Iranian Cyber Response to Death of IRGC Head Would Likely Use Reported TTPs and Previous Access

recordedfuture.com/iranian-cyber-response

January 7, 2020

January 7, 2020 • Insikt Group®

Recorded Future's Insikt Group® reviewed available information to analyze the likelihood of Iranian response to the killing of Qassem Suleimani. This report serves to provide a compilation of likely tactics, tools, and groups involved in a cyber-based retaliation.

This report will be of greatest interest to organizations concerned with being targeted by an Iranian state-sponsored group, especially in the wake of heightened tensions in the Persian Gulf, as well as those following Middle Eastern geopolitical events.

Insikt Group will provide updates as new findings surface surrounding these incidents or cyber threat activities related to them are detected. See these links for additional background on how Iran manages state-directed cyber operations and on the history of some state-sponsored and patriotic hackers. Sources include intelligence surfaced in the Recorded Future® Platform and other open sources.

Executive Summary

In the early hours of January 3, Iran's Qassem Suleimani, head of the Islamic Revolutionary Guard Corps – Quds Force (IRGC-QF), Iraq's Abu Mahdi al-Muhandis, the deputy head of the Popular Mobilization Forces (PMF), and several others were killed in a U.S. missile strike near Iraq's Baghdad International Airport. We assess that the deaths of Suleimani and al-Muhandis in particular are highly likely to provoke a response from Iran and its allies, which could include a pattern of retaliatory asymmetric measures executed by Iranian military assets and their allied militias against U.S. and partner government and business interests regionally, in the Middle East.

Key Judgments

- We anticipate a measured but direct response from Iran. We assess this is in part to help insulate the Iranian ruling regime, which is deeply concerned with remaining in power and hesitant to engage the U.S. in a direct military confrontation. Despite our expectation for a measured response from the ruling regime, we believe that Iranian proxies will likely retaliate more aggressively in the region.

- Iran possesses highly capable cyber operational forces, and we believe the most likely targets of cyberattacks remain the United States and partner government, military, and commercial interests within the Middle East.
- Based on our observations of chatter among hacktivist forces (which we define as pro-regime but not government directed), we assess that attacks are likely to escalate against softer targets, such as loosely protected websites, servers, and databases.
- Recent documented instances of Russian state-sponsored groups hijacking and utilizing Iranian infrastructure for cyber operations could cause increased uncertainty and confusion for victims attempting to attribute cyber activities. It is less clear today whether operations using known and tracked Iranian cyber infrastructure are actually being run and directed by the Iranian government. This raises the potential for misattribution and mistaken escalation because we do not know the extent to which Russia has compromised Iranian cyber operational infrastructure.

Background

Late in the evening on January 2, 2020 ET, press reporting revealed that a U.S. missile strike had occurred near Iraq's Baghdad International Airport. The airstrike killed several people, including Qassem Suleimani, the head of Iran's Islamic Revolutionary Guard Corps – Quds Force (IRGC-QF), and Abu Mahdi al-Muhandis, the deputy head of an Iraqi militia called the Popular Mobilization Forces (PMF). Among those reportedly killed were several other representatives from the PMF, including Mohammed Ridha Jabri, the group's public relations chief. A statement from the U.S. Department of Defense, as well as press reports from Iranian government outlets, confirmed the strike and that Suleimani was the target of the attack.

Threat Analysis

Insikt Group assesses that the death of Suleimani in particular will likely provoke a response from the Iranian government, including multiple scenarios involving retaliatory asymmetric measures executed by Iranian military assets, proxies, or their allied militias against U.S. government and business interests in the Middle East, as well as U.S. regional partners, such as Saudi Arabia, the United Arab Emirates (UAE), and Israel.

As of this writing, Recorded Future has observed a unanimous response by Iranian military, diplomatic, and political leaders that a retaliatory attack will take place, although such statements did not include any specifics as to when, how, and where a response will occur. Iran's Supreme Leader Ali Khamenei declared on January 3, 2020, that a "harsh revenge" awaited those who led the strike against Suleimani and initiated three days of national mourning to commemorate the fallen IRGC-QF Commander. On January 5, the military advisor to Iran's Supreme Leader, Major General Hossein Dehghan, stated that Iran's response would "for sure be military" and directed against U.S. "military sites."

Reading the Need to Retaliate

Over the past few years, General Soleimani has reportedly enjoyed widespread domestic support, due in part to the notion that he was responsible for the strategies that shielded the country from terrorist attacks and threats posed by the Islamic State (IS) group. Several reports

have suggested that Soleimani's death has led to a distinct call for retaliation, which is uncommon in recent Iranian military history, except in cases where extreme acts of violence have impacted government or Iranian military personnel. Examples of this include the June 2017 IS attack against the Iranian parliament, and the August 2017 beheading of an IRGC officer, Mohsen Hojaji, by IS. The former led to a ballistic missile attack against IS, while the IRGC officer Hojaji became a symbol in the fight against IS. At the time, Soleimani, among many senior IRGC officials, spearheaded the response to Hojaji's death.

One historic example which we believe depicts the more calculated approach that Iran is likely to pursue in response to Soleimani's death was the slaying of Iranian diplomats by the Afghan Taliban in 1998. In 1998, almost a dozen Iranian diplomats were killed by the Afghan Taliban, an incident that resulted in a popular outcry against the Taliban group and the mobilization of approximately 200,000 Iranian military forces. Research from the RAND Corporation depicted a pragmatic decision-making process within the Iranian government to deal with its Afghan crisis. Notwithstanding hardline interests from the IRGC and radical political fronts to engage militarily against their ideological nemesis, Supreme Leader Khamenei instead opted for a response "without the risk of war." Similarly, on January 5, 2020, IRGC general Hossein Dehgan, a top adviser to Khamenei, claimed that Iran would respond militarily to the killing of Soleimani, but would not seek war.

Insikt Group assesses that Iran is likely to pursue a measured asymmetric response, as it balances the need to offset the pressure of Soleimani's death without further fueling the potential for direct military engagement with the U.S.

Examples of Recent Asymmetric Retaliatory Attacks

Previous suspected retaliatory measures taken by Iran or Iranian-backed forces in the past include but are not limited to:

- Throughout 2019, the IRGC-QF was suspected of being behind the missile strike of Saudi Arabia's oil facilities in Abqaiq and Khurais, as well as the seizure and commandeering of the Swedish-owned oil tanker Stena Impero.
- Iran has been accused of using its influence with Shia groups to incite rebellion in locations known to be fertile grounds for sectarian and anti-government activity, such as Bahrain. This kind of influence likely motivated the violent protests held at the U.S. embassy in Iraq between December 31, 2019 and January 2, 2020. Reports suggest that these protests were executed by supporters of Kata'ib Hizballah, an Iranian-backed proxy force led by al-Muhandis.
- Iran has also been accused of supporting acts of sabotage against regional oil and gas infrastructure. Throughout 2019, reports have linked Iran to coordinated attacks with Yemeni allies, the Houthi rebels (Ansar Allah), to against Saudi Arabia's oil and gas infrastructure. In Bahrain, Iran purportedly supports a slew of Shia militia groups, and was allegedly linked to a high-profile attack on Bahraini oil and gas infrastructure in November 2017.

Iran has a number of highly capable computer network operations teams that may be involved in a response against the United States, regional partners, and Western interests. Recorded Future believes that previous accesses gained from espionage operations will very likely facilitate these

retaliatory actions. Most notably, Iranian teams have used a destructive cyber capability in prior escalations, which we assess demonstrates both a willingness and ability to deploy such malware in similar situations. Iranian actors are also known to favor web shells, password spraying, and a combination of custom and commodity malware to gain access to target environments. Despite the use of destructive malware in previous cyber response scenarios, the death of General Soleimani in a U.S. airstrike is a unique situation and injects significant uncertainty into our assessments regarding which cyber capabilities Iran will likely leverage against which regional U.S. and partner interests.

In June 2019, Recorded Future observed APT33 malware activity targeting U.S. industry, critical infrastructure, and government entities. Rapidly following this, on June 22, U.S. President Donald Trump stated that the administration used cyber strikes against Iran's missile systems amid heightened tensions in the Persian Gulf. Iran was also accused of placing limpet mines on a Japanese oil tanker in the Gulf, which fueled tension in the region. At that time, in June 2019, the U.S. Cybersecurity and Infrastructure Security Agency reported an increase in Iran-related actors deploying wiper malware to their targets; however, the NSA's Threat Operations Center technical director stated that Iranian actors were continuing normal intelligence-gathering operations focused on espionage, not destruction.

Previous Access and Tools May Tip Cyber Response

Recorded Future anticipates continued targeting of U.S. industry, critical infrastructure, and government entities by Iranian threat actors during this period of heightened tension. Although we assess that Iranian actors will continue to target domestic U.S. government, military, and commercial entities for cyberespionage purposes, organizations in the Persian Gulf region are at the greatest risk for destructive cyberattacks. Further, we judge that Iranian actors APT33, APT34 (also known as OilRig), or MUDDYWATER will also likely target United States allies and partners in the Middle East in cyberespionage operations. We anticipate the continued mixture of custom and commodity tooling, and recommend that organizations monitor for suspicious Powershell and WMIC-based behavior in particular.

- MUDDYWATER actors have used politically flavored spearfishing and macros, or stolen credentials, to drop malware and steal information. MUDDYWATER relies heavily on a Powershell-based backdoor called POWERSTATS. MUDDYWATER makes use of compromised third-party domains that are used as proxies to distribute POWERSTATS, and for command and control (C2) purposes.
- APT33 is one of the most active groups currently operating in the Middle East and has demonstrated an ability to continually revise its tactics and pursue a variety of tools and techniques to compromise its victims. The actor uses a wide range of tools in its custom malware toolkit, including POWERTON, while also relying heavily on open source remote access trojans (RATs), including njRAT, Powershell Empire, Nanocore, and PupyRAT.

- APT39 has primarily leveraged the Chafer and Remexi trojan families, targeting those in the telecommunications sector, with additional targeting of the travel industry and supporting IT firms. We assess that the group's primary focus on telecommunications and travel indicates an interest in both monitoring specific individuals and collecting proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities. Researchers from FireEye have noted that APT39 operations are similar to that of APT34 (OilRig) in terms of Middle East targeting patterns, infrastructure, and timing. More specifically, both APT39 and APT34 share the same malware distribution methods, infrastructure nomenclature, and targeting overlaps.
- The Lab Dookhtegan leaks showcased APT34's custom tooling: PoisonFrog, Glimpse, Hypershell, HighShell, Fox Panel, and Webmask. The PoisonFrog implant is a Powershell-based downloader that pulls down a VBS backdoor. Assessments from Chronicle and Palo Alto show that PoisonFrog is the BONDUPDATER backdoor, previously analyzed by FireEye, Booz Allen, and Palo Alto's Unit 42. Webmask is likely part of the DNSpionage DNS hijacking campaign disclosed by Cisco Talos.

We assess that previous credential-gathering activities conducted by APT33, APT34, and APT35 may be used to gain initial access to targeted environments. Notable recent events include:

- In October 2019, APT33 reportedly took special interest in industrial control system (ICS) hardware and software vendors in the United States and worldwide, conducting a focused password-spraying campaign against those organizations. The actors typically targeted between 50,000 to 70,000 organizations at a time, selecting a small number of credentials to attempt to gain access to each organization. The breadth of this targeting was curtailed significantly between October and November 2019, when APT33 purportedly targeted only around 2,000 organizations per month, attempting to use various password combinations on 18 to 20 accounts in each organization, a 900% increase. Commands used in password-spraying and on-host activity can be found in this GitHub.
- Similarly, FireEye also found APT34 using the credential-stealing malware families LONGWATCH, VALUEVAULT, and TONEDEAF in a targeted spearphishing campaign. These malware families largely sought to harvest credentials from targeted individuals. The actors used LinkedIn messages with malicious links to entice the victims to download a legitimate datasheet that used VBA macros to download the malware families.
- Data gathered from APT35 (Newscaster, PHOSPHORUS) credential harvesting via watering hole attacks, phishing emails, and fake social media profiles may also be leveraged. On October 4, 2019, Microsoft disclosed that, for 30 days from August to September 2019, APT35 was observed making 2,700 attempts to breach a U.S. presidential campaign, later identified as the Trump campaign, in addition to targeting current and former U.S. government officials, political journalists, and "prominent" Iranian expatriates. The group targeted 241 email accounts, and was successful in compromising four accounts that were not associated with U.S. government officials or the campaign.
- Previous access or information gleaned from DNS hijacking activity from SeaTurtle, and the DNSpionage/APT34 cluster may also facilitate further intelligence-gathering.

Destructive Malware

APT33 and APT34 have been linked to destructive malware attacks against the oil and gas sector, using Shamoon, DEADWOOD, and ZeroCleare.

- During a presentation at the CYBERWARCON conference in Arlington, VA in late 2019, Microsoft analysts discussed APT33 dropping a destructive malware family called DEADWOOD onto a VPN server in Saudi Arabia in June 2019. Recorded Future cannot provide insight into the malware family described by Microsoft. However, on June 22, 2019, a file uploaded to VirusTotal was flagged as being a wiper; it was later flagged by the user "THOR scanner" as a wiper used in the Middle East. It is likely that this file (857ef30bf15ea3da9b94092da78ef0fc) is the wiper in question.
- In 2012, APT33 deployed the destructive malware Shamoon, and is suspected along with other Iran-nexus APT groups to have participated in the December 2018 operation against Italian petrochemical contractor SAIPEM.
- In early December 2019, IBM's X-Force Incident Response and Intelligence Services (IRIS) published their discovery of the ZeroCleare wiper malware that was observed targeting energy and industrial sectors in the Middle East. According to IBM IRIS, APT34 (OilRig) was likely involved with ZeroCleare's deployment. During their discovery efforts, IBM IRIS researchers found that ZeroCleare shared characteristics with the Shamoon malware, specifically in that the ZeroCleare malware overwrites the master boot record (MBR) as well as the disk partitions on Windows machines.
- Analysis of a recent sample that called itself "Dustman" revealed similarities to ZeroCleare and contained anti-Saudi messaging, making use of the same raw disk driver; however, the sample had all of the tooling needed bundled into a single executable. The sample contained anti-Saudi messaging, and dropped an anti-Saudi mutex ("Down With Bin Salman").

Nationalistic and Pro-Regime Hacktivism

We assess that the Iranian regime will likely take its time contemplating a response to the killing of General Suleimani. In stark contrast, pro-regime (but not government-directed) cyber actors will likely continue to conduct disruptive activity. Recorded Future is aware of hacktivist defacement activity occurring within hours of the news breaking of Suleimani's death, including against U.S. government institutions. Further, we also observed the distribution of disinformation among IRGC supporters. Based on our observations of chatter among hacktivist forces, we assess that attacks are likely to escalate against softer targets, such as loosely protected websites, servers, and databases.

It is not outside the realm of possibility for actors to deploy SamSam ransomware or similar campaigns under the guise of criminal activity. While there is no evidence to suggest that the two actors were affiliated with the Iranian government, Tehran is undoubtedly aware of those operations and their tools.

Outlook

We assess that Iran may exercise a response to the killing of General Qassem Suleimani that will more aggressively rely on cyberattacks rather than kinetic ones, which will likely take the form of espionage or sabotage.

This cyber response — likely one of several potential asymmetric countermeasures — may be carried out directly by Iranian intelligence or military groups, by their contractors, or by other proxies. These measures will very likely be fueled by previous accesses and information gained from espionage operations. Attributing these intrusions and distinguishing them from other opportunistic intrusions will likely prove difficult.

Further, the recent documented instances of Russian state-sponsored groups hijacking and utilizing Iranian infrastructure for cyber operations have injected further uncertainty into tracking and attributing Iranian espionage or destructive activities. We assess that this infrastructure hijacking and increased uncertainty raises the potential that an incident could be misattributed and mistakenly be interpreted as an escalation. There are more sides with interests in the Middle East than just the U.S. and its partners and Iran and its proxies; the injection of further uncertainty via Russian operations masquerading as Iranian could contribute to an atmosphere of chaos or confusion in the wake of a cyber intrusion. This raises the potential for misattribution and mistaken escalation because we do not know the extent to which Russia has compromised Iranian cyber operational infrastructure.

Suggested Mitigations

- APT33 continues to favor dynamic DNS (DDNS) hosting; Recorded Future's Weaponized Domains Security Control Feed can be used to identify and block these domains.
- Recorded Future proactively detects and logs malicious server configurations in the Command and Control Security Control Feed.
- Recorded Future recommends that organizations monitor for sequential login attempts from the same IP against different accounts. This type of activity is more difficult to detect than traditional brute forcing, but will help insulate organizations from a favored tactic used by APT33.
- The introduction of multi-factor authentication has proven to be a highly effective mitigation practice for many organizations that have historically experienced a high level of credential stuffing and password-spraying attacks.
- Monitor criminal underground communities for the availability of new configuration files targeting your organization, acquire those files, and thoroughly analyze them for additional attack indicators.
- End users can reduce the risk of being victimized by password spraying by using a password manager and setting a unique strong password for each online account.
- Social engineering training for company employees can help mitigate threats posed to the organization by disclosure of information used to conduct password spraying and attacks.
- Log analysis (through an IDS) can aid in the identification of unsuccessful login attempts across multiple user accounts. Cross-referencing log data may help to detect incidents involving high-frequency lockouts, unsanctioned remote access attempts, temporal attack overlaps across multiple user accounts, and fingerprint unique web browser agent information.