


CYBER
THREAT
ANALYSIS

IRAN

Recorded Future®

By Insikt Group®

March 30, 2022

A man with a beard, wearing a light-colored shirt, is shown emerging from a large, dark smartphone screen. His right arm is raised, and a stream of digital particles or data points is trailing behind his hand as it moves upwards. The background is a green-tinted image of a circuit board or technical drawing, with various lines, circles, and text visible. The overall theme is digital technology and cybersecurity.

Social Engineering Remains Key Tradecraft for Iranian APTs

This report covers Iranian social engineering cases and methodologies. It serves those looking to better understand, prepare for, and preempt an attack by Iranian operators against their personnel and organization and benefits Iran-focused analysts researching topics associated with Iranian social engineering to understand their typical targets, organizations, and objectives. Sources include the Recorded Future® Platform and industry reporting from Microsoft, Proofpoint, ClearSky, FireEye, Mandiant, and CitizenLab, among other open sources.

Executive Summary

Since 2010, pro-Iranian government cyber intrusions have relied on social engineering as a component of the cyberattack life cycle, whether executed through spearphishing attacks or more directly through one-to-one engagements. Iranian operators have targeted members of foreign governments, militaries, businesses, and political dissidents. Their operations appear to use many of the studied “principles of influence” and overlap with human intelligence (HUMINT) recruitment practices, both of which influence social engineering methodologies.

Research on the Iranian government’s strategic and tactical approaches to the offensive and defensive “Soft War” also suggests that social engineering is an indispensable element of the government’s cyber capabilities, which it has relied on for at least a decade. Tehran views the ability for a foreign power to incite domestic upheaval as being as dangerous as a military attack on its territory. Equally so, the ability to foment social unrest internationally is a capability at its disposal to attack its perceived enemies. Understanding and dissecting foreign societies, languages, cultures, and political systems has enabled Tehran to leverage social engineering in ways comparable to Russian threat activity groups.

Large-scale social engineering campaigns have predominantly been executed by APT35, Tortoiseshell, and APT34, and their associated sub-groups. While their operations do not diminish those run by other advanced persistent threat groups (APTs), these 3 Iran-nexus groups have depicted substantial tradecraft overlaps in how they target their victims. These include the use of charismatic sock puppets, the lure of prospective job opportunities, solicitation by journalists, and masquerading as think tank experts seeking opinions. These are just some of the personas which these 3 Iranian APTs have continued to use since the first major disclosure on Iranian social engineering — Operation Newscaster — was publicly reported in 2014.

Key Judgments

- The use of social engineering is a central component of Iranian APT tradecraft when engaging in cyber espionage and information operations. Iranian APTs will continue to modify their tradecraft, including phishing, spoofing, smishing, and other techniques to target their victims.
- Multiple Iranian threat activity groups use social engineering. APT35, APT34, and Tortoiseshell remain among the earliest and most aggressive adopters of social engineering to aid their intrusion or credential theft operations. We expect these groups to continue to lead attacks using social engineering techniques in the future.
- Patterns in Iranian social engineering attacks suggest they aim to drive targets to multiple platforms; this increases the attack surface by incorporating email, social media, and chat messengers as attack vectors. Malicious documents and applications will continue to be disseminated via one-to-one sock puppet engagements with their targets.
- Various reported Iranian social engineering attacks share approaches, including recruitment offers, offers to solicit targets for journalistic purposes or political analysis, romantic engagements, and supposed anti-government activism.
- The use of foreign languages and knowledge of foreign societies and cultures will continue to play a central role in targeted social engineering attacks. Iranian APTs are improving their command of major languages such as English and major European, Middle Eastern, and South Asian languages.

Background

The growth of Iranian social engineering can be traced to Iranian hacker forums, with many including sub-threads on the techniques necessary to target unsuspecting victims. Some of the earliest examples include the “Simorgh Security Team”, among the first to differentiate social engineering from other hacking disciplines.¹ Members of that group claimed that a social engineer must be persuasive, articulate, and possess strong analytical and intelligence gathering skills.

Social engineering, a component of Iran’s defensive and offensive cyber capabilities embedded in pro-government Iranian cyber doctrine, can be traced to institutionalized ideologies such as the “[Soft War](#)” (جنگ نرم). The concept of Soft War was [established](#) as far back as 2010 and aims to counter subversion, or political, religious, economic, and cultural ideals that may lead to the destabilization and fall of the Islamic Republic. These goals are likely achieved by networks of trusted experts rooted deeply in Iran’s military and intelligence organizations.

For example, the commander of the Islamic Revolutionary Guard Corps (IRGC) in Kerman province (Sarullah Corps) recognized the role of repatriating Iranian “elites” in countering enemy influence and disinformation campaigns,² declaring them key in the struggle against “the disproportionate soft war and psychological operations [PSYOPS] of the enemy”. In this context, elites refer to highly educated Iranians close to the regime who have been directed to seek education and employment opportunities abroad.

The IRGC and its auxiliary force the Basij, as well as the Ministry of Intelligence and Security (MOIS), have cemented their role in the field to counter the Soft War since 2010; they have established multiple operational bases that, at least in name, are dedicated to the Soft War, such as the Baqiatallah al-Azam Social and Cultural Base (قرارگاه بقیة الله الاعظم). The Baqiatallah base is currently headed by the former commander of the IRGC, General Mohammad Ali Jafari, who on this matter claimed in November 2021 that the Islamic Republic’s enemies aimed to destroy it and that “soft, cultural, and media wars” were harder to combat than a kinetic war.³

Open source [analysis](#) has referred to Tehran’s strategic threat perceptions within this space. As early as 2010, Iran viewed social media platforms as “elements of a cyber warfare threat ... particularly in the way rumors are spread online to ‘stir up’ discord within Iran”, following its own threats to the [establishment](#) that arose from the 2009 Green Movement. Iran has proven to strategically leverage the same threat calculus, along with the other Big Four (Russia, China, and to a lesser extent North Korea) adversarial nations, against its adversaries, including the US government.

Operationally, Iranian social engineering depicts a strong emphasis on the use of foreign languages and cultures to execute defensive and offensive campaigns against domestic foes, such as anti-revolutionary fronts like the Mojahedeen Khalq Organization (MEK) and the National Council of Resistance of Iran (NCRI), and nations which Iran perceives to be its adversaries: the US, the UK, Israel, and Saudi Arabia. Pro-government operators understand adversarial societies and cultures well enough to mimic them; this capability manifests, whether successful or not, in information operations, psyops, and cyber intrusions.

Threat Analysis

The cases below outline several successful and unsuccessful social engineering attacks by Iranian operatives. Some cases are associated with cyber intrusion or credential phishing operations, others with influence and psychological operations. Most cases were reported by cyber research groups such as ClearSky, CitizenLab, and Proofpoint. In some cases, anti-government reporting provided additional examples of social engineering tradecraft.

The reporting is also marked by the different naming conventions (cryptonyms) associated with Iranian APT groups. These predominantly involve APT35, Tortoiseshell, and APT34, which are tracked by multiple industry vendors with different cryptonyms. These APTs also have their own subgroups, such as UNC788 and LYCEUM, which at times complicates attribution analysis attempts. To simplify associations, we have included a deconfliction table below.

As part of this research, we selected these 3 Iranian APT groups due to various social engineering cases that have been publicly reported and their ability to provide insight on attack tradecraft.

1 [http://www.webhostingtalk\[.\]ir/showthread.php?t=65453](http://www.webhostingtalk[.]ir/showthread.php?t=65453)

2 [https://www.tasnimnews\[.\]com/fa/news/1400/08/27/2610378/](https://www.tasnimnews[.]com/fa/news/1400/08/27/2610378/)

3 [https://www.isna\[.\]ir/news/1400081108669](https://www.isna[.]ir/news/1400081108669)

APT	Industry Names
APT35 (FireEye)	Charming Kitten (CrowdStrike), Phosphorus (Microsoft), TA453 (Proofpoint), UNC788 (Mandiant/FireEye), ITG18 (IBM X-Force)
Tortoiseshell (Symantec)	Imperial Kitten (CrowdStrike), TA456 (Proofpoint), Curium (Microsoft)
APT34 (FireEye)	Helix Kitten (CrowdStrike), Cobalt Gypsy (Secureworks), OilRig (PaloAlto), LYCEUM (Secureworks)

Table 1: APT cryptonym deconfliction table (Source: Recorded Future)

The Approach

Extensive studies discuss social engineering tradecraft (that is, persuasion principles) and its effects on [human psychology](#). The principles considered to be key drivers are “authority”, “conformity”, “reciprocity”, “commitment”, “scarcity”, and “liking” (flattery). Applications from such studies are readily visible in the Iranian social engineering approach. For example, in the [study](#), commitment is defined as the “likelihood of sticking to a cause or idea after making a promise or adhesion ... which increases the likelihood of compliance”. The process of liking “puts that person in a favourable position” where “People tend to like others who are similar in terms of interests, attitudes, and beliefs”, while with reciprocity “the target feels indebted to the requester for making a gesture and even the smallest gift puts the requester in an advantageous position”.

Iranian methodologies apply many of these techniques to their attacks; some commence with a sense of authority and infuse reciprocity, while others use flattery to hook the target before escalating to a commitment phase. Notably, the process of commitment is observed among all of the threat actor interactions with victims discussed in this report, with benign documents being shared to establish trust and initiate the psychological mechanism of compliance with an attacker’s request. Flattery, or the prospect of being courted by a charismatic persona or high-profile recruiter, is another common tactic, technique, and procedure (TTP) used by various Iranian APTs.

APT	Common Techniques				
APT35	Soliciting Opinions (Journalistic or Other)	Enlist Immediate Action/ Google Recovery	Romantic Engagement	Greetings/ Seemingly Benign Engagements	Engaging Professional Counterpart
Tortoiseshell	Romantic Engagement	Professional Opportunity			
APT34	Romantic Engagement	Professional Opportunity	Online Survey		
Unattributed activity	Elicit Assistance	Engaging as a Dissident	Professional Opportunity	Engaging as a Political Activist	

Table 2: Major characteristics of Iranian social engineering tradecraft (Source: Recorded Future)

In lesser cases, challenging conventional thought or making provocative and factually inaccurate statements is a reverse psychology trick to draw in and engage a target. For example, Iranian APTs may impersonate a news reporter or claim to be an expert from a reputable think tank. Under this guise, they may state something a target is likely to hold an opposing analytical view on in the hope of eliciting a response from the target. As [described](#) by one reputed Iran analyst, this tactic was used in an attack which eventually aimed to have the target to proceed to a fake login portal where their credentials would be stolen:

The email from a prominent Israeli think tank offered some provocative suggestions on US policy towards China. “We must understand that China is at war with the United States”, it declared, citing the [covid-19 pandemic](#) as evidence. Its authors recommended that the Trump administration set up a team of “top China experts” such as Stephen K. Bannon and former House speaker Newt Gingrich to confront “Red China” in the wake of the coronavirus crisis.

When the target did not reply, the attackers chose to escalate, first, by sending a new email depicting spoofed correspondence in Hebrew from an analyst the target held a professional working relationship with. When the target again did not respond, the attackers sent a new email impersonating “a president of a prominent Washington think tank offering his critiques of the paper”.

Persona	Purported Profession	Known Platforms	Known Connections
Sandra Maler	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	226
Adia Mitchell	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Wordpress	281
Amanda Teyson	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	310
Sara McKibben	Reporter, NewsOnAir	LinkedIn, Facebook	Unknown
Joseph Nilsson	Founder, NewsOnAir	LinkedIn, Facebook	231
Jane Baker (Ava T. Foster)	Reporter, NewsOnAir	LinkedIn	30
Mary Cole	Recruiter for Defense Contractor	LinkedIn, Facebook, Google	500+
Berna Achando	Web Designer for Defense Contractor	LinkedIn, Facebook	151
Jeann Macclin	Systems Administrator for US Navy	LinkedIn, Facebook, Blogger, YouTube	500+
Alfred Nilsson	Talent Acquisition for Defense Contractor	LinkedIn, Facebook	Unknown
Josh Nilsson (Josh Furie)	IT Manager for Defense Contractor	LinkedIn, Facebook	130
Dorothea Baasch	IT Analyst for Defense Contractor	LinkedIn, Facebook	Unknown
Kenneth Babcock	CPA and Tax Advisor for Payment Processor	LinkedIn, Facebook, Google	Unknown
Donnie Eadense	Information Systems Manager for Defense Contractor	LinkedIn	118

Figure 1: Operation Newscaster fake personas and their social media presence (Source: [iSight](#))

The examples listed in this report also correlate to some publicized HUMINT principles and agent recruitment techniques. Following the MICE or RASCLS [frameworks](#), the use of financial rewards, or surreptitiously stimulating the target's ego, have proven to be traits that many Iranian social engineering attacks have adopted. The comparative study also suggests that target manipulation reportedly depends on the "principles of influence and persuasion and they [recruitment case officers] have learned how to manipulate without appearing to be manipulative". A direct example of this is the case of Mona Rahman from the Endless Mayfly campaign, where the operators attempted to piggyback on negative Saudi sentiment to recruit a social media audience to a physical protest.

Social Engineering Components

While Iranian social engineering attacks vary between groups, and many use open source or bespoke malware, some observable traits remain constant. The characteristics of Iranian operations focus on the theft of credentials, delivery of malicious programs, or delivery of fake information as part of broader influence operations.

Phishing for Credential Theft

Credential theft is among the most prevalent and consistent elements of Iranian social engineering operations. For example, the operators associated with Charming Kitten develop extensive infrastructure networks to enable authentication-themed credential theft activity. These domains mimic popular services such as Google, Hotmail, and Yahoo, as well as countless spoofed login portals associated with information technology (IT) and high-tech groups, telecommunications providers and internet service providers (ISPs), private business, and public offices associated with multiple governments.

The authentication-themed domains discovered by Insikt Group replicate much of the known tradecraft used by Charming Kitten throughout 2021. Similar to the previous examples, the operators predominantly register domains using the .site, .online, .top, .mobi, .network, and .info Top Level Domains (TLDs). The domains investigated are predominantly registered using the OnlineNIC or Namecheap service. Furthermore, in continuation with its known TTPs, Insikt Group research revealed a continued reliance on OVH and Hetzner GmbH hosting providers.

Strategic Web Compromise

In 2021, at least one Iranian social engineering campaign was marked by strategic web compromise (SWC) activity to lead intrusion operations against their victims. The group responsible (see the TA453 campaign below) compromised a legitimate website to steal credentials from targets.

Malicious Applications

Malicious applications form a component of the social engineering threat. Industry research has [reported](#) throughout 2021 that a malicious application they dubbed LittleLooter was used for attack operations. Another sample was detected and [reported](#) by Google's Threat Analysis Group in October 2021. The applications are used to target victims from various sectors inside and outside Iran. These applications are delivered to victims via social engineering attacks, sometimes involving the operators directly engaging with victims.

Malicious Documents

Almost every major social engineering campaign in this report suggests that highly targeted operations revolve around disseminating malicious documents to enable intrusions. The threat actors have used both open source and bespoke malware, such as PupyRAT and LEMPO (LIDERC), respectively, to launch attacks.

Fake News Outlets and Journalists

Since the discovery of the [Newscaster](#) network, Iranian social engineering activities have revolved around the use of journalistic personas, malicious fake news websites (see APT35 below), or the dissemination of disinformation to trick or manipulate targets (see Influence Operations below). As noted in this report, Iranian operators have been identified on various occasions assuming the personas of journalists or activists when conducting intrusion or influence operations against targets. Iranian influence operations have similarly been tracked and disrupted by [industry](#) researchers, [social media](#) organizations, and the [US government](#).

Charismatic Personas

The use of charismatic personas has been a formative characteristic of Iranian social engineering campaigns. Almost every case discussed in this report refers to at least one fabricated profile used to target unsuspecting victims. In some cases, the profiles were so successful (see Mia Ash) that a victim, potentially acting under the false illusion of a romantic engagement, provided their personal details to register domains used by the threat actor.

Social Engineering Campaigns

Phosphorus

On November 16, 2021, Microsoft's Threat Intelligence Center (MSTIC) [outlined](#) its observations of Iranian threat actor activity without giving specific operational examples. Prime among the groups MSTIC observed were Phosphorus and Curium. MSTIC reported that Phosphorus was increasingly devoting more time to engage with its victims by sending benign questions and engaging in several "back-and-forth conversations" before sending an "interview request" with links masquerading as Google Meeting invites. Insikt Group has identified similar examples that focused on the use of the IMO chat service (Figure 3).

MSTIC analysis revealed that Phosphorus operators have become more aggressive with their targets, "almost demanding a response". On November 20 and 24, 2021, threat actors impersonated a well-known New York Times Bureau Chief Thomas Erdbrink, who has covered Iran, in an attempt to target a dissident activist, Mahsa Alimardani (Figure 3). While the MSTIC disclosure is not likely related to the Erdbrink impersonation attempt, it highlights the group's ongoing attempts to target its victims notwithstanding public disclosures against it. Additionally, impersonating journalists is a well-reported tactic used by the operators associated with the Iran-nexus group (additional evidence in Appendix).

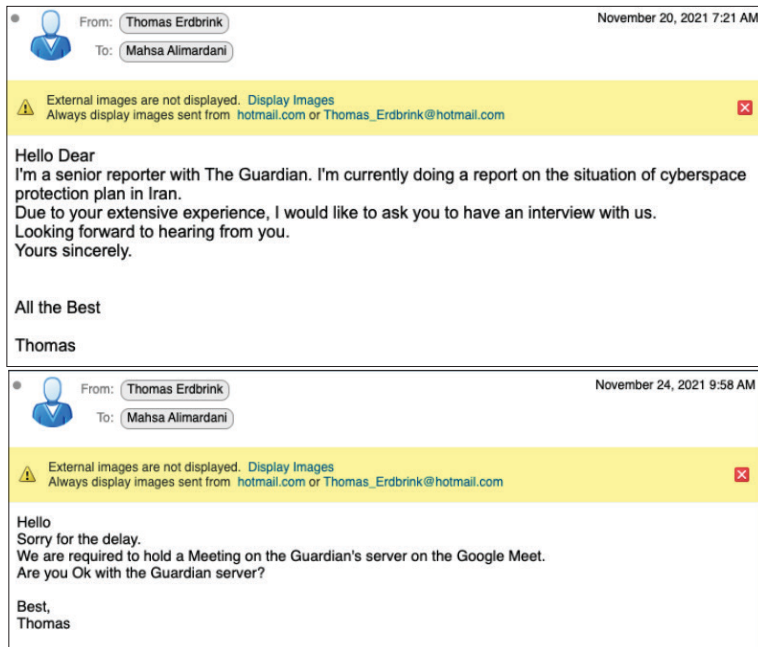


Figure 2: Typical social-engineering example of an email-led interview request (Source: social media)

A day after the MSTIC disclosure, the advocacy group United Against Nuclear Iran (UANI) [claimed](#) cyber operators associated with the Iran-nexus group targeted its organization. It specifically claimed that “its leadership and members of its Advisory Board” were targeted by the group by procuring “data outside of the public realm, [and] impersonated our leadership in communications with former senior officials of the US government, and attempted to harvest Gmail credentials”. The impersonation of stakeholders is, as noted throughout many of the cases associated with the APT, a predominant characteristic of the APT group.

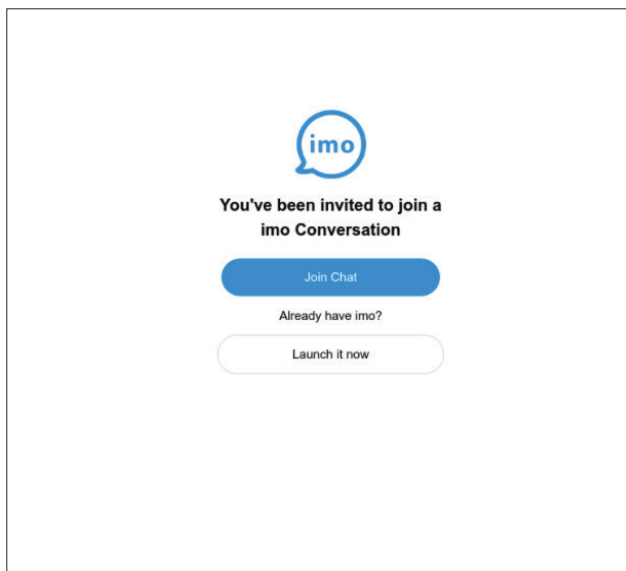


Figure 3: URLScan of a suspected Charming Kitten-linked domain identified by Insikt Group led to a

login page for IMO chat video (Source: [URLScan](#))

According to MSTIC, Curium, which highly likely overlaps with Tortoiseshell, uses more long-term tradecraft. Curium engages via social media or professional networking accounts, and will exchange multiple benign files with the victim prior to sending a malicious document. The act of exchanging files and visual content is, according to MSTIC, a process of lowering the victim's guard. Additional information and a well-known case are cited in the coverage of TA456 below. Again, throughout many of the reported social engineering examples, Iranian operators regularly interact with their victims. For strategic, long-term targets, groups like Curium and APT34 have proven to attempt to establish trust and multiple attack vectors to ensure access to their victim.

TA453

The threat actor tracked by Proofpoint, which it classifies as TA453, was highly active throughout 2020 and 2021. The group released 2 reports on their attempts to social engineer research professionals in the US, UK, and Israel during the reporting time frame. Between December 2020 and March 2021, the group was detected launching spearphishing attacks against senior US and Israeli researchers associated with the medical sciences sector in a campaign dubbed BadBlood. More specifically, the victims of the campaign worked in genetic, neurological, and oncological research. No live engagements with victims were reported; however, Proofpoint evidence suggests the operators spoofed the persona of an Israeli physicist and used that as a front to target at least 25 other senior researchers in the US and Israel.

The lure used — a report on Israel's nuclear capabilities — was benign and unrelated to the medical sciences sector. Proofpoint claimed the operators used known spearphishing techniques, such as sending emails with the purported assessment on Israel's nuclear capabilities attached to them, to steal the victim's email credentials. It is unknown what follow-on activity transpired after successful credential theft or whether the end goal was to penetrate the medical sector or use their access to victim accounts to target other members of their networks beyond medical research.

TA453 was detected again targeting senior researchers throughout 2021 in an operation dubbed SpoofedScholars. As part of this campaign, the threat actors masqueraded as scholars from the University of London's School of Oriental and African Studies (SOAS). The fake personas targeted experts in foreign policy, journalism, and academia that focused on Middle East politics. The effort was reported as an attempt to garner strategic insight on the possible effects of future relations vis-a-vis Tehran. This effort by TA453 operatives revealed that it was driven to establish extensive relations with targets, communicate with them, and then drive them to a conference registration link hosted on a compromised website. The compromised website belonged to SOAS Radio, which likely contributed to appearing as a legitimate action.

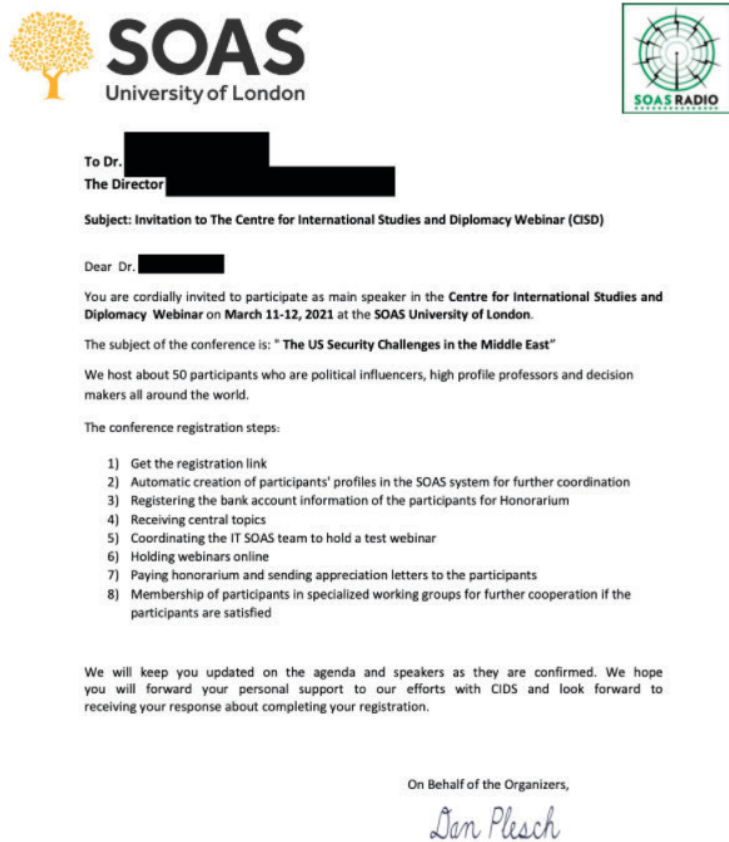


Figure 4: A fake invite sent to a victim of Operation SpoofedScholars (Source: [Proofpoint](#))

TA456

In late July 2021, Proofpoint disclosed a campaign on TA456 called "[I Knew You Were Trouble](#)". The campaign reported by Proofpoint also overlapped with [Facebook's](#) own action, reported in mid-July 2021, against this threat actor group. The social engineering component is reported to have involved the creation of a fictitious social media persona, "Marcella (Marcy)

Flores". The targets were US defense contractors operating in the Middle East and subcontractors associated with larger defense companies. Facebook's report highlighted the nature of the likely connected broader campaign, which involved different accounts posing as "recruiters and employees of defense and aerospace companies from the countries their targets were in...Other personas claimed to work in hospitality, medicine, journalism, NGOs and airlines".

The persona is categorized as a traditional "honey trap" operation, where charisma and an attractive image are used to entice unsuspecting targets. It is [reported](#) that honey traps are a TTP historically used by Iranian threat actor groups to target enterprises.

Honey traps are a historically common TTP used by Iranian threat actor groups to target [enterprises](#).

The fake profile identified by Proofpoint is likely to have been active for at least 2 years, established in late May 2018. At least 1 victim of the "Marcy" honey trap had been in direct communication with the fake profile since November 2020; however, they officially became Facebook "friends" in 2019, which reveals the methodical and long-term strategic approach TA456 operators adopted to engage with high-value targets.

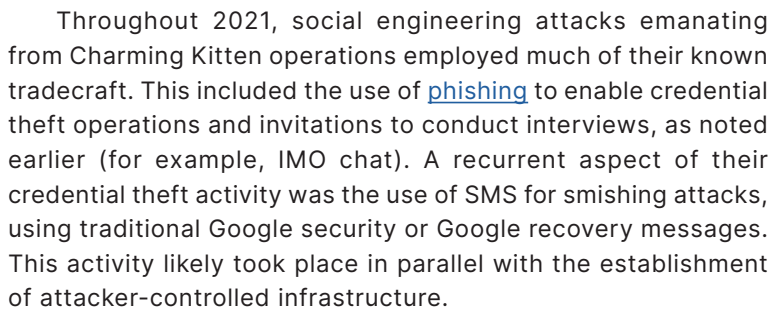


Marcella Flores

Cuando suena la melodía, los pasos se mueven, el corazón canta y el espíritu comienza a bailar

Figure 5: The fake profile used to target US defense contractors (Source: [Proofpoint](#))

Marcy eventually also used a fake Gmail account associated with the front to deliver malware, known as LEMPO (LIDERC). According to the research, private and corporate accounts were affected by TA456's operation.



In 2020, ClearSky Security released its third edition of “[The Kittens Are Back in Town](#)”, a report detailing persistent attempts by Charming Kitten operators to engage directly with victims. The objective of the engagement was to drive victims to encrypted chat platforms, such as WhatsApp, and onward to join fake video conferences where, presumably, the victims would fall further down the chain of compromise. All of the detected cases began with spearphishing emails; the attackers developed fake personas that spoofed real journalists and fake email accounts to enable the ruse. The group has [spoofed](#) major news entities, including the New York Times, the Wall Street Journal, CNN, and Deutsche Welle.

Figure 6: Example of email used to deliver malware to the victim (Source: [Proofpoint](#))

Charming Kitten is one of the most widely reported Iranian threat activity groups with a strong focus on social engineering to target its victims. Above we covered its overlapping campaign tracked as TA453, while below we highlight the activities tied to the group from other vendors.



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. *****	Attacker
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.	
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

Figure 8: The attackers brazenly attempt a call as part of their first interaction with the victim (Source: [ClearSky](#))

Figures 9 and 10 depict a conversation between the attackers **APT35** and a victim, revealing persistent attempts to engage, even when victims did not respond to the attackers' lure.

Beyond persistence and a sense of authority ("I am Yalda ... from Deutsche Welle") the attackers employed other techniques to strengthen their relationship with victims. This included flattery ("we invited you as a special speaker"), and a form of reciprocity (the sign-up walkthrough) which potentially made the target feel indebted to the attacker for "assistance" offered. As noted in the Mitigation section, multiple social engineering techniques depend on human psychology to aid the attacker through their plot.

In February 2019, the US Department of Justice (DoJ) unsealed an [indictment](#) against a former US Air Force Intelligence Officer, Monica Elfriede Witt, and APT35. Witt, after defecting to Iran, cooperated with its intelligence and cyber operatives to supply classified and compromising information against US intelligence agents. Four years before the indictment, members of APT35 established a fake Facebook profile under the name "Bella Wood" to enable the operation. The operators used the Facebook account to send a friend request to a US intelligence officer deployed to Afghanistan for a US Central Command (CENTCOM) joint intelligence unit. APT35 operators also used an email, bella.wood87@yahoo[.]com, to contact the same intelligence officer. The following is an account of their engagements:

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. ***** 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	Attacker
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

Figure 9: The correspondence shows the attacker's persistence toward the victim (Source: [ClearSky](#))

Hello my dear ... invitation card sent to you by email I got this pretty card accept me as a kind friend.

I'll send you a file including my photos but u should deactivate your anti virus to open it because i designed my photos with a photo album software, I hope you enjoy the photos i designed for the new year, they should be opened in your computer honey.

APT35 continued to execute social engineering attacks as part of the same operation against US intelligence officers. Presumably due to the information they had collected as part of their cooperation with Witt, they created a fake Facebook profile that impersonated another US intelligence officer. According to the indictment, the attackers also used information and pictures from the officer's real account to enable their operation. The Iran-nexus group continued their activities, using the fake profile to engage with another 2 US intelligence officers, including attempts to disseminate malware via Facebook and penetrating a closed Facebook group of other US intelligence officers. APT35 operatives also led a watering-hole attack against US officers using a fake news website and devised spoofed domains used to launch credential theft spearphishing attacks.

APT34/COBALT GYPSY

Hard Pass and Rebecca Watts

The Hard Pass campaign was [reported](#) by FireEye in July 2019 and captured Iran-nexus operatives highly likely associated with APT34 that impersonated a member of Cambridge University called "Rebecca Watts". The operators behind Watts developed and used a LinkedIn profile to engage professionals in the utilities, government, and oil and gas sectors.

The operators used the profile first to seek candidate resumes and then used the established trust to send back an Excel spreadsheet with an embedded exploit. Notably, the language used by the operators also claimed that Watts was rushed when sending the request to access the spreadsheet, which could excuse the allegedly native English speaker from making grammatical errors. Under normal circumstances, such grammatical errors as shown in Figure 11 may raise suspicion from a native English speaker. The group used the image of Cambridge University with a top-level domain that mimicked the institution's domain-naming convention. With little to no knowledge of the institution's real domain structure, an unsuspecting victim would not have easily identified the ruse.

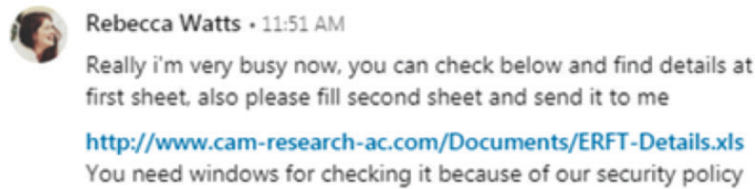


Figure 10: The "Hard Pass" campaign revolved around the use of a fake recruiter profile (Source: FireEye)

The use of LinkedIn mimics APT34's use of social media to deliver malicious documents to unsuspecting victims and is likely part of the group's attempts to evade security technologies to block malicious email traffic.

"Mia Ash"

In July 2017, SecureWorks [reported](#) one of the first known public cases of a long-term social engineering operation associated with APT34/Cobalt Gypsy. The case focused on the use of a traditional honey trap sock puppet to deceive an employee of a targeted company. Mia Ash reportedly contacted the target via LinkedIn, claiming she was "part of an exercise to reach out to people around the world". The operators behind Ash used the receptiveness of the victim to establish a virtual relationship, exchanging professional and personal information, a technique also used at great lengths in the Marcy Flores campaign outlined previously. The relationship spread to social media through a "friendship" on Facebook but also continued via email and via WhatsApp. Two months after the initial exchange, a PupyRAT-laden Excel document was sent to the personal email of the victim.

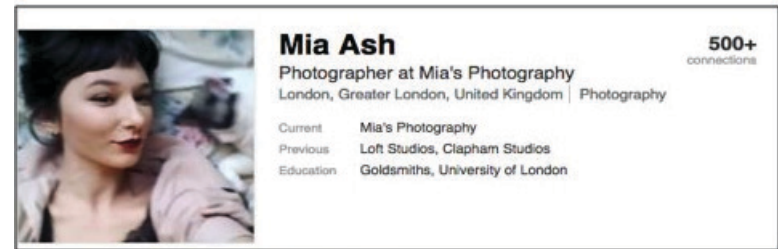


Figure 11: A captured screenshot of the fake LinkedIn profile of Mia Ash (Source: Secureworks)

According to Secureworks, "Victim A", a target of the Mia Ash campaign with approximately 10 years of experience in the oil and gas, aviation, and telecommunications sectors, possibly shared his personal information to register domains for the attackers. Secureworks provided the following hypotheses to explain the act:

- Victim A registered a domain for Mia Ash, and the threat actor reciprocated by registering a domain for Victim A to keep Victim A as an active, unknown participant in the threat actor's operations.
- The threat actor compromised Victim A's accounts.
- Victim A registered both domains as a romantic or friendly gesture.
- Domains were registered using fraudulent information.
- Victim A works for the threat actor.

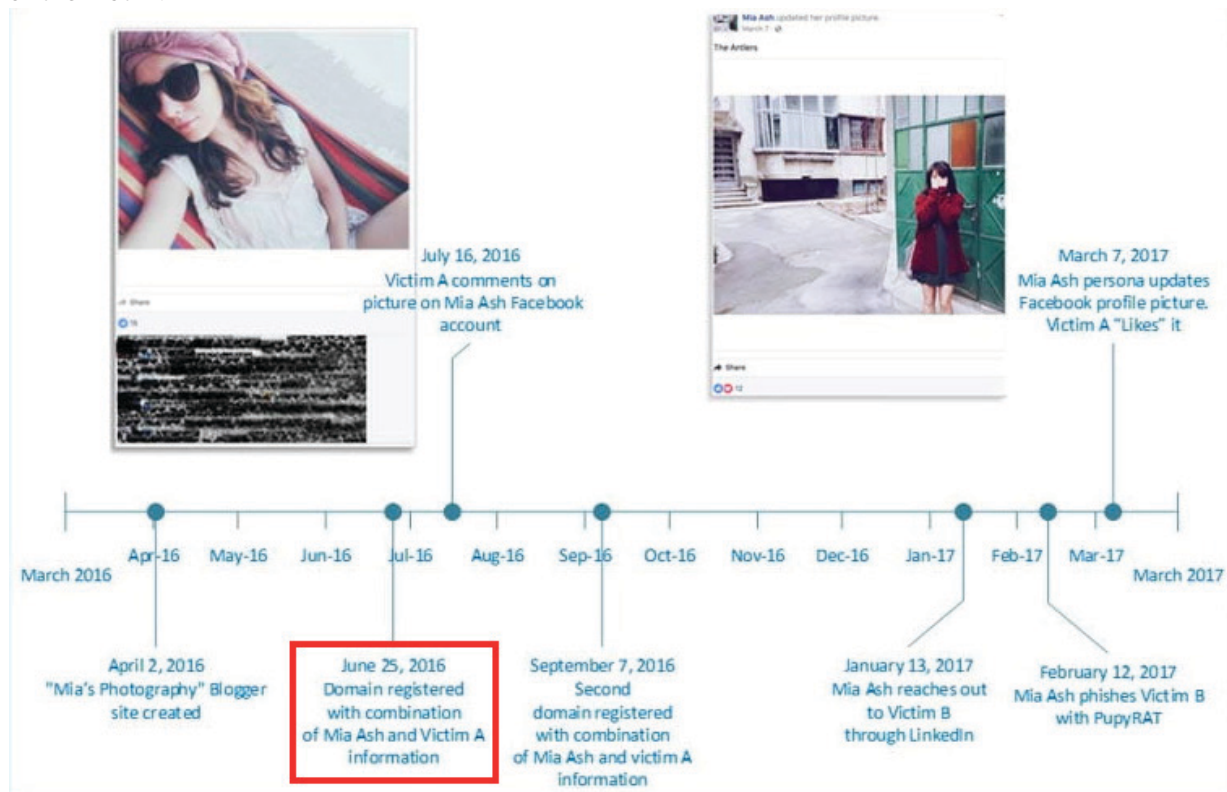


Figure 12: A timeline for the Mia Ash operation (Source: Secureworks)

Social Engineering and Dissidents

Targeting Dissidents and the Diaspora

The Islamic Republic of Iran uses social engineering to target entities and individuals they perceive to be threats or enemies of the state. In some instances, their operations have proven to be successful, brazen, and apparently meticulously planned. Some reported cases involve targeting dissidents living in the United States, with plans of extracting them to Iran to face prosecution by the Islamic Republic, as noted most recently in a July 2021 [unsealed indictment](#) by the US Department of Justice. The case details revealed Iranian intelligence services established a ruse that concealed their motives and hired a private intelligence group in North America to conduct surveillance against a journalist, human rights activist, and author living in Brooklyn, New York. The case revealed that MOIS agents, or individuals associated with the organization, claimed to represent a private party in Dubai and that the targets of the intelligence operations had stolen or owed money to the client in the UAE. As part of the plot, MOIS agents provided contact information, including a telephone number with a UAE country code, to convince the private investigator that the request was coming from the UAE. The following is an excerpt from the indictment, which cites the statement from the attackers:

I am contacting you on behalf of a client looking [for] a missing person from Dubai, UAE who has fled to avoid debt repayment. We require your services to conduct a surveillance on potential address of missing person... Will need high quality pictures/video of persons living in the address and cars they drive.

Other major cases involve using the profile of [journalists](#) to target diaspora Iranians involved in various sectors, or to target dissident activists, such as Ruhollah Zam. Zam, the former leader of the dissident news group AmadNews, was tricked into leaving France, where he had asylum, in October 2019 to travel to [Iraq](#). Reportedly, the IRGC's Intelligence Organization (IRGC-IO) took responsibility for the operation. Open source reporting [suggests](#) he was duped into believing he was to interview Iraq's most senior Shia leader, Ayatollah Ali Sistani. Supposedly, the interview was a prelude to the establishment of a new television channel sponsored by an "individual claiming to be an Iranian businessman". Upon his arrival, he was captured by pro-regime elements that transferred him to Iranian custody. Zam was [executed](#) by the Islamic Republic in December 2020.

The lesser-known case of Asal Kaviani (عسل کاویانی), reported by a Persian-language anti-government source, also reveals the Iranian system's ability to set up ruses against its targets. According to the dissident report, Kaviani contacted the anti-government source, revealing she was the sister of an IRGC cyber engineer. In exchange for a government-issued laptop presumably full of information regarding the IRGC's cyber programs, Kaviani wanted the source to help her brother escape from the organization.



Figure 13: Iranian dissident report highlights social engineering attack by Iranian government. For a full translation, see Appendix (Source: Iranian dissident reporting)

The dissident organization claimed that while highly suspicious of Kaviani, they entertained the approach for 3 months to gather more information. Kaviani proposed a physical exchange with the dissident organization to provide the laptop as proof; the encounter was supposed to take place at a well-known metro stop in Tehran. The dissident organization claimed that the exchange was aborted due to an increased chance that the meeting was in fact a counterintelligence sting operation. No additional information was supplied to verify the attempt, except for screenshots of emails allegedly written by Kaviani (Figure 14).

If in fact a targeted operation, the incident reveals the group was acutely aware of the dissident source's efforts to report on the activities of the IRGC, its personnel, and its cyber wing, the IRGC-Electronic Warfare and Cyber Defense Organization (IRGC-EWCD).

Social Engineering and Influence Operations

Social engineering operations, albeit not traditional ones, have also started to become increasingly intertwined with influence operations in what Iranian strategists would term the offensive Soft War. The identified incidents suggest Iranian threat actors operating for entities linked to APTs are adopting fake personas and attempting to use them to influence behaviors. In at least one related case, the dissemination of malware also potentially occurred when a sock puppet account was linked to Android and Windows-based malware.

Proud Boys

On November 18, 2021, the US Department of Justice, in coordination with the US Department of the Treasury, unsealed an indictment and designated for sanctions Iranian companies and nationals associated with cyber intrusions and US elections interference, respectively. The Department of Justice specifically indicted Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian, both members of Iranian entity Eeleyanet Gostar, now known as Emennet Pasargad, for a “targeted, coordinated campaign to erode confidence in the integrity of the US electoral system and to sow discord among Americans”. The operation was devised by those indicted and impersonated the far-right American extremist group the Proud Boys.

Vote for Trump or else!



Figure 14: Proud Boys email sent to Democratic voters (Source: [Pensacola News](#))

Anti-Dissident Operations

In December 2020, [Treadstone71](#) issued a report on a large-scale coordinated social media operation run by the IRGC, the Basij, and MOIS to penetrate and influence Farsi-language audiences that converged around a real-life conference. The operation targeted entities affiliated with the NCRI and MEK and involved members of these agencies masquerading as regime opponents. Their objective was to blend in as members of opposition movements or general diaspora Iranians and manipulate and misinform online discussions. From there, they used their position apparently to support general, high-level anti-government statements but in actuality to target anti-government movements and personalities such as the MEK and NCRI. This aspect of their tradecraft was likely devised to prevent increased skepticism and suspicion of the target audiences versus the cyber operator's sock puppet.

Endless Mayfly

Another efficacious example of Iran's social engineering capabilities relating to information operations is represented in the Endless Mayfly campaign. The campaign was [disclosed](#) by CitizenLab in May 2019 and represents one of the more aggressive publicly known campaigns run by Iranian operatives. In this campaign, the use of fake personas, fake news sites, and potentially malware converged for disinformation and intrusion activities. Among the many fake profiles, one was identified of “Mona A. Rahman”, a self-proclaimed political analyst and writer. The profile held anti-Saudi Arabian government views and covered the murder of Jamal Khashoggi. The profile engaged with real-life activists to incite physical protests. In the latter stages of the Endless Mayfly campaign, the Mona Rahman profile also directly engaged with activists and critics.

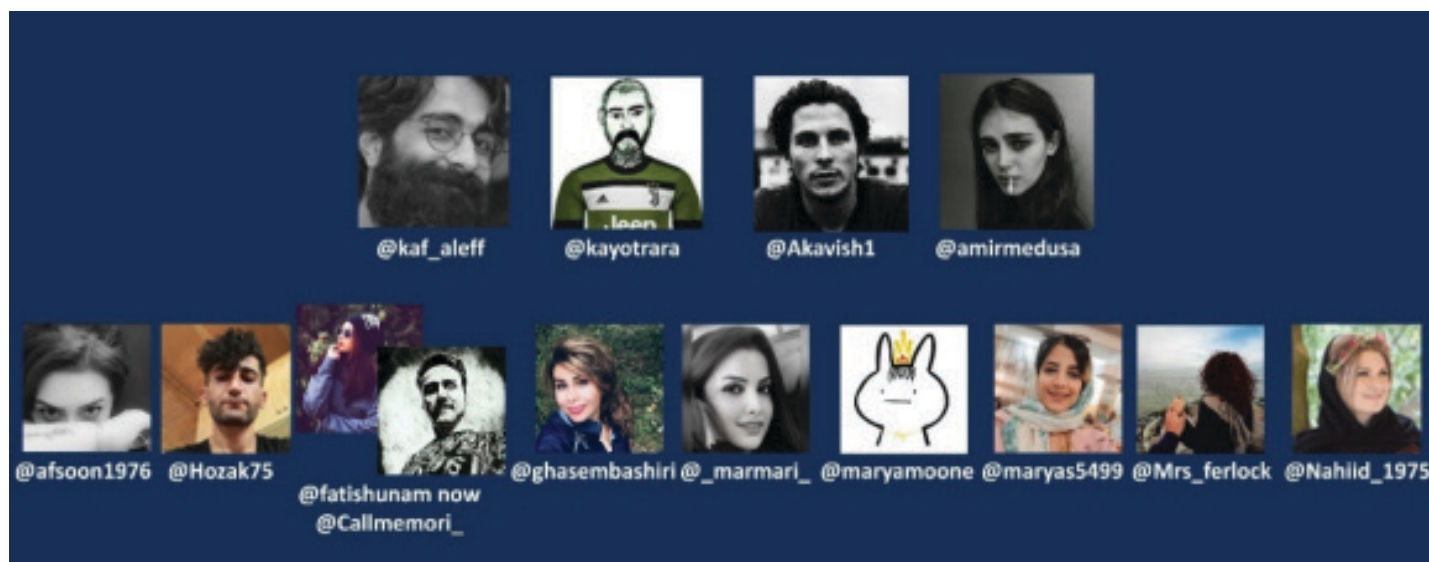


Figure 15: IRGC fake accounts masqueraded as political opposition (Source: [Treadstone71](#))

The majority of the Endless Mayfly campaign focused on influence activity and disinformation efforts, but a smaller component also revealed how a domain was linked to malware samples. The website associated with the domain, according to CitizenLab, “hosted inauthentic profiles and tweets for prominent figures... [including] spoofed tweets by Turkish Prime Minister Recep Tayyip Erdoğan and Saudi Crown Prince Mohammed Bin Salman”. At the time of writing, CitizenLab researchers could not confirm whether the identified malware was used to target victims via the Endless Mayfly network.

Mitigations Against Social Engineering

Strategic

- Establish robust policies and carry out social engineering and anti-phishing awareness exercises to help detect and prevent attacks.
- Create testing environments to ensure the workforce is certified to counter social engineering attacks.
- Provide social media best practices awareness training to help mitigate the possibility that employees inadvertently release confidential information.
- Ensure that effective two-factor authentication (2FA) mechanisms are in place to help stop social engineering attacks.

Operational/Tactical

- Iranian operators have repeatedly used fake charismatic profiles or those that impersonate recruitment offers to engage with victims. Treat all unrecognized social or professional correspondence as suspicious.
- Attackers aim to drive victims to platforms where they are empowered, via a malicious program or otherwise. Avoid unsolicited requests to establish communication through additional methods, especially unapproved chat or messaging applications.
- “Cold-calling”, either via email or social media, is a prime method Iranian social engineering operators use to engage with victims. Be on the lookout for signs of inauthentic or reused material, as the social engineer will attempt to emulate these common practices.
- Some reported cases of social engineering and phishing aim to create a sense of fear or emergency (for example, “Google Security Team” messages). If you receive any message that appears urgent, pause and evaluate the situation before reacting.
- The use of SMS phishing has been associated with Iranian social engineering attacks.

Outlook

Since the first reports emerged in 2014, Iranian social engineering campaigns have persisted and continued to innovate. While many of the early operations, such as Newscaster, were littered with rudimentary grammatical mistakes and weak operational security, these defects have disappeared. Those perpetrating the social engineering attacks are now executing operations impersonating high-ranking think tank directors, journalists, business officials, scientists, anti-government threat actors, and even government officials. This characteristic of their operations has not diverged extensively and is expected to continue, as they mimic their targets or attempt to establish relationships with them based on professional interests.

With time, the operators are likely to continue to improve their approach and ability to target their victims. It is highly likely that these approaches will focus on tried and tested methods, such as using a journalistic persona, soliciting interviews and analytic opinions, and sharing reports with targets to enable credential theft operations. Social engineering will also likely continue to evolve as long-term operations as depicted by the TA456 “I Knew You Were Trouble” campaign. With the growing role of social media among younger generations, fake and imposter accounts may even take on a more significant role and may even employ [deep fake](#) technologies.

Although the adoption of new technologies such as deep fakes is likely, threat actor operations may also be limited in scope by these technologies. For example, it is unclear whether APT groups will adopt “deep fakes” to facilitate intrusions or only for influence operations, similar to the Proud Boys election interference activity.

Iranian operators are also expected to become more competent in using foreign languages in social engineering attacks. As depicted in the large-scale Proud Boy operation, threat activity groups are ready to engage with large audiences, even during periods of increased scrutiny. Their capabilities have also spread well beyond the English language, as depicted in various influence and cyberattack operations around the world that incorporated Arabic, Spanish, French, Hebrew, and Turkish, among others. This suggests that a supply of foreign-language capable or trained operatives is tasked with social engineering operations.

Open source reporting indicates that APT35 is more likely to attempt to drive victims to engage with them in one-on-one dialogues in the future. While Insikt Group cannot verify such assessments, industry reporting has supplied ample evidence of the group's desire to engage with victims. Additionally, the use of malicious software is also highly likely to continue to enable this activity in the future, as the group and others like it attempt to hook their targets.

Appendix

Von: Farnaz Fasihi <farnaz.fasihi@gmail.com>
 Gesendet: Dienstag, 12. November 2019 12:50
 An:
 Betreff: WSJ Interview



Translation:

Hello *** *****

My name is Farnaz Fasihi. I am a journalist at the Wall Street Journal newspaper.

The Middle East team of the WSJ intends to introduce successful non-local individuals in developed countries.

Your activities in the fields of research and philosophy of science led me to introduce you as a successful Iranian. The director of the Middle East team asked us to set up an interview with you and share some of your important achievements with our audience. This interview could motivate the youth of our beloved country to discover their talents and move toward success.

Needless to say, this interview is a great honor for me personally, and I urge you to accept my invitation for the interview.

The questions are designed professionally by a group of my colleagues and the resulting interview will be published in the Weekly Interview section of the WSJ. I will send you the questions and requirements of the interview as soon as you accept.

*Footnote: Non-local refers to people who were born in other countries.

Thank you for your kindness and attention.

Farnaz Fasihi

Source: [Certfa Lab](#)

Kaviani Email:

Hello,

I'm Asal, thank you for your good reporting. Unfortunately, my brother is a computer engineer working with the sepah [IRGC], and I'm really upset about it because I hate them. I asked him many times to stop working with them, but he says the pay is good. But in any way possible I would like his cooperation [with the IRGC] to stop.

Last time he was browsing your site he became very upset to see your site content.

I want to do whatever I can, but I care for my brother and I do not want his name ...

But the least I can do for you is to be able to talk about where he is and what he does, who he works with and ...

If I can help in any way just say it.

Thanks

asalkaviani1989@gmail[.]com

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.