# Iran’s Cyber Ecosystem: Who Are the Threat Actors?

carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Return to Iran’s Cyber Threat: Espionage, Sabotage, and Revenge

While the relationships between proxies and governments can range from passive support to complete control, Iran’s indigenous threat actors maintain an arm’s-length relationship to the state, with certain operations orchestrated to meet the needs of the government.

Published January 04, 2018

Resources

Print Page

Table of Contents

Table of Contents

The Islamic Republic of Iran is unique in that its most powerful officials—namely Supreme Leader Khamenei and the Islamic Revolutionary Guard Corps—are inaccessible, while its most accessible officials—including Foreign Minister Javad Zarif—are far less powerful. Iran’s offensive cyber activities are almost exclusively overseen by the IRGC—likely without the oversight of the country’s publicly “elected” officials—and composed of a scattered set of independent contractors who mix security work, criminal fraud, and more banal software development. While the relationships between proxies and governments can range from passive support to complete control, Iran’s indigenous threat actors maintain an arm’s-length relationship to the state, with certain operations orchestrated to meet the needs of the government.[36]

After successfully suppressing the 2009 Green Movement and first detecting the Stuxnet attack in 2010, Iranian threat actors conducted sustained campaigns against domestic and foreign adversaries. These indigenous operations appear to be performed by small groups of individuals that have varying levels of technology experience with no more than ten people per team. These campaigns and the resources produced by the groups range from rudimentary to relatively professional, but most actors still face a low capacity ceiling.[37]

Though U.S. officials and some cybersecurity companies have speculated that Tehran has received technical assistance from countries like Russia and North Korea, the level of sophistication is commensurate with the established practices of amateur hacking communities inside Iran.[38] While Iranians have demonstrated talents in social engineering and embedding themselves in compromised networks, this alone is not indicative of external training or technological transfers.

On several occasions, Iranian threat actors have used off-the-shelf or pirated versions of professional penetration testing tools to conduct campaigns, but there is little indication of Tehran acquiring exploits or malware from foreign governments. Iran *has* acquired hardware for internet surveillance from Chinese telecommunication firms and maintains cooperative agreements with Russia on cybersecurity; however, these relationships differ from providing Tehran with offensive cyber capabilities.[39] No publicly documented or privately observed attack has demonstrated the use of tools or resources that are beyond the capacity of Iranian threat actors.

In principle, the tools and tactics used in cyber operations are subject to an exposure risk. Unlike conventional weapons, malware attacks or other cyber activities lose their effectiveness when discovered and when their functionality and infrastructure is documented. Describing a missile does not provide effective countermeasures, but describing malware can provide antivirus companies and system administrators the ability to protect systems. State-aligned threat actors will likely not employ the most sophisticated tools and strategies available to them unless the target is well protected and worth potentially exposing tradecraft to compromise. However, unlike in other countries, there are not observed examples from Iranian threat actors of escalation into more sophisticated attacks against hardened targets.[40]

Iranian threat actors conduct campaigns with established toolkits that sometimes last for years and ensnare hundreds of targets. However, the fluid nature and decentralization of these groups make them relatively difficult to track. Malware that is publicly attributed to Tehran is often abandoned immediately on exposure, and identifiable members appear to change groups over time. Some groups seem to split up, have members move elsewhere, or even collaborate, further blurring lines.[41] For example, while an IRGC-affiliated group labeled Rocket Kitten was the most active operator for a two-year period (2014–2016), attracting press attention as Iran's premiere threat, it has since faded into quiescence, eclipsed by the actor Oilrig.[42]

Despite their substantial financial impact, Tehran's disruptive operations against foreign targets have been technically simple. The compromise of a small number of IT personnel enabled the destruction of data on computers maintained by Saudi Aramco, eventually resulting in hundreds of millions of dollars in damage.[43] In only a few campaigns have Iranian threat actors shown the professionalism and sophistication approaching that expected of a nation-state actor; in one such case, the operation could be tied directly to the Ministry of Intelligence (Magic Kitten, discussed later).[44]

Success can often be attributed to security failures and to poor protection of infrastructure on the part of the victim, alongside opportunistic targeting and patience by the attacker. The defacement of Voice of America's websites by the Iranian Cyber Army, one of the first disruptive attacks by Iran against the United States, was accomplished through social engineering the news agency's domain name service provider.[45] Other basic security failures gave Iranians a toehold in the networks of Las Vegas Sands Corp. after its owner, Sheldon Adelson, advocated military force against Iran.[46] Symantec, an American cybersecurity company, noted that the perpetrators of a recent Saudi-focused campaign had invested a "significant amount of preparatory work for the operation," but the custom malware was described by Russian cybersecurity firm Kaspersky as "generally of low quality" partially derived from open-source toolkits.[47]

Similarly, a major attack on the American financial sector—known as Operation Ababil—which caused hundreds of millions of dollars in damage, was described as one of the largest DDoS attacks known at the time. Yet it took only a few young Iranian computer experts, breaching thousands of websites that were running vulnerable software, to pool enough bandwidth to overwhelm the infrastructure of banks and cause unpredicted software failures.[48] Thus, while Iranian threat actors have limited capacity, through basic tradecraft and persistence they can still be effective at espionage and sabotage.

The overall sophistication and dedication observed in such campaigns has not significantly changed in the decade that Iran has engaged in offensive cyber operations—the attacks documented against Las Vegas Sands Corp. in 2014 are comparable to those used against Saudi Arabia in renewed hostilities over the course of 2016-2017. Indeed, many research disclosures cover groups that have been active for several years, using the same malware with only incremental changes over the course of time.

While sophistication alone can be a superficial metric of posed threat, Iranian operations do not demonstrate the common technical precautions taken by other nation-state actors (such as obfuscating malware), and, even with strong social engineering capabilities, attacks are often betrayed by a lack of investment in nontechnical resources (such as fluency in English or personal tailoring of messages).[49] These resource constraints also account for why Iranians are more effective at compromising dissidents—Iranian threat actors understand their target's context and language, as opposed to when they are tasked with European languages or other cultures. Iran shows little indication of becoming a first-tier cyber power in the foreseeable future unless it begins to further organize its operations and invest in professionalism.

## Magic Kitten

In January 2015, the German news outlet *Der Spiegel* released previously unpublished documents on cyber espionage conducted by American intelligence agencies.[50] One of them revealed an NSA tactic labeled "fourth party collection," which is the practice of breaking into the command and control infrastructure of foreign-state-sponsored hackers to look over their shoulders. The presentation describes a real-life example of acquiring intelligence and stealing victims from a group code-named VOYEUR by the NSA, otherwise known as Magic Kitten.

Magic Kitten appears to be among the oldest and most elaborate threat actors originating in Iran. It is also distinct from other groups because of its apparent relationship with the Iranian Ministry of Intelligence rather than the IRGC. However, Magic Kitten's activities mirror those of other groups, with the primary targets being Iranians inside Iran and Tehran's regional rivals. The earliest observed samples of Magic Kitten's custom malware agent dates to 2007, well before other known malware apparently originated, and the threat actor continues to be active.

Magic Kitten appears to exercise the most mature tradecraft of Iran-based threat actors. It has opportunistically compromised dozens of websites at random (including those of an Indian hospital, an Italian architect, and a well-known Canadian comedian) to create a relay network to hide its operations. Such attention to tradecraft appears elsewhere in Magic Kitten's operations, including in the design of malware, which is modular in nature.

Magic Kitten has not been observed using sophisticated exploits and instead appears to rely on social engineering and other common tactics to deceive users. In the case of the journalist Vahid Pour Ostad, the malware was sent by his former Ministry of Intelligence interrogator with a threat attached and relied on private records that would have been available only to government actors. This coordination represents both independent confirmation of the NSA's attribution and an extreme example of the strategies employed by Magic Kitten. Other samples of the malware agent appear to have been delivered posing as Turkish asylum forums for Syrian refugees.

The NSA presentation also provides a window on Magic Kitten's targets up to May 2011, portraying an operation focused on North America, Europe, and the Middle East. These campaigns continued through the June 2013 presidential election of Hassan Rouhani, provoking a blogpost from Google about related attacks.[51] As the election approached, exposed logs showed the daily capture of dozens of accounts connected to Iranian cultural and media figures, graduate students, and social activists (including individuals that would later join the Rouhani administration). Magic Kitten continued to target Iranians after the election, attempting to unmask pseudonymous internet users by baiting them with content on women's rights and the security establishment.

Like other Iranian operations, Magic Kitten maintains a strong secondary interest in conducting espionage against regional targets and international foreign policy institutions. CrowdStrike, another American cybersecurity company, accounts for part of this focus on "international corporations, mainly in the technology sector" and other political targets.[52] An NSA slide with a victim map portrays a broad-reaching operation targeting nearly every country in the Middle East. Sinkhole data collected from expired domains previously used as relays and other fallback infrastructure suggest that Magic Kitten, or the malware agent used, continues to actively compromise individuals in Germany, Indonesia, Iraq, Lebanon, the Netherlands, Palestine, Pakistan, Qatar, Sweden, Switzerland, Thailand, and the United Arab Emirates. Notably, compromised individuals in Iraq were also typically in Iraqi Kurdistan, mirroring a common pattern with other threat actors.

A diagram within the NSA presentation suggests that the malware agent employed by Magic Kitten was also used at the time by Iran's Shia Lebanese proxy Hezbollah, under independent infrastructure. While Hezbollah has been known to maintain its own offensive cyber operations and engage in intelligence sharing with Iran, there has been little prior evidence of direct sharing of tools.[53]

## Understanding Iranian Government Involvement and Attribution

It is often difficult to determine the origins and perpetrators of Iranian offensive cyber operations, as these campaigns may disappear as quickly as they appear. Public exposure often leads them to change tactics and abandon tools, making tracking even more difficult. The history of cyber operations targeting Iranians and originating from Iran is populated by groups that arise out of nowhere and conduct campaigns for ambiguous reasons over a finite time span, then disappear. This unusually frenetic character conspicuously differentiates the Iranian hacking ecosystem from that found elsewhere, particularly those tied to state actors in advanced countries.

> The history of cyber operations targeting Iranians and originating from Iran is populated by groups that arise out of nowhere and conduct campaigns for ambiguous reasons over a finite time span, then disappear.

The amateur hackers connected to the Iranian defacement community have long been politically engaged and have often vandalized foreign sites for ostensibly nationalistic reasons.[54] In one of the first international incidents attributed to Iran, domestic hacking groups in mid-2008 exchanged tit-for-tat defacements with competitors in neighboring Arab countries after the official sites of Grand Ayatollah Ali al-Sistani were vandalized with anti-Shia content by an Emirati hacker. Such defacement activities can often evolve into state-affiliated activities: one of the participants in the anti-Sunni website-defacement campaign in 2008 was later linked to the Iranian Cyber Army. This transition from patriotic hackers to state-aligned threat actors, and the ambiguity between civic nationalism and state involvement, mirrors the apparent development of cyber communities in China and elsewhere.[55]

In only two incidents have Iranian government entities taken direct credit for the defacement of political opposition sites, both attributed to branches of the Revolutionary Guard. The first case was the March 2010 takedown of sites connected to the organization Human Rights Activists in Iran, which was alleged to be training cadres to mobilize against the regime like the Velvet Revolution. The attack relied on the arrest of a website administrator inside the country rather than on complicated tactics. The arrests and destruction of data had a lasting impact on the organization by instilling fear in members and giving rise to rumors about collaboration with the government.

The second government-initiated campaign, carried out during a Shia holiday in December 2013, led to the defacement of nine human rights and independent media websites with a Quranic verse in Arabic and Persian. The IRGC’s Public Relations Department announced that the operation had been conducted by the Revolutionary Guard’s Kerman Branch and claimed that the defaced websites had been established by the country’s enemies and supported by internal seditionists.

In most cases, Iran uses cutout or proxy organizations, allowing it to keep some distance from the disruptive incidents and propagandistic defacements. These cutouts represent themselves as patriotic Iranians or pan-Islamic movements acting independently in defense of the supreme leader, national sovereignty, and religious ideals. Conducting offensive cyber operations through covert organizations provides Tehran plausible deniability for any attacks, thereby protecting its claim to victimhood while also allowing the state to signal its intentions to its opponents. These tactics are effective: there is still no definitive public agreement on who was behind the Yemen Cyber Army's attacks that led to stolen Saudi Arabian Ministry of Foreign Affairs documents being published by WikiLeaks, with the consensus split between Iran and Russia.[56] The cutouts tend to develop their own mythology and continue to be treated as active threats past their expiration date, bolstering perceptions of Iran's capability.

> Conducting offensive cyber operations through covert organizations provides Tehran plausible deniability for any attacks, thereby protecting its claim to victimhood while also allowing the state to signal its intentions to its opponents.

Nevertheless, a comprehensive study of Iran-linked cyber operations often reveals Tehran's hand in such proxies. When the U.S. Justice Department unsealed its Operation Ababil indictment in March 2016, it named two Iranian corporate entities that employed at least seven individuals who had been contracted by the Iranian government.[57] The indictment implicated three of the participants as being part of the Sun Army, an Iranian cutout defacement group. The Sun Army followed the typical pattern found with the Iranian Cyber Army and other state-aligned defacements, arising out of nowhere to perform targeted political acts over a short life span. Its first documented defacements, in February 2010, were of sites connected to now-detained opposition leader Mehdi Karroubi. The vandalism accused him of being a traitor and was timed to blunt planned antigovernment street protests.[58]

As Iran's cybersecurity landscape has professionalized, some defacement groups have sought to convert their infamy into corporate success. Based on the disclosure of personal information about threat actors, there are indications that those engaged in Iranian offensive cyber operations work within corporate entities (such as IT consultancies) or contractors of Iranian security forces.[59] For example, aspects of the Madi espionage campaign implicated the Mortal Kombat Underground Security Team, a small Iranian group that has attempted to sell spyware and other hacking tools since at least 2008.[60] The frequent overlap of legitimate digital commerce sites and servers used for intrusion campaigns is demonstrative of these blurred lines—a company might simultaneously provide web design services for businesses and hack for the government.[61]

The transition of amateur hackers into contractors for state security agencies is reflected in basic qualities and patterns of life found across most threat actors. There are clear indications that the threat actors documented are solely Iranians operating inside Iran, not diaspora Iranians or non-Iranians. At the most basic level, they tend to follow the normal patterns of life of office workers, being active during the Iranian workweek (Saturday through Wednesday) and dormant during Iranian holidays, particularly the long holiday of Nowruz, the Persian New Year.

> Iranian threat actors have often used pornography as bait in their spearphishing campaigns and display an irreverent sense of humor.

Disclosures of aliases and real names, which may be discoverable because of a disregard for operational security due to insulation from repercussions or a lack of professionalism, help reveal both the lives and the motivations of Iranian threat actors. While those behind the groups may be nationalists or ideologically aligned with the regime, they do not appear to be enrolled members of the military or security apparatus. These individuals and groups also differ in social and religious predilections; some participants promote the use of narcotics and trade pornography on personal social media, while others are devoutly religious and embed Islamic references in malware code. Iranian threat actors have often used pornography as bait in their spearphishing campaigns and display an irreverent sense of humor.

## Criteria for Independent Assessment of State Involvement

Campaigns conducted against dissidents and others inside Iran provide the most direct evidence of government involvement. Whereas it can be difficult to trace the consequences of foreign espionage, for those on the ground the implications are more direct and tangible.[62] As a pattern builds between cyber operations and the offline actions of security forces, the relationship between both becomes clearer.[63] While these cases of collaboration are discernible in only a few threat actors, the patterns support a broader narrative around the intrusion ecosystem.[64] Indications that Iranians undertaking offensive cyber operations are associated with the government include the following:

- The campaigns have been conducted based on information that appears to have been provided by security agencies. In certain cases, the campaigns have been carried out in coordination with government employees and in advance of the arrest of the target.
- The targets of such operations align with the sensitivities of the Islamic Republic, and certain individuals are targeted repeatedly by multiple threat actors over time.
- Persistent and costly campaigns have been sustained against thousands of targets without an apparent financial motive and without clear indication of the end use of the data obtained by intrusion.

In rare cases, potential ties to the government are even disclosed by the participants themselves. A malware developer associated with the Rocket Kitten group, Yaser Balaghi, was identified by name based on a pseudonym found in the malware's code. In a résumé from 2013, Balaghi listed past information security projects and a history of conducting hacking projects under contract to an otherwise unnamed "cyber-organization."[65] Balaghi is not alone in listing his hacking activities on his résumé; still other pseudonyms embedded in malware code used against Saudi Arabia and internal dissidents can be associated with LinkedIn profiles describing their experience as an "Information Security Researcher" with a "Secret" group.

To add a complication common in cybersecurity research, it is often difficult to distinguish commonplace electronic fraud from politically motivated disruptions and state-sponsored surveillance efforts, especially where the attacks are not sophisticated. In at least one case, Iranians that had staged persistent attempts against U.S. foreign policy organizations and two European foreign ministries had also maintained infrastructure linked with commercial banking fraud.[66] In another example, the same social engineering skills used by an individual behind the Iranian Cyber Army defacements also proved successful in a career in the commercial theft of domains and PayPal fraud. More recently, in an indictment against an Iranian accused of attempting to extort HBO with stolen copies of unreleased television episodes in the summer of 2017, the U.S. Department of Justice claimed that the same individual had worked on behalf of the Iranian government to target military systems and Israeli infrastructure.[67]

Analyses of Iranian offensive cyber operations often rest on the country's strict domestic controls as an indication of endorsement—that the government would not allow something to happen that it didn't want to occur. However, Tehran's controls are not so absolute, and many of the operations could occur surreptitiously given their simplicity. Cyber activity emanating from Iran could theoretically be conducted without the state's sanction, consent, or even knowledge. Daily, millions of Iranians circumvent censorship using antifiltering tools that allow them to bypass network restrictions and encrypt their communications against surveillance. These tools provide space for Iranians to engage in actions against the government without persecution, and similarly can conceal cyber activities. Therefore, an Iranian origin does not alone indicate state sponsorship.

Nor does the financial damage resulting from an operation, the political implications of the campaign, or the number of targets necessarily directly correlate with the probability of government involvement. The destructive operations conducted against Saudi Aramco resulted in millions of dollars in damages, yet the malware was unsophisticated and the attack did not require significant resources, putting the incident plausibly within reach of a sole individual acting without sponsorship. Such straightforward metrics of harm, then, are poorly informative of the degree of governmental involvement in cyber activities originating from Iran.

## Government Entities and Threat Actors

The coordinated timing of cyber operations with politically motivated arrests are a strong indication of the Iranian government's direct involvement. Since at least July 2014 a pattern has emerged: individuals in the custody of the IRGC are forced to provide access to their online accounts and devices, which are then immediately used to conduct spearphishing attacks associated with known threat actors.

A vivid example of this coordination is the case of Iranian-American Siamak Namazi, a forty-six-year-old Dubai-based energy consultant and previously a scholar at the Woodrow Wilson International Center for Scholars in Washington, DC. In October 2015, he was arrested by

Iranian security forces months after having had his passport confiscated while visiting the country. Within hours of his arrest, Namazi's Google and Facebook accounts initiated conversations with his wide array of foreign policy and media contacts. The intruder, pretending to be Namazi, sent contacts an article about the recent nuclear deal and in poor English solicited edits on the document. This message was accompanied by an email directing the target to a fake Google site requiring visitors sign in to their account to view the document, a credential theft attempt connected to Rocket Kitten. Numerous individuals were compromised in this campaign, including scholars, U.S. State Department employees, and one prominent journalist whose Gmail account—which included communications with former U.S. secretaries of state, CIA directors, and other foreign ministers—was overtaken by the Iranian hackers for nearly two days. [68] This pattern has been repeated in numerous cases involving other Iranians, dual nationals, and foreign nationals detained in Iran.

Cyber operations have also been documented in preparation for arrests.[69] A prominent example of target selection prior to arrest is the case of Babak Zanjani, an Iranian-Danish businessman who had been personally sanctioned by the United States and European Union for involvement in Iranian sanctions evasion. After months of claims regarding his role in the embezzlement of oil revenue, a process that included a parliamentary investigation, at the end of December 2013 Zanjani was arrested and subsequently charged with "corruption on earth."[70] After an opaque judicial process, in March 2016 he was condemned to death, a sentence the Ministry of Justice indicated could be commuted if Zanjani cooperated in recovering Iran's foreign assets.

> This overarching trend points to probable relationships between certain threat actors and the intelligence agencies, a business relationship that has been revealed when Iranians have been indicted by the United States for hacking.

A persistent effort targeted Zanjani's personal accounts and business infrastructure in the weeks immediately preceding his arrest. Iranian threat actors sought access to Zanjani's iCloud services and successfully compromised employees associated with his holding company, the Sorinet Group.[71] These activities indicate that in advance of the arrest of Zanjani, the group (Flying Kitten) had acquired access to the confidential information of Sorinet subsidiaries and personnel; however, it is not clear whether any material accessed during this time was used in the investigation or prosecution of Zanjani. The case of Zanjani reflects a broader trend witnessed with other cases; Iranian threat actors frequently pursue online the types of individuals commonly persecuted by the Islamic Republic offline.

The association between Iranian-origin cyber activities and Iran's intelligence agencies is further supported by the fact that the data acquired during such operations is rarely disclosed. The Navy Marine Corps Intranet breach, the Las Vegas Sands Corp. incident, and the compromise of State Department employees have all led to the exfiltration of substantial amounts of highly sensitive information. There is no indication of ulterior motives, such as fraud, extortion, humiliation, or disclosure to the hardline press.[72] The operations required costly infrastructure, including dedicated servers and dozens of domain names, in addition to personnel time. The activities must have provided some degree of income to their members, with the primary value being espionage. This overarching trend points to probable relationships between certain threat actors and the intelligence agencies, a business relationship that has been revealed when Iranians have been indicted by the United States for hacking.

## Notes

[36] Ibid.

[37] The tools and resources developed by Tehran have been almost uniformly described by outside investigators as unsophisticated, particularly in comparison with malware produced by other state and nonstate actors. The information security company Mandiant affirmed this observation in a 2014 report: “Mandiant’s observations of suspected Iranian actors have not provided any indication that they possess the range of tools or capabilities that are hallmarks of a capable, full-scope cyber actor. They rely on publicly available tools and capitalize solely on Web-based vulnerabilities—constraints that suggest these cyber actors have relatively limited capabilities.” See: Mandiant, “M-Trends 2014 Annual Threat Report: Beyond the Breach by Mandiant, a FireEye Company,” accessed December 5, 2017, https://www2.fireeye.com/fireeye-mandiant-m-trends-report.

[38] For example, former representative Peter Hoekstra speculated at a U.S. House hearing that Iran’s advances in cyberwarfare came from the “cooperation they have with Russia.” Other former and current officials have commented, often on background, that Russia was a potential partner in warfare. For the subcommittee hearing on Iran’s support terrorism worldwide, see the following: “Iran’s Support for Terrorism Worldwide,” Foreign Affairs Committee, March 4, 2014, https://foreignaffairs.house.gov/hearing/joint-subcommittee-hearing-irans-support-for-terrorism-worldwide/ . Elsewhere, claims have been made by lesser known cybersecurity companies, but these analyses have been flawed and not well accepted. For more on these flawed analyses, see: Collin Anderson, “Bears and Kittens, and Startup Cybersecurity Companies,” Medium, May 18, 2017, https://medium.com/@collina/bears-and-kittens-and-startup-cybersecurity-companies-5c8e037ea75c .

[39] Steve Stecklow, “Exclusive: Huawei Partner Offered U.S. Tech to Iran,” Reuters, October 25, 2012, http://www.reuters.com/article/us-huawei-iran/exclusive-huawei-partner-offered-u-s-tech-to-iran-idUSBRE89O0E520121025 ; and “Iran and Russia Announce Plans for Cyber Security Cooperation,” YouTube video, 2:03, posted by “PressTV News Videos,” March 15, 2017, https://www.youtube.com/watch?v=NaCukjiECWM.

[40] This could be either indicative of the ceiling of Iran’s capabilities or reflective of Iran not facing the sort of existential threat that would provoke it to use any latent resources in its arsenal. The former appears more likely.

[41] Rocket Kitten and Flying Kitten are examples of how the line demarcating intrusion groups is not always clear. The structural similarities of certain intrusion tools and the reuse of lesser known infrastructure indicate that parts of Flying Kitten and Rocket Kitten may have had a common heritage, including common members and shared tools; see: Collin Anderson, “Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code,” Iran Threats, December 5, 2017, https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/. In the Shamoon 2 campaign, McAfee attributed unusual errors to the “involvement of different groups/individuals with different skills, whereas in 2012 we believe one group was responsible for the attack.” See: Christiaan Beek and Raj Samani, “The State of Shamoon: Same Actor, Different Lines,” McAfee, April 25, 2017, https://securingtomorrow.mcafee.com/executive-perspectives/state-shamoon-actor-different-lines/.

[42] The authors associate Rocket Kitten with the IRGC due to its involvement in post-arrest hacking. For more on Rocket Kitten, see: “Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks,” *ClearSky Cybersecurity* (blog), September 1, 2015, http://www.clearskysec.com/rocket-kitten-2/ . For more on Oilrig, see: Robert Falcone and Bryan Lee, “The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor,” Palo Alto Networks, March 26, 2016, https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/ .

[43] Reportedly, the attacker found sensitive passwords saved in a file named “Administrator Passwords.” See: Sam Jones, “Cyber Warfare: Iran Opens a New Front,” *Financial Times*, April 26, 2016, http://app.ft.com/cms/s/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html?sectionid=companies. No official numbers have been provided on the economic loss, and in its annual review report for the year, Aramco downplayed the impact of the attack. “Shaping Tomorrow: 2012 Annual Review,” Saudi Aramco, April 10, 2013, http://www.saudiaramco.com/en/home/news-media/publications/corporate-reports/annual-review-2012.html.

[44] The caveat attending this statement is that it is possible more incidents and actors have yet to be disclosed.

[45] Based on a Freedom of Information Act request by the authors to the Broadcasting Board of Governors on cybersecurity incidents related to Iran, which returned details of the attack, involving compromising the VOA’s account through impersonation with falsified documents sent through a fax.

[46] The intruders were able to find a weakness in a web development server for the Bethlehem, Pennsylvania, location, and doing so then gave them access to the internal corporate network. Benjamin Elgin and Michael Riley, “Nuke Remark Stirred Hack on Sands

Casinos That Foreshadowed Sony," *Bloomberg*, December 10, 2014, http://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony.

[47] Symantec Security Response, "Shamoon: Back From the Dead and Destructive as Ever," *Symantec Connect* (blog), November 30, 2016, https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever ; "From Shamoon to StoneDrill: Wipers Attacking Saudi Organizations and Beyond," Kaspersky Lab, July 3, 2017, https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf .

[48] ITSec Team, one of the companies cited in the indictment, has a known track record as the developer of a web penetration testing product (Havij Pro), and is attributed in a number of vulnerability disclosures and tools for controlling remote systems that have been made available to security researchers. The infrastructure used in the attacks even remains publicly exposed to the internet years after its use.

[49] Seth Hardy, et al., "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," *23rd USENIX Security Symposium* (2014): 527–41, https://www.usenix.org/node/184440 .

[50] Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, et al., "NSA Preps America for Future Battle," *Der Spiegel*, January 17, 2015, http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

[51] Curiously, when Google disclosed the spearphishing campaigns that Magic Kitten was involved in, it noted to the *New York Times* that there was a relationship between the operation and the DigiNotar incident. Nicole Perlroth, "Google Says It Has Uncovered Iranian Spy Campaign," *Bits* (blog), *New York Times*, June 12, 2013, https://bits.blogs.nytimes.com/2013/06/12/google-says-it-has-uncovered-iranian-spy-campaign/.

[52] "CrowdStrike Global Threat Report: 2013 Year in Review," CrowdStrike, January 2014, https://scadahacker.com/library/Documents/Threat_Intelligence/CrowdStrike%20-%20Global%20Threat%20Report%202013.pdf.

[53] The lack of clarity in the slides is also compounded by the age of the document and could reflect an arrangement that is no longer in effect. However, within observations of activity, there does appear to be a clustering of victims, with some samples of the malware agent specifically used to compromise Lebanese and Qatari victims, but not Iranians or other targets of exclusive interest to Iran.

[54] Members of the infamous Ashiyane hacking community and others commonly broke into Arabic media and U.S. government sites with political messages, such as protesting alternative names for the Persian Gulf, Western perceptions of Islam, nuclear rights, the administration of George W. Bush, and the crimes of other countries—often in broken

English and always bearing attribution. In a few cases these campaigns were sustained over longer periods of time and were intended to make a point, especially when it came to Israeli and Saudi targets. “Al Khaleej Newspaper Website Hacked,” Gulf News, March 7, 2017, http://gulfnews.com/news/uae/general/al-khaleej-newspaper-website-hacked-1.106195 ; Zone-H mirror page, “fdfhome.gsfc.nasa.gov hacked. Notified by Mafia Hacking Team,” archived on May 26, 2005, http://www.zone-h.org/mirror/id/7494752 ; Zone-H mirror page, “lvis.gsfc.nasa.gov hacked. Notified by Ashiyane Digital Security Team,” archived on August 11, 2005, http://www.zone-h.org/mirror/id/2757516 ; Zone-H mirror page, “technology.jpl.nasa.gov hacked. Notified by hamid,” archived on December 28, 2005, http://www.zone-h.org/mirror/id/3183620.

[55] Aspects of this can be found in the individuals documented in Dan McWhorter, “APT1: Exposing One of China’s Cyber Espionage Units,” Mandiant, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf .

[56] Sheera Frenkel, “Meet the Mysterious New Hacker Army Freaking Out the Middle East,” BuzzFeed News, June 24, 2015, https://www.buzzfeed.com/sheerafrenkel/who-is-the-yemen-cyber-army ; and Brian Bartholomew and Juan Andres Guerrero-Saade, “Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks,” *Virus Bulletin Conference* (October 2016): 1–11, https://cdn.securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf .

[57] In its indictment, it even went as far as claiming that one individual had received relief from mandatory military service in return for participation. *United States of America v. Ahmad Fathi et al.*, unsealed March 24, 2016, https://www.justice.gov/opa/file/834996/download. The attribution for the campaigns and indication of the American intelligence community’s early attribution of the participants are evident in screenshots from a presentation on the NSA’s CyberCOP program from April 2013, which describes the scale of the DDoS attacks and the infrastructure behind the botnet in its later phases of operation. See: “CyberCOP,” presentation, CyberCOP Product Manager, April 11, 2013, http://www.ndr.de/ratgeber/verbraucher/cybercop100.pdf.

[58] Zone-H mirror page, “www.karroubi.ir hacked. Notified by Sun Army,” archived on February 17, 2010, http://www.zone-h.org/mirror/id/10269967.

[59] Florian Egloff, “Cybersecurity and the Age of Privateering: A Historical Analogy,” Cyber Studies Program Working Paper no. 1 (Oxford: University of Oxford, March 2015), http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.1_Egloff.pdf.

[60] Richard Barger, “There’s Something About Mahdi,” Threat Connect, July 23, 2012, https://www.threatconnect.com/blog/there-is-something-about-mahdi/ ; and “Summary of Mortalkombat.com,” Wayback Machine Internet Archive, accessed September 17, 2017, https://web-beta.archive.org/web/20080415000000*/m0rtalkombat.com .

[61] Flying Kitten has also established Pars Security (Pars Pardazesh Hafez Shiraz). The FBI had made similar allegations not only for the culprits of Operation Ababil, companies named Mersad and ITSecTeam, but also in the Arrow Tech Associates theft. The FBI's indictment claims that two other individuals formed a company, Andisheh Vesal Middle East Company, to steal software on behalf of the Iranian government. *United States of America v. Mohammed Saeed Ajily and Mohammed Reza Rezakhah*, unsealed July 17, 2017, https://www.justice.gov/opa/press-release/file/982106/download .

[62] For those on the ground the threats posed are more complex and multifaceted. For example, Iranian telecommunications firms appear to have cooperated with the government in order to provide access to the recovery and two-factor authentication codes sent by text. These then allowed access to Google, Telegram, and other accounts on foreign platforms.

[63] The most significant counterevidence of state-alignment is that when the Infy group was disclosed by Palo Alto in May 2016, the domains used in the communications of the malware were filtered by the censorship apparatus, blocking access to those victims. There are explanations for this action that would not conflict with the theory that Infy was acting on behalf of the government, including that the censorship was intended to hide evidence of the operation from the Iranian public.

[64] Specifically, we observed direct interactions between the Iranian state and the groups Charming Kitten, Flying Kitten, Magic Kitten, and Rocket Kitten. More tenuous links exist for Infy based on this criteria.

[65] "Rocket Kitten: A Campaign With 9 Lives," Check Point Software Technologies Ltd., November 9, 2015, https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf.

[66] The incident was orchestrated by a threat actor who had registered domains under cmprus1394[@]mail[.]ru and teymurov1984[@]gmail[.]com, which impacts a vast network of espionage and criminal activity.

[67] *United States of America v. Behzad Mesri, a/k/a "Skote Vahshat,"* unsealed November 21, 2017, https://www.justice.gov/usao-sdny/press-release/file/1013001/download.

[68] Robin Wright, "An American Hostage in Iran – Again," *New Yorker*, October 30, 2015, http://www.newyorker.com/news/news-desk/an-american-hostage-in-iran-again.

[69] A dual national who had previously worked with a foreign broadcaster was arrested two weeks after his email was also compromised after a phishing attempt. According to one account, the attacker attempted to extract a ransom to keep the victim's private information, which was ignored. Then, after the arrest, the accounts were again used to target others.

[70] "Iranian Billionaire Babak Zanjani Sentenced to Death," BBC News, March 6, 2016, http://www.bbc.com/news/world-middle-east-35739377.

[71] These intrusions reflected a studied understanding of Sorinet's operations and included names such as "Baharak Zanjani" that appear on the corporate registrations of the company's subsidiaries but are believed to be false identities. See article in Persian, Young Journalists Club, February 2, 2013, http://www.yjc.ir/fa/news/4744029/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%DB%8C-%D8%AE%D9%88%D8%A7%D9%87%D8%B1%D8%A7%D9%86-%D8%AC%D8%B9%D9%84%DB%8C-%D8%A8%D8%A7%D8%A8%DA%A9-%D8%B2%D9%86%D8%AC%D8%A7%D9%86%DB%8C.

[72] Iranian security and intelligence agencies have however frequently used blackmail and humiliation to intimidate or coerce individuals, including BBC Persian journalists. It is possible that material compromised through intrusions has been used for political manipulation, as this would be difficult to observe without acknowledgement from the victim. For examples of blackmail threats, see: Elise Knutsen, "Iranian Agents Blackmailed BBC Reporter With 'Naked Photos' Threats," *Arab News*, November 19, 2017, http://www.arabnews.com/node/1195681/media.

Table of Contents

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.