INTSIGHTS
Defend Forward™

Threat Brief:
Iranian Cyber Warfare

www.intsights.com

INTRODUCTION

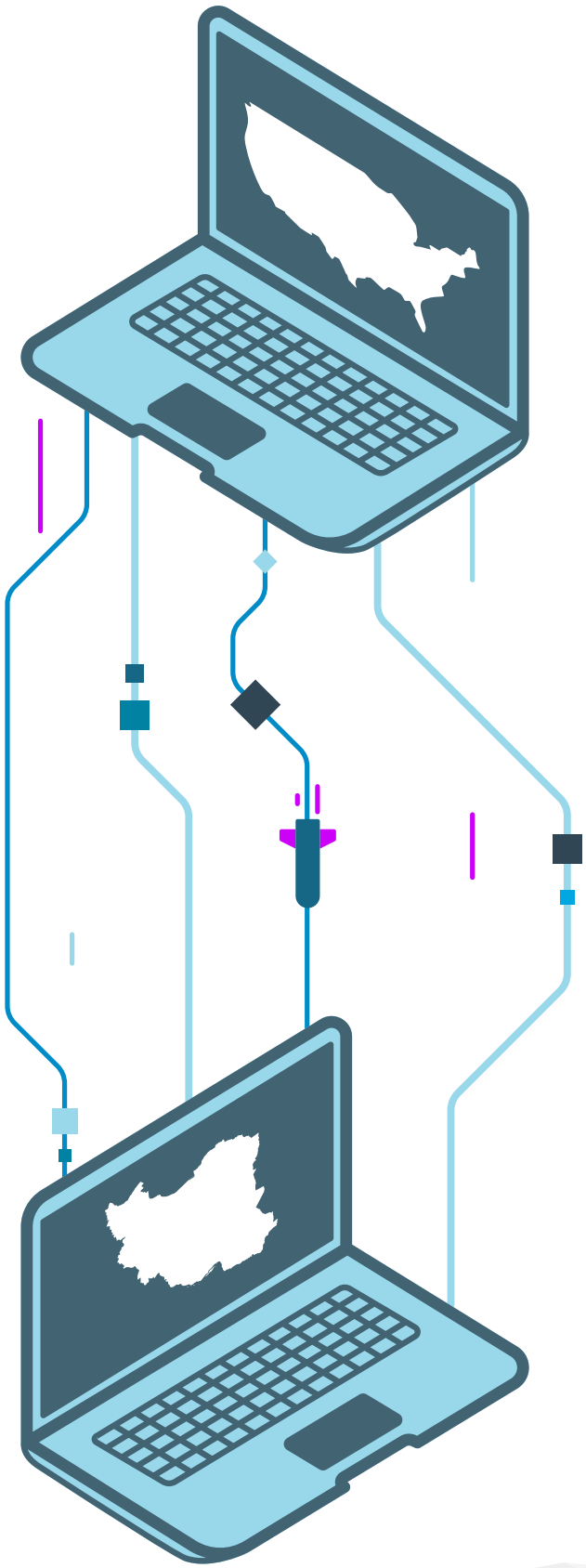
Tensions are escalating between Iran, the United States, and U.S. allies. Iran has sworn revenge for the recent U.S. assassination of a top military official, General Qasam Soleimani, and carried out a targeted missile attack. It is highly likely that Iran will retaliate with a cyberattack on U.S. and allied entities. However, Iran has not advanced its tactics, techniques, and procedures significantly over the last year, and it is highly unlikely that it will reveal anything new or groundbreaking in the weeks to come. Most U.S. organizations have already been monitoring and defending against Iranian advanced persistent threat (APT) groups for years. Now is not the time to panic about an impending attack.

With that said, this is a good opportunity to assess whether your organization is a likely target of Iranian state-sponsored cyber operations, and determine if your team is ready and trained to respond. Now is the time to:

1. **Know your enemy.** This threat brief provides a background and overview of Iranian cyber threats, tactics, preferred targets, and motivations.

2. **Defend against the threat.** Armed with Iran's known tactics, hacking tools, and indicators of compromise in this report, you are better able to identify an attack when it happens, shut it down, and determine motives.

3. **Prepare your security teams for incident response.** If you do not have procedures in place, now is the time to create step-by-step processes for responding to cyber incidents. Document everything, train your SOC and Incident Response teams on their roles, and practice it repeatedly. This will ensure a calm and effective response to sophisticated state-sponsored attacks.



BACKGROUND

Iran's cyber program has advanced dramatically over the past five years but has not changed course or mission from its original purpose: aggressively defending the Islamic Republic of Iran and protecting the Iranian regime. Several APTs have been identified working directly for the regime, but independent hacktivists and hacker groups have also taken credit for cyberattacks on Iranian adversaries and private companies worldwide. Hacker culture in Iran is gradually being forced into submission by the regime through increasingly controlled infrastructure and internet laws, and recruitment to state-sponsored cyber warfare groups.

Iranian cyber operations are undergoing drastic changes to infrastructure and organization as a result of recent disclosures. A recent campaign shows that Iran has pivoted to social media and "psychological operations" to influence Westerners against Israel and the United States, and in favor of Iran. This new tactic may indicate an effort to mimic successful Russian cyber-psychological warfare. Although this is a new tactic for Iran, it is a behavior that can be detected through close monitoring of known Iranian social media accounts and alerting on suspicious accounts that may target your organization and its VIPs. The following is an overview of Iran's cyber capabilities, threat actors, and recent campaigns.

GEOPOLITICAL CONFLICT

Iran's cyber warfare strategy has revolved around power struggles in the Middle East, strategic intelligence that will help the country influence decisions, and retaliation against dissidents and adversaries for political and economic damage. The latter of these objectives has led to several known conflicts with organizations in adversarial nations, like Israel and the United States. Over the years, Iran has expanded its strategic goals to include offensive cyberattacks on other nations, espionage on other governments and militaries, and destructive hacking of private organizations.

Recent violent escalations between the United States and Iran have prompted grave concern worldwide. In April 2019, President Trump designated all Iranian Revolutionary Guard Corps (IRGC) as a foreign terrorist organization, which has widespread implications including economic and travel bans. On May 8, 2019, Mr. Trump announced that the United States was withdrawing from the Iran Nuclear Deal (adopted by President Obama in 2015) and would pose new economic sanctions against the regime. After Mr. Trump's announcement, Iran's Supreme National Security Council designated the United States Central Command (CENTCOM), which oversees American military operations in the Middle East, as a terrorist organization.

On January 3, 2020, President Trump ordered the assassination of General Qasam Soleimani (قاسم سلیمانی), Iran's highest-ranking IRGC leader and commander of the Quds Forces (the equivalent of the U.S. CIA). U.S. forces killed Soleimani in a rocket attack on his vehicle as it was leaving Baghdad Airport in Iraq. The event has been a catalyst for mass grieving and counter-U.S. protests throughout the Middle East and Muslim world.

In the past, U.S. presidents have been hesitant to take such drastic actions against Iran for fear of potential violent retaliation toward U.S. and allied presence in the Middle East. Current concerns revolve around both physical violence and cyberattacks, as Iran's leadership and Soleimani's family have sworn to take grave revenge against the U.S. and Israel.

DARK WEB INTELLIGENCE

In April and May of 2019, several individuals released secret documents from the Iranian Ministry of Intelligence to open sources such as Telegram and dark web forums. This information has caused great damage and likely postponed or delayed Iranian cyber operations. Much of the disclosed information details a previously unknown Iranian state-sponsored cyber operation dubbed "Rana." Additionally, someone by the pseudonym "Lab Dookhtegan" disclosed secrets around attack tools used by APT34, or "Oilrig" (Figure 1).

It is possible that Lab Dookhtegan was a former member of APT34. They claim to have access to APT34's servers and released these TTPs in a file called "Poison Frog" (Figure 2), which includes access to a server-side module that is the c2 made in node.js and an agent that is the payload in Powershell.

The disclosures detail a target list that includes 97 organizations across 27 countries. These include government, media, energy, transportation, logistics, and technology service providers. Most of the targets are in the Middle East region. Two other actors that go by the names of GreenLeakers and Revealer are also credited for leaking valuable intelligence about other Iran cyber operations, including a new group dubbed "MuddyWater" or "BlackWater" (Figure 3).

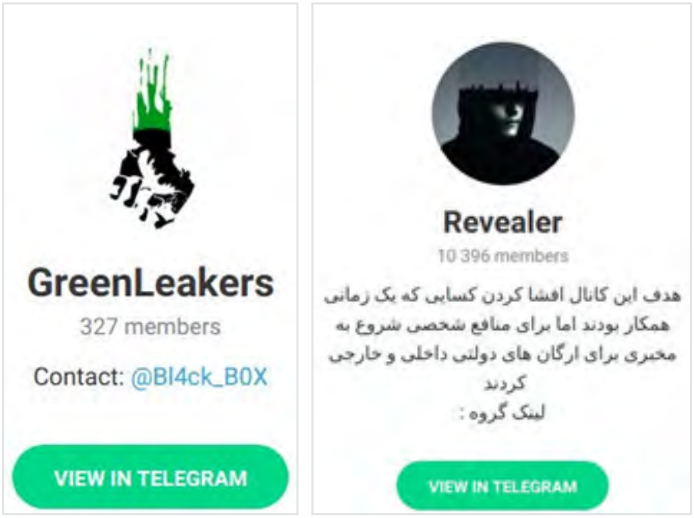


Figure 3: Screenshots of the official GreenLeakers and Revealer Telegram profiles

Figure 1: Screenshots of Lab Dookhtegan Telegram profile and posts

Figure 2: Poison Frog Disclosure

ADVANCED PERSISTENT THREAT GROUPS

APT33

APT33, also known as "Elfin Espionage group," began operating around 2015. Their primary focus is U.S. and Saudi Arabian targets (Figure 4).

This group specializes in scanning for vulnerable websites and then using the websites to identify potential targets, either for attacks or creation of command and control (C&C) infrastructure. APT33 is known to use custom malware, commodity malware, and publicly available hacking tools. It has compromised government, research, chemical, engineering, manufacturing, consulting, finance, telecom, and several other types of organizations.

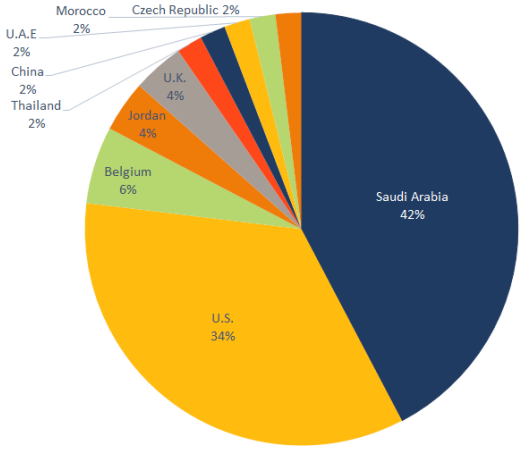


Figure 4: APT33 targets by country, 2016-2019
Source: Symantec

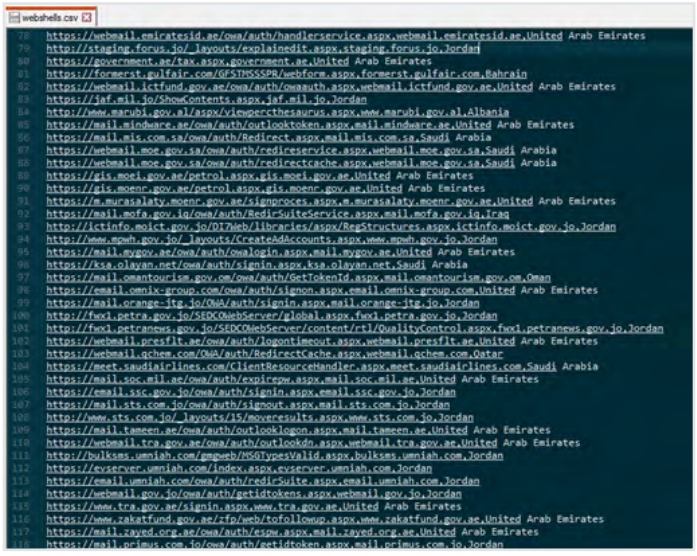


Figure 5: List of webshell targets

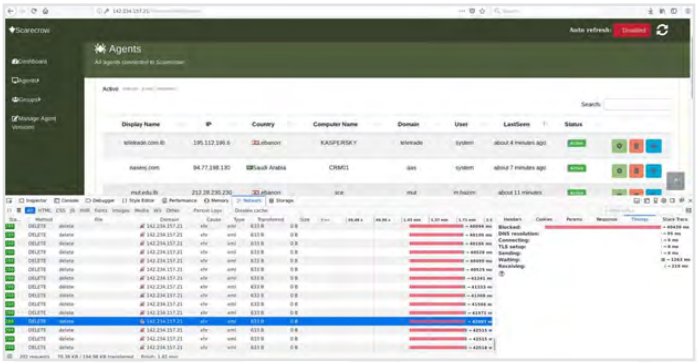


Figure 6: APT34 hacking tool dashboards and servers

APT34

APT34, or "OILRIG," is one of the most well-known and established Iranian APT groups. OILRIG became active around 2015 and is one of the most sophisticated Iranian threat groups. It is known to conduct supply chain attacks, leveraging the relationship between organizations to attack their primary targets. OILRIG's primary targets are in the Middle East, including the financial, government, energy, chemical, and telecommunications sectors. New disclosures of classified documents have revealed six different attack tools that this group uses: Glimpse, PoisonFrog, HyperShell, HighShell, FoxTunnel, and Webmask (the main tool behind DNSpionage). These hack tools do not have a reputation of being high-value, sophisticated tools. It is likely that APT34 will pivot to new, more advanced tools following the disclosure. In addition to the source code for these tools, past campaign artifacts were also revealed. One image (Figure 5) shows a list of target domains where the group has deployed webshell.

The recent disclosure by "Dookhtegan" could temporarily disable APT34 and prompt it to reorganize. "Dookhtegan" also claims that it has access to APT34 hacking tool control panels and internal servers and has threatened to destroy them (Figure 6).

APT35

APT35, also known as "Newscaster Team;" "Phosphorus;" "Ajax Security Team;" and "Charming Kitten;" conducts long-term cyber operations to collect strategic intelligence. APT35 typically targets U.S. and Middle Eastern military, diplomatic, and government personnel, organizations in the media and entertainment, energy, and defense industries, as well as engineering, business services, and telecommunications sectors. APT35 is highly skilled at social engineering and is known to target victims' personal accounts, set up fake social profiles, and convince victims to divulge sensitive information and download malicious files. The group is known for several major hacks, including a 2017 attack on HBO that led to the leaking of 1.5 TB of data including staff contacts, account credentials, financial data, and unaired episodes of "Game of Thrones." In March 2019, the group used spoofed websites of well-known companies, including Microsoft and Yahoo, to conduct cyber espionage against multiple organizations. Microsoft responded with a court order to have the sites sinkholed. Microsoft is now using the sinkholed sites to gather intelligence on the functions of the spoofed sites.

APT39

APT39 sets itself apart with a mission unlike the others: widespread theft of personal credentials. APT39 focuses on personal information to support surveillance operations that serve Iran's national priorities. It uses the personal information to create additional accesses to enable future campaigns. Past campaigns have been observed targeting telecommunications and travel industries, which is a strong indicator that the group is conducting surveillance operations against specific individuals, such as dignitaries and organizational leadership. While APT39's targeting scope is global, its activities are concentrated in the Middle East.

HACKTIVISTS

Hacktivism has had an active place in the Iranian cyber landscape over the years. Some notable names include Shield Iran, Iran Cyber Security Group Hackers, r3dm0v3, Cair3x, HUrr!c4nE!, Sun, and Tapandegan (Palpitaters). On January 4, 2020, a threat group that refers to itself as "Iran Cyber Security Group Hackers" conducted a defacement attack on the Federal Depository Library Program website, a little-known entity of the U.S. government (Figure 7).

The group claimed to be working on behalf of Iran in retaliation for Soleimani's death. It is highly unlikely that the group operates on behalf of the Iranian state. The low-level attack and the lack of technical sophistication indicate the group is a hacktivist venture. Furthermore, the low-profile target may indicate that the group did not have other means to target higher-level targets.

Most Iranian hacktivists advocate anti-U.S., anti-Saudi, anti-Israeli, and pro-Palestinian causes, as well as supporting specific U.S. policies favorable to Iran, such as the U.S.-Iran nuclear deal (JCPOA). Over the years, however, the Iranian regime has recruited local hacktivists and independent hacking teams into the ranks of the most notorious Iranian APT groups in order to control the narrative being presented and make more strategic moves in cyber warfare.

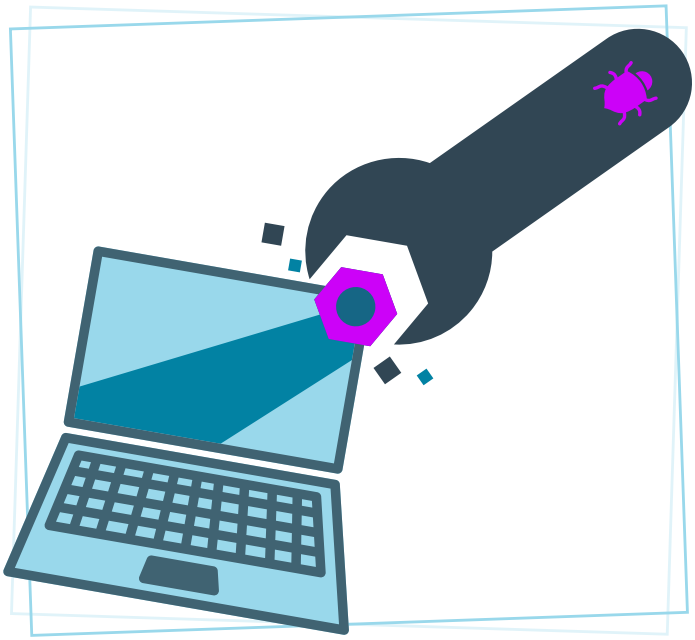
Figure 7: www.fdlp.gov defaced by Iranian hacktivists

RECENT HACKING TOOLS

ZeroCleare – A destructive wiper malware discovered targeting the energy and industrial sectors in the Middle East in late 2019. It is named after the program database (PDB) pathname of its binary file and bears similarities to Shamoon malware. ZeroCleare is attributed to Iranian state-sponsored threats by IBM X-Force.

Shamoon – A notorious destructive wiper malware used against Saudi national oil company Aramco and Qatar's RasGas in 2012. The attack wiped data from over 35,000 computers at Saudi Aramco alone. In 2018, following a Shamoon Version 3 attack on an Italian oil company, McAfee reported that they attributed the malware to Iranian state-sponsored APT33.

Other tools attributed to Iranian state-sponsored activity include **Nautilus and Neuron**, which were reportedly stolen and used by Turla Group, an allegedly Russian APT group. Further details on tools can be found at the MITRE ATT&CK framework website.



RECOMMENDATIONS

IntSights recommends a comprehensive approach to defending against Iranian cyber threats, including the following:

1. **Maintain awareness of Iranian tactics, techniques, and procedures through cyber threat intelligence (CTI).** Ensure that your CTI team is alerted to any new developments or threats from Iranian forces to your industry or organization. Clear, deep, and dark web intelligence proves valuable to analyze new emerging threats.

2. **Update your defense mechanisms with indicators of compromise (IOCs) from past Iranian cyberattacks.** This should include common hacking tools and malware, such as Shamoon, ZeroCleare, and recent cases of account takeovers (ATO) and phishing. Attached to this report is an appendix that lists recent indicators of compromise for Iranian cyber threats. We recommend utilizing these tactically for internal threat monitoring. New indicators of compromise can be found in malware intelligence forums.

3. **Map your attack surface to Iranian threats using intelligence frameworks,** such as MITRE ATT&CK. Each cyber threat group has a specific mission, target, tactics, and history. By identifying where your organization lands on each group's target map, you can effectively focus your defenses and intelligence collection on those tactics and tools most likely to affect your organization, employees, customers, and third parties

4. **Prepare your security teams for a worst-case scenario,** ensure your teams are prepared to:
   - Identify a cyberattack and alert key stakeholders
   - Know the incident response processes and steps to take to stop the attack
   - Practice incident response to ensure your teams can remain calm and rational during the stressful moments

CONCLUSION

Iran has prioritized cyber warfare operations as a vital part of its strategic military plan. Iranian APTs are advancing their tactics, techniques, and procedures at a rapid pace; adopting new methods; developing native custom malware; and pivoting to strategic targets. They have been very successful in the past, and are expected to continue to pursue and develop future operations as they are fueled by ideology and revenge. Although recent disclosures have exposed many of their operations and tactics, they are expected to make a full recovery and continue operating on behalf of the Iranian regime in order to advance the objectives of the state. Utilize IntSights external threat intelligence and monitoring to maintain up-to-date indicators of compromise, tactics, and techniques, and dark web monitoring of emerging Iranian threats.

Keep track of known Iranian IOCs by using our Appendix.

Iranian IOCs Appendix

ABOUT INTSIGHTS

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

To see the IntSights External Threat Protection Suite of solutions in action, **schedule a demo today.**