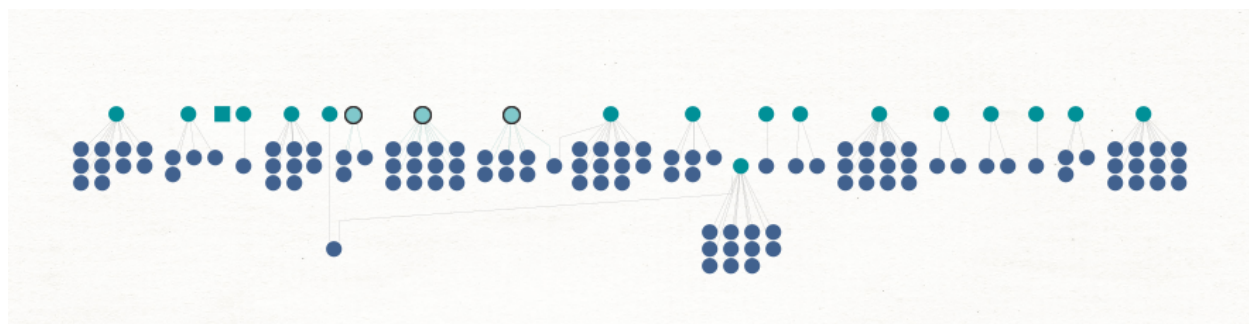


00. Exposing a Currently Active Domain Portfolio Managed and Operated by Members of the Ashiyane Digital Security Team - An OSINT Analysis

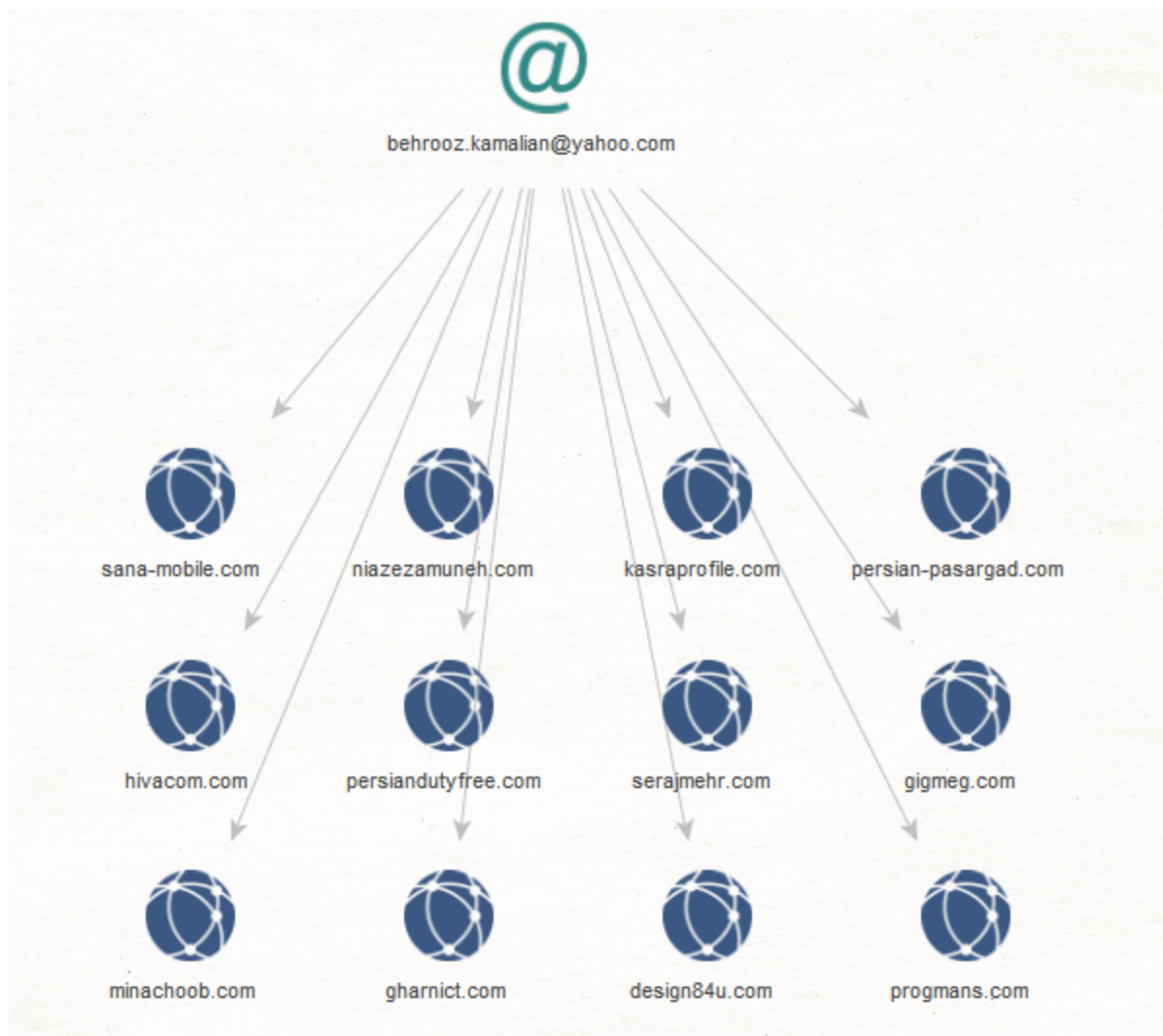


We've decided to take a closer look at the current and historical domain portfolio managed and operated by members of Iran's Ashiyane Digital Security Team using Maltego in combination with WhoisXML API's integration for the purpose of providing actionable threat intelligence including to assist fellow researchers vendors and organization on their way to track down and monitor the Internet connected infrastructure of key members of Iran's Ashiyane Digital Security Team for the purpose of monitoring it and attempting to take it offline.

In this article, we'll provide actionable intelligence on some of the currently active domains managed run and operated by Iran's Ashiyane Digital Security Team with the idea to assist fellow researchers vendors and organizations on their way to track down and monitor the infrastructure managed run and operated by Iran's Ashiyane Digital Security Team.

A list of currently active domain portfolio known to be managed and operated by members of Iran's Ashiyane Digital Security Team:

life-guard[.]jir
sepahan-trans[.]jir
kashanit[.]jir
websazangroup[.]jir
namvarnameybastan[.]jir
ashiyane-ads[.]com
tamamkar-chalous[.]jir
padidehafagh[.]com
padideafagh[.]com
bahmanshahreza[.]com
vatanpaydar[.]com
pkpersian[.]net
xn--wgba3di6y7p[.]com
jonoobhost[.]net
mahmoudbahmani[.]jir
piremehr[.]jir
shahrepars[.]jir
3diamond[.]jir
mhdcard[.]com
ashiyanecrm[.]com
tabta2[.]com
ashiyane-bot[.]jir
projejob[.]jir
rizona[.]jir
iedb[.]jir
unmobile[.]jir
razmaraa[.]jir
tabrizigold[.]jir
galleryfirozeh[.]jir
foroozanborj[.]jir
unicornart[.]jir
rahnamayeiran[.]jir
iranhack[.]jir
shomalbeauty[.]jir
andishehig[.]jir
meelk[.]jir
tamamkar-sari[.]jir
namehybastan[.]jir
chemiiran[.]jir



A list of currently active domain portfolio known to have been registered managed and operated by members of Iran's Ashiyane Digital Security Team:

websazanco[.]ir
rahnamayeiran[.]ir
maz-laa[.]ir
esnikan[.]ir
foroozanborj[.]ir
royall-shop[.]ir
ashiyane[.]ir
chemiiran[.]ir
account-yahoo[.]com
arshiasanat-babol[.]ir
ashiyane-ads[.]com

jahandarco[.]ir
momtazbarbari[.]ir
pouyaandishan-mazand[.]ir
shomalbeauty[.]ir
tractorsazi[.]com
aleyaasin[.]com
farsmarket[.]com
englishdl[.]com
zproje[.]ir
projejob[.]ir
songdownload[.]ir
ashiyanesms[.]com
ihybrid[.]us
drsjalili[.]com
ashiyane[.]org
ashiyanecrm[.]com
ashiyanehost[.]com
ashiyanex[.]com
rasht-samacollege[.]ir
instapacks[.]ir
bahmanshahreza[.]com
shaahreza[.]com
shahrezanews[.]com
taktaweb[.]net
javannovin[.]com
padidehafagh[.]com
padideafagh[.]com
sahebnews[.]com
nasiri[.]info
taktaweb[.]org
bamemar[.]com
talakesht[.]com
sepahan-trans[.]ir
opencart5[.]ir
rasulsh[.]ir
kashanit[.]ir
facebooktu[.]com
life-guard[.]ir
pr0grammers[.]ir
lammer[.]ir
sepahantrans[.]ir
facecode[.]ir
iranhack[.]org

aryanenergy[.]org
khsmt-sabzevar[.]com
orveh[.]com
tipec[.]org
iranhack[.]ir
shantya3d[.]ir
razmaraa[.]ir
soroshland[.]ir
galleryfirozeh[.]ir
unicornart[.]ir
shahrepars[.]ir
3diamond[.]ir
ashiyane-bot[.]ir
mahmoudbahmani[.]ir
piremehr[.]ir
dcligner[.]com
tabta2[.]com
chipiran[.]org
ashiyanebot[.]ir
bnls[.]ir
lamroid[.]com
persiandutyfree[.]com
iran3erver[.]com
hivacom[.]com
irantwitter[.]com
persian-pasargad[.]com
chatafg[.]com
kasraprofile[.]com
gharnict[.]com
minachoob[.]com
gigmeg[.]com
shoka-chat[.]com
serajmehr[.]com
asrarweb[.]com
niazezamuneh[.]com
sana-mobile[.]com
rizona[.]ir
iedb[.]ir
unmobile[.]ir
progmans[.]com
design84u[.]com
istgah-salavati[.]com
iranhack[.]net

shantya3d[.]com
kamelannews[.]com
rangeshab[.]com
dihim[.]com
hdphysics[.]com
cgsolar[.]net
vahidelmi[.]ir
maincoretechnology[.]com
bastanteam[.]com
vvfa[.]com
lrsecteam[.]org

We'll continue to monitor for new domain registrations courtesy of Iran's Ashiyane Digital Security Team and we'll post updates as soon as new developments take place.