

Domains

1.google[.]ph - C&C server
12371829hkdanm[.]fbi.am - C&C server
139[.]5.202.82 - C&C server
149[.]28.31.166 - C&C server
1qw6etagydbn2peifj8hf[.]fbi.am - C&C server
2.google[.]ph - C&C server
3.google[.]ph - C&C server
42[.]200.181.116 - Disease vector
45[.]76.199.119 - C&C server
45[.]77.22.215 - C&C server
adobe-flash[.]wiki - Disease vector
adobe[.]name - C&C server
agph[.]jivi66.net - C&C server
bos[.]github.wiki - C&C server
caonimade[.]11i.me - C&C server
d[.]github.wiki - Disease vector
darknet[.]rootkit.tools - C&C server
darwin[.]github.wiki - C&C server
download[.]mircrosoftscoulds.com - C&C server
dust[.]github.wiki - C&C server
exmail[.]googie.com.ph - C&C server
fbi[.]fuckbc.com - C&C server
flash[.]wy886066.com - C&C server
fuckeryoumm[.]nmb.bet - C&C server
fuckyou[.]fbi.am - C&C server
gb[.]googie.ph - C&C server
helloworld[.]11i.me - C&C server
helloworld[.]daj8.me - C&C server
hk.whoamis[.]info - C&C server
hk dust[.]github.wiki - C&C server
huaidan[.]fbi.am - C&C server
linux[.]daj8.me - C&C server
linux[.]daji8.me - C&C server
linux[.]shoppingchina.net - C&C server
linux[.]wy01.com - C&C server
linux[.]wy01.vip - C&C server

linux1[.]shoppingchina.net - C&C server
linux2[.]shoppingchina.net - C&C server
list[.]whoamis.info - C&C server
localhost[.]11i.me - C&C server
mail[.]whoamis.info - C&C server
mmimdown[.]oss-cn-hongkong.aliyuncs.com - Disease vector
mmr[.]whoamis.info - C&C server
poer[.]whoamis.info - C&C server
rc[.]dajuw.com - C&C server
rootkit[.]tools - C&C server
shoppingchina[.]net - C&C server
steam[.]dajuw.com - C&C server
test[.]microsoftscoulds.com - C&C server
tools[.]daji8.me - C&C server
update[.]adobe.wiki - Disease vector
win[.]googie.ph - C&C server
wmgnews[.]daji8.me - C&C server
wps[.]daj8.me - C&C server
wpsup[.]daj8.me - C&C server
www[.]adobe.name - C&C server
www[.]whoamis.info - C&C server
yabo[.]googie.ph