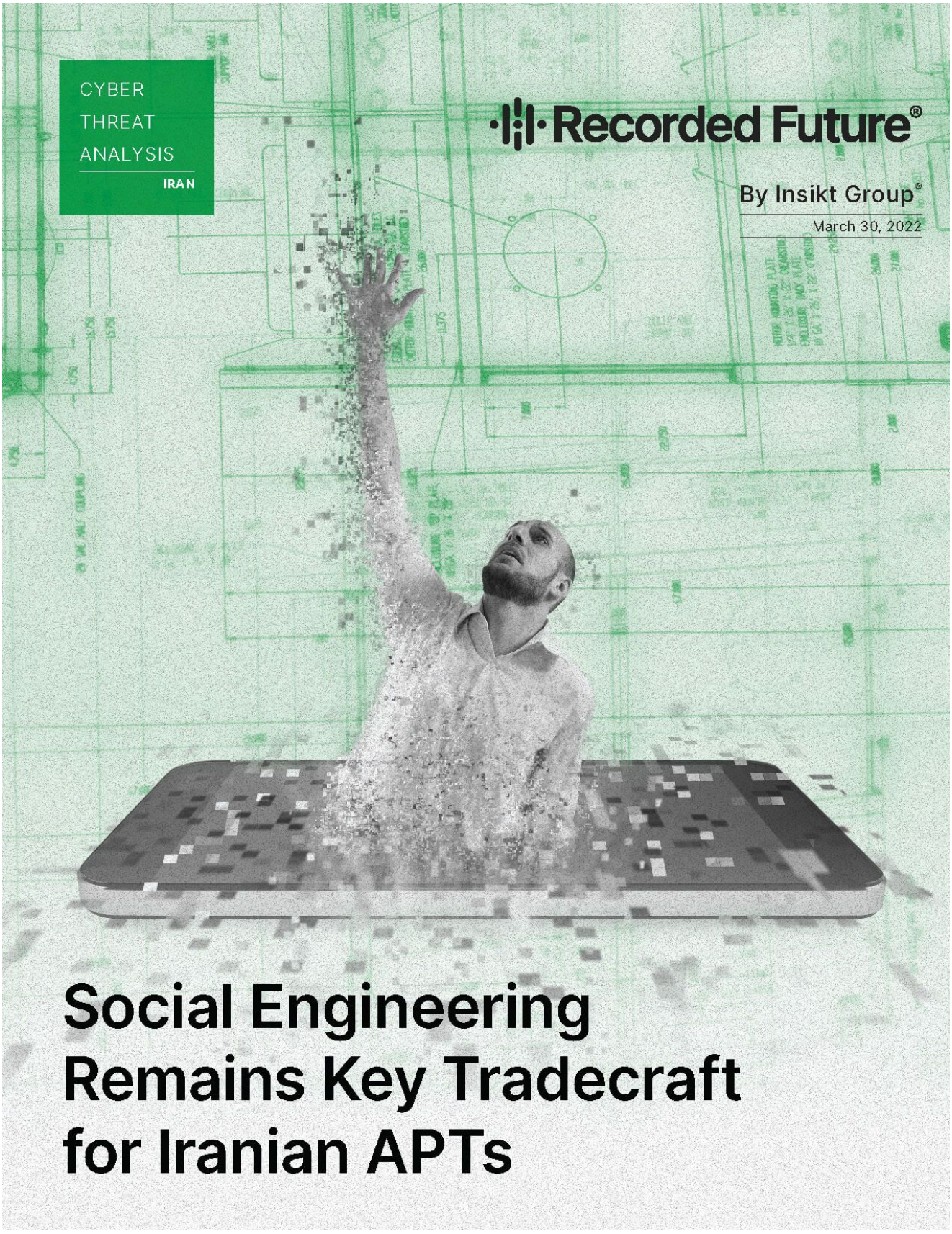
Social Engineering Remains Key Tradecraft for Iranian APTs

recordedfuture.com/social-engineering-remains-key-tradecraft-for-iranian-apts/



Insikt Group

***Editor's Note**: The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

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. 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, 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 بقیةالله 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.

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.

***Editor's Note**: This post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*