Global Iranian Disinformation Operation

ClearSky Cyber Security

November 2018

Large-scale Fake News Infrastructure Promoting Iranian Interests

www.clearskysec.com
info@clearskysec.com

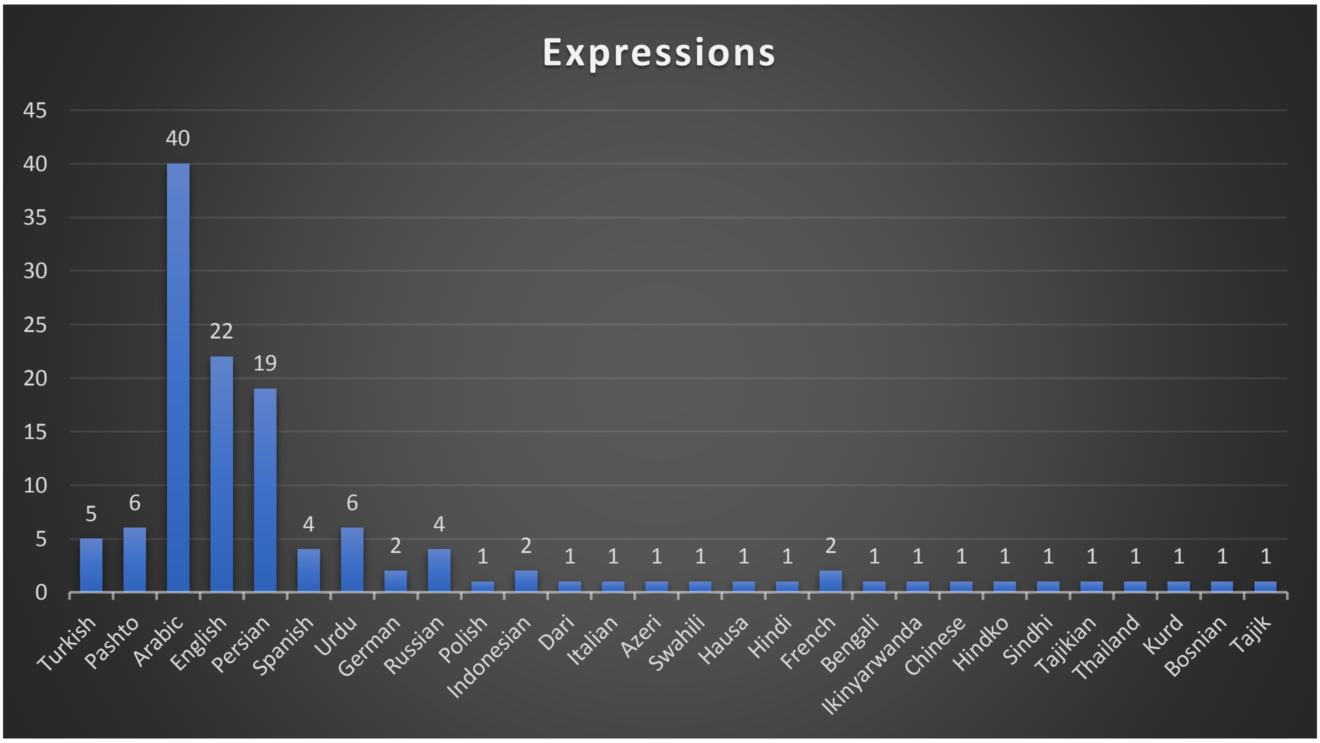
Table of Contents

Summary

Throughout 2018, Clearsky Cyber Security has uncovered several disinformation campaigns operated by Iran. In this report we expose a massive fake-news infrastructure targeting numerous regions and populations around the world.

In our investigation, partly based on a FireEye report that exposed the initial findings[1], we uncovered the full infrastructure, comprised of least 98 fake media outlets; each with its own websites, social media accounts and pages that distribute fake news worldwide. Note that a number of the fake media outlets also created fraudulent mobile apps.

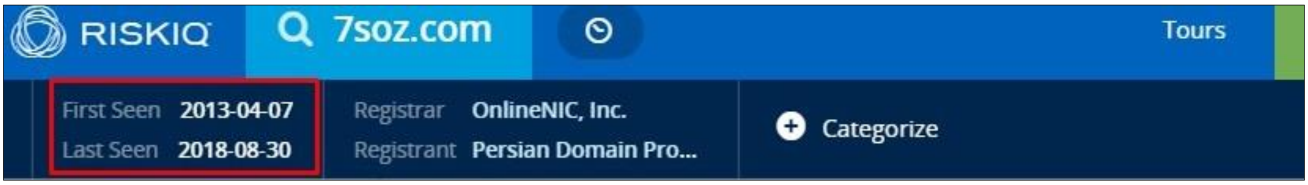
This infrastructure targets 28 countries, authorities and geographical areas (such as North Africa and Eastern Europe). The most commonly used language is Arabic, with 40 expressions across various websites. Other languages of note are English (22 expressions), Persian (19 expressions) and then Urdu and Pashto (6 expressions each).



Graph 1 – number of expression instances across different languages

The main method of this infrastructure is copying or stealing articles from legitimate media outlets around the world, include the US, several countries in Europe, Africa and Asia. In some websites, we identified modification of the content and adding fake content to the original, along with publishing only articles that fit their agendas. In order to aid the credibility of the websites, the operators of the infrastructure uploaded irrelevant content.

This infrastructure was established by Iranian actors, and has been active since at least 2012. Seen in the image below are the details of one of the first websites created in this campaign.



First Seen 2013-04-07
Last Seen 2018-08-30
Registrar OnlineNIC, Inc.
Registrant Persian Domain Pro...

Image 1 – details of 7soz[.]com, one of the first websites created in this campaign

[1] https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

We identified that in its initial stages, most of the efforts were focused on propagating Fake News across various countries of interests to Iran; chiefly in the middle-east, including Turkey, Egypt and Afghanistan. These countries are considered by Iran as strategic places to distribute the Islamic revolution and the Vilayat-e Faqih[2] ideologies. Since then, the operators expanded their scope of operation and began creating dedicated websites for each country and authority that the Iranian wish to establish influence in.

We categorized the websites into 4 groups, each representing different regions around the world. Note however that most of the websites in each group have the same overarching goals and agendas.

Region	Purposes
United State and Europe	Propagate disinformation primarily about the current US and Europe governments – presents them as failures, depraved and undeserving. We asses that Iranian actors are trying to manipulate peoples' thoughts and turn them against governments that do not support Iran or the Iranian Regime. For example, currently the main methods against POTUS Trump regime is promoting collaboration with Iran regardless the secession of USA from the nuclear deal, and pro Jeremy Corbin as a legitimate leader in the UK.
Middle east and north Africa	Propagate disinformation primarily about issues in the middle east that are relevant to Iran or its alias. The fraudulent media outlets targeting Iran's enemies (Israel and Saudi Arabia) publish deterrence information. We asses that this is aimed to present Iran in a positive light as a balancing political power, while presenting Israel and Saudi Arabia as countries that violate global order and the peace.
Muslim countries in Africa and Asia	Propagate disinformation about the positive rule of Iran in the Islamic world. We asses that this act is part of the Iranian efforts to be seen as the leader of the Islamic world. Note that most of the targets in this group are countries that have minority group of Shias people, like Nigeria, Pakistan and Afghanistan.
Alias of Iran (such as Syria, Turkey and Russia)	Propagate disinformation primarily against the shared opponents of Iran and its political partners. We asses that this act is part of the Iranian efforts to position Iran as a valuable political ally.

Table 1 – Iranian fake news websites grouped by region and purposes

Based on the scale of the operation, which includes websites, apps, fake social media profiles, we believe that the infrastructure is operated by an organized group that coordinates various operators such as - editors, writers, graphic designers, web developers, social media specialist and more. Further, many of the content creators are fluent in one or more languages in addition to Persian.

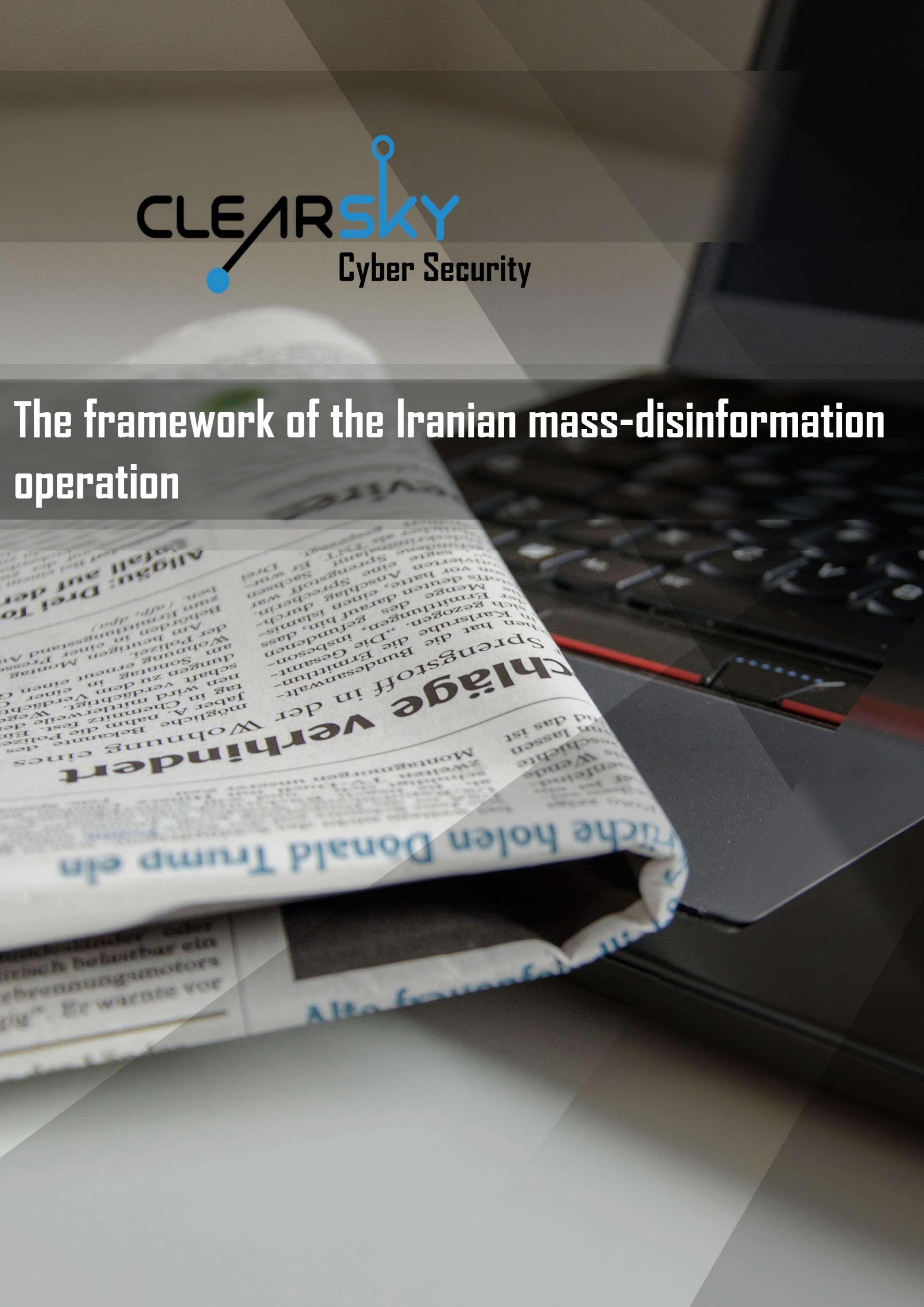
In conclusion, Iran has succeeded to operate a large-scale disinformation and fake news infrastructure uninterruptedly for over half a decade. As a result, Iran reached and influenced hundreds of thousands, and possibly even millions of readers, who were unaware that they are exposed to inauthentic information.

Note – the full digital infrastructure can be seen in "Appendix 2 – full list of Iranian fake news websites"

[2] Vilayat-e Faqih – the Guardianship of the Islamic Jurist is the theocratic republic system of government in Iran. According to this system, the Fagih (Islamic jurist) is the main leader of the Shias' people and his rule is to custodianship over the people, both religiously and politically.

CLEARSKY Cyber Security

The framework of the Iranian mass-disinformation operation

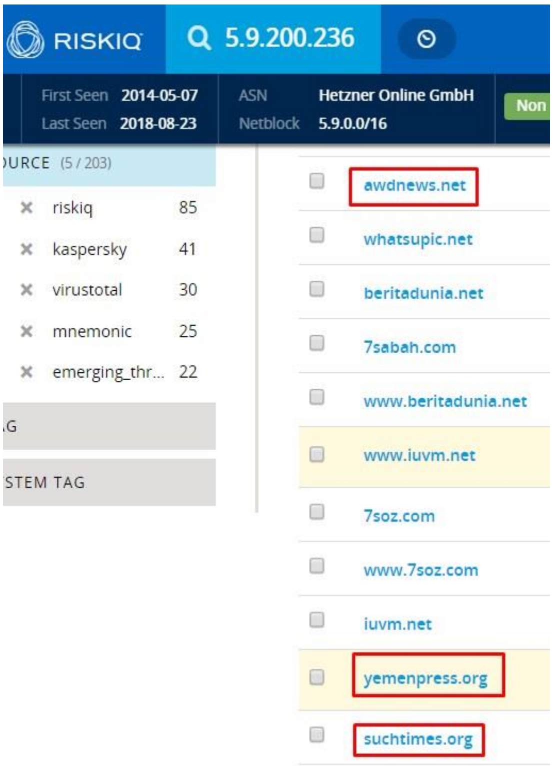


The Framework of the Iranian Mass-disinformation Operation

In our investigation we identified repeated thematic issues. We believe that each website in the infrastructure has a dedicated purpose and is loyal to the group's cause. With that, we identified few common denominators.

News media outlets

The fake websites impersonate legitimate local media outlets. One of the most common characteristics of the fraudulent websites is that they contain in their URL the word "News", or a variation of it (e.g. Times, Journal, Press, etc.)[3]. Seen below is a list of domains on one of the infrastructure's IPs hosting fake news websites.



First Seen 2014-05-07
Last Seen 2018-08-23
ASN Hetzner Online GmbH
Netblock 5.9.0.0/16

URCE (5 / 203)

×	riskiq	85
×	kaspersky	41
×	virustotal	30
×	mnemonic	25
×	emerging_thr...	22

G

STEM TAG

□ awdnews.net
□ whatsupic.net
□ beritadunia.net
□ 7sabah.com
□ www.beritadunia.net
□ www.iuvm.net
□ 7soz.com
□ www.7soz.com
□ iuvm.net
□ yemenpress.org
□ suchtimes.org

Image 2 – several notable fake news domains hosted on the same IP

Website design methodology

Each "news organization" has a distinct design, logo and theme that matches the sites' name.

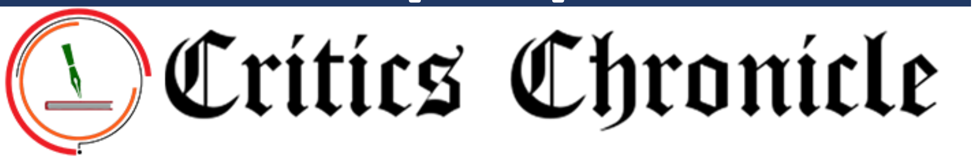
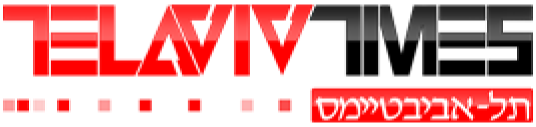
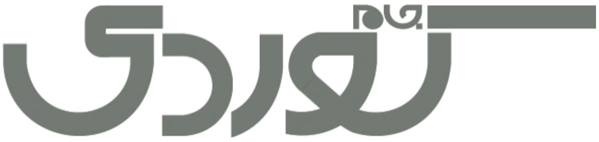
URL	Logo and design
Criticschronicle[.]com	
Tel-avivtimes[.]com	
Jamekurdi[.]net	

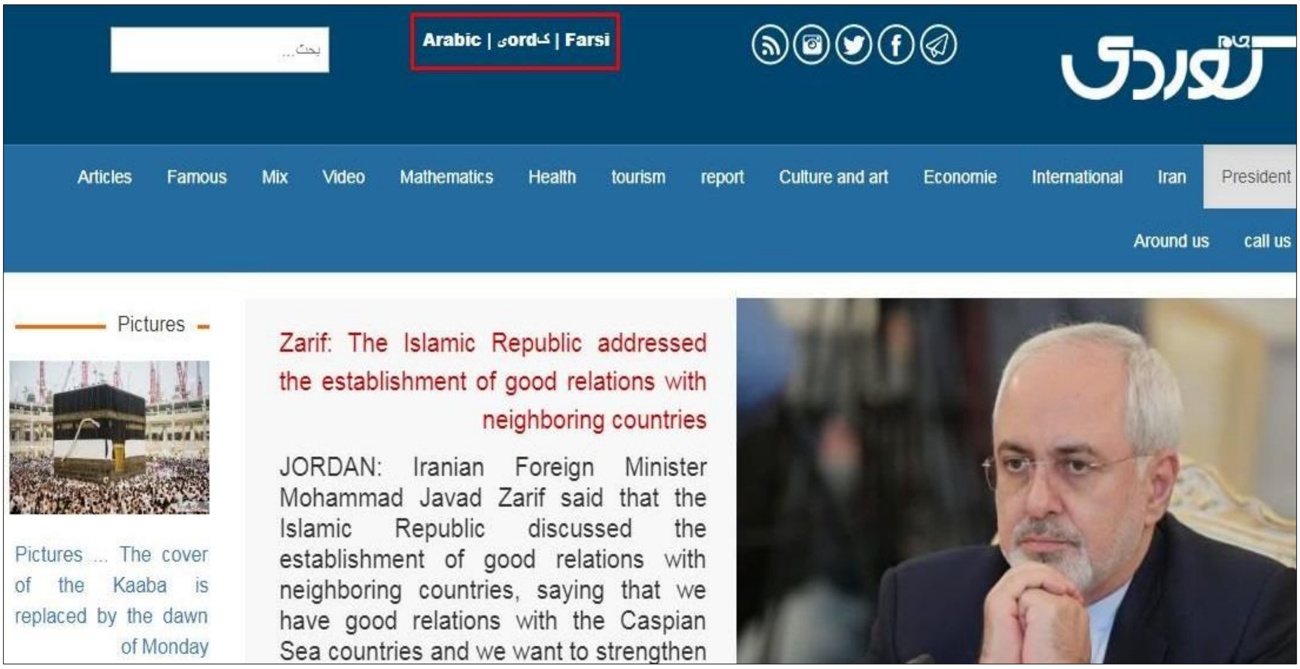
Table 2 - Examples of the fake news websites' design

[3] Note that this method is very common in disinformation campaigns. In another fake news network that we and Reuters uncovered, unknown actors used this method to pose as authentic Arabic-language news outlets, have spread false information about the Saudi government. https://www.reuters.com/article/us-saudi-khashoggi-disinformation/fake-news-network-vs-bots-the-online-war-around-khashoggi-killing-idUSKCN1N63QF

Multi-language operation

Many of the websites have also versions in different languages. The language is determined based on the target audience of the websites and their messages. For instance, the website jamekurdi[.]net impersonates Kurdish news media outlets. Accordingly, the main version is in Kurdish.

However, due to the fact that there is a Kurdish population in Iran, Syria and Iraq, the website has additional versions with local languages, such as Persian and Arabic.



Pictures ... The cover of the Kaaba is replaced by the dawn of Monday

Zarif: The Islamic Republic addressed the establishment of good relations with neighboring countries

JORDAN: Iranian Foreign Minister Mohammad Javad Zarif said that the Islamic Republic discussed the establishment of good relations with neighboring countries, saying that we have good relations with the Caspian Sea countries and we want to strengthen

Image 2 – fake news website with multiple language options

Although the sites are often consistent in themes and designs, we noticed a number of sites with different design and logos between different pages and languages variants of the same "media outlet".

For example, seen below are two different pages of the fake news website – Yemen Press. Note that the top banner is of the English pages while the bottom one is of the Arabic pages.

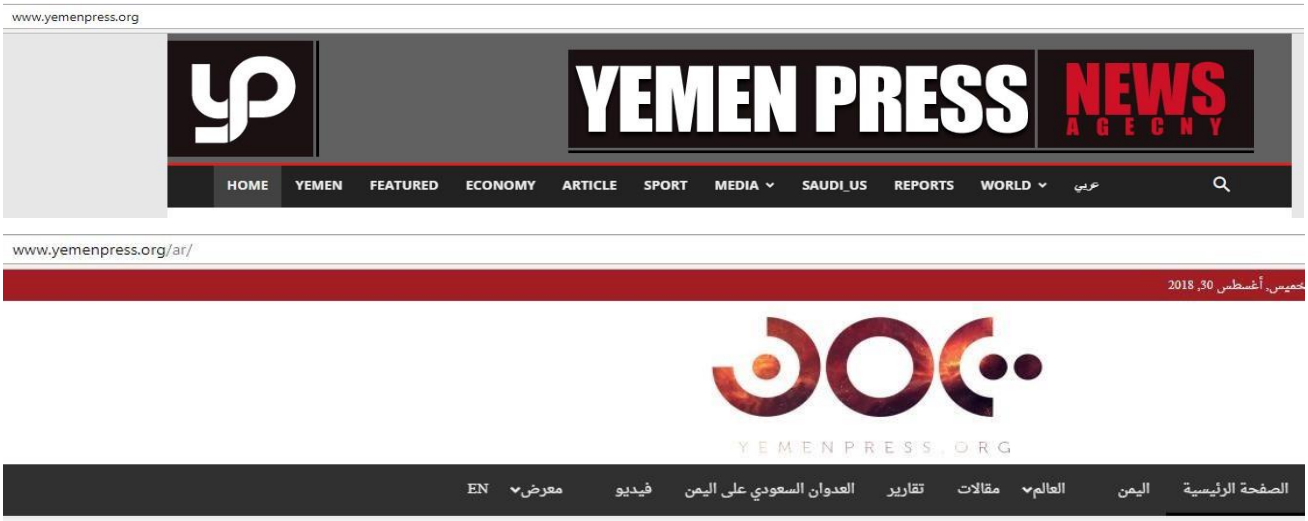
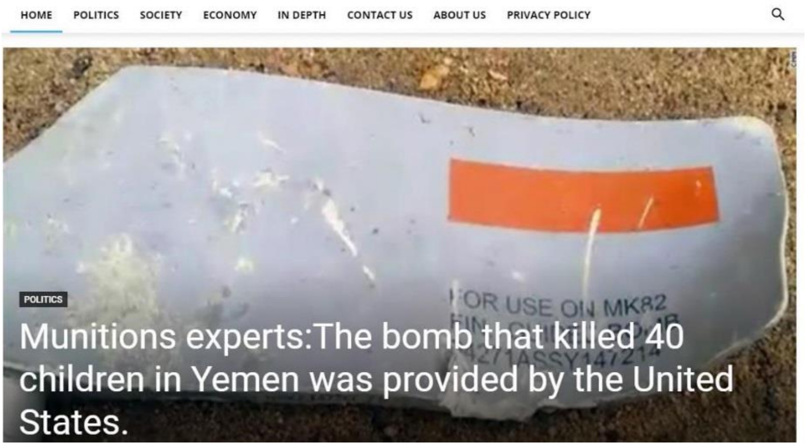
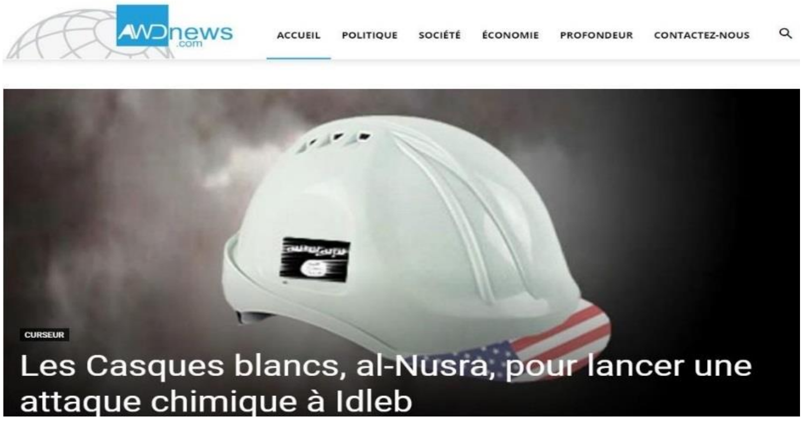


Image 3 – two different designs and logos of the same website "Yemen Press"

The reason for this inconsistency is unclear. Presumably one is a new design that for some reason was not yet applied to the rest of the website. Alternatively, these changes may be designed to increase appeal and influence for different audiences. Seen below, are 4 versions of the same website (awdnews[.]com, targeting European audience) each with different content and messages, while promoting the same overarching agenda:

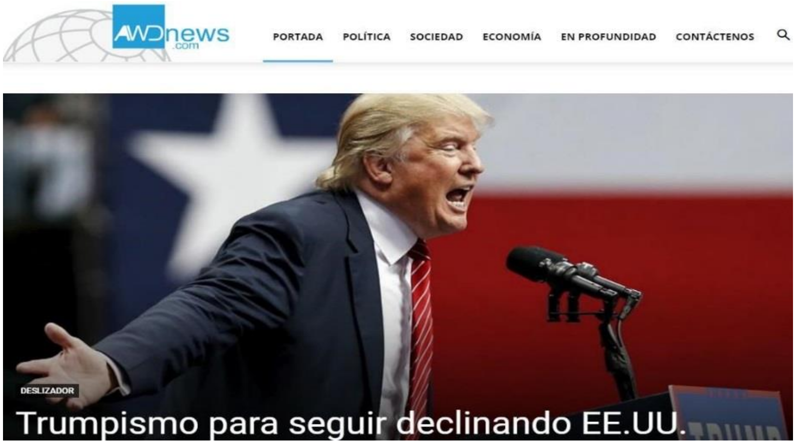


Munitions experts:The bomb that killed 40 children in Yemen was provided by the United States.



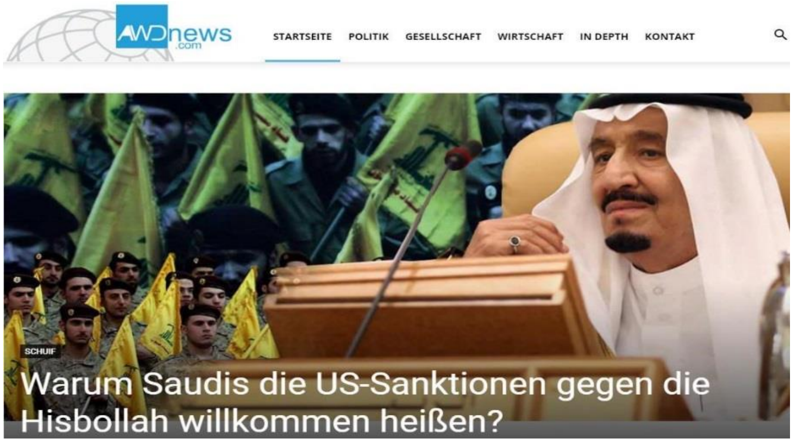
Les Casques blancs, al-Nusra, pour lancer une attaque chimique à Idleb

Image 4 – bottom screen capture - Translation via google translate from French "White helmets, al-Nusra, to launch Idleb chemical attack". Note that the photo juxtaposes ISIS Flag on a helmet with a US flag to present them as partners.



Trumpismo para seguir declinando EE.UU.

Image 5 - Translation via google translate " Trump to continue declining European union"



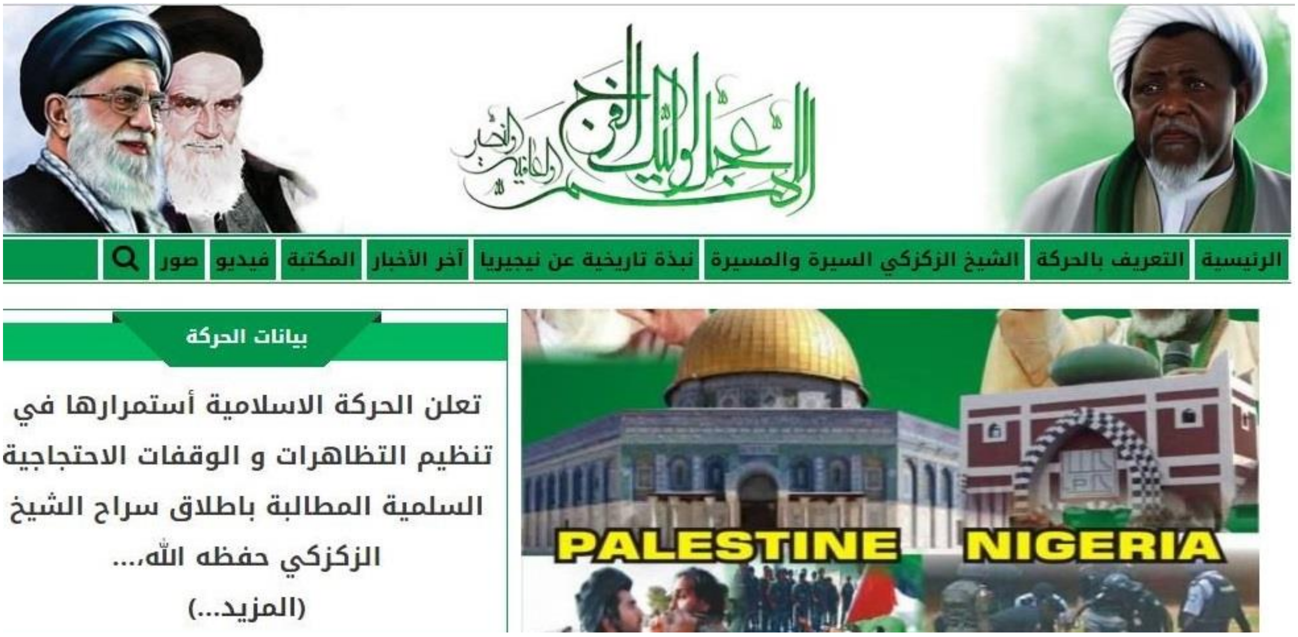
Warum Saudis die US-Sanktionen gegen die Hisbollah willkommen heißen?

Image 6 - Translation via google translate: "Why Saudis welcome US sanctions against Hezbollah?". Note that Saudi Arabia is considered by Iran as an enemy.

Iranian disinformation targeting Muslim countries in Africa and Asia

Regarding Muslim countries in Africa and Asia, the content and the visual elements promote Iran as a significant and positive cultural and political power in the Islamic world. This can be seen for example in the banner of website impersonating a Nigeran news media outlet.

The website targets the local Nigerian Shia population and contains photos of Iran's leaders alongside a Nigerian sheikh named "Ibrahim Zakzaky", who is a known Iranian supporter. This might be interpreted by the audience as Zakzaky being the "official" representative of the Vilayat-e Faqih (Iranian leadership) in Nigeria.



بيانات الحركة

تعلن الحركة الاسلامية أستمرارها في
تنظيم التظاهرات و الوقفات الاحتجاجية
السلمية المطالبة باطلاق سراح الشيخ
الزكزكي حفظه الله،...
(المزيد...)

Image 7 - Iran's leaders alongside Nigerian sheikh Ibrahim Zakzaky

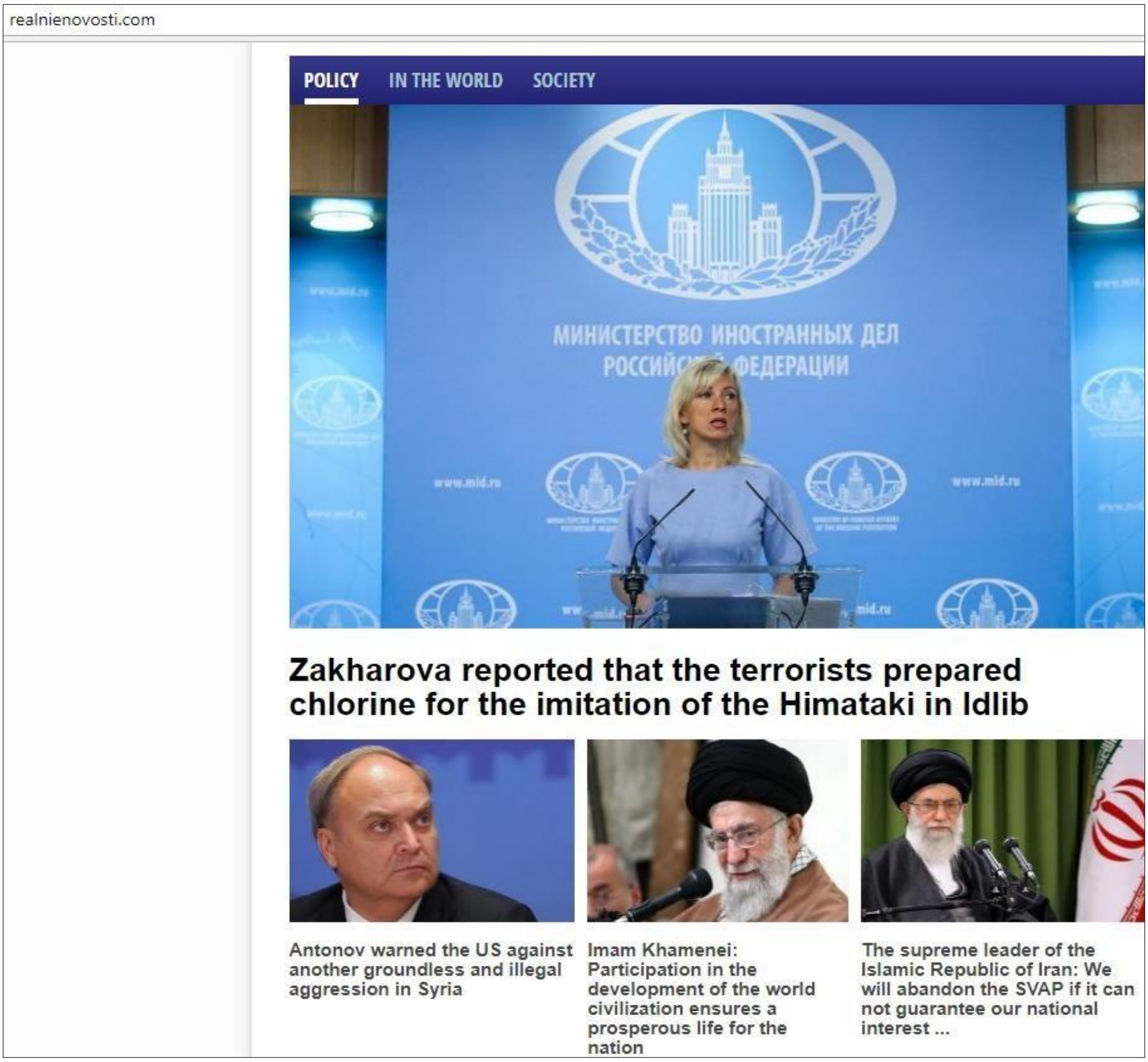
Alias of Iran

Regarding countries from the group "Alias of Iran", we see websites present content that shows Iran's collaboration intentions with their ally, while also preserving their geo-political interests. For examples:

Theme	Examples of Messages
Iran as a strong and major political power	Iran intends to cancel the nuclear deal with all remaining members unless they receive guarantees protecting Iran's national interests.
Alarming "news" regarding other countries	Terrorist are preparing to attack in Idlib, Syria.
Promoting collaboration with Iran	Iran leadership promotes global development. Russian expert claims that the US operation in Syria is unchecked and unreasonably aggressive.

Table 3 - Examples of messages

Example of these messages can be seen on the main page of fake Russian website realnienovosti[.]com from august 30th 2018:



realnienovosti.com

Zakharova reported that the terrorists prepared chlorine for the imitation of the Himataki in Idlib

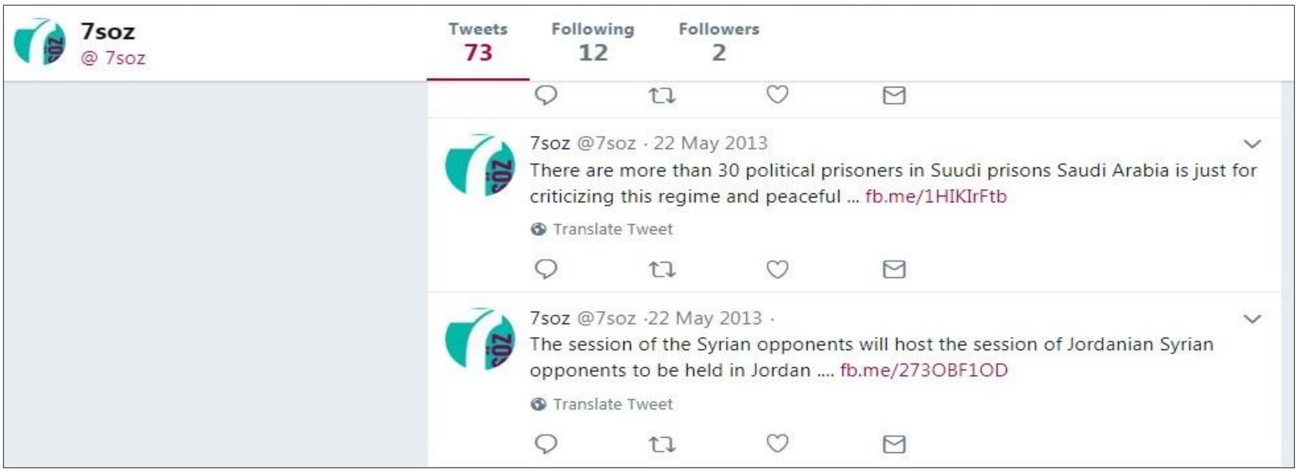
Antonov warned the US against another groundless and illegal aggression in Syria

Imam Khamenei: Participation in the development of the world civilization ensures a prosperous life for the nation

The supreme leader of the Islamic Republic of Iran: We will abandon the SVAP if it can not guarantee our national interest ...

Image 7 – Russian fake news website promoting articles with pro-Iranian agenda

It should be noted that early on (around 2013) there were number of "Turkish" websites that were part of the group "Middle east and north Africa". But, with recent development and growing political relations between the two states, the aforementioned websites were shut down and replaced by a new website that better fit the agenda of "alias of Iran" group. Indications of the defunct websites can be found on various social media networks, such as twitter:



7soz @7soz · 22 May 2013
There are more than 30 political prisoners in Suudi prisons Saudi Arabia is just for criticizing this regime and peaceful ... fb.me/1HIKIrFtb

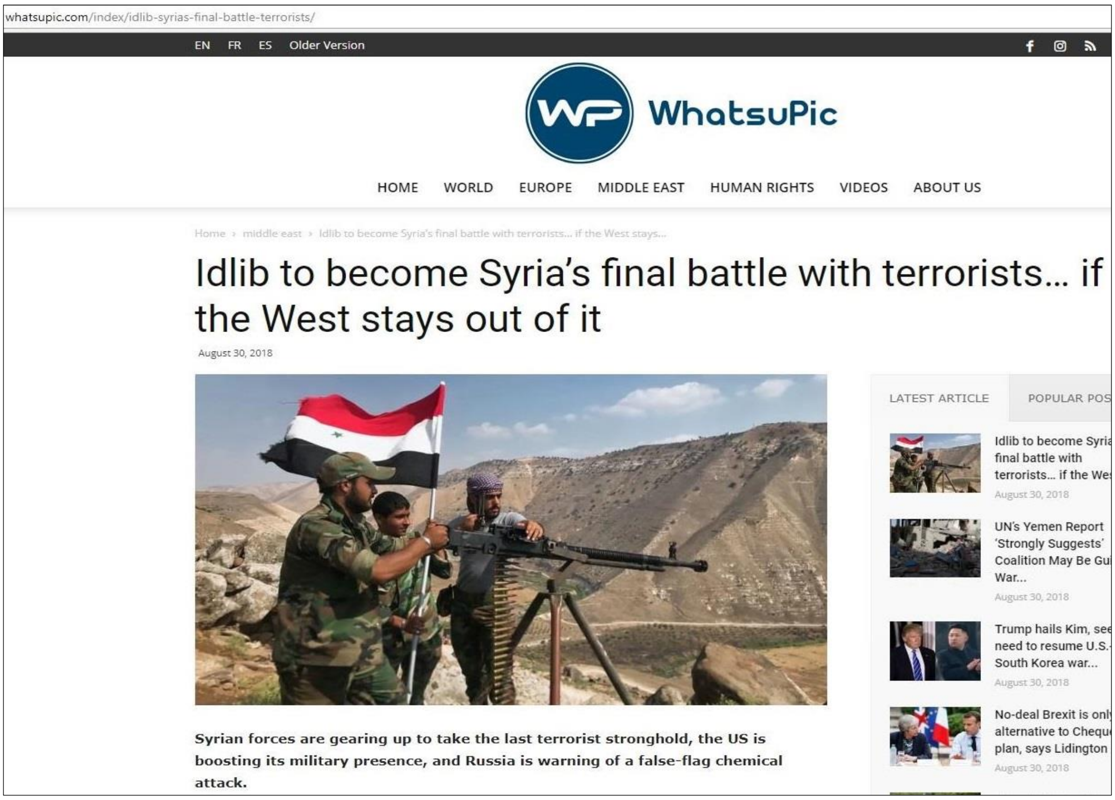
7soz @7soz ·22 May 2013 ·
The session of the Syrian opponents will host the session of Jordanian Syrian opponents to be held in Jordan fb.me/273OBF1OD

Image 8 – Twitter messages referring and linking to the defunct websites

Stolen / Copied content

Much of the websites' content is blatantly copied from legitimate news sources. At times they even keep original links in the article. Below is an example of this practice. The top image is from a website by the name WhatsuPic, which targets US and European audience. Most of the articles deal with subjects like US interference with local politics (in Yemen for example), the "subservience" of Israeli lobby in the US, the Palestinian issues and more.

On August 30th, an article titled "*Idlib to become Syria's final battle with terrorists… if the West stays out of it*" was published, accusing the US for using chemical weapons against Assad loyalists. This article was copied in full, from the website rt.com (seen in the bottom image). Note that RT is considered to be a propaganda website of the Russian government.



whatsupic.com/index/idlib-syrias-final-battle-terrorists/

EN FR ES Older Version
WhatsuPic
HOME WORLD EUROPE MIDDLE EAST HUMAN RIGHTS VIDEOS ABOUT US
Home › middle east › Idlib to become Syria's final battle with terrorists… if the West stays…

Idlib to become Syria's final battle with terrorists… if the West stays out of it

August 30, 2018

LATEST ARTICLE | POPULAR POS

Idlib to become Syria final battle with terrorists… if the We
August 30, 2018

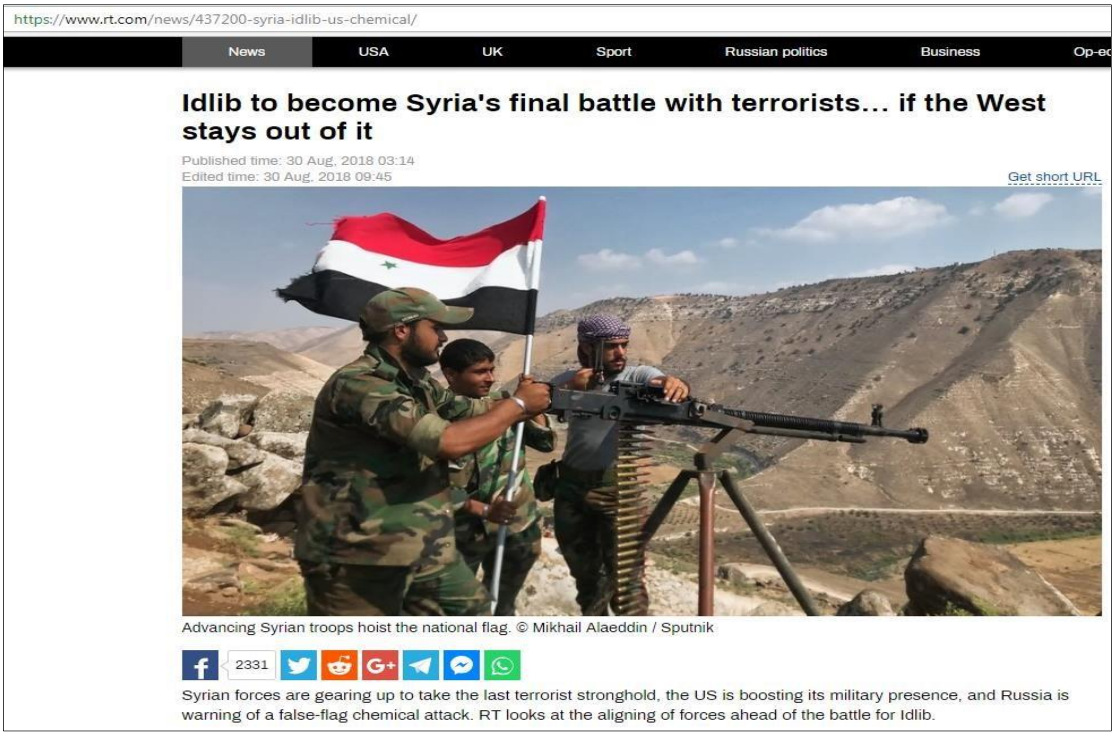
UN's Yemen Report 'Strongly Suggests' Coalition May Be Gui War...
August 30, 2018

Trump hails Kim, see need to resume U.S.- South Korea war...
August 30, 2018

No-deal Brexit is only alternative to Chequ plan, says Lidington
August 30, 2018

Syrian forces are gearing up to take the last terrorist stronghold, the US is boosting its military presence, and Russia is warning of a false-flag chemical attack.

Image 9 – stolen content posted on WhatsuPic



https://www.rt.com/news/437200-syria-idlib-us-chemical/

Idlib to become Syria's final battle with terrorists… if the West stays out of it

Published time: 30 Aug, 2018 03:14
Edited time: 30 Aug, 2018 09:45

Advancing Syrian troops hoist the national flag. © Mikhail Alaeddin / Sputnik

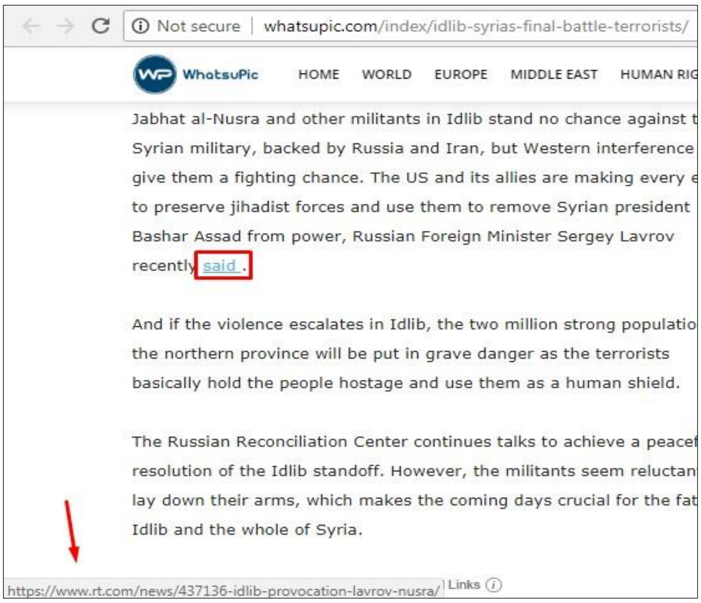
Syrian forces are gearing up to take the last terrorist stronghold, the US is boosting its military presence, and Russia is warning of a false-flag chemical attack. RT looks at the aligning of forces ahead of the battle for Idlib.

Image 10 – the original article from RT

Note that rt.com references were deleted. However, a link from the original article was kept in the plagiarized article (image to the right).

Moreover, in many articles, the operators copy verbatim the article with minor changes in the order of paragraphs and sentences. Thus, modifying the original narrative of the article.

Below is an article that was published originally on the Israeli media outlet "Israel Hayom" (Israel today) that was copied and modified to present the spokesperson's speech in as more belligerent:



Not secure | whatsupic.com/index/idlib-syrias-final-battle-terrorists/

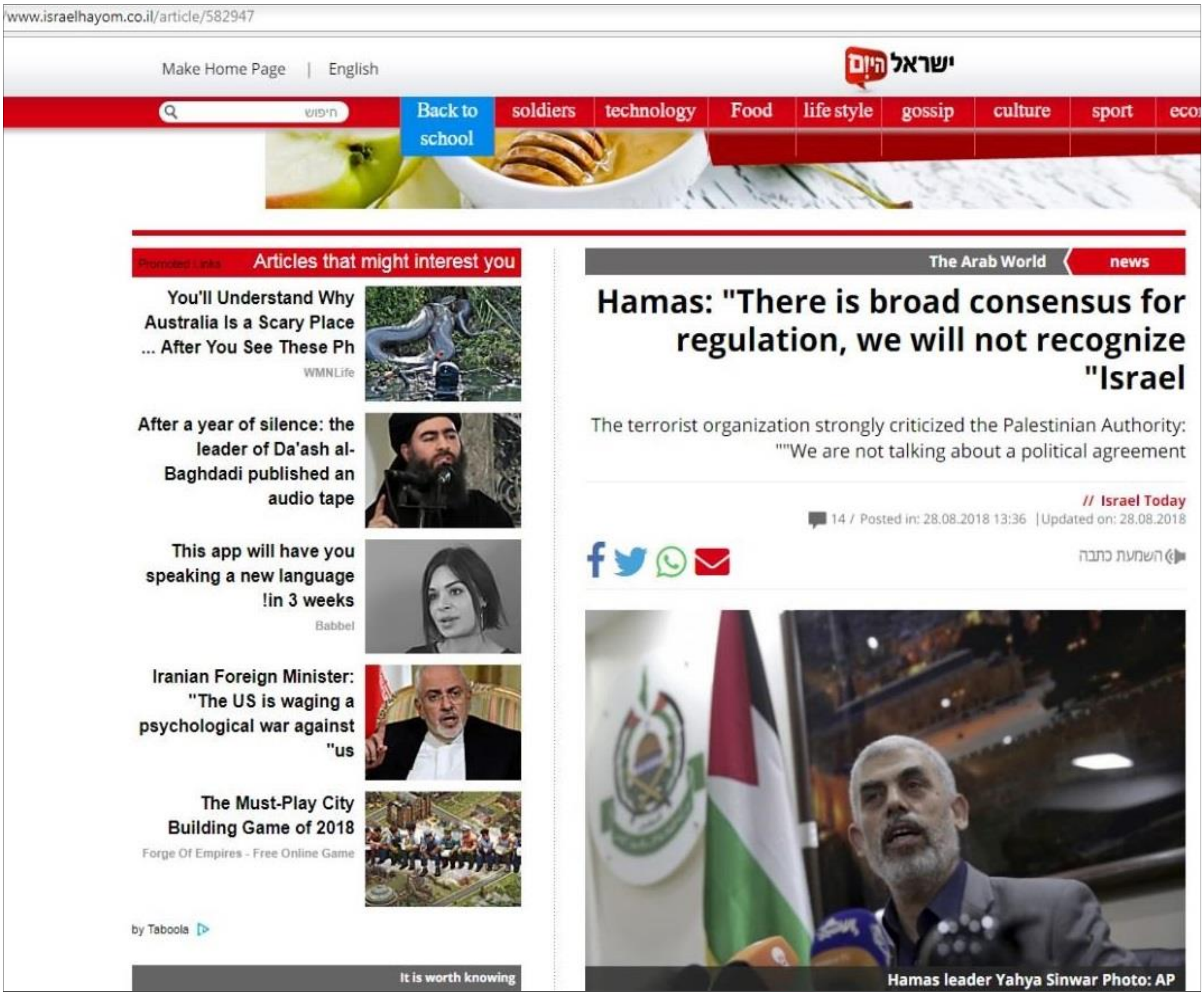
Jabhat al-Nusra and other militants in Idlib stand no chance against t
Syrian military, backed by Russia and Iran, but Western interference
give them a fighting chance. The US and its allies are making every e
to preserve jihadist forces and use them to remove Syrian president
Bashar Assad from power, Russian Foreign Minister Sergey Lavrov
recently said .

And if the violence escalates in Idlib, the two million strong populatio
the northern province will be put in grave danger as the terrorists
basically hold the people hostage and use them as a human shield.

The Russian Reconciliation Center continues talks to achieve a peacef
resolution of the Idlib standoff. However, the militants seem reluctan
lay down their arms, which makes the coming days crucial for the fat
Idlib and the whole of Syria.

https://www.rt.com/news/437136-idlib-provocation-lavrov-nusra/

Image 11 – copied references and links



www.israelhayom.co.il/article/582947

Promoted Links Articles that might interest you

You'll Understand Why Australia Is a Scary Place ... After You See These Ph
WMNLife

After a year of silence: the leader of Da'ash al-Baghdadi published an audio tape

This app will have you speaking a new language !in 3 weeks
Babbel

Iranian Foreign Minister: "The US is waging a psychological war against "us

The Must-Play City Building Game of 2018
Forge Of Empires - Free Online Game

by Taboola

It is worth knowing

The Arab World | news

Hamas: "There is broad consensus for regulation, we will not recognize "Israel

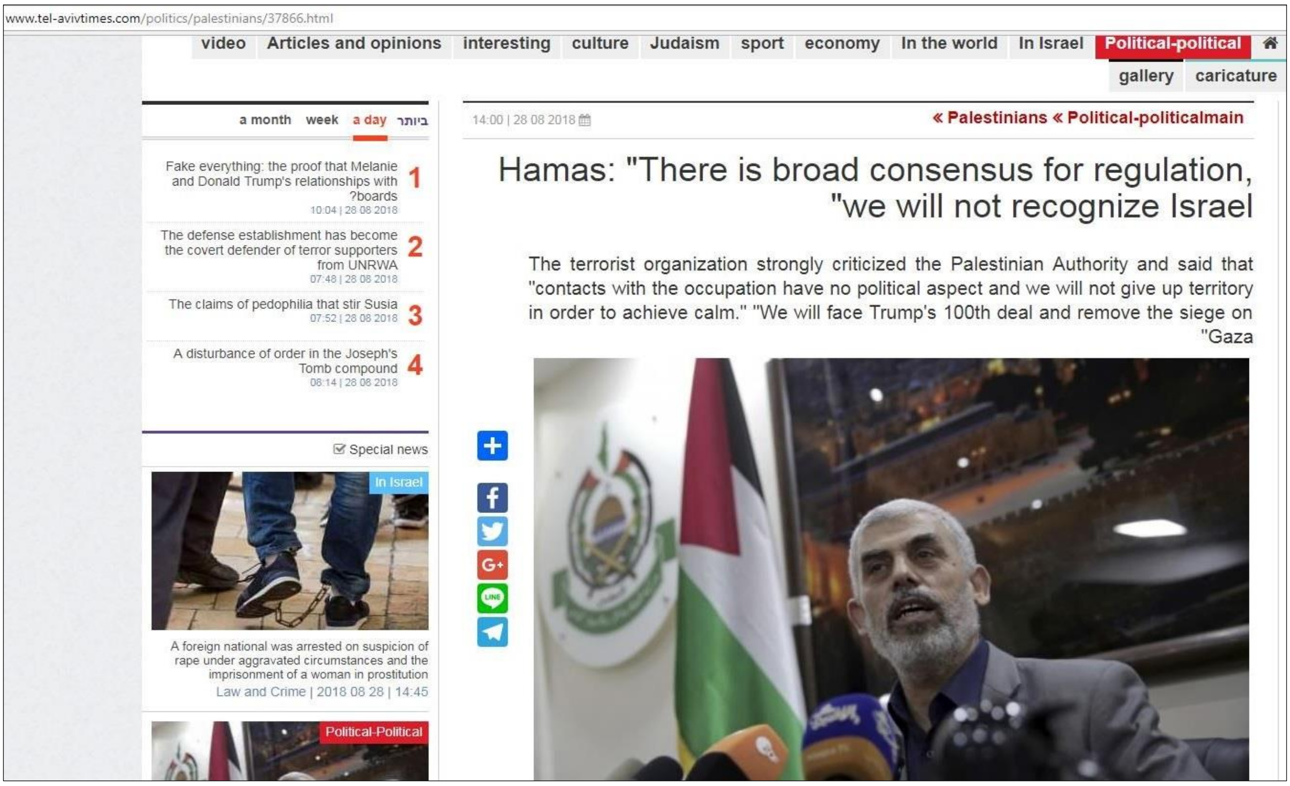
The terrorist organization strongly criticized the Palestinian Authority: ""We are not talking about a political agreement

// Israel Today
14 / Posted in: 28.08.2018 13:36 |Updated on: 28.08.2018

השמעת כתבה

Hamas leader Yahya Sinwar Photo: AP

Image 12 – the original article



www.tel-avivtimes.com/politics/palestinians/37866.html

14:00 | 28 08 2018

« Palestinians « Political-politicalmain

Hamas: "There is broad consensus for regulation, "we will not recognize Israel

The terrorist organization strongly criticized the Palestinian Authority and said that "contacts with the occupation have no political aspect and we will not give up territory in order to achieve calm." "We will face Trump's 100th deal and remove the siege on "Gaza

1 Fake everything: the proof that Melanie and Donald Trump's relationships with ?boards
10:04 | 28 08 2018

2 The defense establishment has become the covert defender of terror supporters from UNRWA
07:48 | 28 08 2018

3 The claims of pedophilia that stir Susia
07:52 | 28 08 2018

4 A disturbance of order in the Joseph's Tomb compound
08:14 | 28 08 2018

☑ Special news

A foreign national was arrested on suspicion of rape under aggravated circumstances and the imprisonment of a woman in prostitution
Law and Crime | 2018 08 28 | 14:45

Image 13 – the copied and modified article

The table below compares the original articles that were published in Israeli media outlets and article with modified content that were published on fake news website (the headlines were translated via google translate):

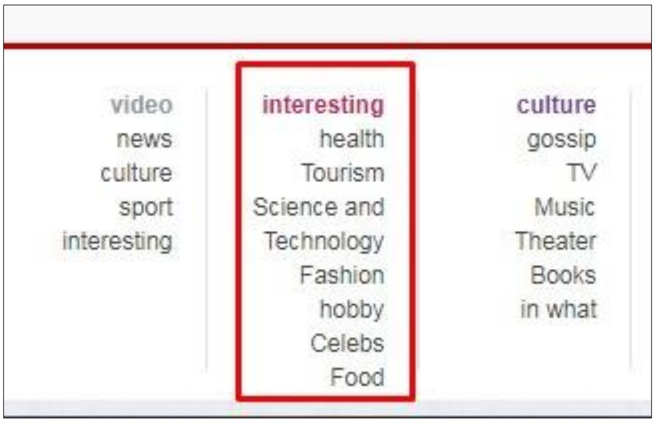
Original media outlet	Original Headline	Fake Headline	Changes
Maariv[4]	"Israel must be ready for war in order to prevent Iran from growing stronger in Syria"	"Israel **must go to war** in order to prevent Iran from growing stronger in Syria"	The term "must be ready" was replaced by "Israel must go to war". The reader may understand that the quoted, an IDF general, thinks that Israel must start a war in Syria.
Globes[5]	An Iranian force fired 20 rockets into the Golan; The IDF attacked targets in Syria "Iron Dome" intercepted some of the rounds and alarms were activated in the area, and in response Israel bombed a number of targets of the Revolutionary Guards and the Assad regime. IDF: **No rocket hits target, Iran fails**. "Proof Trump was right"	**IDF fear**: Iranian force fired 20 rockets into Golan For the first time, the State of Israel confirms that its forces are acting against Iranian targets in Syria, in response to dozens of missiles fired by Iran. IDF: "Attempt to respond will respond harshly"	Adding the opening "IDF fear" and deleting the response of Israel to this attack. Deleting several points in the original report, such as IDF's declaration.

Table 4 – comparison between original and modified content

[4] http://www.maariv.co.il/news/military/Article-659131
[5] https://www.globes.co.il/news/article.aspx?did=1001235462

In order to increase the websites' credibility, the operators also add non-political content. Nevertheless, in many cases, there are subtle indicators that shows the forgery, such as minor spelling errors. This most often appears in content that was not copied directly from other sources.

For instance, in the fraudulent Israeli website, there are spelling error and missuses of words. For instance, the category "Hobbies and leisure" was translated to the word "Interesting" which means in Hebrew "I find it interesting".


video
news
culture
sport
interesting

interesting
health
Tourism
Science and Technology
Fashion
hobby
Celebs
Food

culture
gossip
TV
Music
Theater
Books
in what

Image 14 – indicator of fake website

Social Network

Each one of the websites has accompanying profiles and accounts on various social media platforms, mainly Facebook, Twitter, Instagram and Telegram. If a website has multiple language variants, there will also be associated social media accounts. Following our report to Facebook and Twitter, some of the profiles have been terminated.

There are generally two types of accounts in this infrastructure:

1. Accounts and pages that claim to be the official pages of the fake media outlets. These pages go by the same handle of the websites.
2. Accounts that impersonate real people, usually attractive woman, from the country the website is targeting. These accounts reach out and contact thousands of people and propagate via their feed the websites' articles.

Seen in the images below, are the various links between the fake Pakistani website sachtimes[.]com and its social media profile trackers, as crawled by RiskIQ[6]:

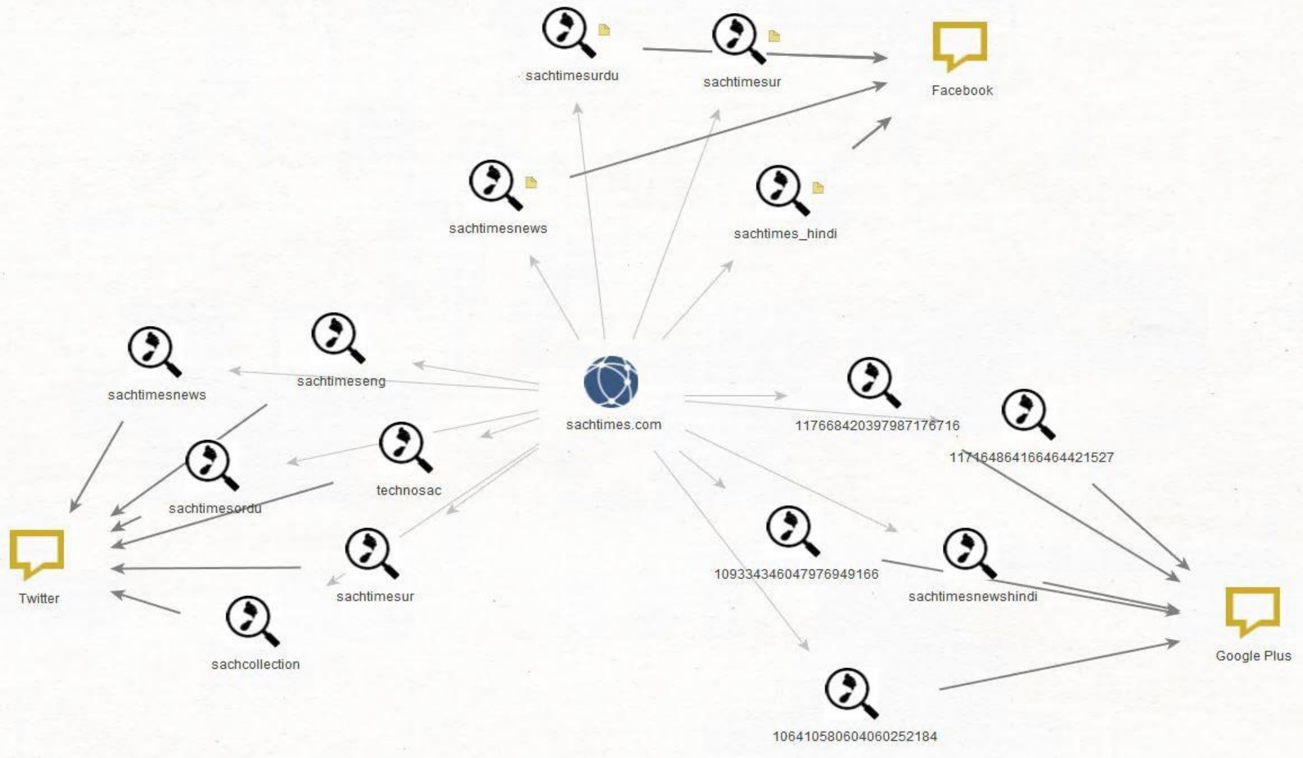


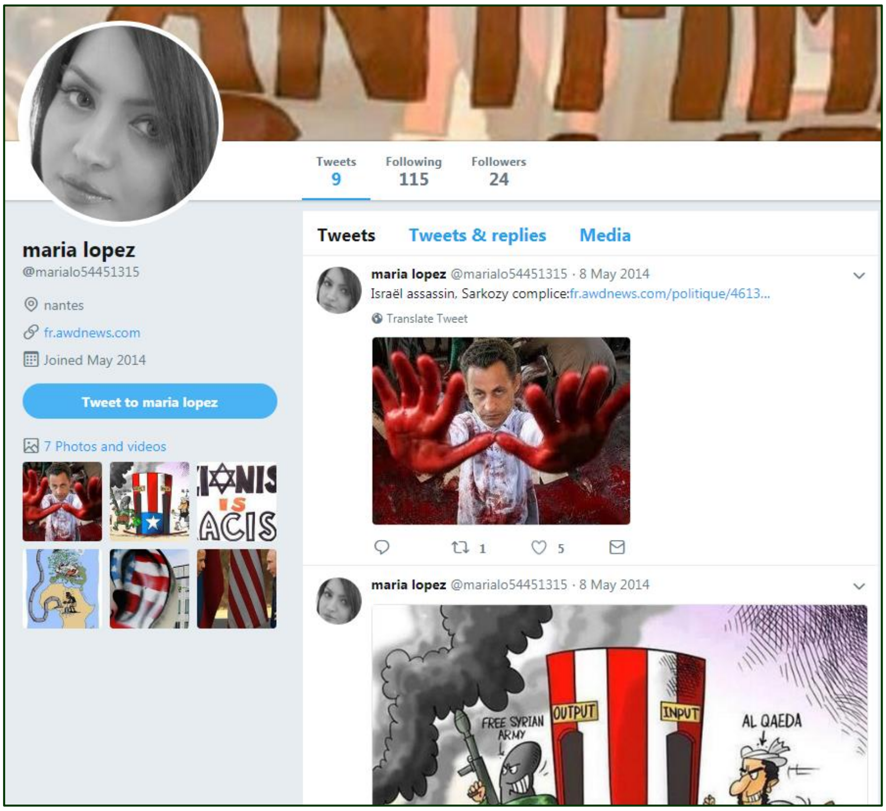
Image 15 – links between a fake website and its proxy social media profiles

[6] https://community.riskiq.com/search/sachtimes.com

Fake profiles

Below are three examples of fake profile spreading articles by the disinformation websites.

Maria Lopez – Impersonates a woman of French nationality. This account promotes the European fake media outlet "AWD news".



Tweets 9 | Following 115 | Followers 24

maria lopez
@marialo54451315
nantes
fr.awdnews.com
Joined May 2014
Tweet to maria lopez
7 Photos and videos

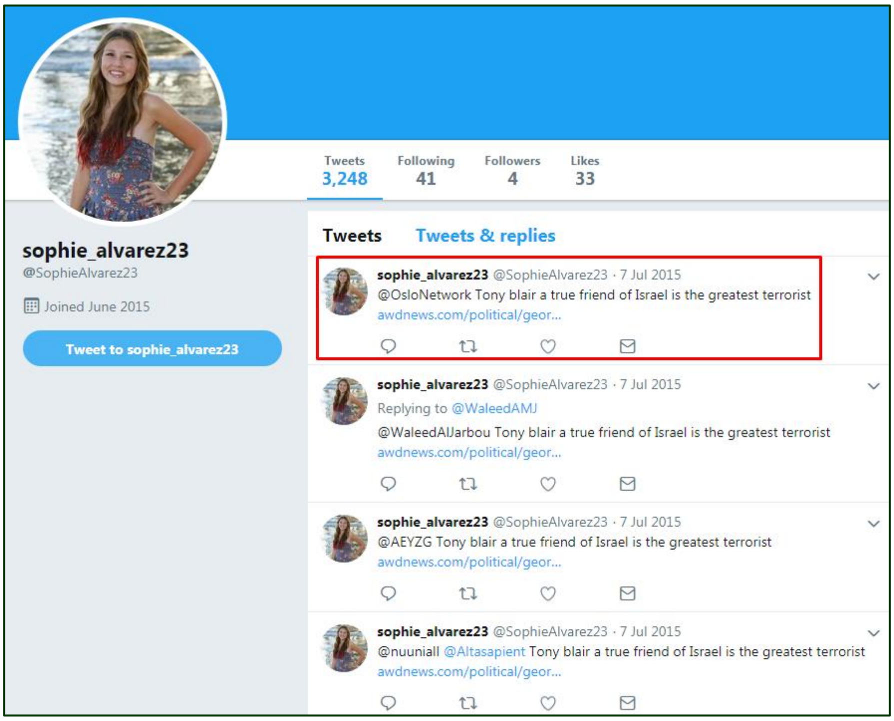
Tweets | Tweets & replies | Media

maria lopez @marialo54451315 · 8 May 2014
Israël assassin, Sarkozy complice:fr.awdnews.com/politique/4613...
Translate Tweet
1 5

maria lopez @marialo54451315 · 8 May 2014

Image 16 – fake social account of "Maria Lopez"

Sophie Alvarez – Impersonates a woman of British nationality. This account promotes the European fake media outlet "AWD news". Note that on 2016, a Facebook's account with the same name was exposed as part a Fake News campaign in French[7].



Tweets 3,248 | Following 41 | Followers 4 | Likes 33

sophie_alvarez23
@SophieAlvarez23
Joined June 2015
Tweet to sophie_alvarez23

Tweets | Tweets & replies

sophie_alvarez23 @SophieAlvarez23 · 7 Jul 2015
@OsloNetwork Tony blair a true friend of Israel is the greatest terrorist
awdnews.com/political/geor...

sophie_alvarez23 @SophieAlvarez23 · 7 Jul 2015
Replying to @WaleedAMJ
@WaleedAlJarbou Tony blair a true friend of Israel is the greatest terrorist
awdnews.com/political/geor...

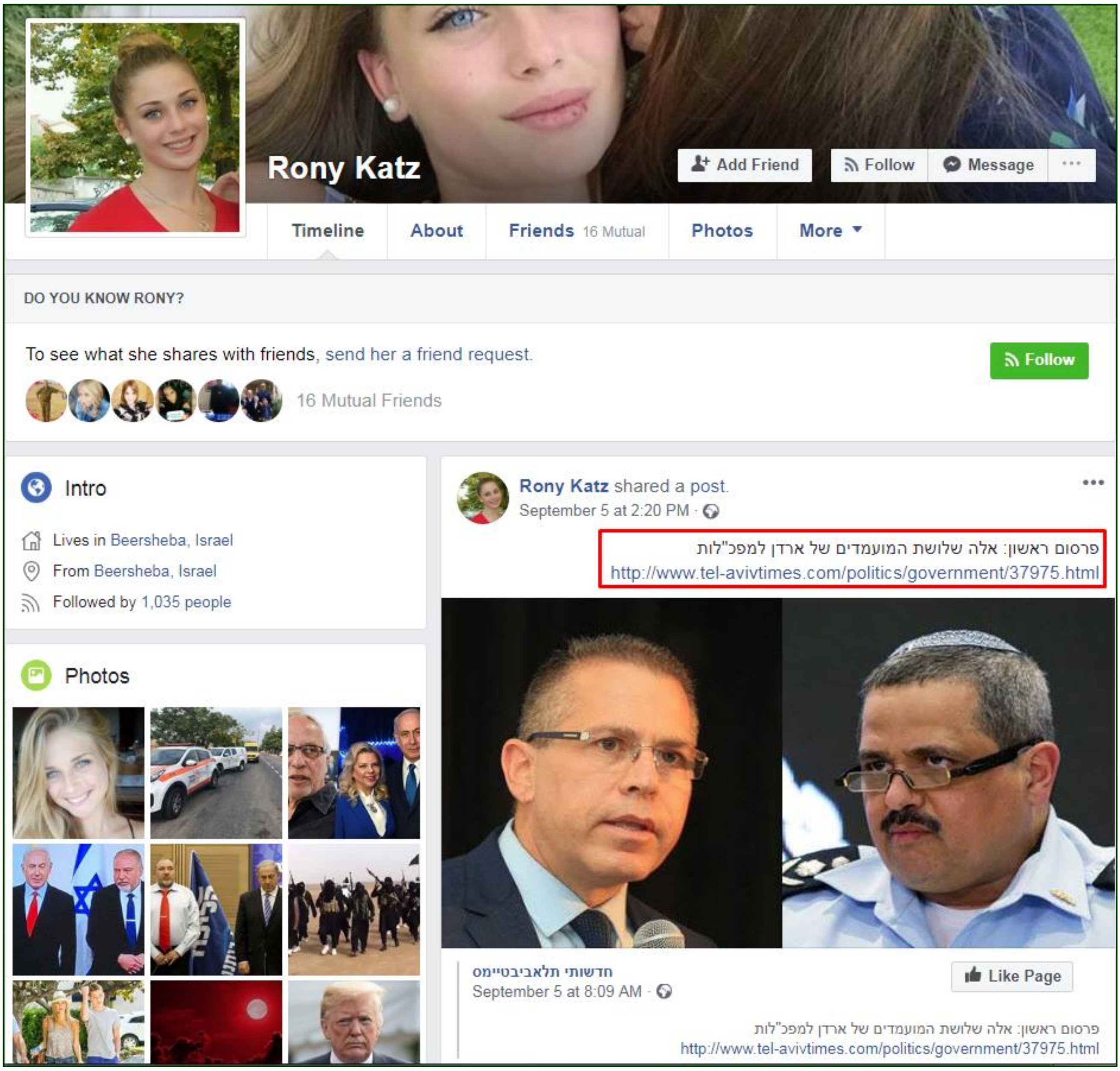
sophie_alvarez23 @SophieAlvarez23 · 7 Jul 2015
@AEYZG Tony blair a true friend of Israel is the greatest terrorist
awdnews.com/political/geor...

sophie_alvarez23 @SophieAlvarez23 · 7 Jul 2015
@nuuniall @Altasapient Tony blair a true friend of Israel is the greatest terrorist
awdnews.com/political/geor...

Image 17 – fake social account of " Sophie Alvarez "

[7] https://arretsurinfo.ch/enquete-sur-un-intrigant-site-internet-de-desinformation-mainstream-awdnews/

Roni Katz – Impersonates a woman of Israeli nationality. This account promotes the Israel fake media outlet "Tel Aviv Times":



DO YOU KNOW RONY?

To see what she shares with friends, send her a friend request.

16 Mutual Friends

Lives in Beersheba, Israel

From Beersheba, Israel

Followed by 1,035 people

Rony Katz shared a post.
September 5 at 2:20 PM ·

פרסום ראשון: אלה שלושת המועמדים של ארדן למפכ"לות
http://www.tel-avivtimes.com/politics/government/37975.html

חדשותי תלאביבטיימס
September 5 at 8:09 AM ·

פרסום ראשון: אלה שלושת המועמדים של ארדן למפכ"לות
http://www.tel-avivtimes.com/politics/government/37975.html

Image 18 – fake social account of " Roni Katz "

Note – additional examples of fake news website and their associated social media accounts can be seen in "Appendix 1 – additional information and images"

CLEARSKY
Cyber Security

Digital Infrastructure

Digital Infrastructure

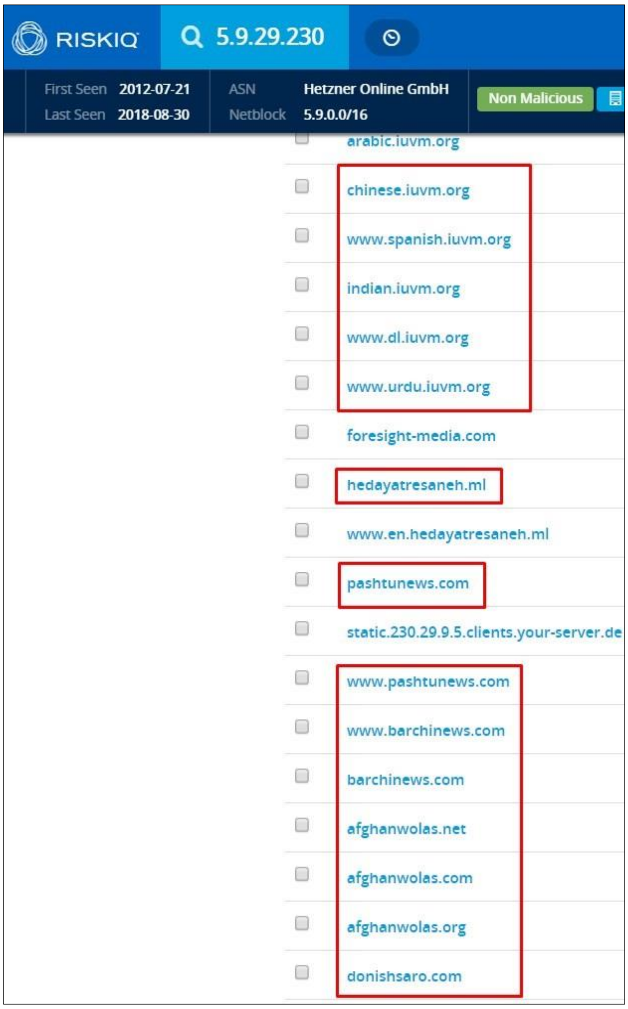
This infrastructure is comprised of over 200 domains, most of which are protected by Cloudflare. However, in its early stages of the operation, the websites were hosted on several different services, with no privacy protection.

In order to determine whether a website is a Fake News website or not, we required a strong indicator that connects the website to the infrastructure; such as IPs and/or specific Whois records attributed to the operators. Then, we examined the content of each website in order to assess whether its content was original or copied from other legitimate websites. We also looked for any indications of inauthenticity such as omission of authors' name, suspicious links, misspelling, different articles in the different languages on the same site, and whether the website promotes the operation's agendas.

Technical Links

The main IP in the infrastructure was 5.9.29.230. We identified 183 domains and subdomains hosted on it. Note that a number of them (e.g. iuvm[.]net) were exposed on the joint Reuters - Clearsky report[8]. This IP was part of the infrastructure between 2016-2017.

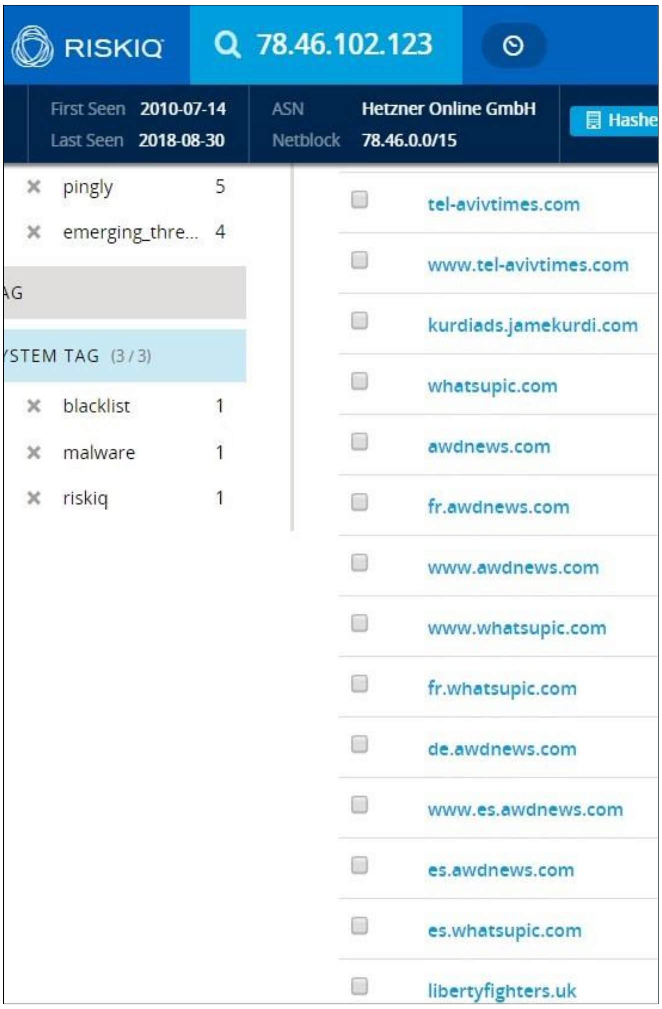
Another malicious IP in this infrastructure is 78.46.102.123. This IP was part of the operation between 2015 to 2017. This IP is of note as it has relatively a small number of domains, however, each one of them has a widely different theme, such as representing different regions (Israel, Europe, US, Kurdistan authority):



First Seen 2012-07-21
Last Seen 2018-08-30
ASN Hetzner Online GmbH
Netblock 5.9.0.0/16

- arabic.iuvm.org
- chinese.iuvm.org
- www.spanish.iuvm.org
- indian.iuvm.org
- www.dl.iuvm.org
- www.urdu.iuvm.org
- foresight-media.com
- hedayatresaneh.ml
- www.en.hedayatresaneh.ml
- pashtunews.com
- static.230.29.9.5.clients.your-server.de
- www.pashtunews.com
- www.barchinews.com
- barchinews.com
- afghanwolas.net
- afghanwolas.com
- afghanwolas.org
- donishsaro.com

Image 19 – domains hosted on IP 5.9.29.230



First Seen 2010-07-14
Last Seen 2018-08-30
ASN Hetzner Online GmbH
Netblock 78.46.0.0/15

pingly	5
emerging_thre...	4
blacklist	1
malware	1
riskiq	1

- tel-avivtimes.com
- www.tel-avivtimes.com
- kurdiads.jamekurdi.com
- whatsupic.com
- awdnews.com
- fr.awdnews.com
- www.awdnews.com
- www.whatsupic.com
- fr.whatsupic.com
- de.awdnews.com
- www.es.awdnews.com
- es.awdnews.com
- es.whatsupic.com
- libertyfighters.uk

Image 20 – domains hosted on IP 78.46.102.123

[8] https://www.reuters.com/article/us-usa-trump-tech/white-house-probes-google-after-trump-accuses-it-of-biasidUSKCN1LD1I1

Most of the domains were linked to both IP address in different times, as seen below:

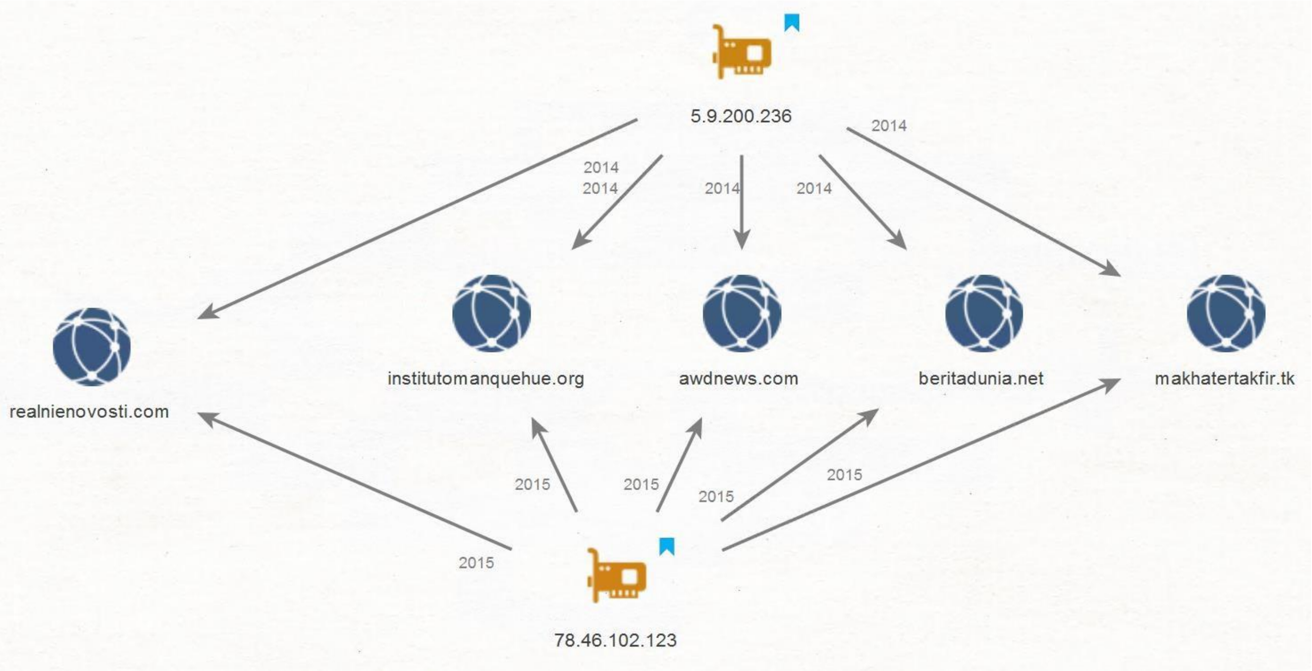
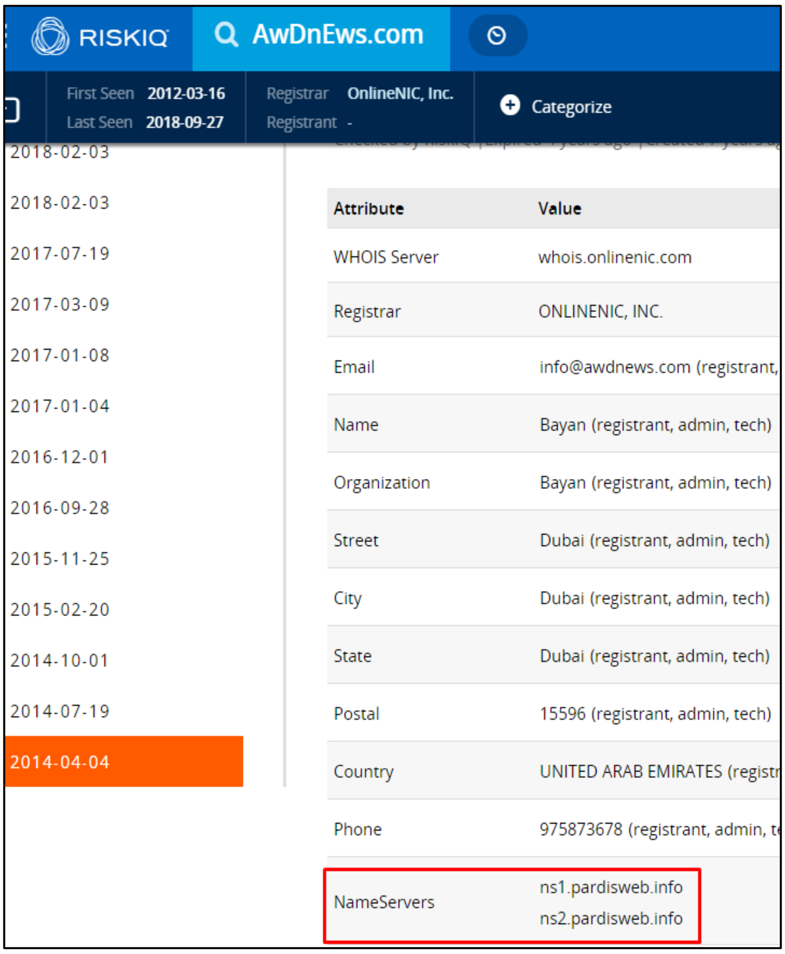


Image 21 – links between domains and IPs

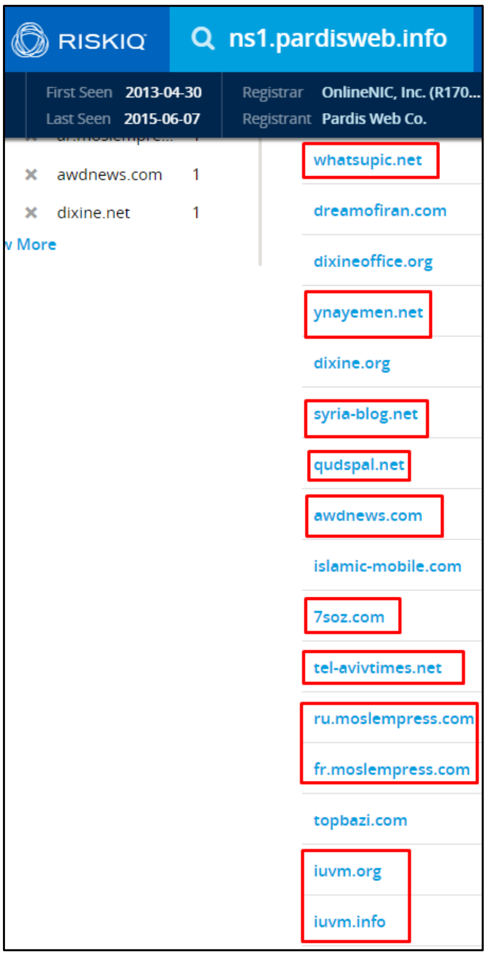
One of the most active domains in this infrastructure is awdnews[.]com[9]. According to the whois records, this website used the name server ns1[.]pardisweb[.]info, which is an Iranian hosting service that we believe is part of this operation. We identified many fake news websites that were hosted in this NS:



First Seen 2012-03-16
Last Seen 2018-09-27
Registrar OnlineNIC, Inc.
Registrant -

2018-02-03
2018-02-03
2017-07-19
2017-03-09
2017-01-08
2017-01-04
2016-12-01
2016-09-28
2015-11-25
2015-02-20
2014-10-01
2014-07-19
2014-04-04

Attribute	Value
WHOIS Server	whois.onlinenic.com
Registrar	ONLINENIC, INC.
Email	info@awdnews.com (registrant,
Name	Bayan (registrant, admin, tech)
Organization	Bayan (registrant, admin, tech)
Street	Dubai (registrant, admin, tech)
City	Dubai (registrant, admin, tech)
State	Dubai (registrant, admin, tech)
Postal	15596 (registrant, admin, tech)
Country	UNITED ARAB EMIRATES (registr
Phone	975873678 (registrant, admin, t
NameServers	ns1.pardisweb.info ns2.pardisweb.info



First Seen 2013-04-30
Last Seen 2015-06-07
Registrar OnlineNIC, Inc. (R170...
Registrant Pardis Web Co.

awdnews.com	1
dixine.net	1

whatsupic.net
dreamofiran.com
dixineoffice.org
ynayemen.net
dixine.org
syria-blog.net
qudspal.net
awdnews.com
islamic-mobile.com
7soz.com
tel-avivtimes.net
ru.moslempress.com
fr.moslempress.com
topbazi.com
iuvm.org
iuvm.info

Image 22 – links between domains and IPs

Image 23 – domains hosted on ns1[.]pardisweb[.]info

[9] https://community.riskiq.com/search/AwDnEws.com

As of late November 2018, several of the websites still have unique whois records. Some of the details point to Iran, even though one would expect them to be registered in countries that the news media outlets claim to represent.

For instance, the Turkish website 7soz[.]net was registered by Ebrahim Erfani from Tehran. This actor registered another domain, imamiaturbiat[.]org. It should be noted that currently this domain is offered to sale, however, originally it was registered by Ebrahim Erfani and Kaveh Khaleghi. Khaleghi himself was the registrant of a few sites in this infrastructure, as presented below:

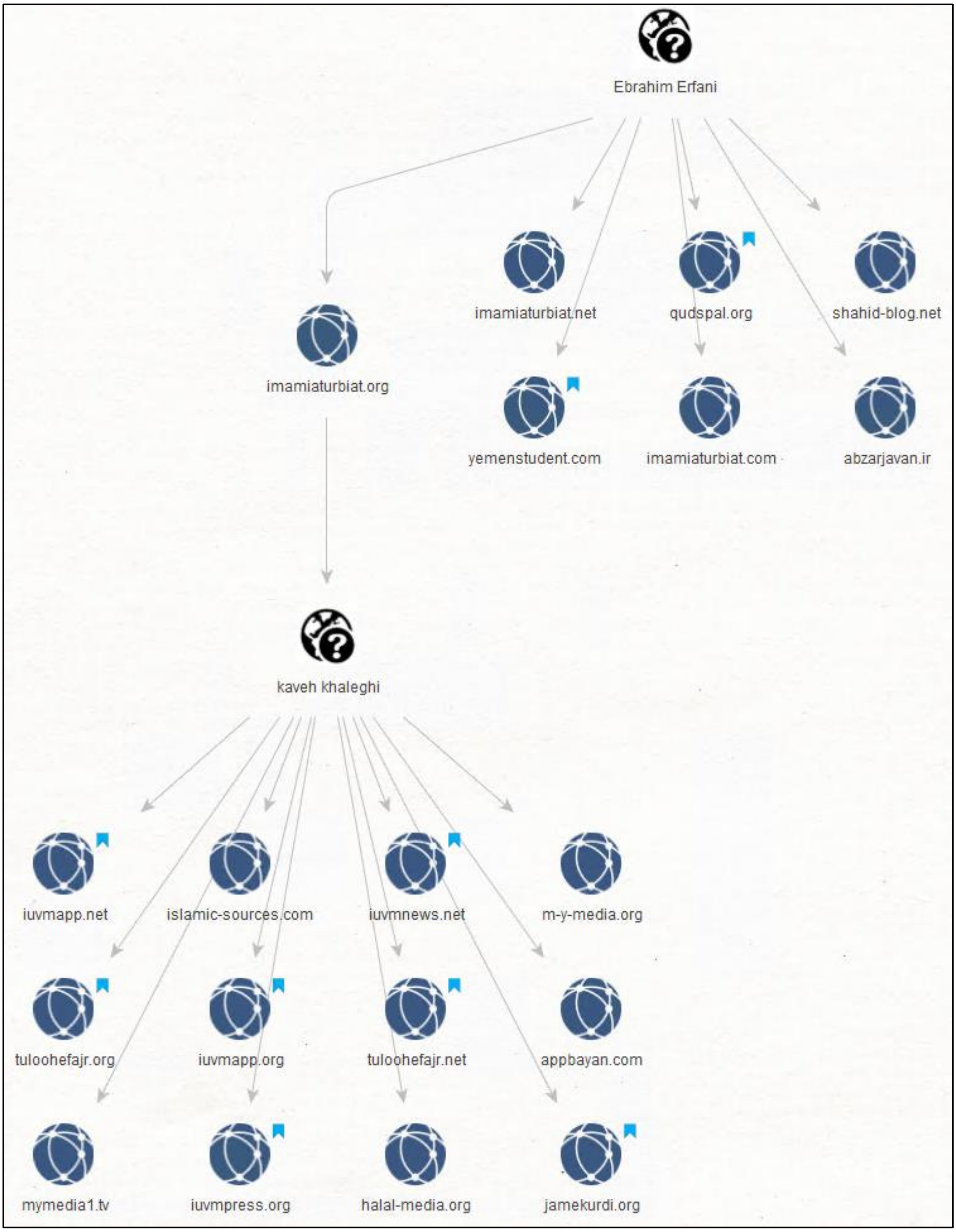
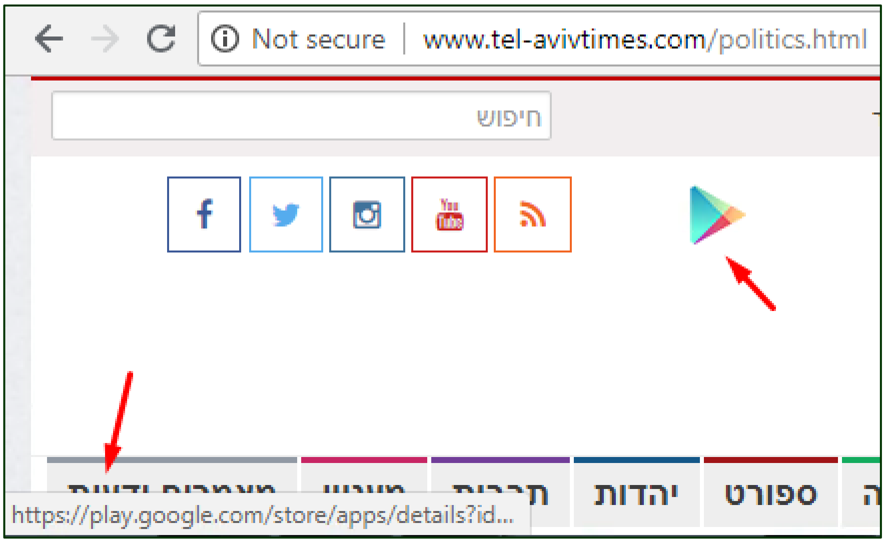


Image 24 – links between Ebrahim Erfani/Kaveh Khaleghi and fake news websites

Mobile Applications

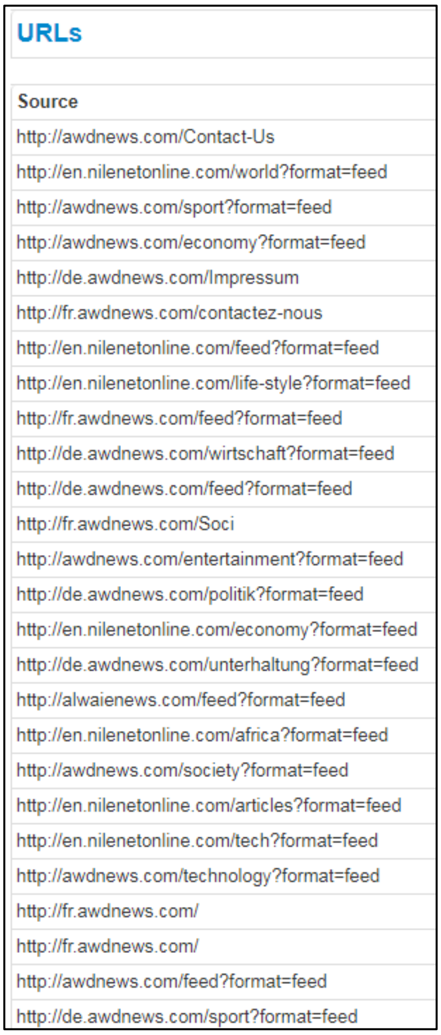
Android news-feed applications are available for several of the fake media outlets. These apps do not contain malicious code. Rather, they are used as another channel of propagation. A number of these apps were available to download from Google's official app store (Google play), as seen in the following image:



https://play.google.com/store/apps/details?id...

Image 25 – fake news-feed apps linked to download from Google Play

We identified multiple URLs that were embedded in the fake Israeli app. Although these URLs are part of the infrastructure, they should not have any connection to the Israeli website[10]:



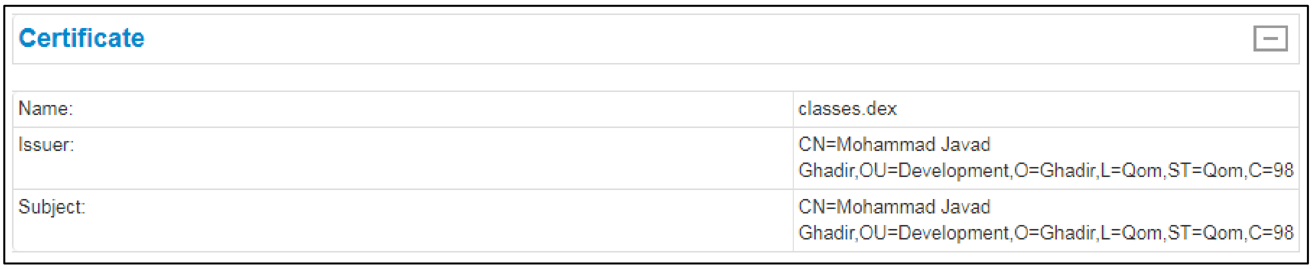
URLs

Source
http://awdnews.com/Contact-Us
http://en.nilenetonline.com/world?format=feed
http://awdnews.com/sport?format=feed
http://awdnews.com/economy?format=feed
http://de.awdnews.com/Impressum
http://fr.awdnews.com/contactez-nous
http://en.nilenetonline.com/feed?format=feed
http://en.nilenetonline.com/life-style?format=feed
http://fr.awdnews.com/feed?format=feed
http://de.awdnews.com/wirtschaft?format=feed
http://de.awdnews.com/feed?format=feed
http://fr.awdnews.com/Soci
http://awdnews.com/entertainment?format=feed
http://de.awdnews.com/politik?format=feed
http://en.nilenetonline.com/economy?format=feed
http://de.awdnews.com/unterhaltung?format=feed
http://alwaienews.com/feed?format=feed
http://en.nilenetonline.com/africa?format=feed
http://awdnews.com/society?format=feed
http://en.nilenetonline.com/articles?format=feed
http://en.nilenetonline.com/tech?format=feed
http://awdnews.com/technology?format=feed
http://fr.awdnews.com/
http://fr.awdnews.com/
http://awdnews.com/feed?format=feed
http://de.awdnews.com/sport?format=feed

Image 26

[10] https://www.joesandbox.com/analysis/75302/0/html

According to the certificate of the app linked to the fake Russian website Realnienovosti, its developer is Mohammad Javad Ghadir from the city of Qom (North-west Iran)[11]:

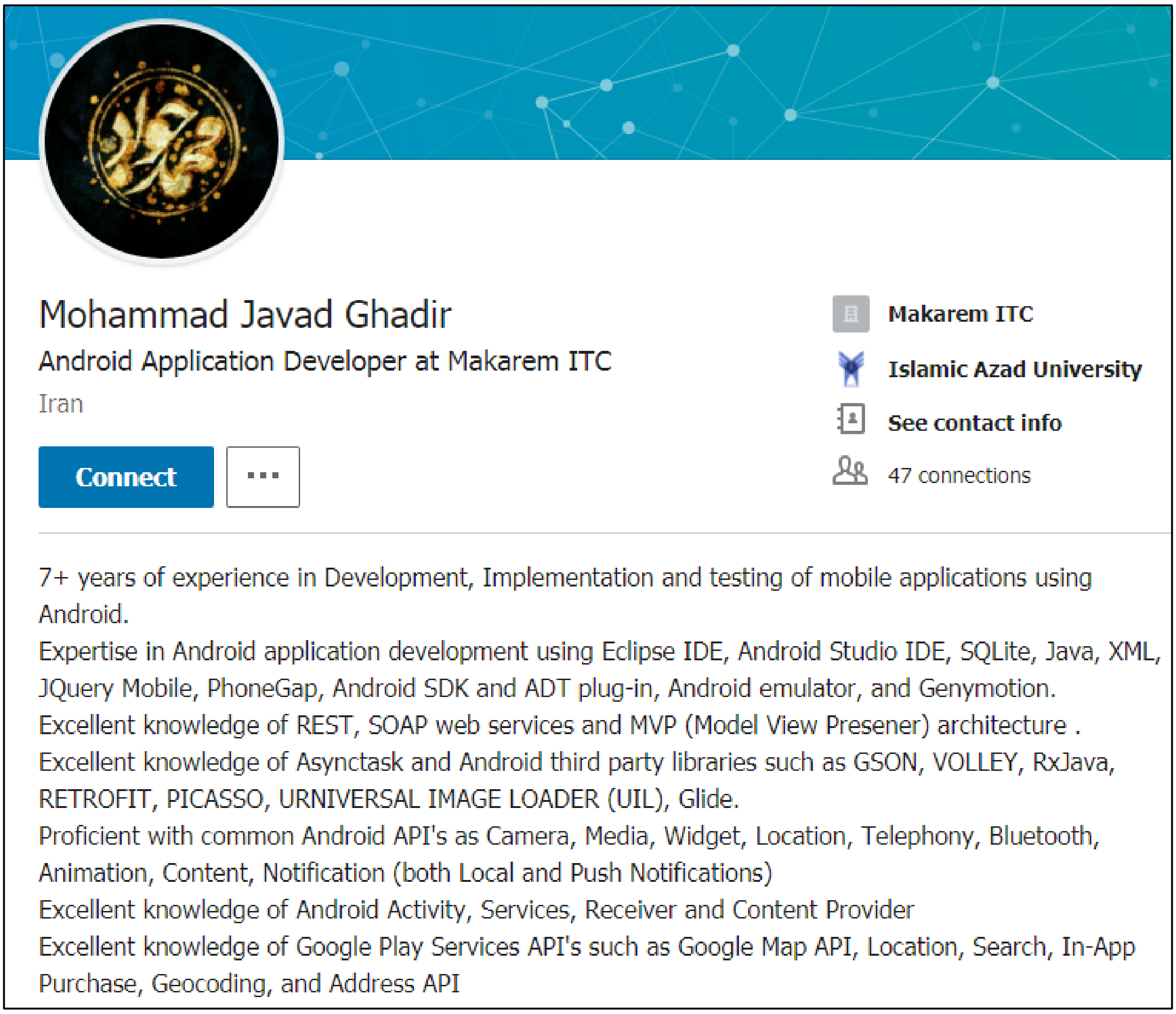


Certificate

Name:	classes.dex
Issuer:	CN=Mohammad Javad Ghadir,OU=Development,O=Ghadir,L=Qom,ST=Qom,C=98
Subject:	CN=Mohammad Javad Ghadir,OU=Development,O=Ghadir,L=Qom,ST=Qom,C=98

Image 27 – certificate details of the app

We identified the LinkedIn of this person, who presents himself as an Android Application Developer in an Iranian company located in Qom[12].



Mohammad Javad Ghadir

Android Application Developer at Makarem ITC

Iran

7+ years of experience in Development, Implementation and testing of mobile applications using Android.
Expertise in Android application development using Eclipse IDE, Android Studio IDE, SQLite, Java, XML, JQuery Mobile, PhoneGap, Android SDK and ADT plug-in, Android emulator, and Genymotion.
Excellent knowledge of REST, SOAP web services and MVP (Model View Presener) architecture .
Excellent knowledge of Asynctask and Android third party libraries such as GSON, VOLLEY, RxJava, RETROFIT, PICASSO, URNIVERSAL IMAGE LOADER (UIL), Glide.
Proficient with common Android API's as Camera, Media, Widget, Location, Telephony, Bluetooth, Animation, Content, Notification (both Local and Push Notifications)
Excellent knowledge of Android Activity, Services, Receiver and Content Provider
Excellent knowledge of Google Play Services API's such as Google Map API, Location, Search, In-App Purchase, Geocoding, and Address API

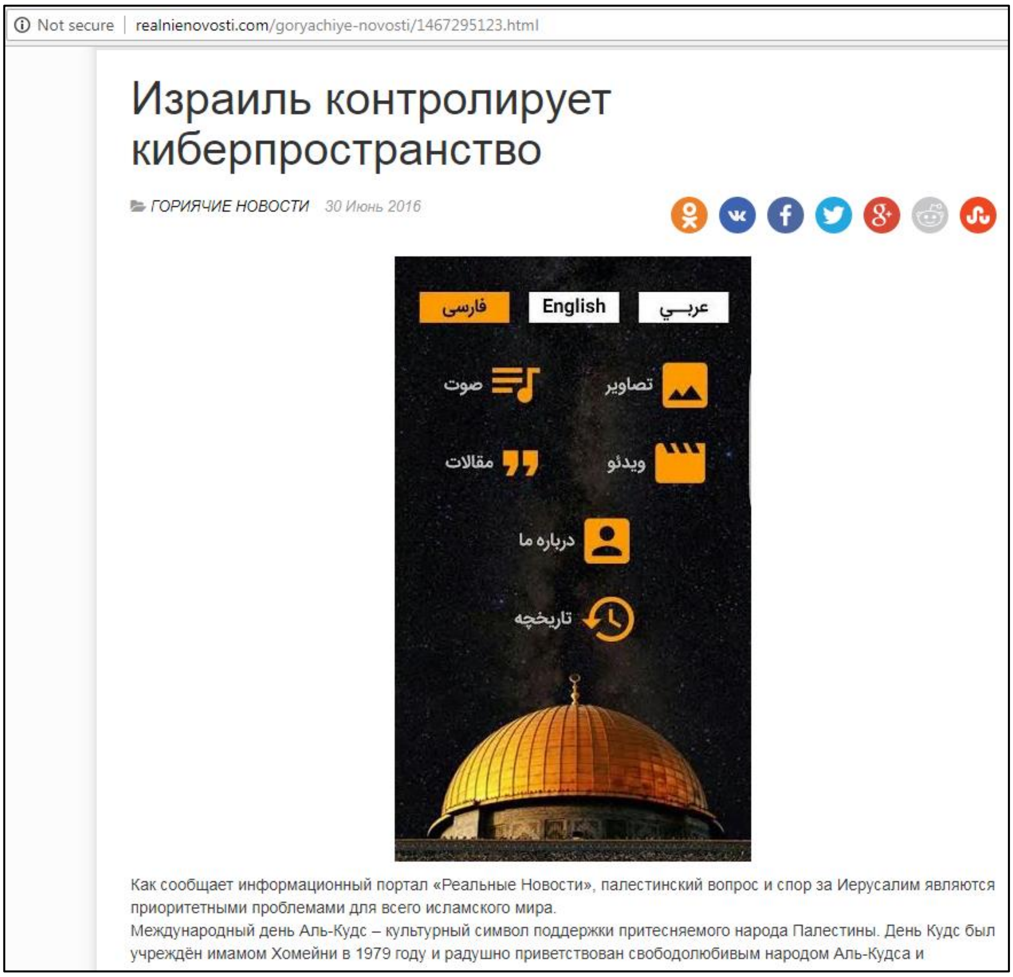
Image 28 - Mohammad Javad Ghadir's LinkedIn profile

The fake Russian website itself promotes other Iranian apps, including an app that distribute information regarding the Quds day[13]. This app is available to download from the Iranian apk market "AppBayan", which is registered by Kaveh Khaleghi, one of the operators of the infrastructure. Note that Bayan was the registrant organization of many sites of the infrastructure.

[11] https://www.joesandbox.com/analysis/80454/0/html

[12] https://www.linkedin.com/in/mjghadir/

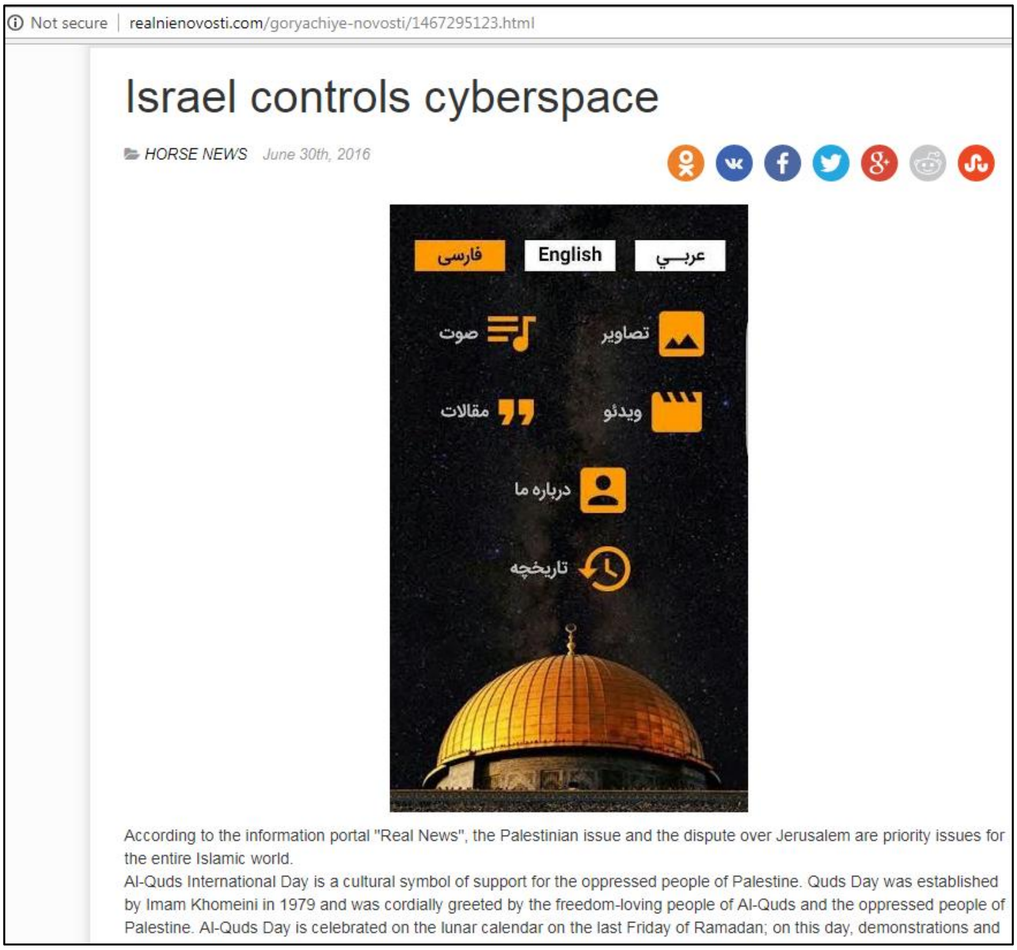
[13] The International Quds Day is an annual event held on the last Friday of Ramadan that was initiated by the Islamic Republic of Iran in 1979 to express support for the Palestinians and oppose Zionism and Israel. In Iran, the government sponsors and organizes the day's rallies, and its celebration in that country has had a long tradition of voicing anti-Semitic attacks. Quds Day events in Iran also feature demonstrations against other rivals of Iran, including the United States and Saudi Arabia.


ⓘ Not secure | realnienovosti.com/goryachiye-novosti/1467295123.html
فارسی
English
عربـــي
صوت
تصاوير
مقالات
ويدئو
درباره ما
تاريخچه

Израиль контролирует киберпространство

ГОРЯЧИЕ НОВОСТИ 30 Июнь 2016

Как сообщает информационный портал «Реальные Новости», палестинский вопрос и спор за Иерусалим являются приоритетными проблемами для всего исламского мира.
Международный день Аль-Кудс – культурный символ поддержки притесняемого народа Палестины. День Кудс был учреждён имамом Хомейни в 1979 году и радушно приветствован свободолюбивым народом Аль-Кудса и


ⓘ Not secure | realnienovosti.com/goryachiye-novosti/1467295123.html
فارسی
English
عربـــي
صوت
تصاوير
مقالات
ويدئو
درباره ما
تاريخچه

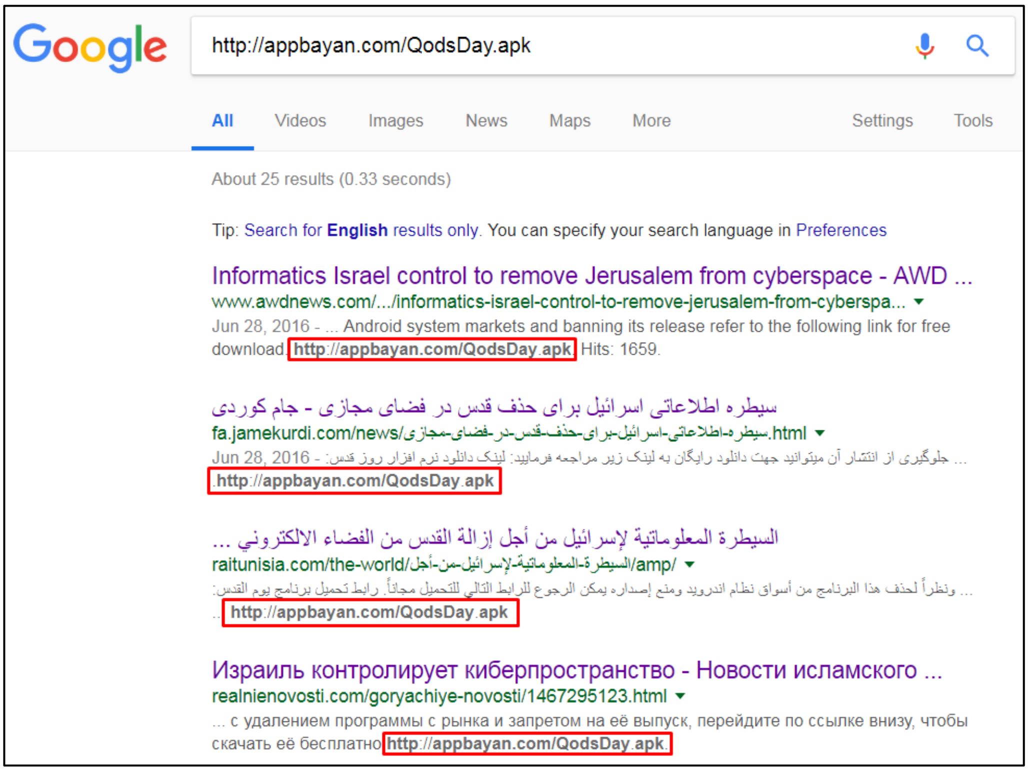
Israel controls cyberspace

HORSE NEWS June 30th, 2016

According to the information portal "Real News", the Palestinian issue and the dispute over Jerusalem are priority issues for the entire Islamic world.
Al-Quds International Day is a cultural symbol of support for the oppressed people of Palestine. Quds Day was established by Imam Khomeini in 1979 and was cordially greeted by the freedom-loving people of Al-Quds and the oppressed people of Palestine. Al-Quds Day is celebrated on the lunar calendar on the last Friday of Ramadan; on this day, demonstrations and

Image 29 and 30 - Realnienovosti website. The translation was done via google translate from Russian

Realnienovosti is not the only website promotes Quds day app. We identified many websites that share the link for Quds Day app. Note that most are part of the infrastructure, but some are legitimate Iranian websites:



About 25 results (0.33 seconds)

Tip: Search for **English** results only. You can specify your search language in Preferences

Informatics Israel control to remove Jerusalem from cyberspace - AWD ...
www.awdnews.com/.../informatics-israel-control-to-remove-jerusalem-from-cyberspa...
Jun 28, 2016 - ... Android system markets and banning its release refer to the following link for free download. **http://appbayan.com/QodsDay.apk**. Hits: 1659.

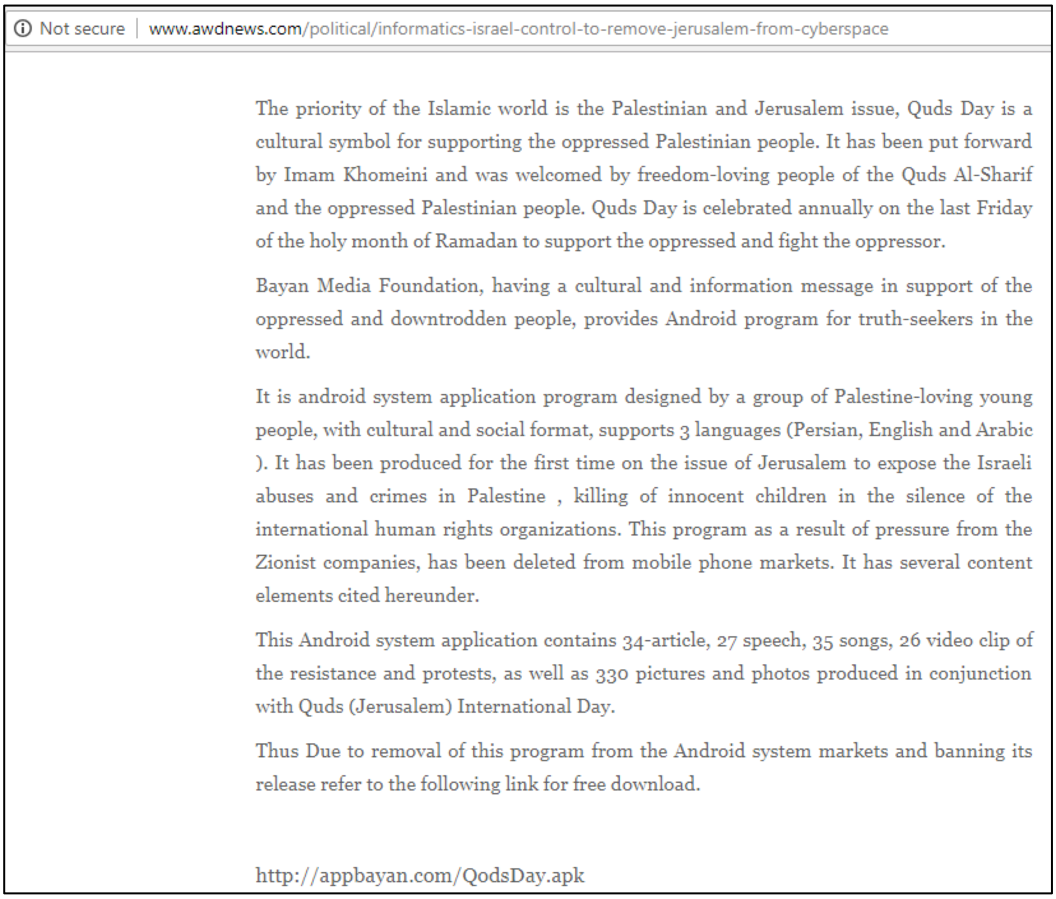
سیطره اطلاعاتی اسرائیل برای حذف قدس در فضای مجازی - جام کوردی
fa.jamekurdi.com/news/سیطره-اطلاعاتی-اسرائیل-برای-حذف-قدس-در-فضای-مجازی.html
Jun 28, 2016 - ... جلوگیری از انتشار آن میتوانید جهت دانلود رایگان به لینک زیر مراجعه فرمایید: لینک دانلود نرم افزار روز قدس:
.**http://appbayan.com/QodsDay.apk**

السيطرة المعلوماتية لإسرائيل من أجل إزالة القدس من الفضاء الالكتروني ...
raitunisia.com/the-world/السيطرة-المعلوماتية-لإسرائيل-من-أجل/amp/
... ونظراً لحذف هذا البرنامج من أسواق نظام اندرويد ومنع إصداره يمكن الرجوع للرابط التالي للتحميل مجاناً. رابط تحميل برنامج يوم القدس:
.. **http://appbayan.com/QodsDay.apk**

Израиль контролирует киберпространство - Новости исламского ...
realnienovosti.com/goryachiye-novosti/1467295123.html
... с удалением программы с рынка и запретом на её выпуск, перейдите по ссылке внизу, чтобы скачать её бесплатно **http://appbayan.com/QodsDay.apk**

Image 31 – Google search showing download links to the app

The fake sites with links to the app are similar and contain the same themes, chiefly explanations about Quds day and the app, and accusation of Israel for "Controlling the cyber space". Moreover, one of the subdomains of appbayan[.]com is ghods[.]appbayan[.]com – Ghods is the right pronouncing of Quds in Persian.


Not secure
www.awdnews.com/political/informatics-israel-control-to-remove-jerusalem-from-cyberspace

The priority of the Islamic world is the Palestinian and Jerusalem issue, Quds Day is a cultural symbol for supporting the oppressed Palestinian people. It has been put forward by Imam Khomeini and was welcomed by freedom-loving people of the Quds Al-Sharif and the oppressed Palestinian people. Quds Day is celebrated annually on the last Friday of the holy month of Ramadan to support the oppressed and fight the oppressor.

Bayan Media Foundation, having a cultural and information message in support of the oppressed and downtrodden people, provides Android program for truth-seekers in the world.

It is android system application program designed by a group of Palestine-loving young people, with cultural and social format, supports 3 languages (Persian, English and Arabic). It has been produced for the first time on the issue of Jerusalem to expose the Israeli abuses and crimes in Palestine , killing of innocent children in the silence of the international human rights organizations. This program as a result of pressure from the Zionist companies, has been deleted from mobile phone markets. It has several content elements cited hereunder.

This Android system application contains 34-article, 27 speech, 35 songs, 26 video clip of the resistance and protests, as well as 330 pictures and photos produced in conjunction with Quds (Jerusalem) International Day.

Thus Due to removal of this program from the Android system markets and banning its release refer to the following link for free download.

http://appbayan.com/QodsDay.apk

Image 32

Global Iranian Disinformation Operation

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

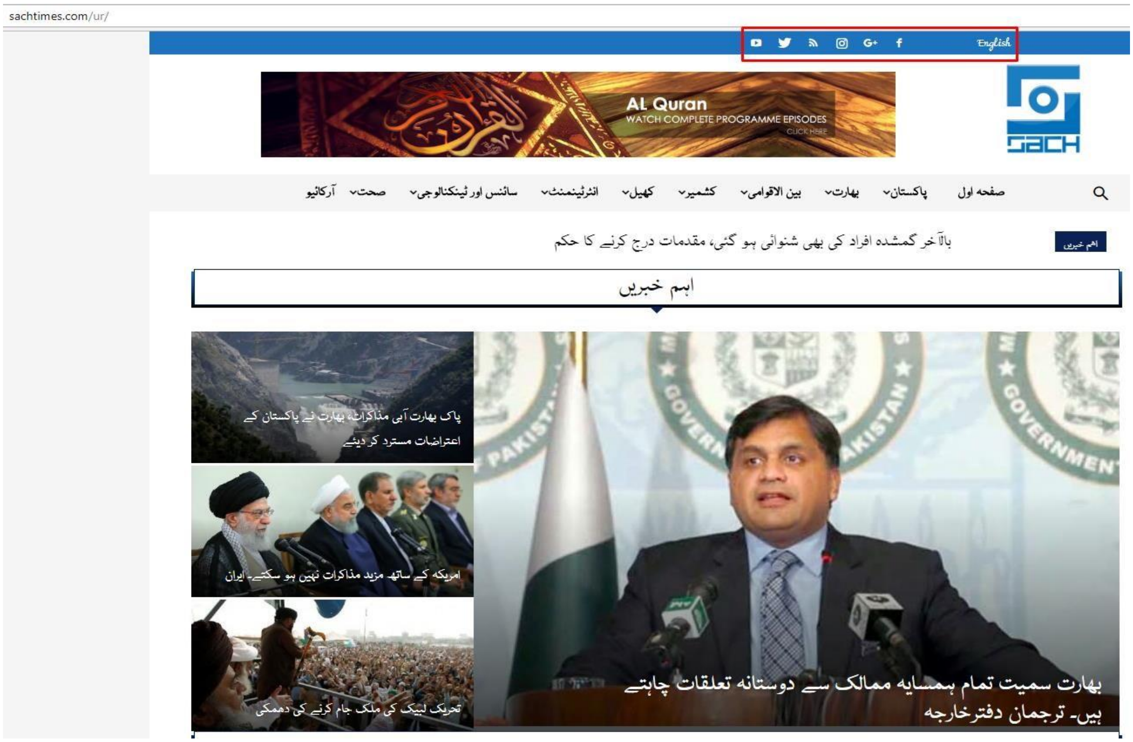
Ahead of the Threat Curve

Large-scale Fake News Infrastructure Promoting Iranian Interests

www.clearskysec.com
info@clearskysec.com

Appendix 1 – additional information and images

Seen in the images below, are the several fake accounts in the social networks impersonate people from UK, France and Israel, distributing articles of the fake websites:



بالآخر گمشدہ افراد کی بھی شنوائی ہو گئی، مقدمات درج کرنے کا حکم

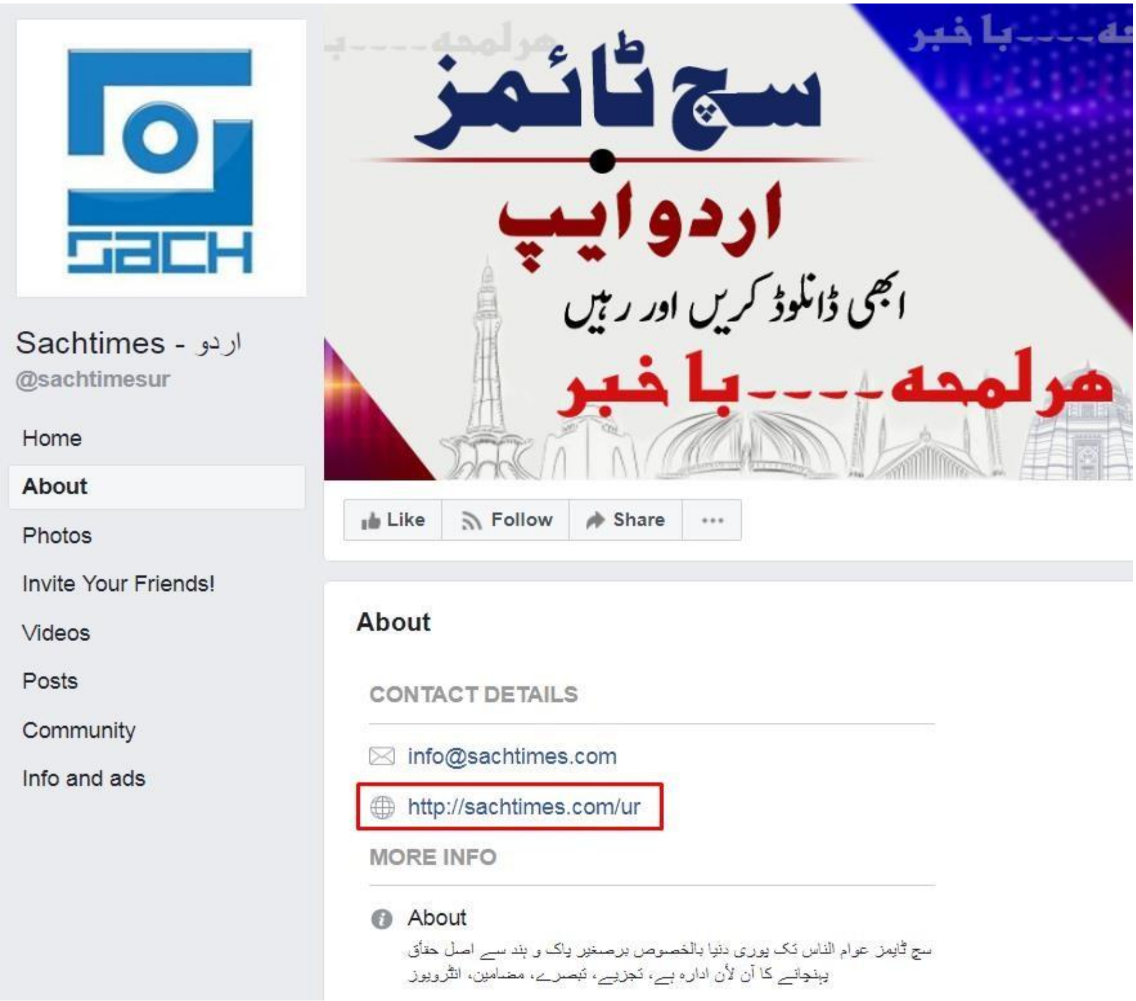
اہم خبریں

پاک بھارت آبی مذاکرات، بھارت نے پاکستان کے اعتراضات مسترد کر دیئے

امریکہ کے ساتھ مزید مذاکرات نہیں ہو سکتے۔ ایران

تحریک لبیک کی ملک جام کرنے کی دھمکی

بھارت سمیت تمام ہمسایہ ممالک سے دوستانہ تعلقات چاہتے ہیں۔ ترجمان دفترخارجہ



Sachtimes - اردو
@sachtimesur

About

CONTACT DETAILS

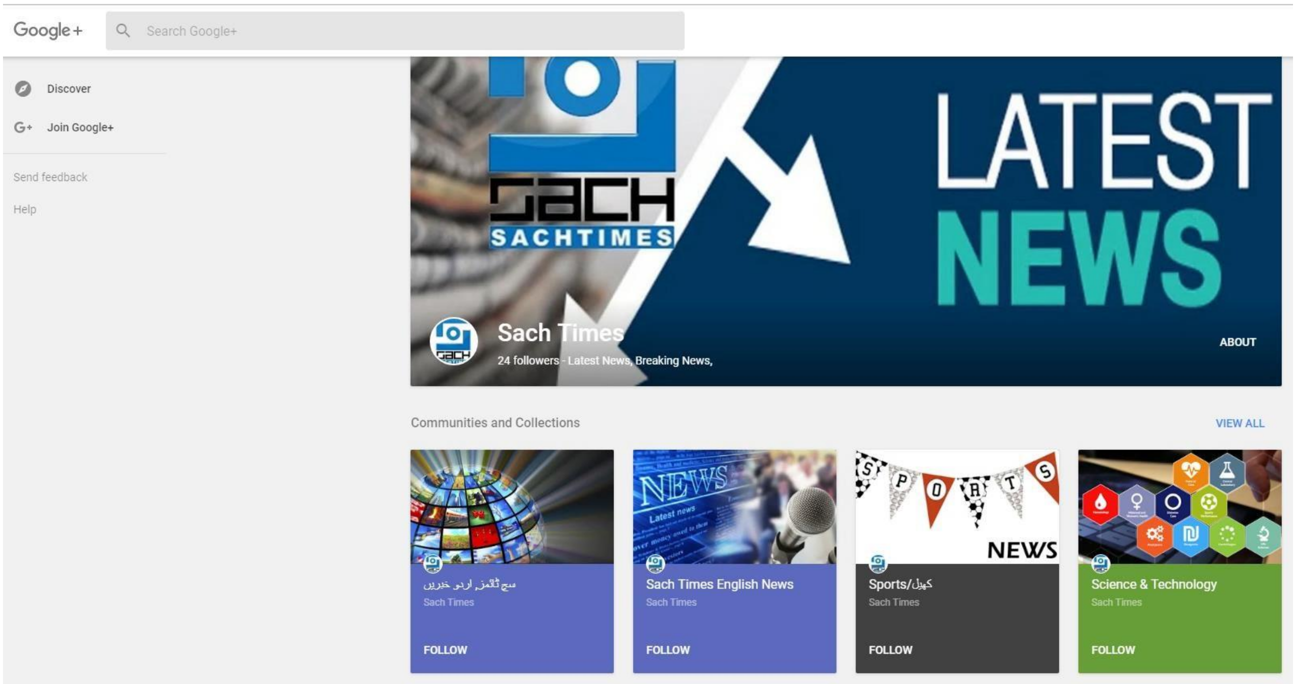
info@sachtimes.com

http://sachtimes.com/ur

MORE INFO

About

سچ ٹایمز عوام الناس تک پوری دنیا بالخصوص برصغیر پاک و ہند سے اصل حقائق پہنچانے کا آن لائن ادارہ ہے، تجزیے، تبصرے، مضامین، انٹرویوز



Google+

Search Google+

Discover

Join Google+

Send feedback

Help

Sach Times

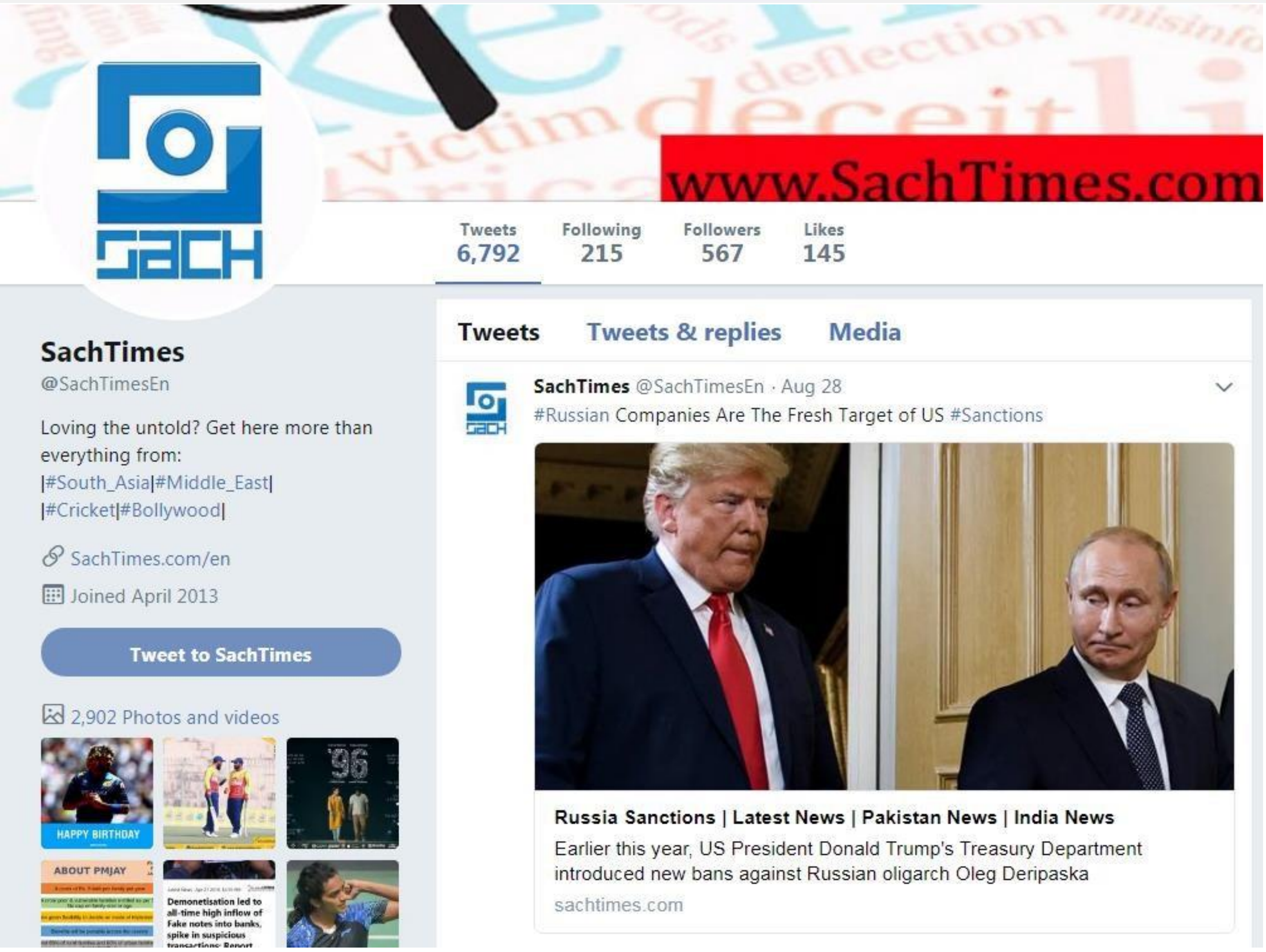
24 followers · Latest News, Breaking News,

ABOUT

Communities and Collections

VIEW ALL

سچ ٹائمز اردو خبریں Sach Times FOLLOW	Sach Times English News Sach Times FOLLOW	Sports/کھیل Sach Times FOLLOW	Science & Technology Sach Times FOLLOW



deflection
deceit
victim
www.SachTimes.com
SACH

Tweets	Following	Followers	Likes
6,792	215	567	145

SachTimes

@SachTimesEn

Loving the untold? Get here more than everything from:
|#South_Asia|#Middle_East|
|#Cricket|#Bollywood|

SachTimes.com/en

Joined April 2013

Tweet to SachTimes

2,902 Photos and videos

HAPPY BIRTHDAY
ABOUT PMJAY
Demonetisation led to all-time high inflow of Fake notes into banks, spike in suspicious transactions: Report

Tweets   Tweets & replies   Media

SachTimes @SachTimesEn · Aug 28

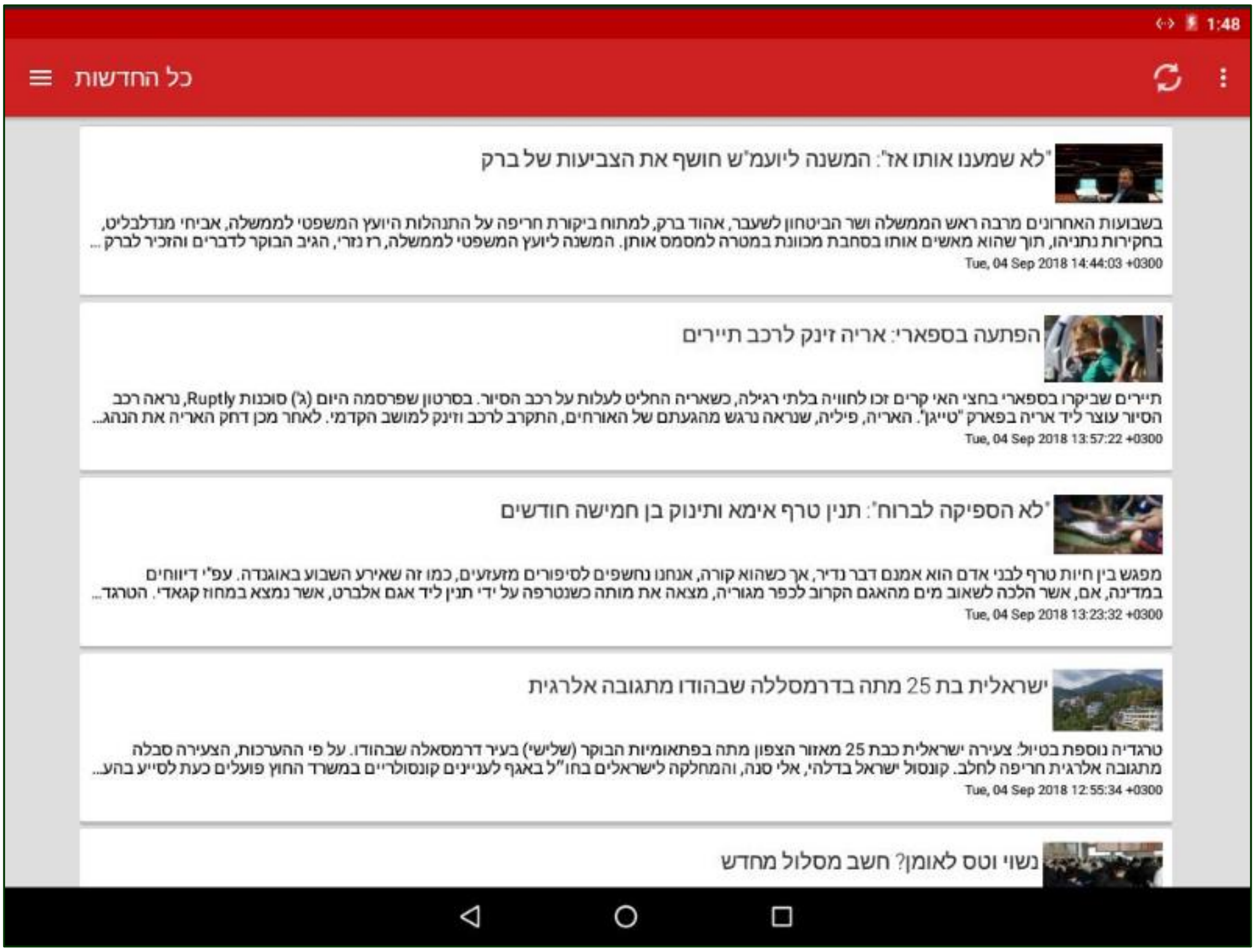
#Russian Companies Are The Fresh Target of US #Sanctions

Russia Sanctions | Latest News | Pakistan News | India News

Earlier this year, US President Donald Trump's Treasury Department introduced new bans against Russian oligarch Oleg Deripaska

sachtimes.com

Below is a screen-capture from the news-feed app



1:48

כל החדשות

"לא שמענו אותו אז": המשנה ליועמ"ש חושף את הצביעות של ברק

בשבועות האחרונים מרבה ראש הממשלה ושר הביטחון לשעבר, אהוד ברק, למתוח ביקורת חריפה על התנהלות היועץ המשפטי לממשלה, אביחי מנדלבליט, בחקירות נתניהו, תוך שהוא מאשים אותו בסחבת מכוונת במטרה למסמס אותן. המשנה ליועץ המשפטי לממשלה, רז נזרי, הגיב הבוקר לדברים והזכיר לברק ...

Tue, 04 Sep 2018 14:44:03 +0300

הפתעה בספארי: אריה זינק לרכב תיירים

תיירים שביקרו בספארי בחצי האי קרים זכו לחוויה בלתי רגילה, כשאריה החליט לעלות על רכב הסיור. בסרטון שפרסמה היום (ג') סוכנות Ruptly, נראה רכב הסיור עוצר ליד אריה בפארק "טייגן". האריה, פיליה, שנראה נרגש מהגעתם של האורחים, התקרב לרכב וזינק למושב הקדמי. לאחר מכן דחק האריה את הנהג...

Tue, 04 Sep 2018 13:57:22 +0300

"לא הספיקה לברוח": תנין טרף אימא ותינוק בן חמישה חודשים

מפגש בין חיות טרף לבני אדם הוא אמנם דבר נדיר, אך כשהוא קורה, אנחנו נחשפים לסיפורים מזעזעים, כמו זה שאירע השבוע באוגנדה. עפ"י דיווחים במדינה, אם, אשר הלכה לשאוב מים מהאגם הקרוב לכפר מגוריה, מצאה את מותה כשנטרפה על ידי תנין ליד אגם אלברט, אשר נמצא במחוז קגאדי. הטרגד...

Tue, 04 Sep 2018 13:23:32 +0300

ישראלית בת 25 מתה בדרמסללה שבהודו מתגובה אלרגית

טרגדיה נוספת בטיול: צעירה ישראלית כבת 25 מאזור הצפון מתה בפתאומיות הבוקר (שלישי) בעיר דרמסאלה שבהודו. על פי ההערכות, הצעירה סבלה מתגובה אלרגית חריפה לחלב. קונסול ישראל בדלהי, אלי סנה, והמחלקה לישראלים בחו"ל באגף לעניינים קונסולריים במשרד החוץ פועלים כעת לסייע בהע...

Tue, 04 Sep 2018 12:55:34 +0300

נשוי וטס לאומן? חשב מסלול מחדש

Appendix 2 - full list of Iranian fake news websites

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
N/A	0enebnews.ga			N/A	N/A	N/A	N/A
7sabah	7sabah.com	5.9.200.236	ftp.7sabah.com	Turkey	Turkish	parstoday.com	Aydin Altay
		78.46.102.123	mail.7sabah.com				
	7sabah.com.tr					parstoday.com	
	7sabah.net	5.9.200.236	ftp.7sabah.net			parstoday.com	
	7sabah.org	5.9.200.236	ftp.7sabah.org			parstoday.com	
		78.46.102.123	ns.7sabah.org				
7soz	7soz.com	5.9.200.236	blog.7soz.com	Turkey	Turkish	parstoday.com	Wiliam Black Kaveh Khaleghi Ebrahim Erfani
		5.9.29.230	ftp.7soz.com				
		67.205.99.12	ns1.7soz.com				
		78.46.102.123	ns2.7soz.com				
			test.7soz.com				
			wp.7soz.com				
	7soz.net	5.9.200.236				parstoday.com	
		67.205.99.12					
	7soz.org	5.9.200.236				parstoday.com	
		67.205.99.12					
aea12	aea12.com		ftp.aea12.com	N/A	N/A	N/A	Ahmad Pishgah
			mail.aea12.com				
			smtp.aea12.com				
Afghanistan nema	afghanistanema.com		ftp.afghanistanema.com	Afghanistan	Pashto	ehyanews.com	Sayid Mahdi Hashemi
			webmail.afghanistanema.com				
Afghan Wolas	afghanwolas.com	144.76.69.80		Afghanistan	Pashto	parstoday.com	Vahid Gohariayan
		5.9.29.230					
		5.9.96.104					
		78.46.102.123					
	afghanwolas.net	144.76.69.80	mail.afghanwolas.net			parstoday.com	
		5.9.29.230					
		5.9.96.104					
	afghanwolas.org	144.76.69.80	mail.afghanwolas.org			parstoday.com	
		5.9.29.230					
		5.9.96.104					
Afkar Blogs	afkarblogs.com	136.243.19.52		Saudi Arabia	Arabic	elaph.com	Vahid Gohariayan

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
		5.9.29.230		Dubai			
Al-ahd	al-ahd.net			Yemen	Arabic	motabaat.com	Imen Samaneh Sepehr Abdul-Latif Mansour Arafat Shoroh
	akhbarye24.net					motabaat.com	
	alahd.tk					motabaat.com	
	al-ahd.com					motabaat.com	
	al-ahd.org					motabaat.com	
N/A	aletthadnews-iq.com		31.aletthadnews-iq.com	N/A	N/A	N/A	Abdul-Latif Mansour
			af.aletthadnews-iq.com				
			ftp.aletthadnews-iq.com				
			owa.aletthadnews-iq.com				
Al Hiwar Aldini	alhiwaraldini.com		ftp.alhiwaraldini.com	Iran	Iraq - Arabic	hawzahnews.com	Mohsen Eslamifar Mohammad Ali Najafi Doust Amir Hamidi
			mail.alhiwaraldini.com				
			old.alhiwaraldini.com				
alwaght	alwaght.net			World Wide	Arabic English Persian Spanish Urdu	sahafah24.com	Ghazanfar Asadi Abdul-Latif Mansour
	alwaght.com					sahafah24.com	
Alrray	alrray.com			N/A	N/A	Inactive	Ghazanfar Asadi Abdul-Latif MansourAbdu
	alrray.net						
Al-Mersad	al-mersad.com			Yemen	Arabic	sahafah24.net	Abdul-Latif Mansour
	almersad.net					sahafah24.net	
	al-mersad.net					sahafah24.net	
	al-mersad.org					sahafah24.net	
al-jeish	al-jeish.com			Syria	N/A	Inactive	Abdul-Latif Mansour
	al-jeish.net						
	al-jeish.org						
Almasirah	almasirahpress.com		ftp.almasirahpress.com	Yemen	Arabic	alkawthartv.com	Jamil Zafer
	almasirahtv.com		ftp.almasirahtv.com			alkawthartv.com	
	almasirahpress.org					alkawthartv.com	
	almasirahpress.net					alkawthartv.com	
Al Sudan Alyoum	alsudanalyoum.com		mail.alsudanalyoum.com	Sudan	Arabic	youm7.com	Ahmed Anwar Mohammed
	alsudanalyoum.net					youm7.com	
	alsudanalyoum.org					youm7.com	
Al elam	al-elam.org			N/A	N/A	Inactive	Ebrahim Erfani
	al-elam.net					Inactive	
Alwaie News	alwaienews.net		en.alwaienews.net	Iraq	Arabic English	shafaqna.com	Abdul-Latif Mansour
	alwaienews.com						
	alwaienews.org						

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
Al hiwaraldini	alhiwaraldini.com			N/A	Arabic	N/A	Mohsen Eslamifar Mohammad Ali Najafi Doust Amir Hamidi
Aletthadnews	aletthadnews-iq.org			N/A	N/A	Suspended	Abdul-Latif Mansour
	aletthadnews-iq.com					Suspended	
	aletthadnews-iq.net					Suspended	
Islamic Movement of Nigeria	alharakah.net	5.9.137.45		Nigeria	Arabic		Hashemi
Islamic Movement of Saudia	3adalah.com	5.9.137.45		Saudi Arabia	Arabic		Basem Al-Khamri
Ansarallah movment	ansar-allah.net			Yemen	Arabic	Inactive	
	ansar-allah.com					Inactive	
	ansar-allah.net					Inactive	
	ansar-allah.org					Inactive	
	ansaroallah.com					sahafaarabia.net	
	ansaroallah.info					sahafaarabia.net	
	ansaroallah.net					sahafaarabia.net	
	ansaroallah.org					sahafaarabia.net	
Ava tv	avatv.net		file.avatv.net	N/A		N/A	Ali-Reza Khajeh Naini Masoud Asgarian
			ftp.avatv.net				
			ns1.avatv.net				
			ns2.avatv.net				
Awd News	awdnews.com	5.9.200.236	analytics.awdnews.com	Europe	English German Spanish Farsi Turkish Russian Polish	independent.co.uk	Bayan Kelvin Middelkoop
		67.205.99.12	de.awdnews.com				
		78.46.102.123	es.awdnews.com				
			fr.awdnews.com				
			ftp.awdnews.com				
			it.awdnews.com				
			ns1.awdnews.com				
			ns2.awdnews.com				
			po.awdnews.com				
			ru.awdnews.com				
			tr.awdnews.com				
			webmail.awdnews.com				
	awdnews.net	5.9.200.236	ftp.awdnews.net			independent.co.uk	
	awdnews.org		de.awdnews.org				
			ftp.awdnews.org				

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
Ayna News Agency	aynanewsagency.net	5.9.29.230		Turkey	Turkish	parstoday.com	Ahmet Demir
		78.46.102.123					
		78.46.126.234					
	aynanewsagency.org	136.243.19.52				parstoday.com	
		5.9.29.230					
		78.46.102.123					
AZ news 24	aznews24.com			Azerbaijan	N/A	Suspended	Kelvin Middelkoop Marlee Barber
Bintolhoda	bintolhoda.com			Iran	Arabic Persian	Inactive	Ebrahim Mattar Kaveh Khaleghi
	bintolhoda.net						
	bintolhoda.org						
Barchi News	barchinews.com	136.243.19.6	ftp.barchinews.com	Iran	Persian	parstoday.com	Seyyed Mohammad Moosavi
		5.9.29.230	ns1.barchinews.com				
		5.9.96.104	ns2.barchinews.com				
Basaer	basaer.org	136.243.19.52	mail.basaer.org	Iran	Persian	insuiute	Basaer Institution
		5.9.29.230					
Berita Dunia	beritadunia.net	5.9.200.236	ftp.beritadunia.net	Indonesia	Indonesian	N/A	Ari Setiawan
		78.46.102.123					
British Left	britishleft.com			UK	English	huffingtonpost.co.uk	Alfonso Zayas
CP islamic	cpislamic.com	5.9.29.230		N/A	N/A	N/A	Naser Habibi
Critics Chronicle	criticschronicle.com			UK	English	rt.com	Andre Schneider Jack Avery
	criticschronicle.org					rt.com	
	criticschronicle.uk					rt.com	
Daily Syria News	dailysyrianews.com			Syria	English Arabic	Inactive	Esmith Shomakher Mehdi Asgari Abdul-Latif Mansour
Do Nish Saro	donishsaro.com			N/A	N/A	Inactive	Yaro Mir
Dari News	darinews.com		ftp.darinews.com	Afghanistan	Persian	sputniknews.com	Seyyed Mohammad Moosavi
			mag.darinews.com				
Did Press	didpress.com		cpanel.didpress.com	Afghanistan	Pashto Dari English	sputniknews.com	Navid Aryan
			ftp.didpress.com				
			webdisk.didpress.com				
			webmail.didpress.com				
Euro Press	europessi.com	67.205.99.12		Europe	N/A	Inactive	Wiliam Black Ebrahim Erfani
	europessi.net						
Enqaz Syria	enqazsyria.com	67.205.99.12		Syria	Arabic	Inactive	Mehdi Asgari Ahmad Mahmood
Farhang Press	farhang-press.com		ftp.farhang-press.com	Iran	Persian	Under construction	Hashemi
Halal Media	halal-media.net		cloud.halal-media.net		English	Inactive	Kaveh Khaleghi

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
			db.halal-media.net	Eastern Asia			
			dns.halal-media.net				
			ftp.halal-media.net				
			imap.halal-media.net				
			kerberos.halal-media.net				
			ldap.halal-media.net				
			ns.halal-media.net				
			ns1.halal-media.net				
			pop3.halal-media.net				
			remote.halal-media.net				
			rpc.halal-media.net				
			smtp.halal-media.net				
			telnet.halal-media.net				
			wildcarddns.halal-media.net				
Haghighah	haghighah.com		ftp.haghighah.com	Iran	Persian	Inactive	Meghdad Montazeri Rad
	haqiqatpress.com		ftp.haqiqatpress.com	Afghanistan	Pashto	Inactive	Habib Hosseini Ebrahim Erfani
			mail.haqiqatpress.com				
			smtp.haqiqatpress.com				
Hedayat Resaneh	hedayatresaneh.ml			Iran	Persian	Inactive	
Haqona	haqona.com			N/A	N/A	Error	AL Erfan Hasan Abdul-Latif Mansour Jurgen Neeme
	haqona.net						
	haqona.org						
Henan - Dubai	henan-dubai.com		ftp.henan-dubai.com	Dubai	Arabic	Inactive	Milad Masoud Far
			mail.henan-dubai.com				
			webmail.henan-dubai.com				
Imam Iatarbiat	imamiatarbiat.com	144.76.69.80		Pakistan	Urdu	bbc.com/urdu	Kaveh Khaleghi
		5.9.200.236					
Instituto Manquehue	institutomanquehue.com	5.9.200.236	en.institutomanquehue.com	Latin America	Spanish	Latin america media outlets	N/A
	institutomanquehue.la	144.76.91.17				Latin america media outlets	
		5.9.200.236					
	institutomanquehue.org	5.9.200.236	en.institutomanquehue.org			Latin america media outlets	
		78.46.102.123	ftp.institutomanquehue.org				
Il Arab Alan	iaanews.net			Palestine	Arabic	shasha.ps npatimes.com	Abdul-Latif Mansour
	iaanews.com						
	iaanews.org						
Islamic Mobile	islamic-mobile.com	67.205.99.12		N/A	N/A	Inactive	Kaveh Khaleghi Ebrahim Erfani
	islamic-mobile.net						
	islamic-mobile.org						
Irtvu	ettehadfestival.com		ftp.ettehadfestival.com	Iran	Persian English Arabic	Inactive	Mohammad Reza Kassiry Hosein Razi

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
			mail.ettehadfestival.com				
			ns1.ettehadfestival.com				
			ns2.ettehadfestival.com				
	irtvu.com		ftp.irtvu.com			Original	
			mail.irtvu.com				
			news.irtvu.com				
			ns1.irtvu.com				
			ns2.irtvu.com				
			pop.irtvu.com				
			smtp.irtvu.com				
			webmail.irtvu.com				
	irtvumedia.com		ftp.irtvumedia.com			Original	
			host.irtvumedia.com				
			mail.irtvumedia.com				
			ns1.irtvumedia.com				
			ns2.irtvumedia.com				
	irtvunews.net		ns1.irtvunews.net			Original	
			ns2.irtvunews.net				
			ns3.irtvunews.net				
			ns4.irtvunews.net				
			ns5.irtvunews.net				
			ns6.irtvunews.net				
	irtvunews.org		ftp.irtvunews.org			Original	
			ns1.irtvunews.org				
			ns2.irtvunews.org				
			ns4.irtvunews.org				
IUVM	iuvm.net	144.76.91.17	ar.iuvm.net	Iran	Persian English Arabic		Kaveh Khaleghi Abia Seif Ebrahim Mattar Majed Fadi
		5.9.200.236	fa.iuvm.net				
		5.9.29.230	ftp.iuvm.net				
		67.205.99.12	news.iuvm.net				
		78.158.161.158	ns10.iuvm.net				
		78.158.184.120	ns11.iuvm.net				
			social.iuvm.net				

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
			tr.iuvm.net				
	iuvm.org	5.9.29.230	arabic.iuvm.org				
		78.158.161.158	chinese.iuvm.org				
		78.158.184.120	dl.iuvm.org				
			english.iuvm.org				
			french.iuvm.org				
			ftp.iuvm.org				
			indian.iuvm.org				
			lms.iuvm.org				
			localhost.iuvm.org				
			mail.iuvm.org				
			ns1.iuvm.org				
			ns2.iuvm.org				
			pashto.iuvm.org				
			persian.iuvm.org				
			pop.iuvm.org				
			russian.iuvm.org				
			smtp.iuvm.org				

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
			spanish.iuvm.org				
			urdu.iuvm.org				
	iuvmapp.com	46.4.8.133					
		78.158.161.158					
	iuvmarchive.com	78.158.184.131	mail.iuvmarchive.com				
	iuvmnews.com	37.58.50.7	az.iuvmnews.com				
		5.9.29.230	en.iuvmnews.com				
			fa.iuvmnews.com				
			forum.iuvmnews.com				
			mail.iuvmnews.com				
			news.iuvmnews.com				
			ns1.iuvmnews.com				
			ns2.iuvmnews.com				
			pop.iuvmnews.com				
			smtp.iuvmnews.com				
			ur.iuvmnews.com				
	iuvmonline.com		en.iuvmonline.com				
			ftp.iuvmonline.com				
			smtp.iuvmonline.com				
	iuvmpress.com	5.9.29.230	ku.iuvmpress.com				
	iuvmtech.com	5.9.29.230	ar.iuvmtech.com				
			fa.iuvmtech.com				
			lms.iuvmtech.com				
	iuvmtech.net	5.9.29.230					
	news.iuvm.net	37.58.50.7					
		5.9.200.236					
	iuvmlearn.ga						
	iuvmpixel.com						
Jame Kurdi	jamekurdi.com	67.205.99.12		Turkey Iran Iraq	Kurd Persian Arabic	irna.ir	Pariya Shiri
	jamekurdi.net	67.205.99.12				irna.ir	
Jesus Journal	jesus-journal.org			US	English	Inactive	Angie Lindeman Barbara L'Italien Julia Geissler
	jesusjournal.net					Inactive	
	jesusjournal.org					Inactive	
Liberty Fighters	libertyfighters.uk		de.libertyfighters.uk	UK	English	Media outlets in UK	Gregory Kistner
			fr.libertyfighters.uk				

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
			ftp.libertyfighters.uk				
Liberty Front Press	libertyfrontpress.com libertyfrontpress.net libertyfrontpress.org	46.4.64.180 5.9.29.230		World Wide	English	independent.co.uk independent.co.uk independent.co.uk independent.co.uk	Ana Line Alton Ryan
N/A	makhatertakfir.tk	5.9.200.236		N/A	N/A	Inactive	N/A
N/A	mawaddat.com	ftp.mawaddat.com		N/A	N/A	Inactive	Ana Line Alton Ryan
Almehwar Almasry	mehwarmasr.com	5.9.29.230		Egypt	Arabic	ahlmasrnews.com	Kamel Ahmad
N/A	muslimpedia.ir	5.9.29.230		N/A	N/A	Inactive	Amir Masrouri
Marsadz	marsadz.com			Algeiria	Arabic	elkhabar.com	mohammad Abdulrahman
MiddleEast Press	middleeastpress.org			N/A	N/A	Under construction	Kaveh Khaleghi
Moslem Press	moslempress.com	67.205.99.12	ar.moslempress.com cp.moslempress.com fa.moslempress.com forum.moslempress.com fr.moslempress.com ftp.moslempress.com mail.moslempress.com ns.moslempress.com ns1.moslempress.com ns2.moslempress.com pop.moslempress.com ru.moslempress.com smtp.moslempress.com localhost.moslempress.com	World Wide	English French Russian Arabic Persian	Inactive	Kelvin Middelkoop
Moslem Youth Media	moslimyouthmedia.net moslimyouthmedia.com moslimyouthmedia.org			N/A	N/A	Inactive	Kelvin Middelkoop
Ilnejan Ilthaqib	nthnews.com nthnews.net nthnews.org			Yemen	Arabic	shafaqna.com	adnantahan tahan
N/A	nationalserver.net	46.4.8.133 5.9.200.236	ns1.nationalserver.net ns2.nationalserver.net	N/A	N/A	Inactive	Ebrahim Mattar
Nile Net Online	nilenetonline.net nilenetonline.com nilenet.tk	67.205.99.12 67.205.99.12 67.205.99.12		North Africa	Arabic	Inactive farsnews.com Inactive	Abdoul-latif Mansour RICHARD SNAITH
NMC yemen	nmcyemen.net	67.205.99.12		Yemen	Arabic	Inactive	

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
PAK onlinenews	pakonlinenews.com		mail.pakonlinenews.com	Pakistan	Urdu	dailypakistan.com.pk	Aslam Abdulhai
Pardis web design	pardisweb.com	67.205.99.12		N/A	N/A	Suspected - Web designer of the array	
	pardisweb.info	67.205.99.12					
Pashtu News	pashtunews.com	136.243.19.6	ns.pashtunews.com	Afghanistan	Pashto	N/A	Noman Shafi Rana Seyyed Mohammad Moosavi
		5.9.29.230	ns1.pashtunews.com				
		5.9.96.104	ns2.pashtunews.com				
podacidana	podacidana.net			Bosnia	Bosnian	Inactive	samir balic
Ofogh TV	ofoghtv.com	67.205.99.12		Iran	Persian	Inactive	Mohsen Vafaeifard
QawafiAlwaie	qawafialwaie.com	67.205.99.12		Iraq	Arabic English	Inactive	
Quds Pal	qudspal.com	67.205.99.12	ns1.qudspal.com	Palestine	Arabic	paltoday.ps	
			ns2.qudspal.com				
	qudspal.net	67.205.99.12				paltoday.ps	
	qudspal.org	67.205.99.12				paltoday.ps	
N/A	radiomoqawema.com	188.40.134.145	ftp.radiomoqawema.com	N/A	N/A	Inactive	
	radiomoqawema.net						
	radiomoqawema.org						
Рисолат	risolattj.com			Tajikistan	Tajik	parstoday.com	
RAI tunisia	raitunisia.com	67.205.99.12	static.raitunisia.com	Tunisia	Arabic	watanserb.com	
ГЛАВНОЕ	realnienovosti.com	5.9.200.236	az.realnienovosti.com	Russia	Russian	tass.ru	
		67.205.99.12	ftp.realnienovosti.com				
		78.46.102.123					
	realnienovosti.net	5.9.200.236	ftp.realnienovosti.net			tass.ru	
		67.205.99.12					
		78.46.102.123					
Syria Alhadath	syriaalhadath.com			Syria	Arabic	Under construction	
Sana News	sana.af	5.9.29.230		Iran	Persian	baztab.news	
Sach Times	sachtimes.com	5.9.200.236	ben.sachtimes.com	Pakistan	Urdu english	khamenei.ir samaa.tv	
			bn.sachtimes.com				
			ftp.sachtimes.com				
			in.sachtimes.com				
			mail.sachtimes.com				
			ns1.sachtimes.com				
			ns2.sachtimes.com				
	sachtimes.net	5.9.200.236	ftp.sachtimes.net				
	sachtimes.org	5.9.200.236	ftp.sachtimes.org				
Syria Blog	syria-blog.com	67.205.99.12		Syria	Arabic	al-akhbar.com	
	syria-blog.net						

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
	syria-blog.org						
Sayyid-ali (Leader)	sayyidali.com	144.76.91.17	ftp.sayyidali.com	Iran	English Arabic	khamenei.ir	
		46.4.64.180					
		5.9.200.236					
		5.9.29.230					
		67.205.99.12					
		78.46.102.123					
	sayyidali.net	5.9.200.236	ftp.sayyidali.net			khamenei.ir	
		5.9.29.230					
		67.205.99.12					
		78.46.102.123					
	sayyidali.org	5.9.29.230				khamenei.ir	
Seratellah	seratellah.org			Iran	Persian	Inactive	
Such Times	suchtimes.com	5.9.200.236	cpanel.suchtimes.com	Pakistan	Urdu	neonetwork.pk	
			epaper.suchtimes.com				
			ftp.suchtimes.com				
			webdisk.suchtimes.com				
			webmail.suchtimes.com				
	suchtimes.org	5.9.200.236				neonetwork.pk	
Tanin Ceter	tanincenter.com	136.243.19.52	ftp.tanincenter.com	Iran	Persian English Arabic	voanews.com	
		5.9.29.230	localhost.tanincenter.com				
			mail.tanincenter.com				
			pop.tanincenter.com				
Tel Aviv Time תל אביב טיימס	tel-avivtimes.com	136.243.19.6	ftp.tel-avivtimes.com	Israel	Hebrew	Israelhayom.co.il Walla.co.il	
		144.76.91.17					
		176.9.1.206					
		37.59.80.101					
		5.9.200.236					
		69.30.238.226					
		78.46.102.123					
	tel-avivtimes.net	176.9.1.206	ftp.tel-avivtimes.net			Israelhayom.co.il Walla.co.il	
		37.59.80.100					
		37.59.80.101					
		37.59.80.103					
		5.9.200.236					
		69.30.238.226					

Fake media outlet	Domain	Main IP	Subdomains	Country	Language	e.g. of origin of Copied Content	First Whois
		78.46.126.234					
	tel-avivtimes.org	176.9.1.206				Israelhayom.co.il Walla.co.il	
		46.4.22.77					
		5.9.200.236					
		69.30.238.226					
TV moqawema	tvmoqawema.com			Palestine	Arabic English	Inactive	
	tvmoqawema.com						
	tvmoqawema.com						
	tvmoqawema.com						
Tuloohefajr	tuloohefajr.com		ftp.tuloohefajr.com	N/A	N/A	Inactive	
	tuloohefajr.net		ftp.tuloohefajr.net			Inactive	
	tuloohefajr.org					Inactive	
Us Journal	usjournal.net			US	English	nymag.com	
	usjournal.us					nymag.com	
Whats U Pic	whatsupic.com	173.208.153.250	es.whatsupic.com	US	English	rt.com	
		176.9.139.199	fr.whatsupic.com				
		46.4.22.77	ftp.whatsupic.com				
		5.9.200.236					
		67.205.99.12					
		78.46.102.123					
	whatsupic.net	176.9.139.199	es.whatsupic.net			rt.com	
		5.9.200.236	fr.whatsupic.net				
		67.205.99.12	ftp.whatsupic.net				
	whatsupic.org	176.9.139.199	ftp.whatsupic.org			rt.com	
		5.9.200.236					
		67.205.99.12					
World Breaks	worldbreaks.tk	5.9.200.236		World Wide	N/A	Inactive	
YNA Yemen	ynayemen.com	67.205.99.12		Yemen	Arabic	Inactive	
YJC News	yjcnews.com			Iran	Persian	Inactive	
	yjcnews.net						
	yjcnews.info						
Yemen Student	yemenstudent.org			Yemen	N/A	Inactive	
	yemenstudent.net						
Yemen Press	yemenpress.org	46.4.22.77	ar.yemenpress.org	Yemen	English Arabic	shafaqna.com	
		5.9.200.236	ftp.yemenpress.org				
	yemenpress.news					shafaqna.com	
Yemen Shia	yemenshia.com	144.76.91.17		Yemen	Arabic	Inactive	
		188.40.134.145					
		78.158.184.103					