The Kittens Are Back in Town

Charming Kitten Campaign Against Academic Researchers

September 2019

TLP:WHITE

Table of Content

Summary

Charming Kitten, also known as APT35 or Ajax, is an Iranian cyberespionage group active since 2014[1]. Their primary targets are Iranian experts working in the Academy, human rights activists and media personnel. Most victims are in the Middle East, US and the UK. Below here is a key event timeline:

- **In 2015** ClearSky discovered the first wave of phishing attacks and issued a report reviewing their activity named "Thamar reservoir"[2].
- **In 2017** ClearSky exposed a vast espionage operation, active from 2016 to 2017, against the aforementioned sectors. Our report uncovered incidents of corporate impersonation, fake organizations and individuals, spear phishing and watering hole attacks.
- **In 2018**, Charming Kitten attempted to attack ClearSky and our customers directly via a fraudulent website impersonating the ClearSky portal[3].

  Later that year we also identified new wave of attacks against researchers in the Middle East, using fake emails and look-alike websites.
- **In 2019** ClearSky observed a sharp increase in Charming Kitten attacks. It appears that group has initiated a new cyber espionage campaign comprised of two stages, pointing at two different targets:
  - Non-Iranian Researchers from the US, Middle East and France, focusing on academic research of Iran.
  - Iranian dissidents in the US.

Despite the considerable unrest in the Iranian cyber sphere, it appears that similarly to the MuddyWater APT, Charming Kitten were unaffected[4].

In August, the campaign has progressed, and unlike July, it seems like the APT group is now expanding its activities toward influential public figures around the world, rather than academic researchers an state organizations. Additionally, in August 2019, we found that the group had begun adding a tracker to their email correspondences, enabling them to follow an email message forwarded to additional accounts and obtain geolocation information.

[1] https://attack.mitre.org/groups/G0058/

[2] clearskysec.com/thamar-reservoir/thamar-reservoir-public/

[3] https://www.bleepingcomputer.com/news/security/iranian-apt-poses-as-israeli-cyber-security-firm-that-exposed-its-operations/

[4] https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf

Attack Vector

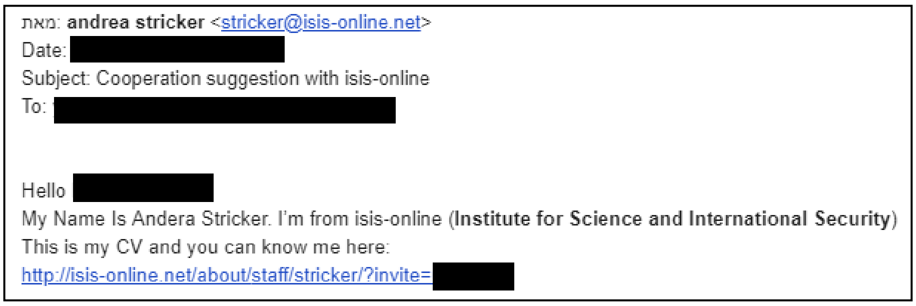
1. The first stage is sending an email message leveraging social engineering methods. The hacker impersonates a well-known researcher or journalist and invites the recipients to an event allegedly organized by the impersonated subject. Note that in certain cases, the hackers use their targets' language.
2. The second stage includes a decoy website impersonating various Google services such as Gmail or Google Drive, to which the victim is redirected from the phishing email. This vector was observed in prior campaigns as well. Please note that in late March 2019, Microsoft filed an official complaint against the group for "establishing an internet-based cyber theft operation referred to as 'Phosphorus'.".[5]
3. Moreover, we identified a new vector of phishing websites that is used by this group – impersonating the Instagram official website. This is the first time we observed an attempt to extract credentials of non-google services.

Emails sent to victims

Analyzing this campaign, we identified two attack scenarios. Based on our investigation, Charming Kitten tried to carry out both of the attack scenarios against the same victims. Note however that in most cases, the attack begun with the first scenario.

First set of Emails

While impersonating to research institution, the attackers try to contact the victims privately and encourage them to review their resume (CV). In order to do so, linked within the email is a unique URL address for the fake website (Please notice the spelling and grammatical error, most notably the mispronunciation of the Sender name. Instead of Andrea, as written in the email address, the attacker mistakenly wrote Andera):

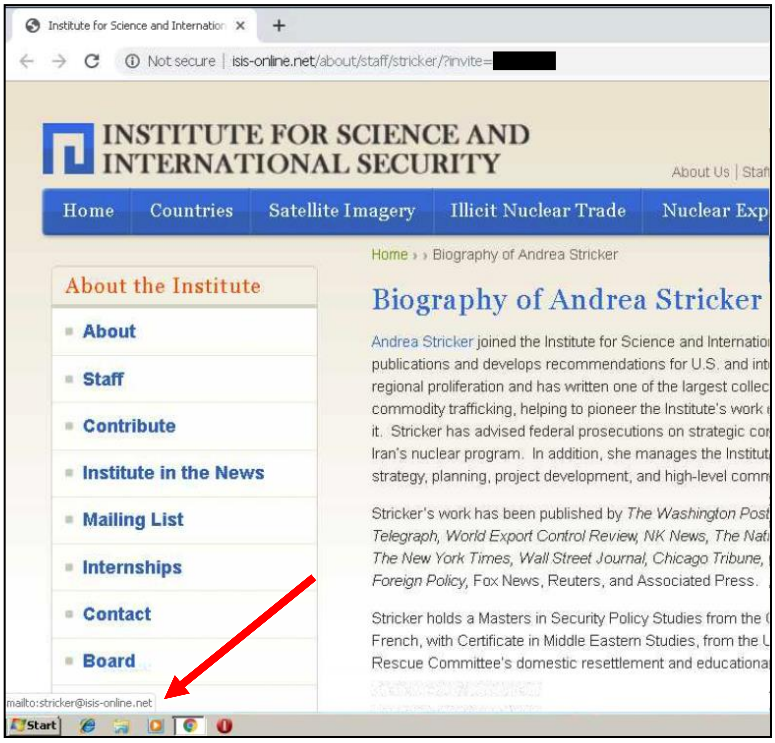


מאת: **andrea stricker** <stricker@isis-online.net>
Date: [redacted]
Subject: Cooperation suggestion with isis-online
To: [redacted]

Hello [redacted]
My Name Is Andera Stricker. I'm from isis-online (**Institute for Science and International Security**)
This is my CV and you can know me here:
http://isis-online.net/about/staff/stricker/?invite=[redacted]

As this link is not malicious, we believe that it is currently used only as the first stage in the attack - gaining the trust of the victims. The website contains the exact page from the original website on which it is based, with one single change – the sender's email address embedded within the website content.

[5] https://noticeofpleadings.com/phosphorus/files/Complaint.pdf



Institute for Science and Internation ×

Not secure | isis-online.net/about/staff/stricker/?invite=[redacted]

INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY

About Us | Staf

Home | Countries | Satellite Imagery | Illicit Nuclear Trade | Nuclear Exp

Home › › Biography of Andrea Stricker

About the Institute

- About
- Staff
- Contribute
- Institute in the News
- Mailing List
- Internships
- Contact
- Board

Biography of Andrea Stricker

Andrea Stricker joined the Institute for Science and Internatio publications and develops recommendations for U.S. and int regional proliferation and has written one of the largest collec commodity trafficking, helping to pioneer the Institute's work it. Stricker has advised federal prosecutions on strategic co Iran's nuclear program. In addition, she manages the Institut strategy, planning, project development, and high-level comm

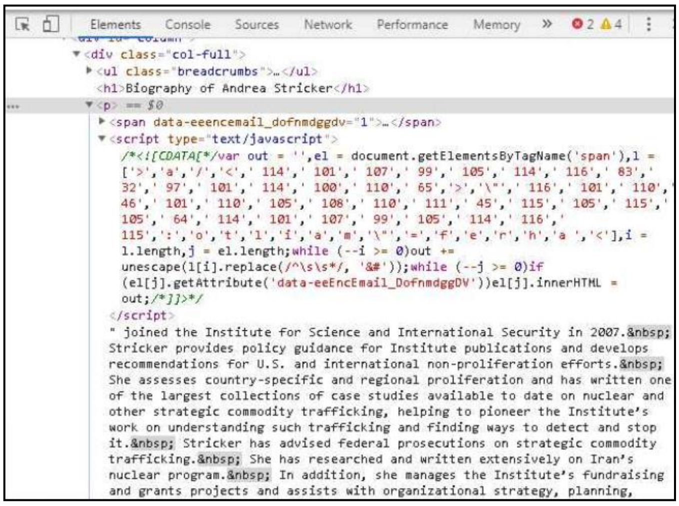
Stricker's work has been published by *The Washington Post Telegraph, World Export Control Review, NK News, The Nat The New York Times, Wall Street Journal, Chicago Tribune, Foreign Policy*, Fox News, Reuters, and Associated Press.

Stricker holds a Masters in Security Policy Studies from the French, with Certificate in Middle Eastern Studies, from the U Rescue Committee's domestic resettlement and educationa

mailto:stricker@isis-online.net

Start

Same as the original website, the email is embedded in the webpage content with a javascript code encoded in decimal. The attackers changed the last 22 numbers – from isis-online[.]org to the fake email address isis-online[.]net, as seen below:



```
▼<div class="col-full">
  ▶<ul class="breadcrumbs">…</ul>
   <h1>Biography of Andrea Stricker</h1>
  ▼<p> == $0
    ▶<span data-eeencemail_dofnmdggdv="1">…</span>
    ▼<script type="text/javascript">
       /*<![CDATA[*/var out = '',el = document.getElementsByTagName('span'),l =
       ['>','a','/','<',' 114',' 101',' 107',' 99',' 105',' 114',' 116',' 83','
       32',' 97',' 101',' 114',' 100',' 110',' 65','>','\"',' 116',' 101',' 110','
       46',' 101',' 110',' 105',' 108',' 110',' 111',' 45',' 115',' 105',' 115','
       105',' 64',' 114',' 101',' 107',' 99',' 105',' 114',' 116','
       115',':','o','t','l','i','a','m','\"','=','f','e','r','h','a ','<'],i =
       l.length,j = el.length;while (--i >= 0)out +=
       unescape(l[i].replace(/^\s\s*/, '&#'));while (--j >= 0)if
       (el[j].getAttribute('data-eeEncEmail_DofnmdggDV'))el[j].innerHTML =
       out;/*]]>*/
     </script>
     " joined the Institute for Science and International Security in 2007.&nbsp;
     Stricker provides policy guidance for Institute publications and develops
     recommendations for U.S. and international non-proliferation efforts.&nbsp;
     She assesses country-specific and regional proliferation and has written one
     of the largest collections of case studies available to date on nuclear and
     other strategic commodity trafficking, helping to pioneer the Institute's
     work on understanding such trafficking and finding ways to detect and stop
     it.&nbsp; Stricker has advised federal prosecutions on strategic commodity
     trafficking.&nbsp; She has researched and written extensively on Iran's
     nuclear program.&nbsp; In addition, she manages the Institute's fundraising
     and grants projects and assists with organizational strategy, planning,
```

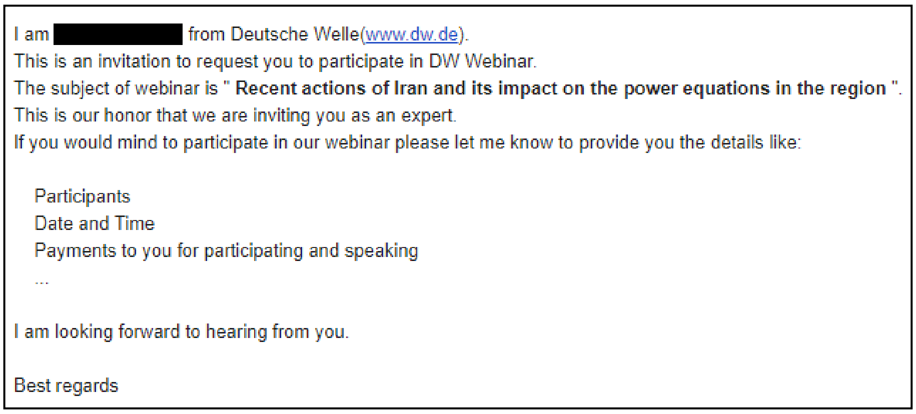
The Fake email code in decimal as presented in the source code of the impersonating website:

```
['>','a','/','<',' 114',' 101',' 107',' 99',' 105',' 114',' 116',' 83',' 32',' 97',' 101',' 114',' 100',' 110',' 65','>','\"','
116',' 101',' 110',' 46',' 101',' 110',' 105',' 108',' 110',' 111',' 45',' 115',' 105',' 115',' 105',' 64',' 114',' 101',' 107','
99',' 105',' 114',' 116',' 115',':','o','t','l','i','a','m','\"','=','f','e','r','h','a ','<']
```

Second set of Emails

In this scenario, the attackers impersonate a known journalist. Unlike the first format, the latter does not contain any link to a fake website. The attacker offers the victim to participate in an online meeting about Iran and other subjects of interest for the target (e.g. recent discourse between Iran and the US). After presenting himself and the subject of the meeting, the attacker would ask whether the victim is interested in participating. If so, they are requested to replay in order to receive the following details:

1. A list of the other participants.
2. Date and time for the meeting.
3. Details regarding the method of payment.



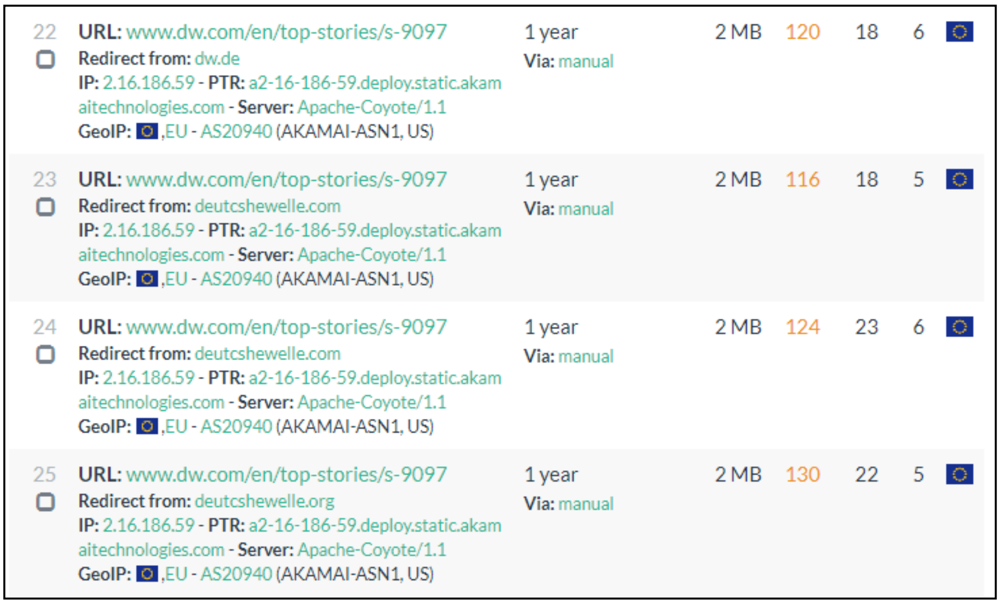
I am [redacted] from Deutsche Welle(www.dw.de).
This is an invitation to request you to participate in DW Webinar.
The subject of webinar is " **Recent actions of Iran and its impact on the power equations in the region** ".
This is our honor that we are inviting you as an expert.
If you would mind to participate in our webinar please let me know to provide you the details like:

Participants
Date and Time
Payments to you for participating and speaking
...

I am looking forward to hearing from you.

Best regards

We identified on the website URLScan a few scans of a link from the website of Deutcshe Welle, a Germany-based international news portal. As presented in the following image, the victims were redirected to the website from malicious domains of the group (which can be found on the ClearSky Twitter account[6]). One of the domains is dw[.]de – a decoy domain which was mentioned in the previous email.



22 □	**URL:** www.dw.com/en/top-stories/s-9097 **Redirect from:** dw.de **IP:** 2.16.186.59 - **PTR:** a2-16-186-59.deploy.static.akamaitechnologies.com - **Server:** Apache-Coyote/1.1 **GeoIP:** 🇪🇺 ,EU - AS20940 (AKAMAI-ASN1, US)	1 year **Via:** manual	2 MB	120	18	6	🇪🇺
23 □	**URL:** www.dw.com/en/top-stories/s-9097 **Redirect from:** deutcshewelle.com **IP:** 2.16.186.59 - **PTR:** a2-16-186-59.deploy.static.akamaitechnologies.com - **Server:** Apache-Coyote/1.1 **GeoIP:** 🇪🇺 ,EU - AS20940 (AKAMAI-ASN1, US)	1 year **Via:** manual	2 MB	116	18	5	🇪🇺
24 □	**URL:** www.dw.com/en/top-stories/s-9097 **Redirect from:** deutcshewelle.com **IP:** 2.16.186.59 - **PTR:** a2-16-186-59.deploy.static.akamaitechnologies.com - **Server:** Apache-Coyote/1.1 **GeoIP:** 🇪🇺 ,EU - AS20940 (AKAMAI-ASN1, US)	1 year **Via:** manual	2 MB	124	23	6	🇪🇺
25 □	**URL:** www.dw.com/en/top-stories/s-9097 **Redirect from:** deutcshewelle.org **IP:** 2.16.186.59 - **PTR:** a2-16-186-59.deploy.static.akamaitechnologies.com - **Server:** Apache-Coyote/1.1 **GeoIP:** 🇪🇺 ,EU - AS20940 (AKAMAI-ASN1, US)	1 year **Via:** manual	2 MB	130	22	5	🇪🇺

This link was scanned via URLScan by an anonymous user less then a month days ago, which might reveal another attack by Charming Kitten[7].

[6] https://twitter.com/clearskysec/status/1006445262003494913
[7] https://urlscan.io/result/12cbdac3-8a98-4dd3-9158-7c875d8db71e/

A second wave of attacks using the same vector took place in August. The attackers sent multiple email messages in a single night to multiple potential victims, impersonating a woman called Samantha Vinograd from who works at CNN.

Similarly to the previous attack wave, the email message distributed to the victims contained multiple spelling mistakes, especially in the names of the reporters the attackers impersonated. For example, in the email address used to send the decoy emails the last name of the reporter is misspelled.

Below here is the phishing email's content:

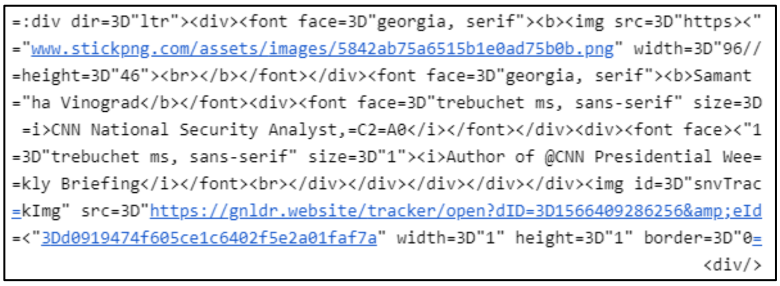
*Hello ** *

*I'm Samantha Vinograd, CNN national security analyst**.*
*CNN News intends to interview some of Israel's successful figures abroad
and broadcast it as a documentary. We have interviewed some of the leading
Israeli figures in the US, Europe and other countries and are very eager to
meet you.*
*Your humanitarian and political activities have determined us to produce a
short documentary of your life and your family.*

*You can specify the time and place of the first meeting for the
documentary pre-production stage.*
* Please advise me of any special mobility or dietary requirements you may
have. I hope you are able to accept this invitation and I look forward to
hearing from you.*

Samantha Vinograd
CNN National Security Analyst ,
Author of @CNN Presidential Weekly Briefing

An analysis of the email's headers reveals that the attackers planted an email tracker within the message. The tracker can be seen below:

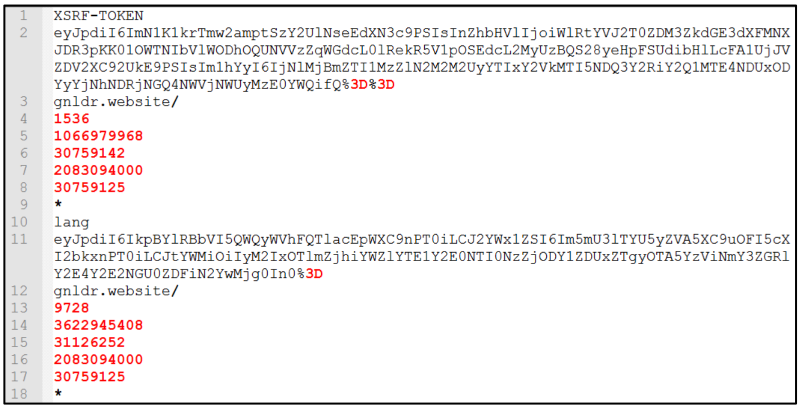


```
=:div dir=3D"ltr"><div><font face=3D"georgia, serif"><b><img src=3D"https><"
="www.stickpng.com/assets/images/5842ab75a6515b1e0ad75b0b.png" width=3D"96//
=height=3D"46"><br></b></font></div><font face=3D"georgia, serif"><b>Samant
="ha Vinograd</b></font><div><font face=3D"trebuchet ms, sans-serif" size=3D
 =i>CNN National Security Analyst,=C2=A0</i></font></div><div><font face><"1
=3D"trebuchet ms, sans-serif" size=3D"1"><i>Author of @CNN Presidential Wee=
=kly Briefing</i></font><br></div></div></div></div></div><img id=3D"snvTrac
=kImg" src=3D"https://gnldr.website/tracker/open?dID=3D1566409286256&amp;eId
=<"3Dd0919474f605ce1c6402f5e2a01faf7a" width=3D"1" height=3D"1" border=3D"0=
                                                                      <div/>
```

The tracker is used by the attackers to check whether the message is forwarded to additional recipients, and to obtain the geolocation and IP address of the victim. Data is collected via a cookie that is installed on the victim machine in the following route:

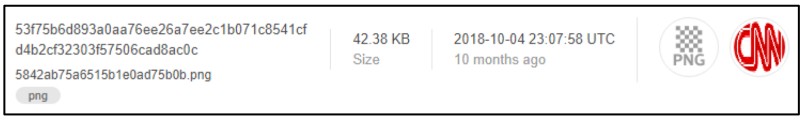
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\admin@gnldr[$].txt

Below here is the content of the cookie:



```
XSRF-TOKEN
eyJpdiI6ImN1K1krTmw2amptSzY2UlNseEdXN3c9PSIsInZhbHVlIjoiWlRtYVJ2T0ZDM3ZkdGE3dXFMNX
JDR3pKK01OWTNIbVlWODhOQUNVVzZqWGdcL0lRekR5V1pOSEdcL2MyUzBQS28yeHpFSUdibHlLcFA1UjJV
ZDV2XC92UkE9PSIsIm1hYyI6IjNlMjBmZTI1MzZlN2M2M2UyYTIxY2VkMTI5NDQ3Y2RiY2Q1MTE4NDUxOD
YyYjNhNDRjNGQ4NWVjNWUyMzE0YWQifQ%3D%3D
gnldr.website/
1536
1066979968
30759142
2083094000
30759125
*
lang
eyJpdiI6IkpBYlRBbVI5QWQyWVhFQTlacEpWXC9nPT0iLCJ2YWx1ZSI6Im5mU3lTYU5yZVA5XC9uOFI5cX
I2bkxnPT0iLCJtYWMiOiIyM2IxOTlmZjhiYWZlYTE1Y2E0NTI0NzZjODY1ZDUxZTgyOTA5YzViNmY3ZGRl
Y2E4Y2E2NGU0ZDFiN2YwMjg0In0%3D
gnldr.website/
9728
3622945408
31126252
2083094000
30759125
*
```

To further disguise the malicious nature of the message, the attackers appended the CNN logo:



53f75b6d893a0aa76ee26a7ee2c1b071c8541cf
d4b2cf32303f57506cad8ac0c
5842ab75a6515b1e0ad75b0b.png
png

42.38 KB
Size

2018-10-04 23:07:58 UTC
10 months ago

Attack Infrastructure: C&C Servers, Domains and Attribution

We Identified more than six unique servers hosting the fake Charming Kitten websites. Of which, four impersonate entities as part of the first stage, while the other two host servers impersonating Google services. We asses that these are likely to be used as in second stage of the attack – data theft.

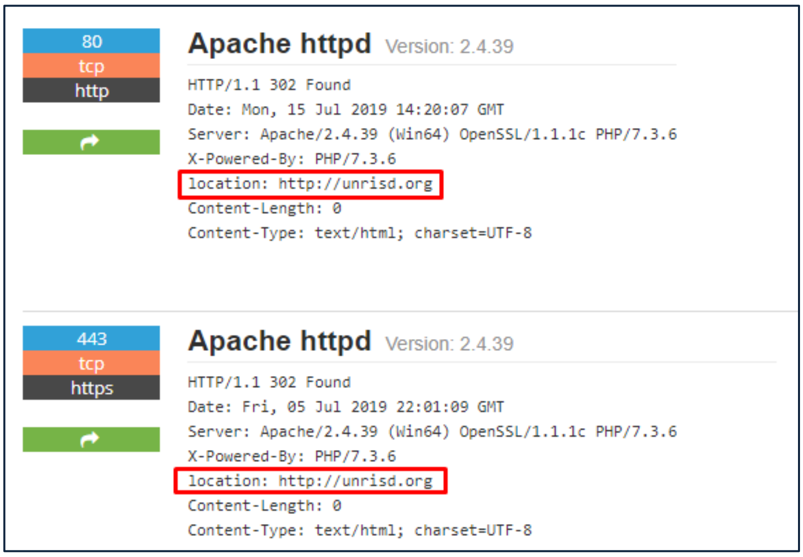
Server	Domain point to the IP	Impersonation subject
185.141.63[.]8	Skynevvs[.]com	Sky News Skynews.com
185.141.63[.]135	Leslettrespersanes[.]net Inztaqram[.]ga	Les lettres persanes (Iranian news website in French) leslettrespersanes.fr Instagram
185.141.63[.]156	Islamicemojimaker[.]com niaconucil[.]org	NIAC (National Iranian American Council)[8] niacouncil.org
185.141.63[.]157	google.drive-accounts[.]com drive-accounts[.]com	Google drive drive.google.com
185.141.63[.]160	unirsd[.]com	UNRISD (United Nation Research Institute for Social Development) unrisd.org
185.141.63[.]161	acconut-verify[.]com	Google Account Verification
185.141.63[.]162	isis-online[.]net	ISIS (Institute for Science and International Security) isis-online.org
185.141.63[.]170	accounts-drive[.]com w3-schools[.]org	Google drive W3Schools w3schools.com
185.141.63[.]172	Seisolarpros[.]org	SEI Professional Services seisolarpros.com

After a month of campaign operations, The attackers switched the servers used to store the email addresses, containing thousands of addresses.

It should be noted that these domains can only be accessed via the aforementioned link in the spear-phishing email. In any other case, the server will redirect the client to the original website (HTTP 302 in port 442 or 301 in port 80). The following image presents the headers of

[8] Please note that in recent days, many Iranian citizens protested in front the office of the National Iranian American Council. They protested against the organization, claiming that it is does not represent the Iranian community in the US.

185.141.63[.]160 from Shodan[9]. The fake domain is unirsd[.]com, however, it redirects to the original website.



80
tcp
http

Apache httpd Version: 2.4.39

```
HTTP/1.1 302 Found
Date: Mon, 15 Jul 2019 14:20:07 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1c PHP/7.3.6
X-Powered-By: PHP/7.3.6
location: http://unrisd.org
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

443
tcp
https

Apache httpd Version: 2.4.39

```
HTTP/1.1 302 Found
Date: Fri, 05 Jul 2019 22:01:09 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1c PHP/7.3.6
X-Powered-By: PHP/7.3.6
location: http://unrisd.org
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

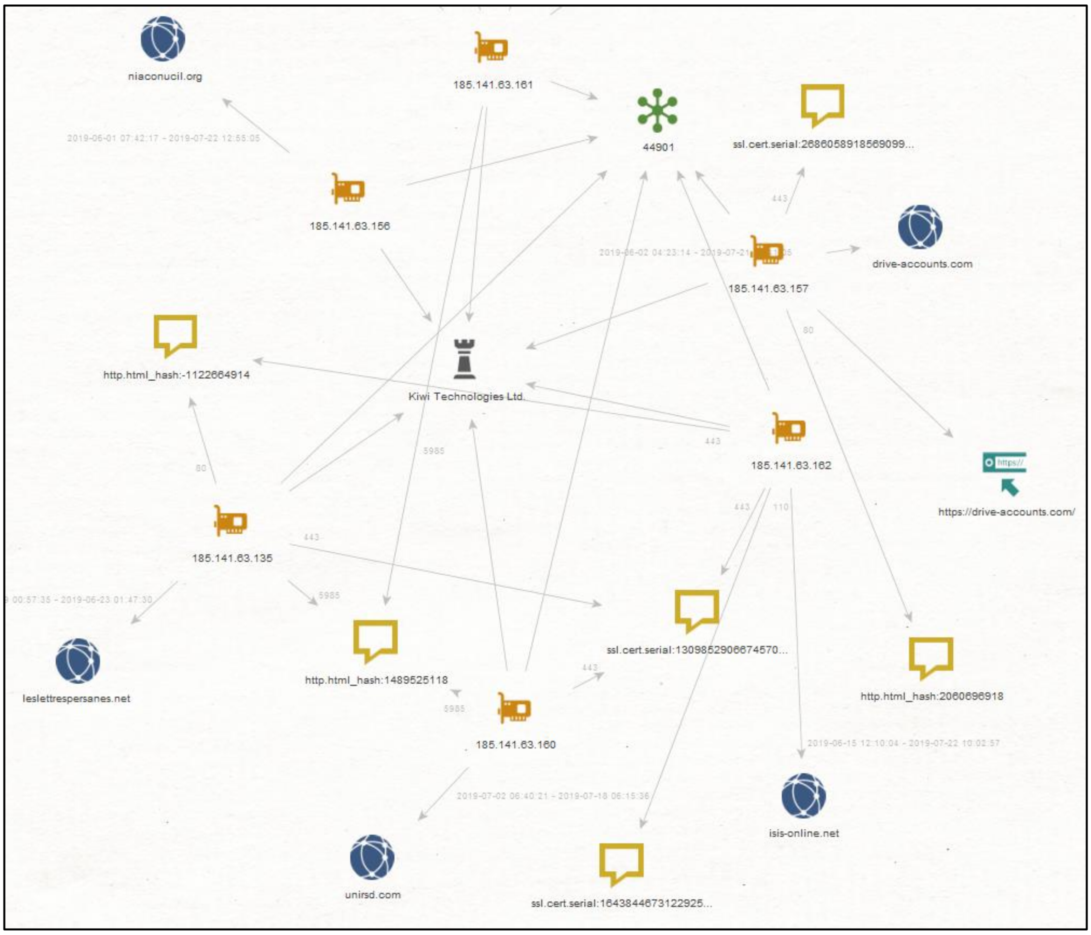
The server 185.141.63[.]135 is the only server that pointing to 2 domains:

1) leslettrespersanes[.]net which is impersonating the French magazine “Les Lettres Persanes”.
2) Inztaqram[.]ga which is impersonating Instagram company. This is **the first time** we observed a phishing website executed by Charming Kitten that impersonate non-google services in order to steal credentials from the victim to other services.

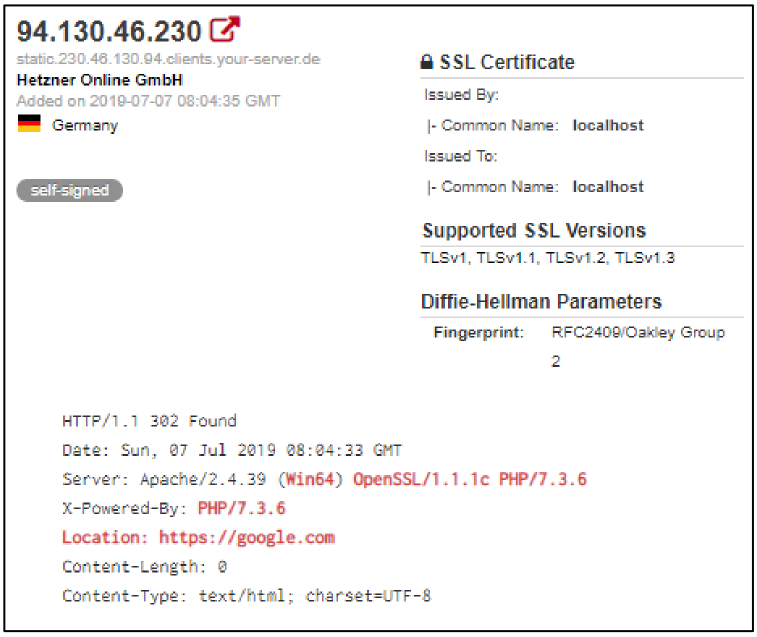
All of the servers used in the latest attack are hosted by BelCloud Hosting Corporation, located in Bulgaria (ISP Kiwi Technologies Ltd.). Older servers in the campaign, such as 46.21.150[.]197, are hosted by other hosting services.

As presented in the last image, all servers are Apache/2.4.39 (Win64), using OpenSSL/1.1.1b and PHP versions 7.3.5 or 7.3.6.

[9] https://www.shodan.io/host/185.141.63.160



Searching other servers with these unique parameters returned less than 300 results. Most of these results are not malicious. We ruled out the legitimate servers that pointed in their redirect to the same IP address or to a domain the server hosts. Within these servers, we identified one server that redirects to Google services, which concurrently hosts two Iranians Name Servers. We consider this server to be part of this campaign in medium-high level of confidence:



94.130.46.230

static.230.46.130.94.clients.your-server.de
Hetzner Online GmbH
Added on 2019-07-07 08:04:35 GMT
Germany

self-signed

SSL Certificate

Issued By:
|- Common Name: **localhost**
Issued To:
|- Common Name: **localhost**

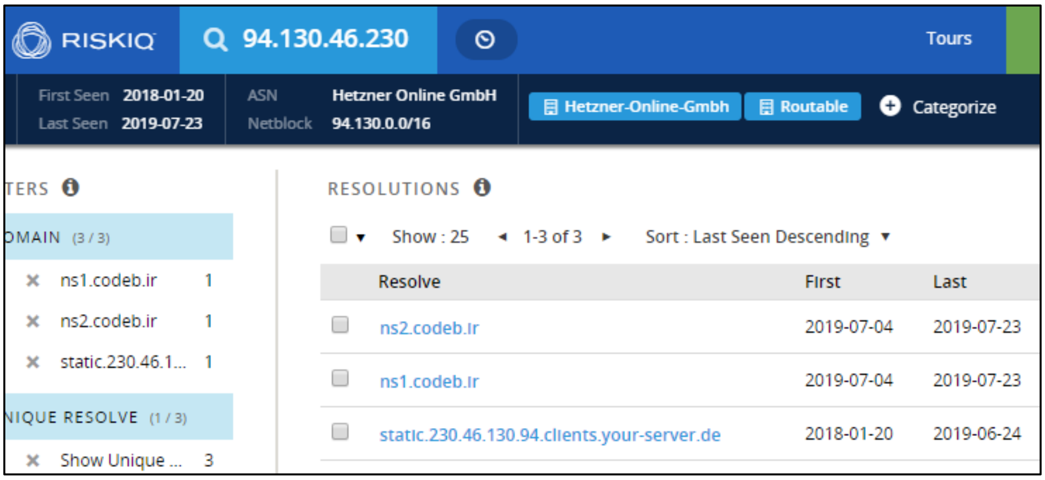
Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

```
HTTP/1.1 302 Found
Date: Sun, 07 Jul 2019 08:04:33 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1c PHP/7.3.6
X-Powered-By: PHP/7.3.6
Location: https://google.com
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```



RISKIQ 94.130.46.230 Tours

First Seen 2018-01-20
Last Seen 2019-07-23
ASN Hetzner Online GmbH
Netblock 94.130.0.0/16

Hetzner-Online-Gmbh | Routable | Categorize

TERS

OMAIN (3 / 3)

✕	ns1.codeb.ir	1
✕	ns2.codeb.ir	1
✕	static.230.46.1...	1

NIQUE RESOLVE (1 / 3)

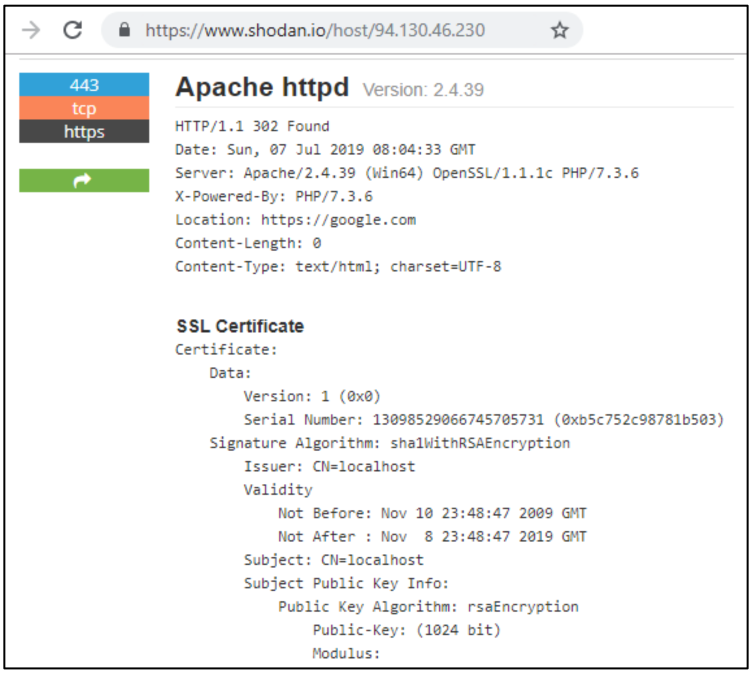
✕	Show Unique ...	3

RESOLUTIONS

□ Show : 25 ◂ 1-3 of 3 ▸ Sort : Last Seen Descending ▾

	Resolve	First	Last
□	ns2.codeb.ir	2019-07-04	2019-07-23
□	ns1.codeb.ir	2019-07-04	2019-07-23
□	static.230.46.130.94.clients.your-server.de	2018-01-20	2019-06-24

First and foremost, it should be noted that the Iranian cyber divisions use servers belonging to Hetzner Online GmbH in many of their operations[10]. Second, there is an overlap of the server version, the SSL version, the PHP version and even the serial number of the SSL certificate.



https://www.shodan.io/host/94.130.46.230

443
tcp
https

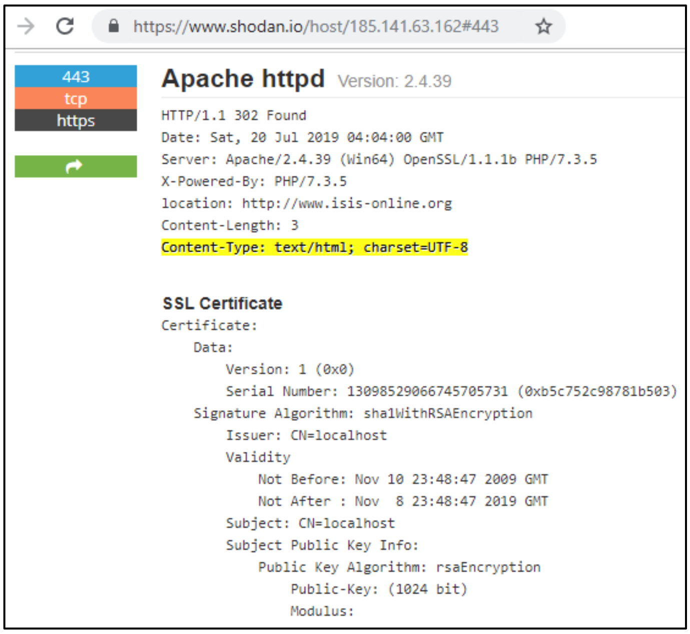
Apache httpd Version: 2.4.39

```
HTTP/1.1 302 Found
Date: Sun, 07 Jul 2019 08:04:33 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1c PHP/7.3.6
X-Powered-By: PHP/7.3.6
Location: https://google.com
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 13098529066745705731 (0xb5c752c98781b503)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=localhost
        Validity
            Not Before: Nov 10 23:48:47 2009 GMT
            Not After : Nov  8 23:48:47 2019 GMT
        Subject: CN=localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
```

[10] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/04/Iran-Memo.pdf
https://www.clearskysec.com/wp-content/uploads/2018/11/Global-Iranian-Disinformation-Operation-Clearsky-Cyber-Security.pdf
https://citizenlab.ca/2016/08/group5-syria/



https://www.shodan.io/host/185.141.63.162#443

Apache httpd Version: 2.4.39

```
HTTP/1.1 302 Found
Date: Sat, 20 Jul 2019 04:04:00 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.5
X-Powered-By: PHP/7.3.5
location: http://www.isis-online.org
Content-Length: 3
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

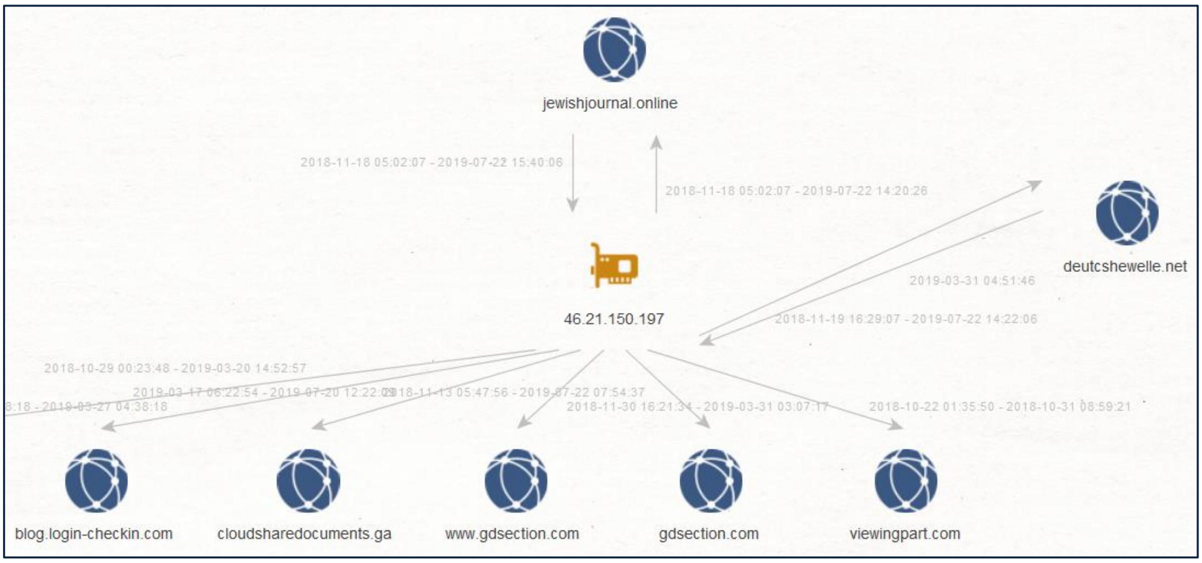
```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 13098529066745705731 (0xb5c752c98781b503)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=localhost
        Validity
            Not Before: Nov 10 23:48:47 2009 GMT
            Not After : Nov  8 23:48:47 2019 GMT
        Subject: CN=localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
```

Attribution

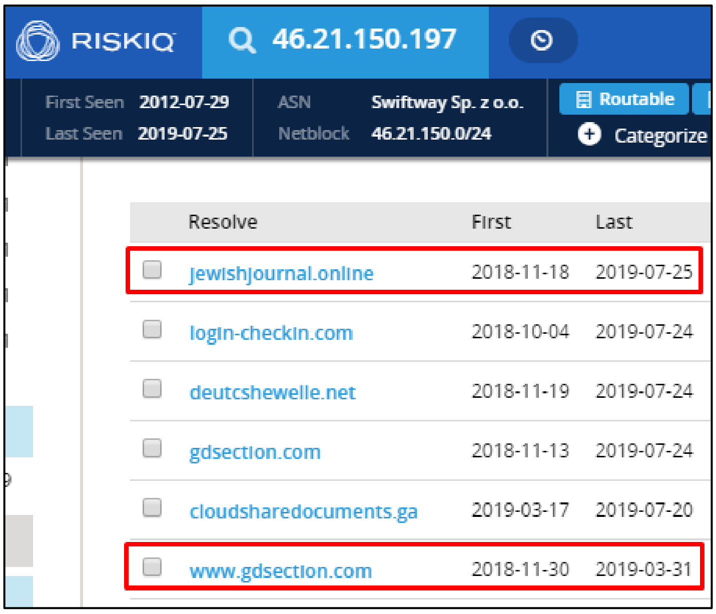
We made an attribution to the Iranian Charming Kitten group based on three main factors:

1. The two main websites linked in the second scenario are:
    - The Jewish Journal (Please see for further information).
    - German magazine - Deutsche Welle.

In March 2019, ClearSky identified another attack as part of this campaign, using an email address pointing to jewishjournal[.]online. From the Passive DNS records of this domain, we identified another domain impersonating Deutsche Welle – deutcshewelle[.]net.



Based on passive DNS records, it seems that Charming Kitten used the decoy Jewish Journal domain once again in July 2019:



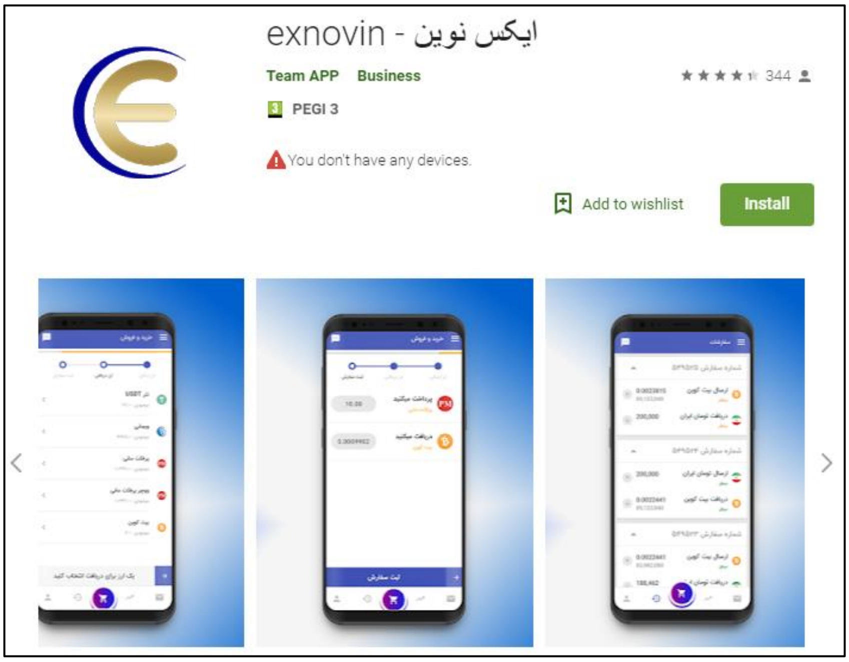
RISKIQ 46.21.150.197

First Seen 2012-07-29 | Last Seen 2019-07-25 | ASN Swiftway Sp. z o.o. | Netblock 46.21.150.0/24

	Resolve	First	Last
□	jewishjournal.online	2018-11-18	2019-07-25
□	login-checkin.com	2018-10-04	2019-07-24
□	deutcshewelle.net	2018-11-19	2019-07-24
□	gdsection.com	2018-11-13	2019-07-24
□	cloudsharedocuments.ga	2019-03-17	2019-07-20
□	www.gdsection.com	2018-11-30	2019-03-31

2. As mentioned, the victims are non-Iranian investigators based in the US, Middle East and France. Their field of expertise fits Charming Kitten's TTPs. The repeating spelling mistakes in the email content are also evidence of the Charming Kitten line of action.
3. The impersonation to NIAC indicates that it is an Iranian actor.

Apart from the above reasons, additional information also ties the group's activity to Iran. One the NetBlock of the IP addresses of the original servers we found the website exnovin[.]org. ExNovin is an Iranian company that developed a platform for money exchange. The domain was previously hosted on Hetzner, a German Internet hosting company. We estimate that these factors are likely related to the Charming Kitten group.



exnovin - ایکس نوین

Indicators

isis-online[.]net

acconut-verify[.]com

leslettrespersanes[.]net

unrisd[.]com

drive-accounts[.]com

niaconucil[.]org

skynevvs[.]com

islamicemojimaker[.]com

w3-schools[.]org

seisolarpros[.]org

exnovin[.]org

185[.]141[.]63[.]161

185[.]141[.]63[.]162

185[.]141[.]63[.]135

185[.]141[.]63[.]160

185[.]141[.]63[.]156

185[.]141[.]63[.]157

185[.]141[.]63[.]8

185[.]141[.]63[.]172

MISP events 1682 and 1438

ClearSky Cyber Intelligence Report

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

Ahead of the Threat Curve

TLP: AMBER - The content of the document is solely for internal use. Distributing the report outside of recipient organization is not permitted.