The Kittens Are Back in Town 3

Charming Kitten Campaign Evolved and Deploying Spear-Phishing link by WhatsApp

August 2020

TLP:WHITE

Contents

Introduction

Executive Summary

During 2017-2019, Clearsky had published several reports about the Iranian APT group "Charming Kitten". One of the group's most common attack vectors is impersonating journalists, particularly those from the German "Deutsche Welle" broadcasting company and the "Jewish Journal" magazine[1].

Starting July 2020, we have identified a **new TTP of the group**, impersonating "Deutsche Welle" and the "Jewish Journal" using emails alongside WhatsApp messages as their main platform to approach the target and convince them to open a malicious link. To gain the victim's trust and ensure the opening of the link, the attackers use fake LinkedIn profiles as well. This is the first time we identified an attack by Charming Kitten conducted through WhatsApp and LinkedIn, including attempts to conduct phone calls between the victim and the Iranian hackers. Charming Kitten chooses to impersonate Persian speaking journalists, to **neutralize detection through accent while having the phone call**. In this report, we expose for the first time the full conversation between Charming Kitten to a victim, conducted on WhatsApp.

The malicious link is embedded in a legitimate, compromised "Deutsche Welle" domain. Each victim receives a personalized link, tailored to their specific email account. We identified an attempt to send a **malicious ZIP file** to the victim as well, additional to a message that was sent to the victim via a fake LinkedIn profile. We assess that in some cases, Charming Kitten would try to infect the victim with malware instead of stealing its credentials.

"Charming Kitten", also known as APT35 or "Ajax", is an Iranian cyberespionage group active since 2014. Their primary targets are Iranian academia experts, human rights' activists, and journalists. In the past few months, it seems that Charming Kitten has expanded their target's list, adding the Baha'i community[2], high-ranking American civil servants and officials (including ambassadors and former employees of the US State Department), and COVID-19 related organizations (such as Gilead[3] and WHO[4]). In the current campaign, we identified attempts to attack Israeli scholars (targeting their institutional email account), and US government employees.

Here is a timeline of their operations involving "Deutsche Welle" and "Jewish Journal" in the past 3 years:

---

[1] clearskysec.com/charmingkitten/
[2] docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.1mxvns31ypem
[3] reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV
[4] bloomberg.com/news/articles/2020-05-07/hackers-target-who-by-posing-as-think-tank-broadcaster

December 2017	• **Charming Kitten: Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets** (Clearsky's report) • Jewish Journal breached, embedding a "watering hole"
July 2018	• **Charming Kitten attempted to attack ClearSky and our customers directly via a fraudulent Clearsky replica website, embedding the same phishing kit that is used in this campaign, additional to Jewish Journal phishing embedded in the fake website.**
September 2019	• **The Kittens Are Back in Town Charming Kitten – Campaign Against Academia Researchers** (Clearsky's report) • "Deutsche Welle" impersonation via email; using a fake "Jewish Journal" website
January 2020	• **Fake Interview: The New Activity of Charming Kitten** (CERTFA report) • "Deutsche Welle" impersonation via email, the subject being "Dimensions of Iran's response to Soleimani's death"
August 2020	• **The Kittens Are Back in Town 3 (**Clearsky's report**)** • "Deutsche Welle" and "Jewish Journal" impersoantion and water-holing

Clearsky alerted "Deutsche Welle" about the impersonation and the watering hole in their website. A "Deutsche Welle" representative confirmed that the reporter which Charming Kitten impersonated, did not send any emails to the victim nor any other academic researcher in Israel in the past few weeks. Note that part of "Deutsche Welle" reporters are originally from Iran – a fact that helps Charming Kitten to hide the accent of their operators during a phone call.

It should be noted that this attack vector is unique to Charming Kitten, but it has not the only attack vector that has been used in recent months by this threat actor. More information about recent campaigns by the group can be found in our raw threat intelligence[5] or on our blog[6].

Deployment Vector: WhatsApp and LinkedIn

In recent months, we identify an increase in the use of WhatsApp and LinkedIn as platforms of communication between threat actors and victims. In the last three years, Charming Kitten has been operating their campaigns mainly by emails and SMS. These two platforms enable the attacker to reach the victim easily, spending minimum time in creating the fictitious social media profile. However, in this campaign Charming Kitten has used a reliable, well-developed LinkedIn account to support their email spear-phishing attacks.

In this campaign, we observed a willingness of the attackers to speak on the phone directly with the victim, using WhatsApp calls, and a legitimate German phone number. This TTP is uncommon and jeopardizes the fake identity of the attackers (unlike emails for example). However, if the attackers have

---

[5] docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/
[6] clearskysec.com/the-kittens-are-back-in-town-2/

successfully passed the phone call obstacle, they can gain more trust from the victim, compared to an email message.

Charming Kitten is not the first threat actor who uses WhatsApp phone call in recent months. In Operation 'Dream Job', which we exposed in August 2020[7], the Lazarus group (North Korea) used the same method to gain the victim's trust.

---

[7] clearskysec.com/operation-dream-job/

Attack Vector

Introduction

This latest campaign of Charming Kitten uses enhanced social engineering techniques already discovered in our report "The Kittens Are Back in Town" in 2019[8]. In the 2019 scenario, the attackers had impersonated a known journalist, almost always from "Deutsche Welle". In 2020 Charming Kitten offers the victim to participate in an online webinar/meeting about Iran and other subjects of interest for the target (e.g. recent discourse between Iran and the US). The Charming Kitten operators introduce themselves as journalists and ask the victim whether they are interested in participating in the webinar. If so, they are requested to reply in order to receive the following details:

1. A full list of other participants

2. Date and time for the webinar

3. Details regarding the payment for attending the webinar.

This attack vector was carried out by Charming Kitten between 2018 to early 2020. Here is an example for the email sent allegedly from Keyarash Navidpour, a reporter in DW, to an Israeli academia scholar[9]:

---

[8] clearskysec.com/the-kittens-are-back-in-town/
[9] ru.reuters.com/article/idUSKBN1ZZ1MS

_____

From: keyarash navidpour <keyarashnavidpour@deuteschewelle.com>
Date: Sat, 4 Jan 2020, 18:45
Subject: Dear Mr. ████████████
To: ████████████████████████

Dear Mr. ████████████████

I am Keyarash Navidpour from Deutsche Welle(www.dw.de).
This is an invitation to request you to participate in DW Webinar.
The subject of webinar is " Dimensions of Iran's response to Soleimani's death".
Most three important topics of webinar are:
- Iran's military capabilities and possible goals.
- Iraq's political and military response and its consequences.
- The Impact of Future Behaviors on Security and Peace in the Middle East.
The participants of webinar are:
- Experts on security, terrorism, Iraq and Iran.
- Military experts in the Middle East.
- High profile politicians from around the world that research on Middle East.
- Professors and students that have deep study on Iran.
- Students of DW Akademie
This webinar is holding by DW Akademie and is supported by Google.
We are glad to meet you in our webinar.
I am looking forward to hearing from you.

Best regards
Keyarash Navidpour
https://www.dw.com/fa-ir

However, in August 2020 we have identified a change in attack methods, which will be presented in detail in the following chapter.

Social Engineering Methods Used to Establish a Credible Communication

First stage – approaching the victim by email

In most of the cases that we handled in the past several months, the targeted academia researchers had high awareness and suspected that they are probably under an Iranian attack. Their suspicion led them to contact us and further contact with Charming Kitten under our guidance (i.e. not opening the emails sent to them). Over the course of the past several weeks, one of the targets was lured to respond to the attackers. The subject of impersonation was an Iranian journalist that speaks fluent Farsi with a local accent.

The correspondence begun with an email sent to the target, initiating a conversation. Unlike previous attacks, the attackers did not display details regarding the alleged webinar; instead, they asked to start a conversation.

Several attempts were made to contact Israeli researchers from **Haifa and Tel Aviv Universities'** email addresses, hosted on a Microsoft email server (Outlook).

From: **Yalda Zarbakhch** <yaldazarbakhch@gmail.com>
Date: Wed, 5 Aug 2020 at 10:56
Subject: Discussion
To: <████████research.haifa.ac.il>

Dear Dr. ████████

May I have a minute of your time?

Yalda Zarbakhch
Deutsche Welle

From: **marcy oster** <marcy.oster.jta@gmail.com>
Date: Mon, Aug 10, 2020 at 6:04 PM
To: ████████████████████

I'm sorry, Dr. ████████
An error occurred. I apologize.
I am Marcy Oster from Jewish Journal (jewishjournal.com).
We are going to hold the webinar with journalists and experts in the field of "Citizenship and freedom of girls and women in Iran and its future"
If possible, I would like to invite you to participate in our online webinar.

Best wishes

In another case, the attacker impersonated an Israeli scholar from Tel Aviv University and invited them to an alleged "Zoom" meeting in Hebrew.

From: ████████████████████@tauex.tau.ac.il>
Sent: Sunday, August 2, 2020
To: ████████████████@univ.haifa.ac.il>
Subject: Read: ישיבת וועד מנהל וועד מנהל מיוחדת-דחופה באמצעות זום

Your message

To:
Subject: ישיבת וועד מנהל וועד מנהל מיוחדת-דחופה באמצעות זום
Sent: Sunday, August 2, 2020 12:10:40 PM (UTC+00:00) Monrovia, Reykjavik

was read on Sunday, August 2, 2020 12:10:36 PM (UTC+00:00) Monrovia, Reykjavik.

After a short conversation with the target, the Charming Kitten attacker requests, for the first time, to move the conversation to WhatsApp. This is not the first use of a mobile messaging service (for instance

phishing using SMS), but the first case where we have seen the use of WhatsApp. If the target refuses to move to WhatsApp, the attacker will send a message via a fake LinkedIn profile. Here's an example of "Marcy Oster" – a fake profile used by the Iranians in their attack.
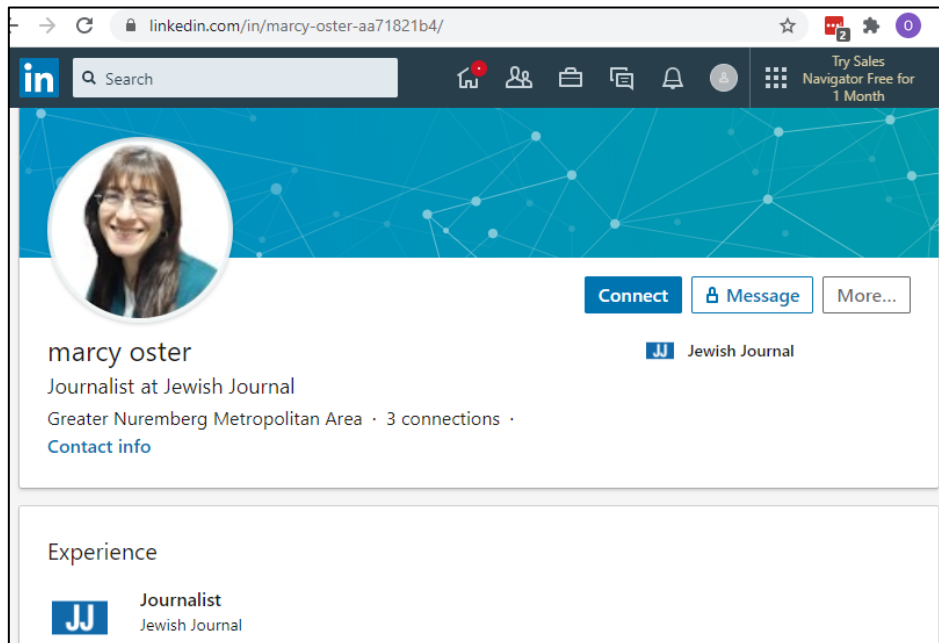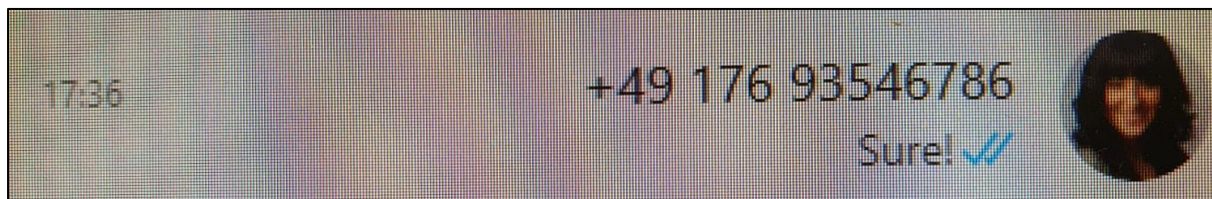

To convince the victim to join the alleged webinar, the attackers tried to entice the victim with nominating them as its main speaker, chosen from more than a hundred participants. They claimed that further information about the alleged webinar will be shared after **approving the invitation.** The subject of the webinar is changed by Charming Kitten from one victim to another, based on their expertise.

_____
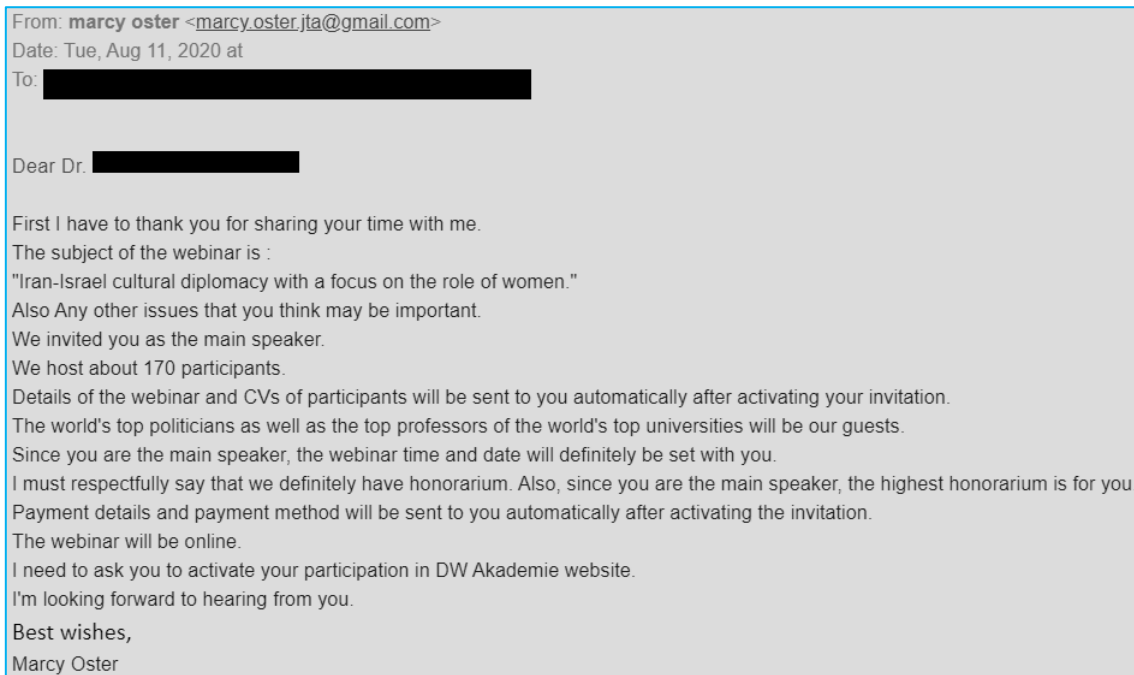
Second Stage – WhatsApp and LinkedIn

After this conversation with the target, the attacker requests that they switch to WhatsApp for further conversation.

Charming Kitten sent **multiple** and repeating messages, sometimes in very short time, until the target responded. The messages were sent from a German number (prefix +49) to create a sense of credibility, and the WhatsApp account bears the image of the journalist being impersonated. Unlike other groups, **Charming Kitten chooses to impersonate Persian speaking journalists, to neutralize detection through the accent.**

Here is the full correspondence (names redacted):

| Message Content	Author
First Day	
Hi.	Attacker
Dear Dr. *******	
May I have a minute of your time?	
Dear Dr. *******	
I am Yalda Zarbakhch from Deutsche Welle	
Attempt at a voice call	
Second Day	
Dear Dr. *******	Attacker
I am Yalda Zarbakhch from Deutsche Welle	
Third Day	
Dear Dr. *******	Attacker
Hi Yalda. What is it about?	Victim
Dear Dr. ******* First I have to thank you for sharing your time with me. If possible, I would like to invite you to participate in our upcoming webinar as a special speaker.	Attacker
Please provide details	Victim
Many thanks. Sure	Attacker
Fourth Day	
Dear Dr. ******, First I have to apologize for this belated message. This delay was due to weekend. Thank you for sharing your time with me. We host about 114 participants. Details of the webinar and CVs of participants will be sent to you automatically after activating your invitation. We invited you as a special speaker. The webinar will be online. The subject of the webinar is: "Iran and Israel, Change or stability in the strategic and security equations of the Middle East". Also: "Israel's reaction to the Iran-China agreement".	Attacker

I need to ask you to active your participation in DW Akademie website. The webinar is on DW Akademie website. I provide you with the invitation link. If you would like let me know, I will send you the link. Best Regards, Yalda	
Fifth Day	
Dear Dr. *******	Attacker
I look forward to your reply with great respect.	
Best	
Yalda	
Dear Dr. *******	
Dear Dr. *******	
May I have your email address?	
Dear Dr. *******	
The victim sent his email address	
Seventh Day	
Hi	Attacker
Many thanks	
Are you available now?	
Eighth Day	
Dear Dr. *******	Attacker
I sent an email to your email address.	
Best	
Yalda	
Hi Yalda. I'm away and be back in a few days.	Victim
Many thanks	Attacker
Respectfully	
Ninth Day	
Dear Dr. *******	Attacker
I am looking forward to hearing from you	
Dear Dr. *******	
Any updates?	
Hey Yalda, I am inundated with work this week. What exactly do you need?	Victim
I really understand you and I apologize a lot for this inconvenience. The subject of the webinar is: "Iran and Israel, Change or stability in the strategic and security equations of the Middle East ." Also: "Israel's reaction to the Iran-China agreement ." We invited you as the main speaker. We host about 114 participants. Details of the webinar and CVs of participants will be sent to you automatically after activating your invitation. The world's top politicians as well as the top professors of the world's top universities will be our guests. Since you are the main speaker, the webinar time and date will definitely be set with you. I must respectfully say that we definitely have honorarium. Also, since you are the main speaker, the highest honorarium is for you. Payment details and payment method will be sent to you automatically after activating the invitation. The webinar will be online. I need to ask you to activate your participation in DW Akademie website. The webinar is on DW Akademie website. I provide you with the invitation link. If you would like and let me know, I will send you the link.	Attacker

Please send me the link	Victim
The attacker sends the link to the victim and attempts to call them under the pretense of taking them through the steps of connecting to the webinar	Attacker
The victim tries to enter fake password, then complains about a password error message received after entering their credentials	
Dear Dr. ******* Did you activate your participation? The link expires after half an hour	Attacker
Dear Dr. ******* Why?	
Did you receive any error?	
What was the problem?	
Tenth Day of Correspondence	
The victim, repeats their issue to the attacker and requests the link through email	
Dear Dr. *******	Attacker
The webinar will be online and is secured by Google and Used Google OpenID to verify participants identification. Read more about Google OAuth 2.0: https://developers.google.com/identity/protocols/OAuth2	
Therefore, it is not possible for us to activate	
The victim requests a different link to the webinar	
Let me coordinate with the technical team	Attacker
The attacker sends the link to the victim	
The link is set for your email address: %login%@univ.haifa.ac.il	
I am in, thank you. What is the next step?	Victim
Great. After successful authentication, everything will be sent to you automatically by the system	Attacker

The Charming Kitten attackers **implore the victim to respond repeatedly for ten days**, and they are prepared to engage in a direct phone call with them to cajole the victim into "activating their account" with the site "Akademie DW" (used as their phishing page). **During our investigation, we addressed DW, which confirmed that the reporter never contacted the victim and that the alleged webinar is fake**. The webinar's subjects were previously used by the group as lures. In May 2020, for example, the group impersonated the INSS and lured victims to a webinar regarding China-related research.

If the victim is not willing to share their personal phone number, the attacker will send him a message from the fake LinkedIn account. This message will contain a promise that the webinar is secured by Google, as they sent to the victim on the tenth day:
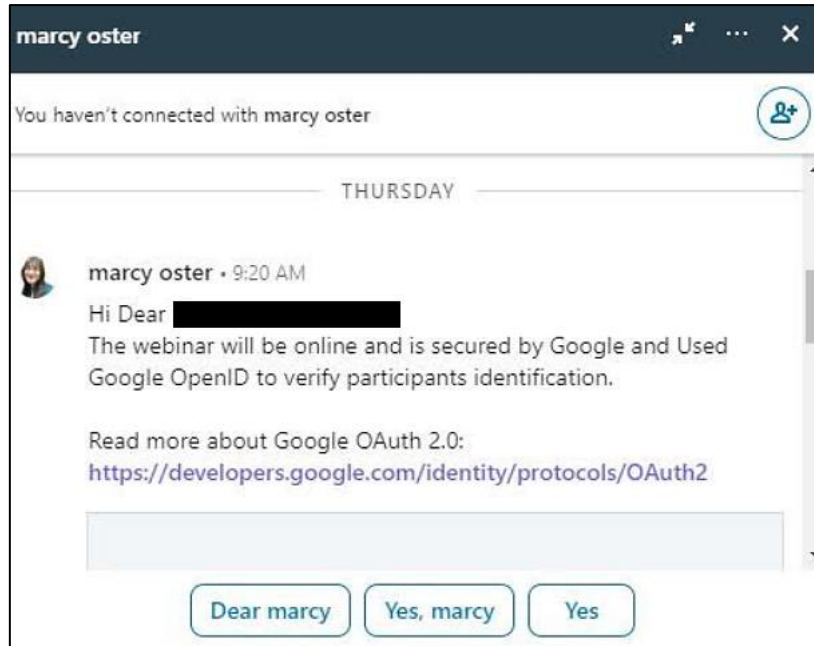
## Third Stage – Approving attending in the webinar

The malicious link was on the Deutsche Welle legitimate domain (dw[.]de). As previously reported in "The Kittens are Back in Town". Each victim receives a personalized link for their own email address – the word "?id=", following by the word SSH and 3 sets of 5 letters and numbers. Here's an example for the format:

hxxp://akademie.dw[.]de/lecture/?id=SSH-******-******-******
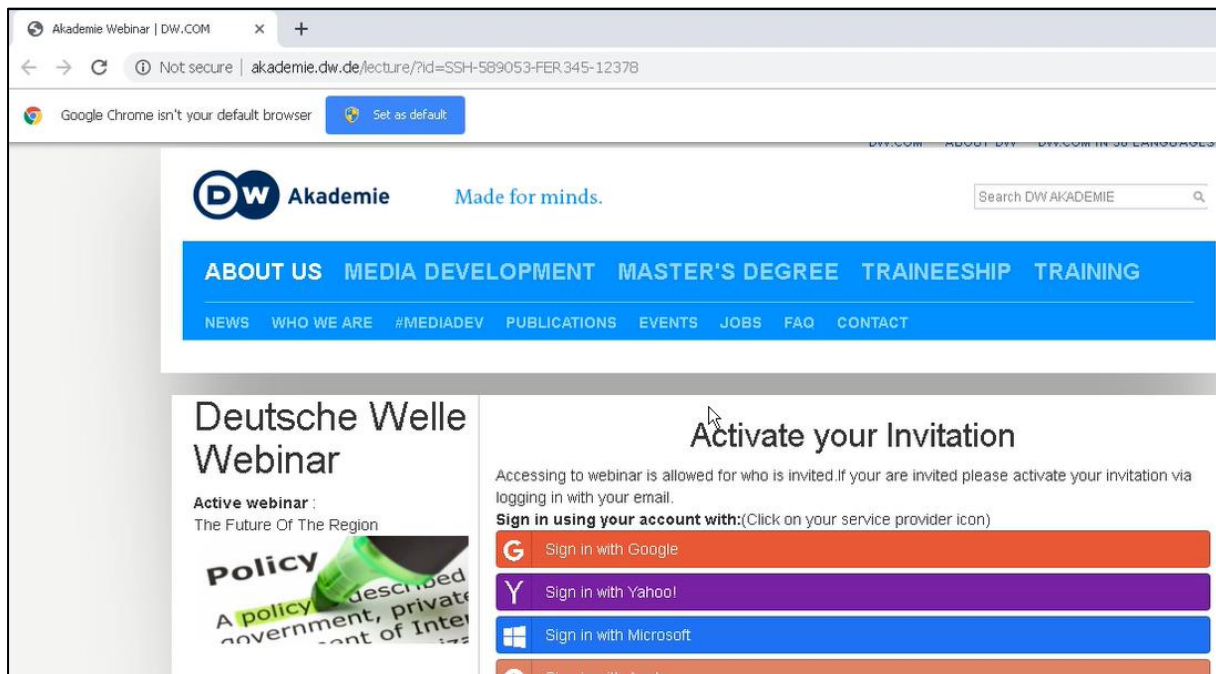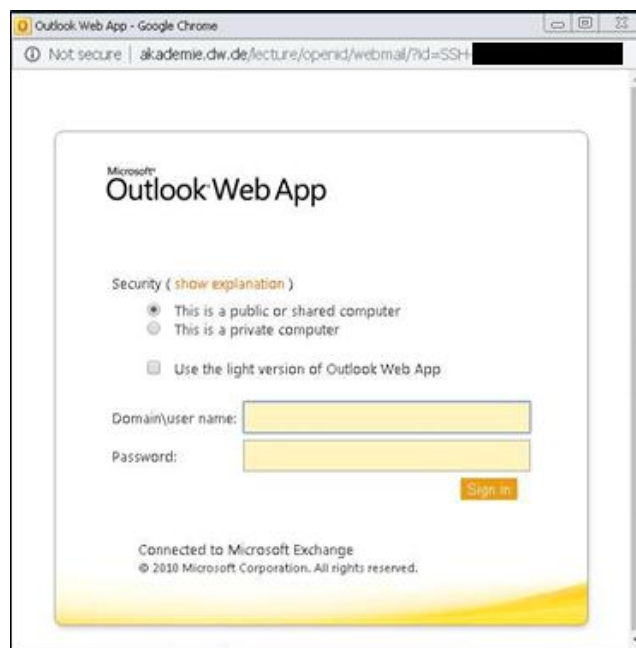

A screenshot from the watering hole page

In 2018, the Charming Kitten group had impersonated Clearsky, embedding the same phishing format in the malicious imposter domain[10]:
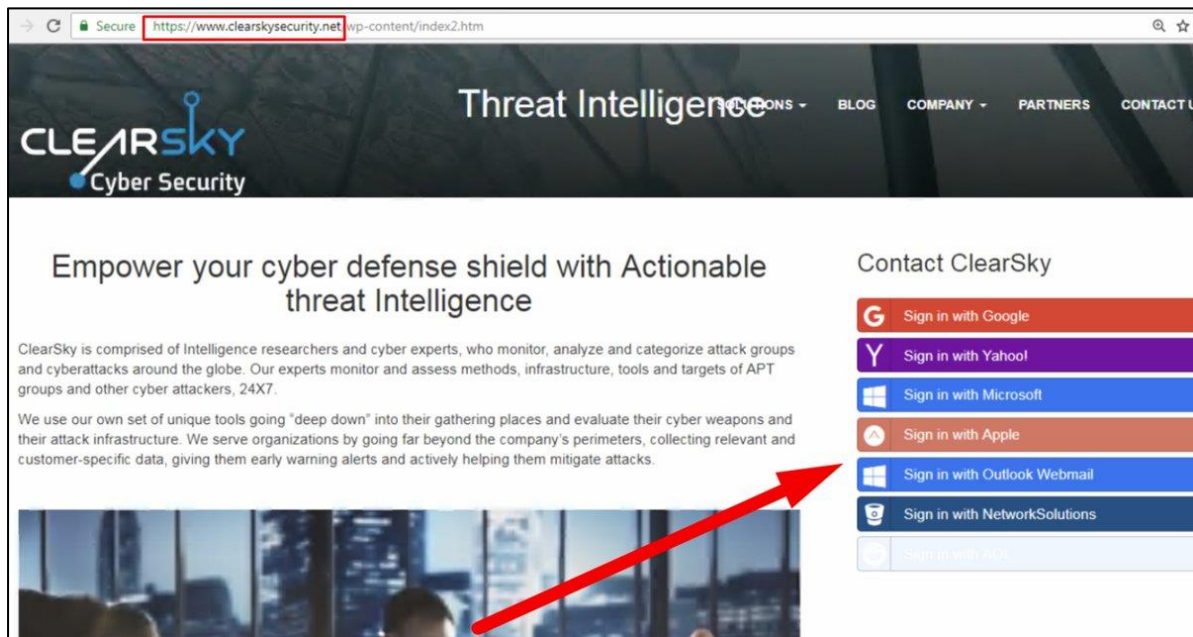
Attempting to access any service other than Outlook leads to a legitimate log-in page. Accessing the Outlook page displays a fictitious log-in field including a victim-specific URI:

The Clearsky impersonation from 2018 presented the same phishing page (we identify in the fake website a page impersonated Jewish Journal as well). Both cases included a file named **lgntopl.gif** on the domain, characterizing Outlook phishing pages. If the victim enters their correct password, they

---

[10] securityaffairs.co/wordpress/74123/apt/charming-kitten-clearsky-phishing.html

are sent to a 2FA page (as previously seen with direct interactions by the group[11]). A wrong password produces an error message. The attackers will then pressure the victim to try again using their university email.

```
<form action="login.php" method="POST" name="logonForm" ENCTYPE="application/x-www-form-urlencoded" autocomplete="off">
<input type="hidden" name="flags" value="0">
<input type="hidden" name="forcedownlevel" value="0">
<table align="center" id="tblMain" cellpadding=0 cellspacing=0>
        <tr>
                <td colspan=3>
                        <table cellspacing=0 cellpadding=0 class="tblLgn">
                        <tr>
                                <td class="lgnTL"><img src="lgntopl.gif" alt=""></td>
                                <td class="lgnTM"></td>
                                <td class="lgnTR"><img src="lgntopr.gif" alt=""></td>
                        </tr>
                        </table>
                </td>
        </tr>
```

This propagation vector is unique compared to other, common vectors by the group (such as ".site" TLD phishing websites), and the WhatsApp correspondence has not been exposed until this case.

---

[11] citizenlab.ca/2015/08/iran_two_factor_phishing/

Malicious file

Another example of a fake LinkedIn account is "Helen Cooper", a senior researcher at Hudson Institute (a think tank and research center dedicated to the analysis of US and international economic, security, and political issues). Charming Kitten created a fake profile for the attack and deleted the account later.
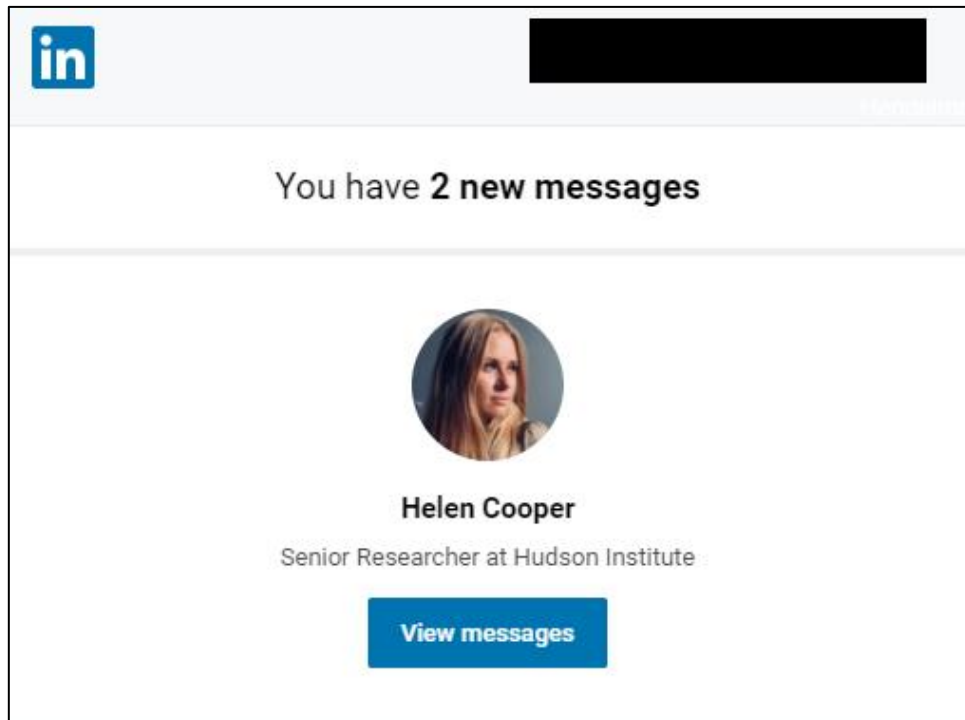
After the initial message via the fake LinkedIn profile, Charming Kitten sent the victim two different types of compromise attempts from this account:

1. An email message with a malicious link
2. An email message with a malicious file attached

Unlike the common TTPs of this threat actor, sending an attached malware is unique and was not seen in recent attacks by them. The victim deleted the file before we were able to analyze it. The following screenshot shows the correspondence between the attacker and the victim.

From: **Helen Cooper** <helen.cooper.official@gmail.com>
Date: Tue, Jun 23, 2020 at 3:43 PM
Subject: Re: Hi dear ▉▉ Did you receive my email?
To: ▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉

I have completed the details of the project
Please read it
Drive-File-Sharing.zip

On Mon, Jun 22, 2020 at 5:11 PM Helen Cooper <helen.cooper.official@gmail.com> wrote:
> I sent it by another email
> no problem
> I will send you the details of the project again
> Drive-File-Sharing.zip
>
> On Mon, Jun 22, 2020 at 3:39 AM ▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉ wrote:
>> This is the first email I've received from you.
>>
>> When did you send it?
>>
>> ▉▉▉▉

ClearSky Cyber Security Intelligence Report

Email: info@clearskysec.com

Website: clearskysec.com

Ahead of the Threat Curve

Photo by Francesco Ungaro from Pexels