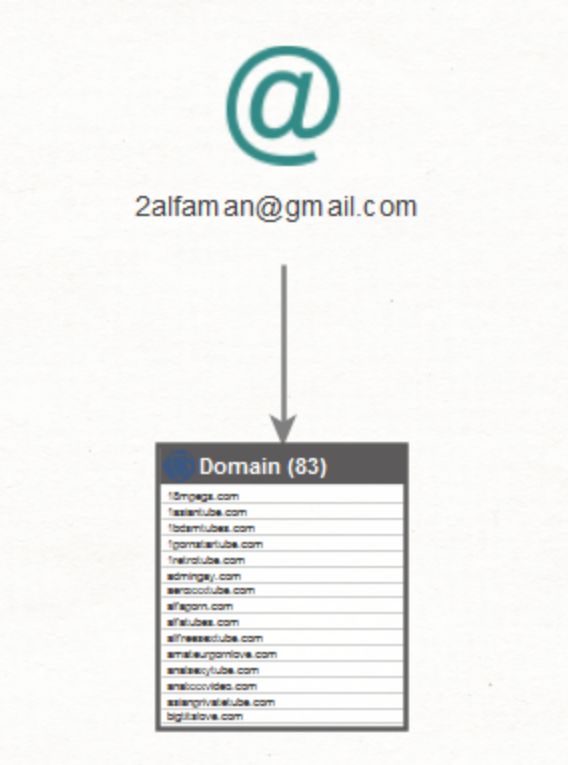
00. Exposing a Currently Active Free Rogue VPN Domains Portfolio Courtesy of the NSA - An OSINT Analysis



01. Introduction to WHOIS XML API

WhoisXML API is one of the Web's and the security industry's primary destinations for threat intelligence and cybercrime research including OSINT type of domain, IP, and current and historical WHOIS data records with billions of domain IP and WHOIS records within WhoisXML API's database where novice and experienced cybercrime researchers threat intelligence analysts including OSINT experts and analysts should consider adopting WhoisXML API's in their arsenal of OSINT tools and public database repositories and databases largely considering the tool as their primary information source and threat intelligence gathering tool and publicly accessible database in terms of using it in their current and ongoing OSINT and cybercrime including threat intelligence type of investigations.

02. How to get a proper account

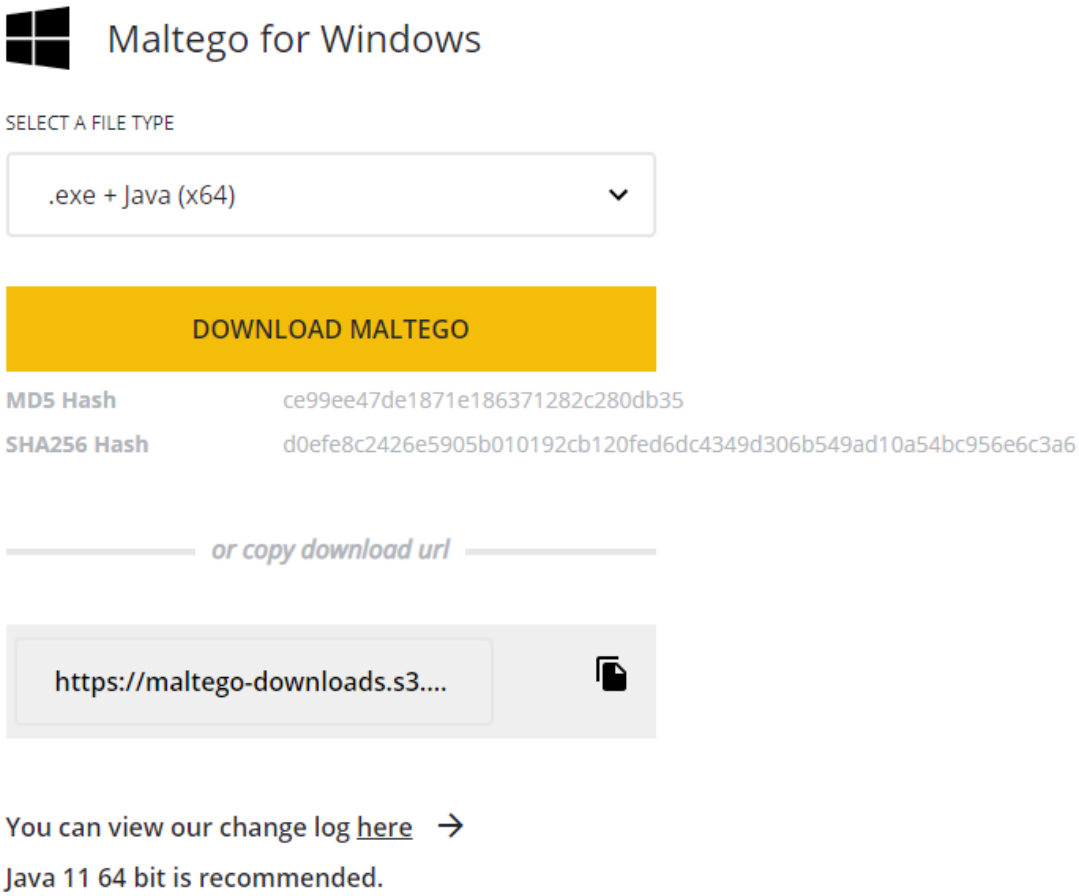
Cybercrime researchers and threat intelligence analysts interested in obtaining access to one of the Web's and the industry's most comprehensive and in-depth data set of real-time and historical domain IP and WHOIS information should grab an account from the following URL - https://main.whoisxmlapi.com/signup for the purpose of beginning their OSINT and cybercrime research including their threat hunting and threat intelligence gathering process.

Product	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6	Units
WHOIS and Bulk WHOIS	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
Domain Availability	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
IP Geolocation	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
IP Netblocks	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
DNS Lookup	100,000	200,000	500,000	1,000,000	2,000,000	4,000,000	Monthly queries
Email Verification	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Domain Reputation	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Website Categorization	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Website Contacts	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries

Sample WhoisXML API Pricing Plans Web Site

03. How to install Maltego

For the purpose of this case study we'll use the popular OSINT gathering and enrichment tool Maltego which you can grab from the following URL - https://www.maltego.com/downloads/ on your way to begin using and utilizing WhoisXML API's advanced domain IP and historical and current WHOIS information and one of the Web's and the industry's most comprehensive and in-depth database.



Sample Maltego Download Web Site

04. How to use the WHOIS XML API Maltego Integration

Before using Maltego, users should follow the instructions and grab a proper WhoisXML API account which they can later one use for the actual research and OSINT research and analysis including the actual enrichment process.

05. The Case Study

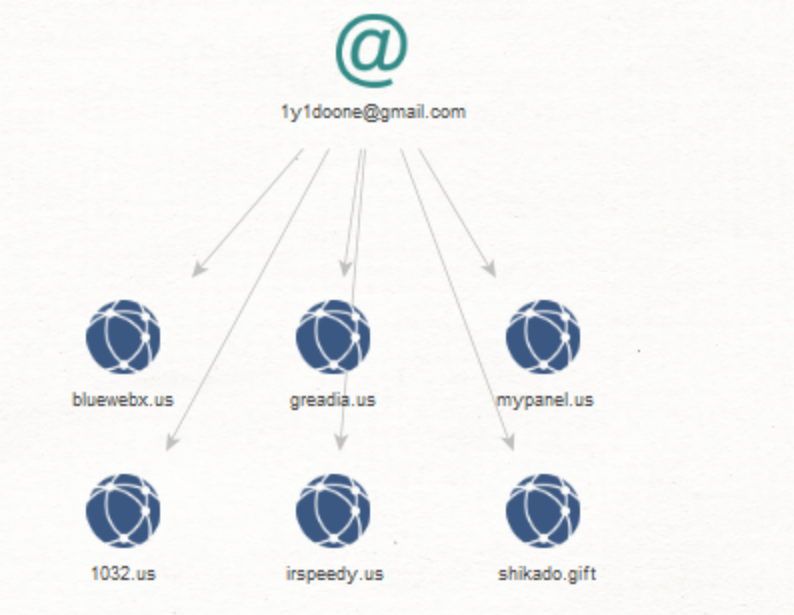
We've recently come across a currently active free VPN domains portfolio which based on our research and publicly accessible sources appears to be run and operated by the NSA where the ultimate goal would be to trick users into using these rogue and bogus free VPN service providers in particular Iran-based users where the ultimate goal would be to monitor and eavesdrop on their Internet activities and we've decided to take a deeper look inside the Internet-connected infrastructure of these domains and offer practical and relevant threat intelligence and cyber-attack attribution details on the true origins of the campaign.

In this case study we'll offer practical and relevant technical information on the Internet-connected infrastructure of this campaign with the idea to assist the security community on its way to track down and monitor this campaign including to offer actual cyber-attack and cyber campaign attribution clues which could come handy to a security researcher or a threat intelligence analyst on their way to track down and monitor the campaign.

Original rogue portfolio of fake VPN service domains courtesy of the NSA:

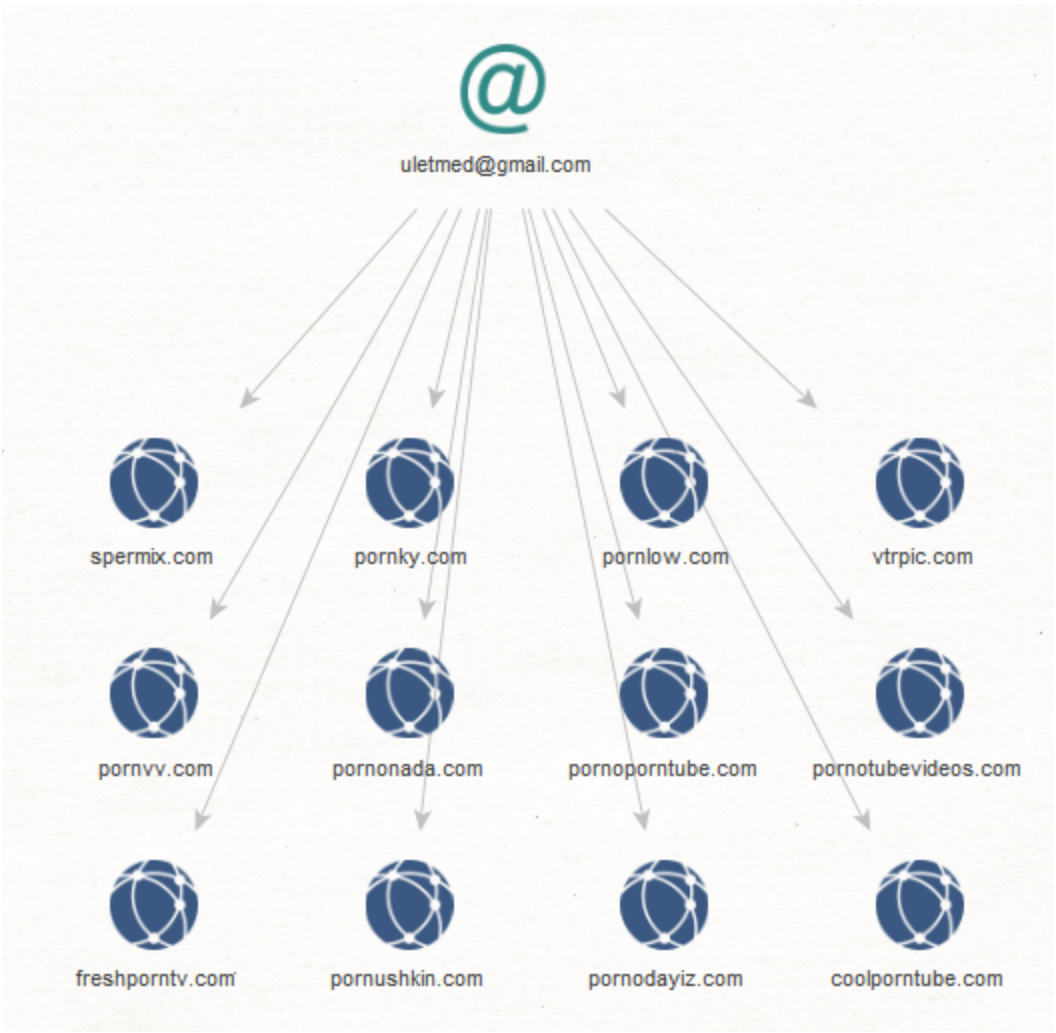
bluewebx[.]com
bluewebx[.]us
irs1[.]ga
iranianvpn[.]net
IRSV[.]ME

DNSSPEEDY[.]TK
ironvpn[.]tk
ironvpn[.]pw
irgomake[.]win
make-account[.]us
make-account[.]ir
IRANTUNEL[.]COM
JET-VPN[.]COM
newhost[.]ir
homeunix[.]net
vpnmakers[.]com
hidethisip[.]info
uk[.]myfastport[.]com
witopia[.]net
worldserver[.]in
music30ty[.]net
misconfused[.]org
privatetunnel[.]com
aseman-sky[.]in



Related domain registrant email addresses known to have been involved in the campaign:
zodaraxe@yandex[.]com
2alfaman@gmail[.]com
rossma@aliyun[.]com

uletmed@gmail[.]com
xy168899@gmail[.]com
baoma123654@gmail[.]com
88guaji@gmail[.]com
deshintawiida@gmail[.]com
2710282345@qq[.]com
youji364558@163[.]com
ngelaa337@gmail[.]com
THEPOUTHOOEB@HOTMAIL[.]COM
michalrestl@email[.]cz
cfwwx2@126[.]com
20702176@qq[.]com
ljytyhdeai@foxmail[.]com
2140426952@qq[.]com
marocsofiane20@gmail[.]com
17891750@qq[.]com
moniqueburorb@yahoo[.]com
rayyxy@163[.]com
chaxun@dispostable[.]com

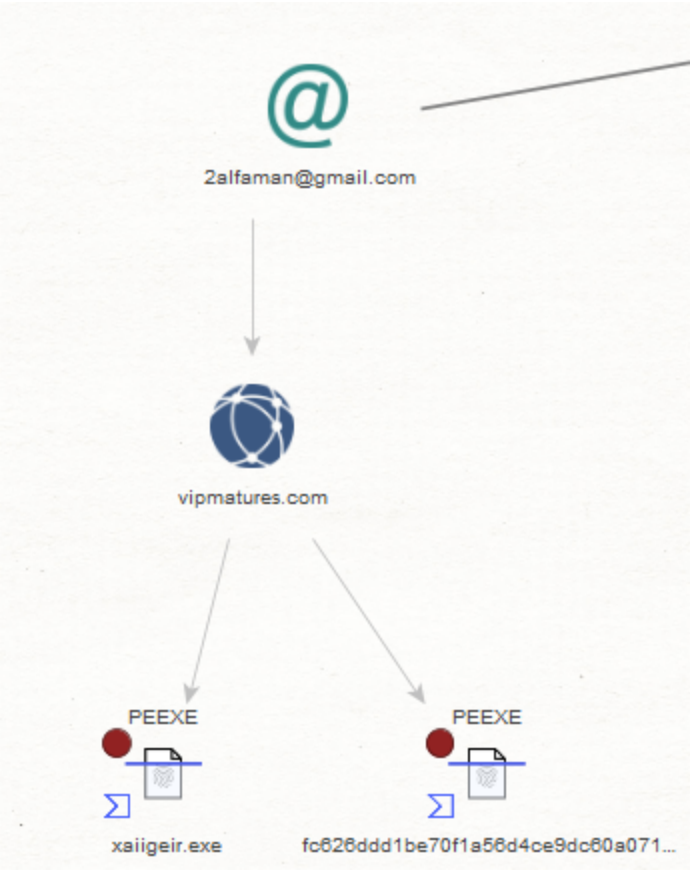


Related domains known to have been involved in the campaign:

gaysexvideo[.]us
keezmovies[.]us
hitporntube[.]com
enjoyfreesex[.]com
allfreesextube[.]com
thegaytubes[.]com
sextubeshop[.]com
pornfetishexxx[.]com
ebonypornox[.]com
freepornpig[.]com
marriagesextube[.]com
searchporntubes[.]com
suckporntube[.]com
darlingmatures[.]com

pornretrotube[.]com
teensexfusion[.]net
rough18[.]us
teendorf[.]us
1retrotube[.]com
typeteam[.]com
biosextube[.]com
hadcoreporntube[.]com
reporntube[.]com
telltake[.]com
asianprivatetube[.]com
hostednude[.]com
alfaporn[.]com
sexbring[.]com
porntubem[.]com
newerotictube[.]com
firstretrotube[.]com
oralsexlove[.]com
1bdsmtubes[.]com
hairytubeporn[.]com
brunettetubex[.]com
tubelatinaporn[.]com
xxxgaytubes[.]com
analxxxvideo[.]com
analsexytube[.]com
aeroxxxtube[.]com
amateurpornlove[.]com
admingay[.]com
xxxretrotube[.]com
xxxshemaletubes[.]com
hotpornstartube[.]com
firsttrannytube[.]com
erotixtubes[.]com
1pornstartube[.]com
1asiantube[.]com
18mpegs[.]com
maturediva[.]com
elitematures[.]com
vipmatures[.]com
pcsextube[.]com
porn-vote[.]com
pornbrunettes[.]com
maturedtube[.]com

alfatubes[.]com
maturetubesexy[.]com
justhairyporn[.]com
hotblowjobporn[.]com
homemadetubez[.]com
homemadexx[.]com
golesbiansex[.]com
fuck-k[.]com
freebdsmxxx[.]com
emeraldporntube[.]com
dosextube[.]com
bigtitslove[.]com
yoursex[.]sexy
tubez[.]sexy
japaneseporn[.]win
hdfuck[.]me
tubelesbianporn[.]com
vipebonytube[.]com
vipamateurtube[.]com
largematuretube[.]com
latinosextube[.]com
xxxhardest[.]com
tubebigtit[.]com
tubesexa[.]com
realfetishtube[.]com
pornways[.]com



Related domains known to have been involved in the campaign:
qhbzkj[.]cn
mmbrbdf[.]cn
daosidanbao[.]cn
txxutmgs[.]cn
sdhsyl[.]cn
butrxmgp[.]cn
aiin[.]com[.]cn
xuxinwuliu[.]cn
qaqbhvnb[.]cn
hnldfm[.]cn
tjtyfs[.]cn
china-sum[.]com
bjyfjh[.]cn
lianstea[.]cn
shufaxuetang[.]cn
wdjjsc[.]cn
hjstory[.]cn
domcc[.]cn
918mzj[.]com

chninvest[.]cn
jfcng[.]com
nksale[.]cn
davidzhu[.]cn
tswfg[.]cn
realpornmovies[.]xyz
freepornosvideo[.]xyz
xxxpornomovies[.]xyz
sexbring[.]com
discountsale[.]xyz
howmanyweeksinayear[.]net
nutridot[.]xyz
doomyaffiliate[.]com
gacha3[.]online
hollybox[.]store
slimevideoyoutube[.]com
gooogle[.]site
vtrpic[.]com
hg301[.]com
pornvv[.]com
voonage[.]com
pornonada[.]com
uscab[.]com
pornoporntube[.]com
beaces[.]com
spaziotorte[.]com
spermix[.]com
eyew[.]com
pornky[.]com
cosmos-nc[.]com
pornlow[.]com
topbridal[.]com
coolporntube[.]com
pornotubevideos[.]com
freshporntv[.]com
pornushkin[.]com
pornodayiz[.]com
fjser[.]com
egreenfusion[.]com
ahbest[.]net
cvm[.]cn
spccsd[.]com
kozw[.]com

finalyearprojects[.]net
ylciyuiw[.]com
ylcimgsm[.]com
ylcddldz[.]com
ylchzhvb[.]com
rhshh[.]cn
ylcksqag[.]com
coodj[.]com
ylckigoa[.]com
qzguangda[.]com
ylcawqoq[.]com
laohe360[.]net
ylcxzlxd[.]com
miracure-bio[.]com
nmhxt[.]com
bjaiweiyi[.]com
hermankardon[.]com
ybcvideo[.]com
vindowsad[.]net
hpimsummit[.]com
wilmassage[.]com
cpfpz[.]com
gaysexvideo[.]us
keezmovies[.]us
ylcaiyay[.]com
lewan123[.]com
tbtmzk[.]com
haigouusa[.]com
ztmzp[.]com
hacctv[.]com
zuikuho[.]com
enping1[.]com
xgfxw[.]com
xzkywx[.]com
alotof-people[.]com
choreographyourhealth[.]us
acwt[.]us
somethinglovely[.]us
onlinestock-investing[.]us
lionheartgallery[.]us
host4bit[.]us
computerpartsdirect[.]us
sjb152[.]com

sjb513[.]com
sjb073[.]com
sjb458[.]com
sjb632[.]com
sjb272[.]com
sjb190[.]com
bighank[.]com
funskip[.]com
funnyjp[.]com
n6i[.]com
forgoodfuture[.]com
dzhfgj[.]cn
wbag[.]com
ceducation[.]cn
ahound[.]com
kenchu[.]net
bigsaks[.]com
7l0[.]com
psichiomega[.]us
blankparkzoo[.]us
ujdah[.]us
my-ask[.]com
yourtutor[.]us
cbdemon[.]us
anweigps[.]cn
szdjt[.]cn
yooyle[.]com[.]cn
maturediva[.]com
ccy-sj[.]com[.]cn
ntdoc[.]cn
024jk[.]cn
cd8888[.]cn
tlmlj[.]cn
bjostore[.]com
lockhan[.]cn
yangqiu[.]cn
bigaq[.]com
szca[.]org[.]cn
cnturtle[.]com[.]cn
gzycdz[.]cn
pdshdzz[.]cn
zhjzzz[.]cn
szms678[.]com[.]cn

taifengzd[.]com
100airport[.]cn
rtchache[.]com
dtcs[.]com[.]cn
szhychem[.]cn
lqqz[.]net
hyfk[.]net
geoer[.]cn
jjzyhhy[.]cn
goroog[.]cn
ey-x[.]com
yabtsf[.]cn
blzyds[.]cn
dgtdzs[.]cn
118km[.]cn
ad-cct[.]com
52huimin[.]com
zeshangze[.]com
0971jz[.]com
scxzt[.]cn
sjzxwg[.]cn
yhyizhneit[.]com
51hikao[.]com
holomovie[.]xyz
alisale[.]xyz
itangv[.]com
qhlqq[.]com
pdsyicheng[.]com
sjb925[.]com
sjb312[.]com
sjb301[.]com
yun034[.]com
zhc240[.]com
youpindaojia[.]cn

We'll continue monitoring the campaign and post updates as soon as new developments take place.