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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Targets</td>
<td>3</td>
</tr>
<tr>
<td>Charming Kitten or Rocket kitten?</td>
<td>4</td>
</tr>
<tr>
<td>The HBO hacker and Charming Kitten</td>
<td>5</td>
</tr>
<tr>
<td>HBO hacking indictment</td>
<td>5</td>
</tr>
<tr>
<td>Connection to Iranian government backed threat agent</td>
<td>5</td>
</tr>
<tr>
<td>From Mesri to Charming Kitten</td>
<td>6</td>
</tr>
<tr>
<td>Delivery and Infection</td>
<td>16</td>
</tr>
<tr>
<td>Made up organizations and people</td>
<td>16</td>
</tr>
<tr>
<td>British News</td>
<td>16</td>
</tr>
<tr>
<td>Made up students and journalists</td>
<td>24</td>
</tr>
<tr>
<td>Impersonating real companies</td>
<td>30</td>
</tr>
<tr>
<td>United Technologies impersonation</td>
<td>30</td>
</tr>
<tr>
<td>Watering holes</td>
<td>32</td>
</tr>
<tr>
<td>Spear Phishing for credential stealing</td>
<td>34</td>
</tr>
<tr>
<td>Wave 1</td>
<td>34</td>
</tr>
<tr>
<td>Wave 2</td>
<td>36</td>
</tr>
<tr>
<td>Wave 3</td>
<td>37</td>
</tr>
<tr>
<td>Email tracking services</td>
<td>45</td>
</tr>
<tr>
<td>Targeted emails with malware</td>
<td>46</td>
</tr>
<tr>
<td>DownPaper Malware</td>
<td>47</td>
</tr>
<tr>
<td>Additional samples</td>
<td>49</td>
</tr>
<tr>
<td>MAGICHOUND.RETRIEVER</td>
<td>50</td>
</tr>
<tr>
<td>Appendix A - Indicators of Compromise</td>
<td>51</td>
</tr>
<tr>
<td>Appendix B - Previous reports about Charming Kitten and Rocket Kitten</td>
<td>59</td>
</tr>
</tbody>
</table>
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\(^2\).

---

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.


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
HBO hacking indictment

In November 21, 2017, the United States Department of Justice unsealed an indictment against Behzad Mesri (A.K.A “Skote Vahshat”) 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.

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 tagged Mesri’s twitter account in a tweet suggesting that Mesri might be related to Charming Kitten.

---

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,” “Balls,” “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
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”:

![Profile page of ArYaiEiRAN](http://www.iran-eng.ir/member.php/77662-ArYaiEiRan?langid=1)

---

10 http://www.iran-eng.ir/member.php/77662-ArYaiEiRan?langid=1
A list of websites he defaced, listed on Zone-H\textsuperscript{11}:

![www.zone-h.org](http://www.zone-h.org/archive/notifier=ArYaleIrAn)

<table>
<thead>
<tr>
<th>Date</th>
<th>Notifier</th>
<th>H</th>
<th>M</th>
<th>R</th>
<th>L</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/05/27</td>
<td>ArYaleIrAn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>forum.ha.cker.ir/aria.php</td>
</tr>
<tr>
<td>2012/07/06</td>
<td>ArYaleIrAn</td>
<td></td>
<td></td>
<td>M</td>
<td></td>
<td>xn--mgbt8db40c.com/aryaieiran....</td>
</tr>
<tr>
<td>2012/07/05</td>
<td>ArYaleIrAn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.parsihackers.com/aryaieiran">www.parsihackers.com/aryaieiran</a>...</td>
</tr>
<tr>
<td>2012/06/20</td>
<td>ArYaleIrAn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mihanhack.com/forums/aryaieiran</td>
</tr>
<tr>
<td>2012/01/27</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.alikkhalifar.ir/aryaieiran">www.alikkhalifar.ir/aryaieiran</a></td>
</tr>
<tr>
<td>2012/01/27</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.vbiran.info/aryaieiran.html">www.vbiran.info/aryaieiran.html</a></td>
</tr>
<tr>
<td>2012/01/16</td>
<td>ArYaleIrAn</td>
<td></td>
<td>H</td>
<td></td>
<td></td>
<td>ads.vbiran.ir/aryaieiran.html</td>
</tr>
<tr>
<td>2012/01/16</td>
<td>ArYaleIrAn</td>
<td></td>
<td>H</td>
<td></td>
<td></td>
<td>hacked.ir</td>
</tr>
<tr>
<td>2012/01/14</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>mihanbit.com/setting.php</td>
</tr>
<tr>
<td>2011/10/31</td>
<td>ArYaleIrAn</td>
<td>H</td>
<td>M</td>
<td></td>
<td></td>
<td>forum3at.info</td>
</tr>
<tr>
<td>2011/10/31</td>
<td>ArYaleIrAn</td>
<td>H</td>
<td>M</td>
<td></td>
<td></td>
<td>forum3at.in</td>
</tr>
<tr>
<td>2011/10/31</td>
<td>ArYaleIrAn</td>
<td>H</td>
<td>M</td>
<td></td>
<td></td>
<td>forum3at.us</td>
</tr>
<tr>
<td>2011/10/31</td>
<td>ArYaleIrAn</td>
<td>H</td>
<td>M</td>
<td></td>
<td></td>
<td>tv.forum3at.us</td>
</tr>
<tr>
<td>2011/10/31</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>persiandesign.org</td>
</tr>
<tr>
<td>2011/09/12</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>ir98music.com/aryaieiran.htm</td>
</tr>
<tr>
<td>2011/08/29</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>aryaieiran.aradserver.net</td>
</tr>
<tr>
<td>2011/08/25</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>donbalier.com/aryaieiran.html</td>
</tr>
<tr>
<td>2011/08/25</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>donbalier.net/aryaieiran.html</td>
</tr>
<tr>
<td>2011/08/25</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>sharetronix.ir/aryaieiran.html</td>
</tr>
<tr>
<td>2011/08/25</td>
<td>ArYaleIrAn</td>
<td>M</td>
<td>H</td>
<td></td>
<td></td>
<td>link.ir/aryaieiran.html</td>
</tr>
</tbody>
</table>

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

![ArYaleIrAn](http://www.zone-h.org/archive/notifier=ArYaleIrAn)

\textsuperscript{11} http://www.zone-h.org/archive/notifier=ArYaleIrAn
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\(^\text{12, 13}\):

---

\(^\text{12}\) https://community.riskiq.com/search/britishnews.org

\(^\text{13}\) 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:

In a defacement, still online at the time of writing, both ArYaleIrAn 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.
persiandns[.]net hosting services, which hosted malicious domains used by charming kitten, redirects to mahanserver[.]ir, indicating it is the same company:

The about page (درباره ما) of mahanserver[.]ir leads to a 404 error page:
The CEO of mahanserver[.]ir is Mohammad Rasoul Akbari (A.K.A ra3ou1), likely the boss or partner of ArYalezrA:
The two follow each other on Twitter:

[Image: Twitter screenshot showing ra3ou1 and AryaleirAn following each other]

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

[Image: Facebook screenshot showing Behzad Mesri and Mohammad Rasoul Akbari as friends]

14 https://www.facebook.com/friendship/sk0te.vahshat/ra3ou1/
On Linkedin, MahanServer only has two employees: CEO Mohammad Rasoul Akbari and Mohammadamin Keshvari:

Interestingly, Mohammadamin Keshvari's profile picture is a pomegranate, like that of ArYaleIrAN's twitter account.  

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

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

[Image of Waybac Machine showing ARia Dc and MahanServer]

[16] Data from DomainTools whois history.
To sum up, the HBO hacker - **Behzad Mesri** is a member of Turk Black Hat along with **ArYaleIrAn**, 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 ArYaleIrAn 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 to analyze these connections and visually depict them, as can be seen below:

---

17 [https://shadowdragon.io/product/socialnet](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”\(^\text{18}\) and “Iranian agents blackmailed BBC reporter with ‘naked photo’ threats”\(^\text{19}\) 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)\(^\text{20}\). 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:

---


\(^{19}\) [http://www.arabnews.com/node/1195681/media](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
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”:
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:
At the bottom of the site are links to social media accounts created by the attackers:

Below are screenshots of the accounts.

Instagram, Instagram[.]com/britishnewslive with over 13,000 followers (unavailable for several months):
Twitter, https://twitter[.]com/britishnewslive (online at time of writing):

Facebook page - facebook[.]com/officialbritishnewslive (unavailable for several months):
LinkedIn company page, linkedin[.]com/company/britishnews (unavailable for several months):

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):
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\(^{21}\):

\(^{21}\) [https://community.riskiq.com/search/whois/email/isabella.careyy@gmail.com](https://community.riskiq.com/search/whois/email/isabella.careyy@gmail.com)
Made up students and journalists

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]
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:
The Download button is a redirection link:


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>

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

"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:
Bahar Azadeh

Fake entity "Bahar Azadeh" (bahra.azadeh88@gmail.com and @baharazadeh1, 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:** yaffa hyatt [mailto:yaffa.hyatt9617@gmail.com]
**Sent:** Tuesday, September 5, 2017 11:17 AM
**To:**
**Subject:** Research And Work

---

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 Center in 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 University I hope you accept me as your student and take advantage of your experience.
Please respond My message
I'm waiting For your Respond

---

**Bahar Azadeh**

---

**From:** bahar.azadeh88@gmail.com
**Date:** 3 September 2017 at 10:18:35 GMT+3
**To:**
**Subject:** Please Guide Me

---

Hello Professor ,

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 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.azadeh88@gmail.com
**Date:** Sep 2, 2017 1:52 PM
**Subject:** Please Guide Me
**To:**
**Cc:**

---

Hello Dear , 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](https://twitter.com/baharazadeh1)
Yet in a third case she claimed to be Baha'i living in Tehran:

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):
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.


\(^24\) [https://iranthreats.github.io/resources/macdownloader-macos-malware/](https://iranthreats.github.io/resources/macdownloader-macos-malware/)
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
3b4926014b9cc028d5fb9d47fee3dbd9376525dcb3b6e2173c5edeb22494cfa9b
```
Watering holes

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

<table>
<thead>
<tr>
<th>Breached website</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hamijoo[.]com</td>
<td>An Iranian crowdfunding platform</td>
</tr>
<tr>
<td><a href="http://www.jewishjournal%5B.%5Dcom">www.jewishjournal[.]com</a></td>
<td>A Jewish news site</td>
</tr>
<tr>
<td><a href="http://www.esterk%5B.%5Dcom">www.esterk[.]com</a></td>
<td>A personal blog of one of JewishJournal's writers</td>
</tr>
<tr>
<td><a href="http://www.boloogh%5B.%5Dcom">www.boloogh[.]com</a></td>
<td>A sex education website for Iranian youth</td>
</tr>
<tr>
<td>levazand[.]com</td>
<td>A personal blog of an Iranian living in United states</td>
</tr>
</tbody>
</table>

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:
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 of records emails

©All rights reserved to ClearSky Cyber Security, 2017
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 emails25.

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 201526). Below is a screenshot of the phishing email:

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/
The phishing page pretends to be a Gmail shared document downed page that requires the visitor to log in:
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\(^{28}\)):

![WebRTC code](https://github.com/diafygi/webrtc-ips/blob/master/README.md)

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.

![Facebook spear phishing](https://iranthreats.github.io/resources/webrtc-deanonymization/)

---

\(^{27}\) [https://github.com/diafygi/webrtc-ips/blob/master/README.md](https://github.com/diafygi/webrtc-ips/blob/master/README.md)

\(^{28}\) [https://iranthreats.github.io/resources/webrtc-deanonymization/](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:

![Email](image1.png)

Which leads to:

![Next](image2.png)
In other cases, 7 different targeted phishing emails were sent to the same victim on the same day from customers.mailservice@gmail.com:
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 Google’s 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"): 
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 account²⁹ ³⁰:

Translation: "The brothers'³¹ new method for hacking e-mails. Do not be fooled by such an email".
Translation: "Ramezān (The month of Ramadan) operation continues."

Other reported receiving 6 spear phishing emails within a few minutes. For example, Soudeh Rad32 board member at ILGAEurope33 (an organization for human rights and equality for lesbian, gay, bisexual, trans and intersex people at European level):

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
Behrang Tajdin⁴⁴ a BBC Persian TV Reporter said⁴⁵ he was targeted in a similar campaign in April 2017:

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."

⁴⁴ https://twitter.com/Behrang
⁴⁵ https://twitter.com/Behrang/status/855761991117484032
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.
+%__________+ invitations to a conversation
View Conversation
<http://google-hangout.verify-account.services/Chat?v=*
+__________+>
This notification was sent to *username* @gmail.com
<https://mailtrack.io/trace/link/"?u=*
+__________+ &name=*
+__________+>
Unsubscribe
<http://google-hangout.verify-account.services/Chat?v=*
+__________+ &signature=*
+__________+>
```

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 ([username]@gmail.com) is being used to recover a Mail Account. If you initiated the recovery process, it is asking you to enter 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 [link to legitimate site]* to ensure your account is safe.

Which redirects several times, eventually reaching the malicious page:
```
```

<table>
<thead>
<tr>
<th>Request URL</th>
<th>Status Code</th>
<th>Remote Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>[link to legitimate site]</td>
<td>302 Found</td>
<td>85.159.235.199:443</td>
</tr>
</tbody>
</table>
```
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).

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 (be207941ce8a5e212be8dede83d05d38d), 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:

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[].cf7/downloader/poster.php", Base64 encoded as can be seen below:

   ```xml
   <data name="WindowsResSource" xml:space="preserve">
     <value>aiR0cD0vlzQ2LjE3LjK3LjM3L2Rvd25sb2Pzk3IvC09zc3VvImhBocA-…(truncated)
   </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:
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\XP000.TMP\sami.exe
   C:\Users\user1\AppData\Local\Microsoft\Windows\wuauclt.exe

Assembly Details:

```
[assembly: AssemblyVersion("7.9.9600.17542")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("© Microsoft Corporation. All rights reserved.")]
[assembly: AssemblyProduct("Windows Update")]
[assembly: AssemblyCopyright("Copyright © Microsoft Corp.")]
[assembly: AssemblyTrademark("")]
[assembly: AssemblyTrademark("")]
[assembly: AssemblyInformationalVersion("")]
[assembly: CompilationRelaxations(8)]
```

PDB path: 
d:\Task\FUD\DownPaper\trunk\Downloader\obj\Debug\wuauclt.pdb
Additional samples

**wuauclt.exe**

```
d6ea39e1d4aa8c977a835e72d0975e3
dsami.exe
```

msoffice-update[.]com
93.158.215.50
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
```

sami.exe

```
3261d45051542ab3e54fa541f132f899
479e1e02d379ad6c3c7f496d705448fa955b50a1
```

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

**20f2da7b0c482ab6a78e9bd65a1a3a92**

```
d:\Task\FUD\Downloader\obj\Debug\wuauclt.pdb
```

**ax haye ayin.exe**

```
276befa70c0b36860c97e3e19f10343
```

```
53f7b95262971d79e676055d239180d653fd838da6f82048ef4a5913f
5.79.69[.]206:4455
```

**pita.exe**

```
60753796905458fa6a4407f48309aa25
```

```
53f7b95262971d79e676055d239180d653fd838da6f82048ef4a5913f
```

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

**aziii.exe**

```
3c01793380bd3f101603af68e96f058
```

```
13ac10cd2595fb86efd0e15c1b82b2c8e1953809f0d1c349641997aeb9f935c
```

**Azita Gallery.exe**

```
30124b5c56cecf2045abd24011bd6f06b
```

```
9aa7fc0835e75cbf7aadde824c484d7dc53fdc308a706c9645878bbd6f5d3ad8
```
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\(^\text{37}\). 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
ecf9b7283fda023fa37ad7f6b15be4eadd3e06
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:

\[^\text{37}\text{https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/}\]
Appendix A - Indicators of Compromise

012mail-net-uwclogin[.]ml
443[.]tcp[.]shorturlbot[.]club
874511478[.]account-login[.]net
8ghefkwdbf6dsg33asdf1[.]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[a]
tivities[.]devices[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]accounts[g]
account[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]drive[.]goog
gle[.]com[.]usersettings[.]cf
accounts[.]activities[.]devices[.]com[.]usersettings[.]cf
accounts[.]activities[.]google[.]com[.]accounts[a]
devices[.]com[.]usersettings[.]cf
accounts[.]activities[.]google[.]com[.]accounts[g]
accounts[.]google[.]com[.]usersettings[.]cf
accounts[.]activities[.]google[.]com[.]usersettings[.]u
sersettings[.]cf
accounts[.]activities[.]google[.]com[.]usersettings[.]cf
accountservice[.]support
account-service-recovery[.]com
accounts-gooooglemail[.]com
accounts-gooooglemails[.]com
account-signin-myaccount-users[.]ga
accounts-logins[.]net
accountrecovery[.]ddns[.]net
accounts-service[.]support
accountservice-support[.]com
account-support-user[.]com
accounts-yahoo[.]us
accounts-goooogle[.]com
account-user[.]com
account-user-permission-account[.]com
account-users-mail[.]com
account-user-verify-mail[.]com
accounts-qqoogie-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
aipak[.]org
aol-mail-account[.]com
apache-utility[.]com
api[.]com-service[.]net
app-documents[.]com
app-faceboook[.]co
appleid[.]apple[.]com[.]account-logins[.]com
araamcol[.]com
araamcol[.]com
archive-center[.]com
asus-support[.]net
asa-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-permission[.]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-accountssrecovery[.]name
com-archivecenter[.]work
com-customeradduser[.]bid
com-customerservice[.]bid
com-customerservice[.]name
com-customerservices[.]name
com-customersuperuser[.]bid
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\(^{47}\)

39 https://citizenlab.ca/2015/08/iran_two_factor_phishing/
40 http://www.clearskysec.com/thamar-reservoir/
43 https://iranthreats.github.io/resources/android-malware/
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/