknown user	vsys1	Visited malware URL pt-static3.awepsi.com/
1	172.25.241.88	unknown user	vsys1	Visited malware URL stats.hkijngy.me/StatisticsService.svc/V1/JSON/LogEvent
1	172.24.85.15	unknown user	vsys1	Visited malware URL watchtvseries.unblckd.ist/search/Harley+Quinn
1	172.25.233.109	unknown user	vsys1	Visited malware URL popcorntime-update.xyz/?app_id=T4P_SEM&hid=945a6265f7dc1cf6e587c35813eacbd0&ver=6.1.2&os=OSX101504
1	172.25.242.116	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=165879947&affiliate_id=11023&aid={idfa}&device_id={device_id}&aff_sub2=5f579793d6efcf0001ea71eb&aff_sub5=108&{gaid}=&{aid}=&{app_id}=stack%20fall%20ios
1	10.255.4.131	unknown user	vsys1	Visited malware URL pudacasa.com/update?os=mac&arch=x64&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=57.0.2987.110&lang=en-US&x=id=ljnfpiodfojmjfbiechgkbkhikfbknjc&v=15.13.25.53&installsource=notfromwebstore&uc&ap=aflt=mcx_sgnsft_18_40_ssg0210&guid=6d34195e-a1f0-492d-b9e5-d0eb95259567&xlp_sess_guid=6d34195e-a1f0-492d-b9e5-d0eb95259567&client=chromium&cd=2XzuyEtN2Y1L1QzutA0FtD0CyEtB0ByEtGyB0FtDtBtGyDzyyB0CtGzzyEzz0DtGtAyC0B0BzztB0D0BtDtDyCyCtN1L1G1B1V1N2Y1L1Qzu2StC0F0E0AzztCyEzztG0C0E0FyBtGyEyDtC0CtGzy0FtDtCtGtB0AyDtByB0ByCzytAtCyEtD2QtN1Q2Zzu0StByEyCzytN1L2XzutAtFyDtFzyzztFtCtN1L1CzutN1T1IzuyEtN1B2Z1V1T1S1Nzu&cr=406090226
1	172.24.17.4	unknown user	vsys1	Visited malware URL appservices.in/engine/gcm/requestgcm?engv=4
1	10.245.240.224	unknown user	vsys1	Visited malware URL cdnrep.reimage.com/downloader_version.xml
1	172.24.21.61	unknown user	vsys1	Visited malware URL smart.maroolatrack.com/
1	172.25.82.157	unknown user	vsys1	Visited malware URL socalledsteadilyeducated.com/
1	10.1.134.102	unknown user	vsys1	Visited malware URL static.json.koreabt.com/
1	10.1.171.84	mhono	vsys1	Visited malware URL socalledsteadilyeducated.com/
1	172.24.83.171	unknown user	vsys1	Visited malware URL app.sizeswatch.com/
1	172.25.49.150	unknown user	vsys1	Visited malware URL www.maxroseforcongress.com/
1	172.24.53.152	unknown user	vsys1	Visited malware URL socalledsteadilyeducated.com/
1	172.25.85.219	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	172.24.17.42	unknown user	vsys1	Visited malware URL greatandfreestuff.com/software/download/sot.php?file=&title=abdul%20kalam%20speech%20in%20english%20pdf
1	172.25.57.179	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	172.25.81.179	unknown user	vsys1	Visited malware URL popcorntimeupd.xyz/?app_id=T4P_SEM&hid=129c9727fc1c2d1a8acf70aeca17d350&ver=UNKNOWN&os=OSX101502
1	172.24.21.12	unknown user	vsys1	Visited malware URL www.computermumbai.com/upg/341DB/updver.bin
1	172.25.148.33	unknown user	vsys1	Visited malware URL skype-soft.com/download/?affiliate_id=000219&wv=60300&wi=f43d51d1-e531-4c9c-a7d4-2f9f2ae31659&wx=x64
1	10.1.166.20	rojones	vsys1	Visited malware URL platform-liquid.onrender.com/
1	172.24.138.18	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=165879947&affiliate_id=11023&aid={idfa}&device_id={device_id}&aff_sub2=5f578358d6efcf0001a13ac8&aff_sub5=108&{gaid}=&{aid}=&{app_id}=freecell%20%e2%96%bb%20solitaire
1	172.25.245.240	unknown user	vsys1	Visited malware URL popcorntime-update.xyz/?app_id=T4PSEC&hid=fb43c1716bfdfd0cd25b8dc5d29fd73e&ver=UNKNOWN&os=WIN060200
1	147.30.161.85	unknown user	vsys1	Visited malware URL check2.zennolab.com/proxy.php
1	172.24.138.20	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=165879947&affiliate_id=11023&aid={idfa}&device_id={device_id}&aff_sub2=5f5701d626106300010a7a7d&aff_sub5=108&{gaid}=&{aid}=&{app_id}=narde%20-%20classic%20backgammon%20online%20(long%20narde)%20free

1	172.25.114.255	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=16587994?&affiliate_id=11023&aid=|dfa|&device_id=|device_id|&aff_sub2=5157150d261083000136a2f4&aff_sub5=108&|gaid|=CAA4A628-9D74-40F6-82F3-E5D0EA0535A0&|aidj|=CAA4A628-9D74-40F6-82F3-E5D0EA0535A0&|app_id|=iFunny%20iOS
1	172.24.48.106	unknown user	vsys1	Visited malware URL adro.pro/ad/ad?rp=1984738&e=5794388d-27b71aad96275322a8f3-1596098537579438&s=247683.259889
1	172.25.236.57	unknown user	vsys1	Visited malware URL popcornfirmeupd.xyz/?app_id=T4P_SEM&hid=f0681491dc04b9f78b0413b0364218364&ver=UNKNOWN&os=OSX101505
1	172.25.247.156	unknown user	vsys1	Visited malware URL cdn.belgorebysson.club/aju.php?zoneid=-3473429
1	172.25.245.117	unknown user	vsys1	Visited malware URL xml.hueadsxml.com/click?i=UNcHndqrTOY_0
1	10.1.157.221	unknown user	vsys1	Visited malware URL rtb-useast.bidmygps.xyz/
1	172.25.233.5	unknown user	vsys1	Visited malware URL jschart.org/c/libs/ga.js
1	10.1.243.114	unknown user	vsys1	Visited malware URL 110.43.81.34/jquery/780664750
1	172.25.50.141	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	172.24.224.229	unknown user	vsys1	Visited malware URL js.wpncdn.com/
1	172.24.19.34	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	172.24.17.199	unknown user	vsys1	Visited malware URL cash.admobe.com/
1	172.24.167.7	unknown user	vsys1	Visited malware URL click.howdoesin.net/aff_track?offer_id=16587994?&affiliate_id=11023&aid=|dfa|&device_id=|device_id|&aff_sub2=5f57f6f3d6efcf0001ae646&aff_sub5=108&|gaid|=&|aidj|=&|app_id|=ip%20cam%20viewer%20lite%20ios
1	172.25.53.18	unknown user	vsys1	Visited malware URL ww1.seehd.uno/
1	172.25.83.218	unknown user	vsys1	Visited malware URL watchtvseries.unblckd.ist/search/The+100
1	172.25.241.142	unknown user	vsys1	Visited malware URL socalledsteadyeducated.com/
1	10.1.243.68	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=16587994?&affiliate_id=92694&aff_sub2=ir_nTrOHA5eLVY-yW7XYaocqJMsKTAcjqLp&aff_sub5=82&gaid=&aid=&app_id=
1	10.255.8.92	unknown user	vsys1	Visited malware URL tracker.yougotupdated.com/statistics/event?origin=updater&invcd=1&name=offer_started&mid=C3340E637B4DDD11E85B9E1E2B1AE4B75&vid=5f9d5190-d760-11ea-949d-6be38ecfe00b&atname=offer_id&atval=4&attname=offer_version&atval=1.1.8&attname=method&atval=run
1	183.101.52.42	unknown user	vsys1	Visited malware URL 94.102.54.78:8080/tmUnblock.cgi
1	83.142.167.28	unknown user	vsys1	Visited malware URL check2.zennolab.com/proxy.php
1	172.25.84.2	unknown user	vsys1	Visited malware URL track.aqcxa.com/aff_c?offer_id=501&aff_id=-239?&aff_sub=42679&aff_sub2=v03040001131adcb61c824f2416c8d215a806200c590&aff_click_id=-1024368fc326dd1a9882d88d4d307b
1	10.1.183.69	unknown user	vsys1	Visited malware URL www.greedy.world/
1	172.24.55.245	unknown user	vsys1	Visited malware URL zazalanosette.com/
1	172.25.235.182	unknown user	vsys1	Visited malware URL reddit.tube/
1	10.1.214.30	unknown user	vsys1	Visited malware URL cdn2121.advancedmaccleaner.com/amc/prefs/webSettings_us.plist
1	172.25.234.203	unknown user	vsys1	Visited malware URL get.mediart.space/
1	172.25.87.5	unknown user	vsys1	Visited malware URL graniteacquitcharacteristic.com/3133db3094273140d1de8027d8310778/invoke.js
1	172.25.139.81	unknown user	vsys1	Visited malware URL veganyumyum.com/2012/11/kitsune-soba/index.html
1	172.24.21.182	unknown user	vsys1	Visited malware URL www.fudtroll.com/
1	172.25.53.140	unknown user	vsys1	Visited malware URL pl-static1.awepsi.com/
1	172.25.237.164	unknown user	vsys1	Visited malware URL cash.admobe.com/
1	172.25.112.73	unknown user	vsys1	Visited malware URL arloreed.com/
1	10.1.133.239	unknown user	vsys1	Visited malware URL socalledsteadyeducated.com/
1	172.25.52.247	unknown user	vsys1	Visited malware URL arloreed.com/
1	172.24.135.56	unknown user	vsys1	Visited malware URL megaanswers.com/images_uploaded/Why%20do%20we%20have%20a%20small%20white%20area%20at%20the%20base%20of%20our%20finger%20nails.jpg
1	172.24.192.226	unknown user	vsys1	Visited malware URL getessay.net/
1	172.24.56.7	unknown user	vsys1	Visited malware URL idgod.ch/
1	172.24.167.214	unknown user	vsys1	Visited malware URL go.ezyhmp.com/
1	10.1.162.116	unknown user	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	10.1.166.34	unknown user	vsys1	Visited malware URL www.aww799.com/
1	10.1.143.121	roshayes	vsys1	Visited malware URL makemoney.mobu-app.com:60001/
1	172.24.19.40	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	172.25.86.92	unknown user	vsys1	Visited malware URL schoolofgamedesign.com/
1	172.25.81.206	unknown user	vsys1	Visited malware URL socalledsteadyeducated.com/
1	172.24.116.164	unknown user	vsys1	Visited malware URL portalas.org/scripts/tts/audio/recs/point1sec.mp3
1	129.49.117.33	unknown user	vsys1	Visited malware URL 104.192.108.109/cloudquery.php
1	172.24.18.166	unknown user	vsys1	Visited malware URL www.fudtroll.com/
1	10.1.157.186	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=16587994?&affiliate_id=92694&aff_sub2=ir_v5muFzX_SXi_PKW4x6UaDApcKXh1oYz&aff_sub5=82&gaid=&aid=&app_id=
1	172.24.88.191	unknown user	vsys1	Visited malware URL go.eroadvertising.com/
1	10.1.156.78	unknown user	vsys1	Visited malware URL socalledsteadyeducated.com/
1	172.25.49.178	unknown user	vsys1	Visited malware URL www.aww799.com/squirrel-log
1	10.1.167.92	unknown user	vsys1	Visited malware URL wwzon.com/
1	10.1.167.45	unknown user	vsys1	Visited malware URL bgtc.mac-autofixer.com/maf/prefs/mafgset.plist
1	172.24.19.37	unknown user	vsys1	Visited malware URL necklace.admobe.com/
1	10.1.150.177	haozhu1	vsys1	Visited malware URL www.aww799.com/squirrel-log
1	172.24.196.198	unknown user	vsys1	Visited malware URL js.sofdl.360pcdn.com/soft_web_download.min.js
1	172.24.202.22	unknown user	vsys1	Visited malware URL www25.gogoanimes.tv/
1	172.24.22.106	unknown user	vsys1	Visited malware URL action.runningbaduza.com/
1	172.24.133.206	unknown user	vsys1	Visited malware URL www.syxo.ga/
1	10.1.143.102	jingju	vsys1	Visited malware URL www.aww799.com/doggy-update/109770679/b0105318b6c4ea4b31945ca5371code0a50956b
1	172.25.235.129	unknown user	vsys1	Visited malware URL bgtc.mac-autofixer.com/maf/prefs/mafgset.plist
1	172.24.169.137	unknown user	vsys1	Visited malware URL click.tracksummer.com/aff_c?offer_id=16587994?&affiliate_id=92694&aff_sub2=ir_ca_IWDju7rWpqxDavcUNyfdh2VLhLKx8&aff_sub5=82&gaid=&aid=&app_id=

1	172.24.225.24	unknown user	vsys1	Visited malware URL 104.192.108.154/cloudquery.php
1	10.1.133.201	unknown user	vsys1	Visited malware URL arloreed.com/
1	10.1.236.209	unknown user	vsys1	Visited malware URL necklace.admobe.com/
1	10.245.202.16	unknown user	vsys1	Visited malware URL creative.schjmp.com/
1	172.24.201.236	unknown user	vsys1	Visited malware URL xml.admeridianads.com/click?i=Lxww1NP1qLM_0
1	172.24.225.140	unknown user	vsys1	Visited malware URL pl-static3.awepsi.com/
1	172.24.201.86	unknown user	vsys1	Visited malware URL cdn.betgorebysson.club/apu.php?zoneid=3473429
1	130.245.192.1	unknown user	vsys1	Visited malware URL ajax.gstatic.info/ajax/libs/bootstrap.js
1	10.1.155.223	unknown user	vsys1	Visited malware URL www.aww799.com/lion-update