A Closer Look at Active Cyber Jihad Web Properties

Table of Contents

Executive Report

Cyber jihad loosely refers to Islamic extremist terrorists' use of the Internet as a communications, fundraising, recruitment, training, and planning tool in their war against their enemies. Some of their most commonly cited enemies include the U.S., Western European countries, secular Arab governments, and Israel.

As far back as 2016, a 20-year-old was sentenced to 20 years in prison for hacking into a U.S. government database to obtain the personally identifiable information (PII) of military members and other employees for ISIL.

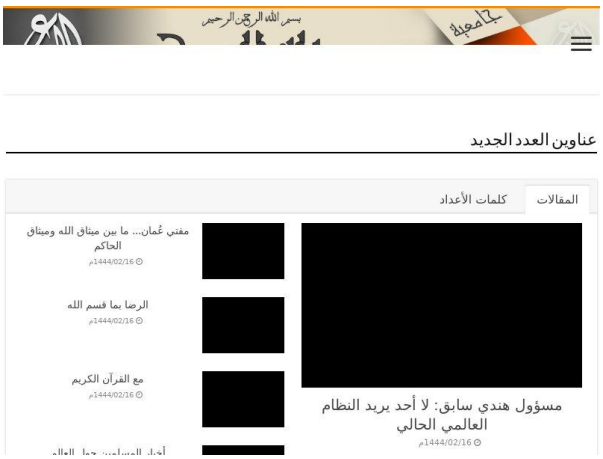
A recent WhoisXML API threat research that sought to expand the publicly available list of indicators of compromise (IoCs), specifically 67 domains, connected to cyber jihad attacks uncovered these additional artifacts:

- 228 IP addresses to which the domains identified as IoCs resolved
- 38 unredacted email addresses used to register the domains tagged as IoCs
- 545 additional possibly connected domains since they shared the IoCs' registrant email addresses or IP hosts, two of which have been dubbed "malicious" by various malware engines

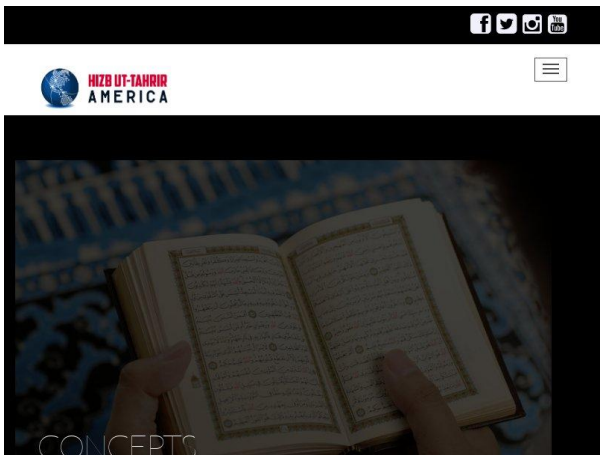
Initial List of IoCs

Over time, researchers have collated several domains hosting sites supporting ISIL/ISIS efforts. Our research team obtained 67 domains, which we used to conduct an IoC list expansion study.

First, however, we subjected the IoCs to screenshot lookups to see which of them currently host live content. A third of the IoCs (26 to be exact) remain live to this day. Here are four of them.

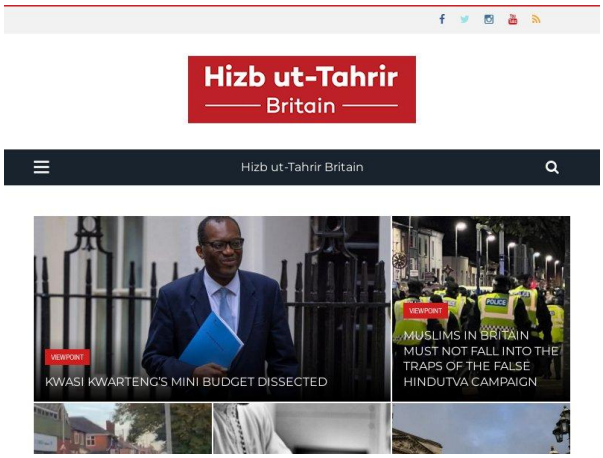


Screenshot of al-waie[.]org



Screenshot of hizb-america[.]org

Screenshot of hizb-australia[.]org



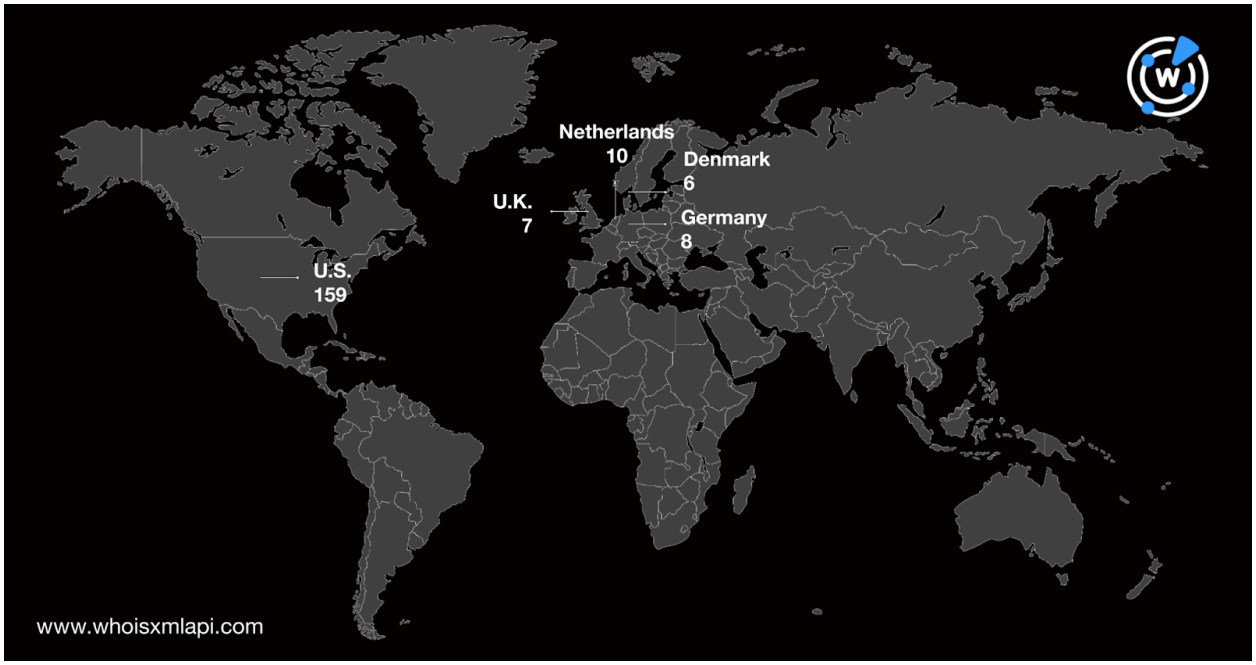
Screenshot of hizb[.]org[.]uk

Most if not all of the domains that continued to host live content look like news sites or personal blogs.

A bulk WHOIS lookup for the IoCs revealed that they were created between 1996 and 2022. It also showed that only one domain—kiblat[.]net—was owned by what seems to be a news agency. The WHOIS records of all the remaining digital properties were either privacy-protected or left blank.

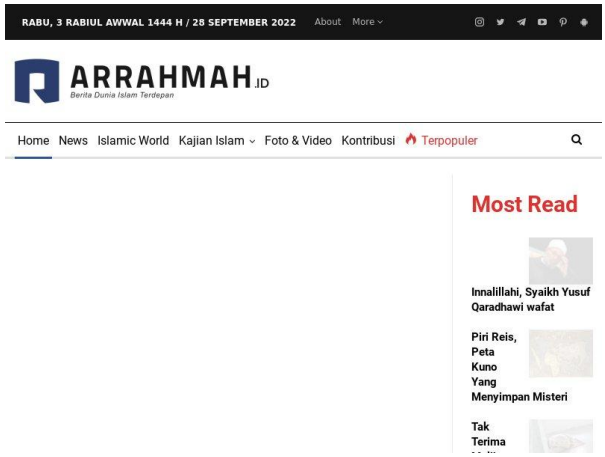
IoC List Expansion

To expand the current list of IoCs, we used the domains as DNS lookup search terms, which gave us 228 IP address resolutions. A bulk IP geolocation lookup for these showed a majority were based in the U.S., followed by Netherlands, Germany, the U.K., and Denmark.



We then ran the IoCs through historical WHOIS searches, which uncovered 38 unredacted email addresses. These could belong to the owners of the websites believed to have ties to cyber jihad activities. A majority of them (24 to be exact) looked like personal Gmail addresses.

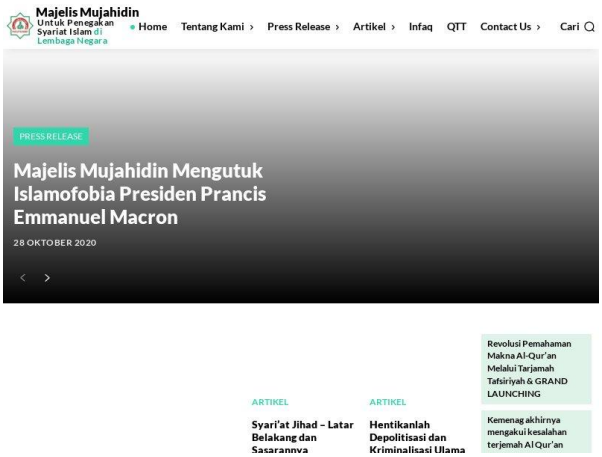
Using the email addresses as reverse WHOIS search terms and the IP addresses as reverse IP lookup terms led to the discovery of an additional 544 domains that could be connected to the threat. Of these, 67 hosted live content that looked similar to that seen on the IoCs, including the four shown below.



Screenshot of arrahmah[.]id

Screenshot of islamdevleti[.]info

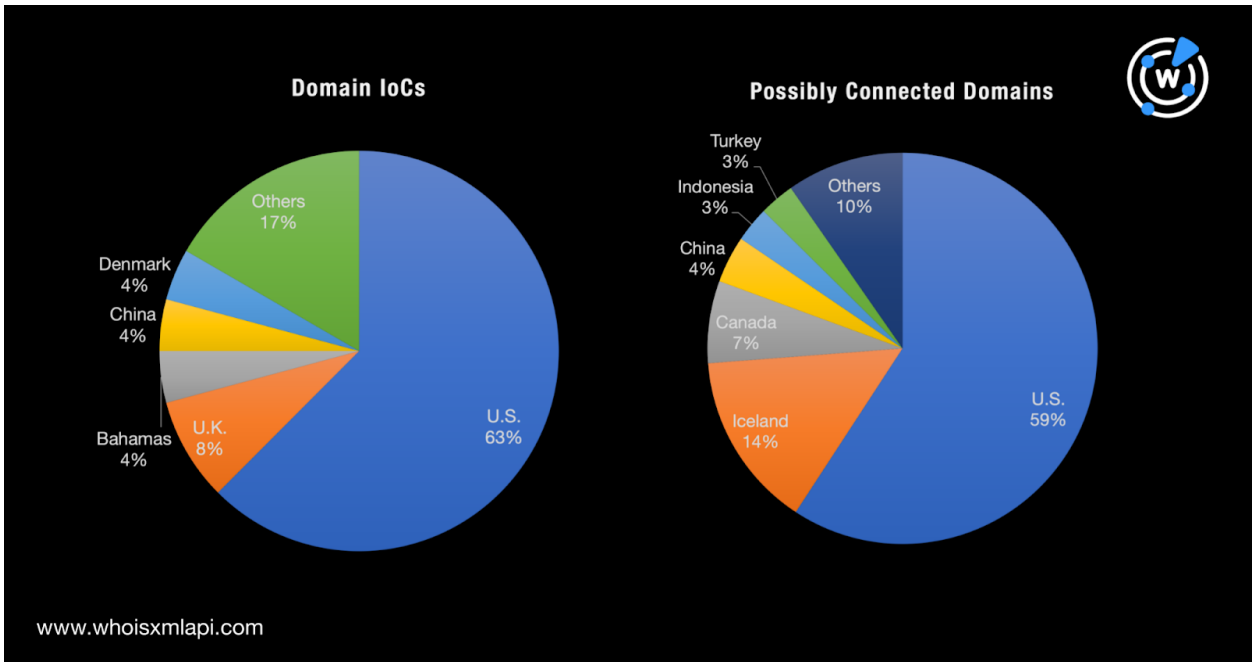
Screenshot of jihadunspun[.]com



Screenshot of majelismujahidin[.]com

A bulk WHOIS lookup for the additional domains showed that they were relatively newer than the IoCs, with creation dates ranging from 2016 to 2022. None of the registrant organization names indicated in the records also pointed to legitimate businesses.

A comparison of the IoCs' and additional domains' registrant countries showed that most of them (around 60% for both categories) were based in the U.S. Also, Canada and China joined the top 5 geolocations for the two sets of domains.



Finally, a bulk malware check for the 545 possibly connected domains showed that two—douglaskemp[.]com and jhuf[.]net—were malicious according to several malware engines.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

IoCs Related to Cyber Jihad Activities

- joinalqarda[.]com
- alintibana[.]net
- dr-algzouil[.]com
- sunnahonline[.]com
- shahamat-movie[.]com
- islaam[.]com
- faithfreedom[.]org
- Qa3edon[.]100free[.]com
- Khilafah[.]com
- daulahisamiyah[.]net
- jihadica[.]com
- ansar1[.]info
- jhuf[.]net
- arrahmah[.]com
- voa-islam[.]com
- kiblat[.]net
- sunnahcare[.]com
- eramuslim[.]com
- al-mustaqbal[.]net
- shoutussalam[.]org
- muqawamah[.]net
- liputan-kita[.]com

- waislama[.]net
- lasdipo[.]com
- soutalhaq[.]net
- shabakataljahad[.]com
- alsomod[.]com
- dolatislam[.]blogspot[.]sg
- hizb-ut-tahrir[.]org
- hizb-ut-tahrir[.]dk
- hizb-ut-tahrir[.]info
- khilafah[.]org
- khilafah[.]net
- hizbut-tahrir[.]or[.]id
- hilafet[.]com
- khilafat[.]org
- kalifaat[.]org
- newcivilisation[.]com
- al-waie[.]org
- kokludegisim[.]net
- expliciet[.]nl
- mindspring[.]eu[.]com
- ramadhan[.]org
- al-nahda[.]com
- al-aqsa[.]org
- islamdevleti[.]org
- albadil[.]edaama[.]org
- islam-in-poland[.]org
- alokab[.]com
- mykhilafah[.]com
- risala[.]org
- hizb[.]org[.]uk
- lebensordnung[.]com
- khilafat[.]dk
- hizb-america[.]org
- turkiyevilayeti[.]org
- hizb-ut-tahrir[.]nl
- globalkhilafah[.]com
- hizb-australia[.]org
- jihadunspun[.]com
- alemarah-iea[.]net
- alemarah[.]info
- falojaa[.]net
- tawheedmedia[.]com
- atahadi[.]tk
- majahdenar[.]com
- ansarnet[.]info

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 172[.]64[.]82[.]171
- 172[.]64[.]81[.]107
- 172[.]64[.]84[.]202
- 172[.]64[.]81[.]207
- 188[.]114[.]98[.]171
- 104[.]21[.]93[.]62
- 104[.]25[.]221[.]41
- 104[.]24[.]22[.]14
- 188[.]114[.]98[.]174
- 104[.]25[.]216[.]101
- 172[.]64[.]81[.]196
- 172[.]64[.]81[.]199
- 172[.]64[.]81[.]251
- 172[.]64[.]86[.]143
- 172[.]64[.]93[.]65
- 50[.]63[.]202[.]91
- 50[.]63[.]202[.]9
- 184[.]168[.]221[.]42
- 93[.]95[.]228[.]158
- 136[.]244[.]99[.]226
- 108[.]61[.]164[.]186
- 185[.]165[.]171[.]7

- 185[.]205[.]209[.]114
- 94[.]199[.]200[.]12
- 74[.]50[.]52[.]242
- 213[.]229[.]84[.]4
- 77[.]73[.]104[.]242
- 104[.]25[.]238[.]7
- 72[.]167[.]183[.]54
- 162[.]159[.]247[.]123
- 146[.]112[.]61[.]107
- 188[.]114[.]96[.]22
- 104[.]21[.]235[.]66
- 104[.]18[.]48[.]106
- 104[.]18[.]49[.]106
- 50[.]87[.]146[.]182
- 198[.]185[.]159[.]144
- 192[.]185[.]4[.]56
- 173[.]249[.]18[.]136
- 172[.]217[.]164[.]19
- 142[.]250[.]180[.]147
- 13[.]248[.]148[.]254
- 216[.]239[.]34[.]21
- 195[.]20[.]42[.]254
- 142[.]250[.]80[.]19
- 94[.]237[.]72[.]168
- 103[.]224[.]212[.]222
- 185[.]53[.]179[.]29
- 141[.]8[.]225[.]179
- 172[.]64[.]91[.]147

Sample Email Addresses Used to Register the Domains Identified as IoCs

- turkiye[.]vilxxxxx@gmail[.]com
- rudolphniemanxxxxx@gmail[.]com
- soutxxxxx[.]net@gmail[.]com
- cancnebut@gmail[.]com
- DOMAIN[.]xxxxx@GMAIL[.]COM
- bev[.]giesbxxxxx@gmail[.]com
- adilxxxxx@yahoo[.]com
- maximusbxxxxx@gmail[.]com
- solomexxxxx@gmail[.]com
- joinalxxxxx[.]com@domainsbyproxy[.]com
- gandasuxxxxx@yahoo[.]co[.]id
- charlie_xxxxx@yahoo[.]com[.]au
- janexxxxx@gmail[.]com
- maillaxxxxx@gmail[.]com
- exxxxx@YAHOO[.]COM
- laxxxxx@gmail[.]com
- akuxxxxx@gmail[.]com
- kandaharxxxxx@gmail[.]com
- aulia_suxxxxx@yahoo[.]com
- contrxxxxx[.]domain@gmail[.]com

Sample Possibly Connected Domains Since They Shared the IoCs' Registrant Email Addresses or IP Hosts

- ht-malaysia[.]com
- championchipmid-south[.]com
- hizbut-tahrir[.]org[.]my
- topdirectory[.]co[.]in
- hyperlocal[.]us
- gamehacker[.]top
- gamescooking[.]us
- phoenixpwnjailbreak[.]com
- headphoneuniverse[.]com
- indomarching[.]net

- cydiaimpactordownload[.]net
- qualitystreetcarts[.]com
- circularsawexpress[.]com
- affpayday[.]com
- fit-messe[.]de
- mykhilafah[.]com
- islam-in-poland[.]org
- annievandusenacupuncture[.]com
- voa-islam[.]id
- southgateinnmissoula[.]com
- voa-islam[.]com
- bestgrouponclone[.]com
- sbmeo[.]com
- joinalqarda[.]com
- hizb-australia[.]org
- suara-media[.]com
- syariah[.]or[.]id
- rumahdhuafa[.]com
- marcoumrah[.]com
- maanaumrah[.]com
- rumahhafizh[.]com
- marcotourgroup[.]com
- fanimedia[.]net
- marcojatiwarna[.]com
- rumahhafizindonesia[.]com
- salurankencing[.]com
- darussalam[.]tv
- wesalonline[.]tv
- zulfara[.]co
- mukhlas-rowi[.]web[.]id
- ngabuburit[.]web[.]id
- khilafah[.]or[.]id
- yasminsquare[.]com
- al-islam[.]or[.]id
- hizbut-tahrir[.]or[.]id
- technoworld-bogor[.]com
- muliaresidence[.]com
- yasmin-group[.]com
- bubulakresidence[.]com
- yasmin-reload[.]com
- propertibogor[.]com
- bogortradeworld[.]com
- habarnews[.]com
- habarnews[.]org
- habarnews[.]media
- habarnews[.]tv
- cypressforestry[.]com
- jihadunspun[.]com
- cypresstreeservice[.]com
- newcivilisation[.]com
- eidinthepark[.]net
- onyxhive[.]com
- dubaivista[.]com
- coolasfunk[.]com
- simplypalmpre[.]com
- thedubailife[.]com
- thedubailife[.]net
- alsomod-iea[.]info
- shahamat[.]info
- shahamat-english[.]com
- shahamat-farsi[.]com
- shahamat-urdu[.]com
- shahamat-arabic[.]com
- shahamat-movie[.]com
- alemarah-urdu[.]com
- alemarahnews[.]org
- islam-iea[.]com
- alemarahnews[.]com
- hizbuttahrir-tr[.]com
- degisimhaber[.]net
- hizbuttahrir-tr[.]net
- hizb-turkiye[.]net
- thewalknctodc[.]com
- mo3ood[.]com
- changfootballsevens[.]com
- syukmagroups[.]com

- padangmtbike[.]com
- buzzxs[.]com
- tokorahmi[.]com
- lafiraindonesia[.]com
- management-consultingsa[.]com
- thoughtleadershipsa[.]com
- sembeo[.]com
- pesinsight[.]com
- haikona[.]com
- host4domains[.]com
- faxfx[.]org
- krugernational[.]com
- terenzoprofessionalhaircare[.]com
- completeofficemovers[.]com