# Charming Kitten: “Can We Have A Meeting?”

blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/

### Important puzzle pieces of Charming Kitten's cyber espionage operations

Certfa Lab · 2022.9.8

Important puzzle pieces of Charming Kitten's cyber espionage operations

## Introduction

Charming Kitten (known as APT42, ITG18, UNC788, TA453, PHOSPHORUS, Yellow Garuda, also APT35) is an Iranian state-sponsored threat group[1] that conducts persistent cyber espionage operations to have extensive surveillance of targeted Iranian and foreign citizens, who have strategic intelligence value for the Islamic Revolutionary Guard Corps (IRGC).

Charming Kitten actors have targeted individuals, academics, journalists, activists, think tankers, institutes, organizations, military and government sectors in the United State, European, and Middle Eastern countries since as early as 2014.

Although a number of technical reports in recent years shows that they used multiple vulnerabilities, semi-advanced and unique tools against different sectors and targets, they predominantly use ‘spear phishing’ methods with g(old) ideas in their cyber-espionage operations.

The Charming Kitten hackers use a combination of fictitious personas, impersonation and abuse of well-known people’s hacked online accounts in their sophisticated attacks and that is how some attempts are successful.

Additionally, as part of the social engineering scheme, they build trust with potential targets in the initial stage, and sometimes they try to have lengthy conversations with victims that can last for several days, and then trick them into clicking on malicious links at scheduled times. “Interview”, “Meeting”, “Discussion”, and “Cooperation” are the most common topics in their phishing scenarios.

Furthermore, it is evident that they are always active and by reviewing the activities of this group, we can say that they regularly have ongoing campaigns throughout the year.

Based on our recent investigation at Certfa Lab, the APT42 has been running multiple phishing campaigns since late 2021 and some of them are ongoing and still active. We believe, based on the details from the latest infrastructure indicators used by Charming Kitten, the similarities between these attacks and related techniques are still important knowledge for the public audience and potentially at-risk individuals. As a result, in the following report, we briefly described some examples of these attacks for public awareness.

## Operation Alfa: French National Center for Scientific Research

Samuel Valable is one of the researchers at the French National Center for Scientific Research (CNRS)[2] who is specialist in imaging and therapeutic strategies for cancers and brain tissues[3].

Our latest findings showed that the Charming Kitten hacking group impersonated him on social media platforms, by using his academic and professional background in CNRS, and created accounts under his name. The Iranian state-backed hackers created a fake LinkedIn account and then targeted researchers and academia in other countries to collect intelligence and hack their accounts.[4]

Figure 1. A screenshot of the fake LinkedIn profile of Sameul Valable, researcher at the CNRS, which was created by Charming Kitten

Figure 1. A screenshot of the fake LinkedIn profile of Sameul Valable, researcher at the CNRS, which was created by Charming Kitten

For example, in one of their operations, the hackers initiated a conversation with a professor at the one of the universities in the US, via a fake profile on LinkedIn, by impersonating Samuel Valable.

Figure 2. Parts of the conversation between the Charming Kitten group and the target via LinkedIn Messaging

Figure 2. Parts of the conversation between the Charming Kitten group and the target via LinkedIn Messaging

The novel and important part of this conversation on LinkedIn Messaging is all sent links by Charming Kitten were legitimate and real and they did not sent any phishing links or malicious files to the target. At the end of their conversation with the target, the hackers sent a link of a video call from Zoom to the target and asked the person to have a video call conversation with them.

Figure 3. The video call between the Charming Kitten and target on Zoom. The identity and voice of the target are redacted by Certfa Lab. Download

Figure 3 shows part of the audio/video conversation that Charming Kitten Hackers had with the target on a Zoom call. The attacker used frames of a fake video (from an unknown source) for webcam input on the Zoom call and explained a long story about the research background of Samuel Valable, and tried to engage with the target. After the hackers got the target’s interest, they shared a link (hxxps://view[.]googlebook[.]com[.]website-main[.]live/view?v=xxxxxx) with the target in the middle of the call and claimed this is the book they talked about. While the link was a fake login page for Google and in reality, if the target enters their username and password in the phishing form, the attacker would capture these details and get access to the target’s Google account.

The view[.]googlebook[.]com[.]website-main[.]live subdomain is hosted on Hetzner Cloud GmbH servers with 65.21.137[.]141 IP address, which was used for other phishing domains as well, such as mail-download-attachment[.]xyz and france24[.]live. Additionally, Attackers used this server to host the fake/clone website of the Islamic Republic of Iran’s Embassy in France, according to the historical records of RiskIQ[5].

Based on the previous operations of Charming Kitten and from our analysis, we believe this server (65.21.137[.]141) has been used by Charming Kitten to run cyber espionage operations against public figures, researchers, academians, organizations, and institutions that are linked to France. We are certain that Charming Kitten used this method to hack online accounts of a few researchers in the last year.

Although we cannot accurately calculate the total number of victims that Charming Kitten has targeted by using the fake profile of Samuel Valable, we believe the number to be high. There is also the chance that Charming Kitten has impersonated other members of CNRS.

## Operation Bravo: Middle East Institute

Paul Salem[6] is president of The Middle East Institute (MEI). This institution is working on providing non-partisan analysis and promoting greater understanding between the people of the US and the Middle East.

We have discovered that Charming Kitten has impersonated Paul Salem and contacted Iranian and non-Iranian activists who work on different topics in the Middle East. They invite individuals for collaboration and partnership in the area where the target is a well known expert.

According to analyzed samples, it appears the attackers targeted at least one LGBTQ+ activist and a media manager with the fake email addresses of paul_sallem@yahoo[.]com and paul_salem@outlook[.]com and impersonated Paul Salem.

Figure 4 shows the initial conversation of attackers with an individual and as it is clear that the hackers tried to build trust by impersonating Paul Salem and convincing the target to participate in a virtual meeting.

Figure 4. The initial conversation of Charming Kitten with the target while impersonating Paul Salem

Figure 4. The initial conversation of Charming Kitten with the target while impersonating Paul Salem

Same as Operation Alfa, after a series of conversations to build trust with the targets, in this campaign attackers use phishing links through a live-load[.]online domain and send it to the target to steal the victims' Google account credentials. It is noteworthy that in some cases, Charming Kitten does not send phishing links without proper planning; they calculate when the target is ready to enter credential details to login to an account. For example, they send phishing links during an online conversation, or after finishing the conversation.

At the time of writing this report, this domain is hosted on Hetzner Cloud GmbH servers; Apart from this domain, view-online[.]live, load-panel[.]online, and panel-archieve[.]live are hosted on the same server and they are affiliated with other Charming Kitten servers and domains.

According to Paul Salem's tweet on 5 March 2021[7] emails of scholars and experts at the MEI were targeted by the foreign-government-backed hackers and we believe these hackers are Charming Kitten.

## Operation Charlie: Atlantic Council

Hagar Hajjar Chemali is an American political commentator and one of the nonresident senior fellows at the Atlantic Council's GeoEconomics Center. She is an expert on sanctions, counter-terrorist financing policy, and the Middle East[8].

According to our findings, Charming Kitten impersonated Hagar Hajjar Chemali in at least two cases and contacted two different targets, where in one case the hackers managed to take control of the Twitter account of a minority rights activist. In these two cases, the Iranian state-backed hackers sent a fake online meeting link and then redirected the target to a phishing website.

The target groups for this impersonation operation were political, media, human rights defenders and women rights activists who are experts in the Middle East.

Figure 5 and 6 are samples of fake pages of legitimate services in this operation where Charming Kitten hosted them on the Google Site (sites.google.com) service, which they used in their previous campaigns[9] [10].

Figure 5. A fake page of Skype call on Google Site

Figure 5. A fake page of Skype call on Google Site

Figure 6. A fake page of Google Meet on Google Site

Figure 6. A fake page of Google Meet on Google Site

In this case, where one of the victims was a minority rights activist, the hackers used a short link such as hxxps://beasze[.]live/xyz in the fake pages on Google Site. This domain (beasze[.]live) was previously used in the TA453 (also known as Charming Kitten) PDF sample, which was mentioned in the Proofpoint report in July 2022[11].

Also, in another case related to this hacking campaign, Charming Kitten contacted journalists, human rights defenders and women rights activists inside and outside Iran through a fake Twitter account, Elina Noomen[12].

A Twitter page of Elina Noomen as an author and researcher, which was created by Charming Kitten

Figure 7. A Twitter page of Elina Noomen as an author and researcher, which was created by Charming Kitten

In at least one case, the hackers contacted a victim with this fake Twitter account and claimed they are working with Hagar Hajjar Chemali and would like to have an online meeting. The hackers used phishing links to steal email account credentials of the victim and they took control of the other online accounts of the victim.

After hijacking the victim's Twitter account, they used the account to start to contact other activists to collect specific information such as the names of Iranian women's rights activists living in Iran, Iraq and European countries who are seeking and eligible for financial support.

It is necessary to mention that this kind of data is significant for Iran's regime and in some cases can lead to the arrest and detention of activists on charges of cooperation with foreign countries.

Our investigation shows Hagar Hajjar Chemali is not the only member of the Atlantic Council who was impersonated by Iranian state-backed hackers and other members were impersonated in recent months. Also, it is important to mention that a part of this operation infrastructure has an overlap with the Meta report in Q1 2022[13] about the Iranian state-backed hacker's cyber operations, in which UNC788 (also known as Charming Kitten) hackers targeted people in the Middle East, including Saudi military, dissidents and human rights activists from Israel and Iran, politicians in the US, Iran-focused academics, activists and journalists around the world.

## Operation Delta: Further Cyber Ops

Hussein Ibish is the senior resident scholar at the Arab Gulf States Institute in Washington (AGSIW), who tweeted about an impersonation operation of him on 29 June 2022[14]. According to his tweet, hackers created an email address, hibish@husseinibish[.]org, and sent phishing emails to others to steal the credentials of multiple targets.

Later on the same day, Claudia Gazzini, who is a senior Libya analyst at the International Crisis Group (ICG), published a thread on Twitter[15] and said hackers contacted her via an email and set up an interview with her, and the hackers did a long interview with her. After the interview, the hackers sent a phishing link to Claudia Gazzini as a draft of the interview for her review. Figure 8 is the details of Claudia Gazzini explanations on Twitter.

##### Figure 8. The Twitter thread of Claudia Gazzini about the hacking operation against her

Figure 8. The Twitter thread of Claudia Gazzini about the hacking operation against her

Additionally, Dareen Khalifa, a senior Syria analyst at ICG, said her colleague and herself received an email from husseinibish8@gmail[.]com[16] and the attackers also contacted them via +1 (951) 638-0854[17].

It is noteworthy that these people are not the only individuals who are impersonated by hackers or targeted by sophisticated attacks. Various documents show many people and organizations have recently been attacked by Charming Kitten. Due to the similarity with other cyber espionage operations of Charming Kitten in terms of techniques and infrastructures, we can confirm that these attacks were carried out by Charming Kitten.

## Conclusion And Recommendations

Although the mentioned examples in these operations are a small pieces of Charming Kitten’s cyber espionage operation puzzle, we believe these snippets are crucial for the general public and at-risk individuals in order to create awareness and to encourage the public and at-risk individuals to act with caution when dealing with unsolicited communication online. We also believe this operation is still active on a large scale and this hacking group has sophisticated phishing attack methods such as impersonation to attack many other organizations and individuals.

According to our findings, Charming Kitten has increased its interest in cyber espionage against individuals who are experts in different areas in the Middle East and North Africa, particularly Iran and Syria.

We strongly recommend using secure multi-factor authentication such as two-factor authentication with security keys[18], for online accounts and also enable an Advanced Protection Program[19] for Google accounts.

Vetting the legitimacy of a request for an online meeting is vital as we have seen that sending an invitation to have a video/audio call has become a permanent method of the phishing operation of Charming Kitten to obtain credentials. One of the best ways to check the legitimacy of these invitations is to double-check them through another channel with the sender or ask a friend/colleague who might know the person and cross check the legitimacy of the meeting request.

> > Update (9.9.2022): Based on the latest report of Mandiant[20] about “APT42: Crooked Charms, Cons, and Compromises” and considering the overlap with APT42 operations, it is necessary to mention that for accurate attribution and classification of attackers’ origin in this report, APT35 has been replaced by APT42.

## IOCs

- paul_sallem@yahoo[.]com
- paul_salem@outlook[.]com
- samuelvalable@gmail[.]com
- husseinibish8@gmail[.]com
- hibish@husseinibish[.]org
- 41002e8ed24836d8a99157c12eba69271fae8511
- 65.21.137[.]137
- 65.21.137[.]139
- 65.21.137[.]141
- 85.10.193[.]10
- 88.80.148[.]161
- 88.80.148[.]162
- 88.80.148[.]188
- 88.80.148[.]189
- 144.76.115[.]26
- 144.76.115[.]28
- 144.76.115[.]29
- 144.76.115[.]59
- 168.119.47[.]242
- app-online[.]live
- icloud[.]app-online[.]live
- itunes[.]app-online[.]live
- basepage[.]xyz
- beape[.]live
- beasze[.]live
- login[.]beasze[.]live
- api[.]beasze[.]live
- beasze[.]online
- admin[.]beasze[.]online
- api[.]beasze[.]online
- remote[.]beasze[.]online
- test[.]beasze[.]online
- bnt2[.]live

- btoltf[.]store
- checkout-panel[.]live
- api[.]checkout-panel[.]live
- login[.]checkout-panel[.]live
- secure[.]checkout-panel[.]live
- staging[.]checkout-panel[.]live
- vpn[.]checkout-panel[.]live
- check-panel-account[.]icu
- download[.]check-panel-account[.]icu
- go[.]check-panel-account[.]icu
- webdav[.]check-panel-account[.]icu
- blog[.]check-reload-page[.]live
- check-reload-page[.]live
- confluence[.]check-reload-page[.]live
- cover-home-page[.]xyz
- cover-home-panel[.]xyz
- direct-view-panel[.]xyz
- france24[.]live
- free-guy[.]xyz
- front-cover-panel[.]xyz
- galil-merkazi[.]co
- home-check-direct[.]icu
- home-reload-page[.]xyz
- ict-amar[.]org
- join-room[.]online
- live-load[.]online
- load-online-app[.]live
- load-panel[.]online
- mail-download-attachment[.]xyz
- blog[.]mail-download-attachment[.]xyz
- maill-support[.]com
- mailupdate[.]info
- msnpayee[.]com
- msn-service[.]co
- msn-services[.]center
- nc5[.]live
- nco2[.]live
- online-dashboard[.]live
- online-live[.]top
- page-home-reload[.]xyz
- panel-archieve[.]live
- panel-check[.]online

- panel-review-check[.]live
- panel-review-home[.]xyz
- pingview-home-panel[.]icu
- dev[.]pingview-home-panel[.]icu
- mysql10[.]pingview-home-panel[.]icu
- service[.]pingview-home-panel[.]icu
- stage[.]pingview-home-panel[.]icu
- webdisk[.]pingview-home-panel[.]icu
- student-rank-number[.]icu
- view-check[.]online
- view-direct-panel[.]icu
- view-direct-panel[.]live
- view-home-panel[.]xyz
- api[.]view-home-panel[.]xyz
- blog[.]view-home-panel[.]xyz
- jenkins[.]view-home-panel[.]xyz
- view-online[.]live
- web-link[.]live
- website-main[.]live
- account[.]security[.]google[.]com[.]website-main[.]live
- view[.]googlebook[.]com[.]website-main[.]live
- watch-video[.]youtube[.]com[.]website-main[.]live

## Footnotes:

1. Mitre.org. “Magic Hound”. Accessed September 5, 2022. https://s.certfa.com/mG0059 ↩

2. CNRS.fr. “Samuel Valable, CNRS researcher”. Accessed September 1, 2022. https://s.certfa.com/cNrsFr ↩

3. Cyceron.fr. “A new article from the unit in collaboration with colleagues from the Burdenko Institute has just been published in Clinical Nuclear Medicine”. Accessed September 2, 2022. https://s.certfa.com/istctF ↩

4. LinkedIn.com. “Samuel Valable”. Accessed September 2022. hxxps://www.linkedin[.]com/in/samuel-valable-70b36b1a9/ ↩

5. RiskIQ.com. Accessed August 29, 2022. https://s.certfa.com/Rcs65t ↩

6. MEI.edu. “Paul Salem, President”. Accessed September 4, 2022. https://s.certfa.com/MeiEdu ↩
7. Twitter.com. Accessed August 30, 2022. https://s.certfa.com/pStc61 ↩
8. AtlanticCouncil.org. “Hagar Hajjar Chemali”. Accessed September 1, 2022. https://s.certfa.com/aCEhhc ↩
9. Certfa.com. “Fake Interview: The New Activity of Charming Kitten”. https://s.certfa.com/bCfick ↩
10. Certfa.com. “Charming Kitten’s Christmas Gift”. https://s.certfa.com/ckCGcb ↩
11. Proofpoint.com. “Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media”. Accessed September 1, 2022. https://s.certfa.com/PpAfiT ↩
12. User id 1504372203969814530 ↩
13. FB.com. “Adversarial Threat Reports”. Accessed September 3, 2022. https://s.certfa.com/MQatrq ↩
14. Twitter.com. Accessed September 1, 2022. https://s.certfa.com/tIs618 ↩
15. Twitter.com. Accessed September 1, 2022. https://s.certfa.com/cG1077 ↩
16. Twitter.com. Accessed September 1, 2022. https://s.certfa.com/dK2150 ↩
17. Twitter.com. Accessed September 1, 2022. https://s.certfa.com/dK0426 ↩
18. Yubico.com. Accessed September 5, 2022. https://s.certfa.com/y22Co0 ↩
19. Google Advanced Protection Programme. Accessed September 5, 2022. https://s.certfa.com/lGapro ↩
20. Mandiant.com. “APT42: Crooked Charms, Cons, and Compromises”, Accessed September 9, 2022. https://s.certfa.com/cHcC42 ↩