Iranian State-Sponsored and Aligned Attacks: What You Need to Know and Steps to Protect Yourself | Proofpoint US

Published: 2020-01-10 · Archived: 2026-04-05 13:09:30 UTC

January 10, 2020

Recent events have led to a surge in concern about possible cyberattacks coming out of Iran. Below are the Proofpoint Threat Research team's latest findings on state-sponsored and aligned Iranian attacks, details on 11 Iranian attack groups and their preferred tactics, and most importantly, security recommendations.

Iranian Threat Actors: Operation Trends and Our Recent Findings

Iranian cyberattack capability first came on the world stage around 2013, three years after the Stuxnet attack. State-sponsored and aligned attackers have been an ongoing threat and have targeted governments, organizations, and citizens around the world with significant impacts.

Proofpoint's Threat Research team is continuing to see activity that is consistent with the campaigns that were started in early December 2019. Based on past actions by Iranian threat actors, it is unlikely that new activity will happen immediately as they are often very methodical and are known to be deliberate over time.

While we cannot predict the likelihood of increased attacks or what they might look like, it is valuable to examine previous attacks to better understand these threat actors. Historical data shows that this is not a threat to be taken lightly. Iranian attackers may not be as well-known as those from other countries, but they've successfully carried out many operations over the years, sometimes with significant, even devastating effects.

Iranian attack groups mostly operate below the radar of major news coverage (with the exception of the Shamoon attacks). This is due to the methodical nature of their work and their ability to avoid causing major headline-grabbing incidents. They choose their targets carefully and infiltrate them slowly, frequently silently, for reconnaissance, espionage, or later attacks. These groups often specifically harvest credentials and hold them over time for maximum damage. This means Iranian attacks could already have information and a presence on target networks that could be mobilized in new attacks.

Iranian attackers target not just the United States, Israel, and Saudi Arabia: they operate on a truly global scale. And while government and military targets are obvious ones, they also pursue telecommunications companies, finance organizations, human rights groups, and even academia. Worldwide organizations, across many sectors, should take this potential threat seriously.

11 Iranian Threat Actor Groups and Their Tactics

Below, you'll find information on major Iranian threat actor groups, the industries and countries and regions they've been known to target, and an overview of their tactics. This list includes information from MITRE's ATT&CK framework on threat actor groups, publicly available information, and Proofpoint's threat research.

Iranian Attack Groups

1. APT 33/Elfin: A group that since 2013 has been targeting aviation, energy, government, health care, and transportation sectors in Saudi Arabia, South Korea, and the United States. Some believe this group is responsible for the Shamoon attacks. Proofpoint tracks this group as TA451 and they have been active as recently as December 2019.
2. APT 39/Chafer: A group that since 2014 has been targeting government, telecommunications, and travel sectors to collect personal information. Proofpoint tracks this group as TA454 and they have been active as recently as June 2019.
3. Charming Kitten: A group that since 2014 has been targeting individuals in academic research, government, human rights groups, media, military, and technology sectors in Iran, the United States, Israel, and the United Kingdom by gaining access to personal email and Facebook accounts. Proofpoint tracks this group as TA453 and they have been active as recently as September 2019.
4. Cleaver: A group or operation that was first tracked in 2014 targeting aviation, energy, military, transportation, health care, and utilities sectors in China, France, Germany, India, Israel, Saudi Arabia, and the United States. They are believed to have used fake LinkedIn accounts as part of their attacks.
5. CopyKittens: A group that since 2013 has been targeting users in Germany, Jordan, Turkey, Saudi Arabia, and the United States.
6. Group5 (Suspected): Attribution to Iran is not definitive but this group has targeted individuals connected to the Syrian opposition with malware through spearphishing and watering hole attacks.
7. LeafMiner: A group that since 2017 has targeted the email of individuals in government and businesses in the Middle East.
8. Magic Hound: A group that since 2014 has targeted the energy, government, and technology sectors in Saudi Arabia.
9. MuddyWater: A group that since 2017 has targeted the energy, government, media, and telecommunications sectors in Europe, the Middle East, and North America. Proofpoint tracks this group as TA450 and they have been active as recently as January 2020.
10. OilRig: A group that since 2014 has targeted the aviation, energy, financial, government, media, technology, telecommunications, and transportation sectors in the Middle East. Proofpoint tracks this group as TA452 and they have been active as recently as December 2019.
11. Silent Librarian/Cobalt Dickens: Silent Librarian is a group that since 2013 has targeted universities around the world. Proofpoint tracks this group as TA407. A related group known as Cobalt Dickens has targeted construction, media, health care, higher education/academia, health care, and transportation sectors. Proofpoint tracks this group as TA4900. These groups were active as recently as December 2019 and September 2019 respectively.

Industries Targeted by Iranian Attack Groups

- Government: APT 33/Elfin, APT 39/Chafer, Charming Kitten, LeafMiner, Magic Hound, MuddyWater, OilRig
- Energy: APT 33/Elfin, Cleaver, Magic Hound, MuddyWater, OilRig
- Media: Charming Kitten, MuddyWater, OilRig, Silent Librarian/Cobalt Dickens
- Telecommunications: APT 39/Chafer, MuddyWater, OilRig

- Aviation: APT 33/Elfin, Cleaver, OilRig
- Health Care: APT 33/Elfin, Cleaver, Silent Librarian/Cobalt Dickens
- Technology: Charming Kitten, Magic Hound, OilRig
- Transportation: APT 33/Elfin, Cleaver, OilRig, Silent Librarian/Cobalt Dickens
- Construction: Silent Librarian/Cobalt Dickens
- Higher Education/Academia: Charming Kitten, Silent Librarian/Cobalt Dickens
- Military: Charming Kitten, Cleaver
- Financial: OilRig
- Human Rights Groups: Charming Kitten
- Travel: APT 39/Chafer
- Utilities: Cleaver

Countries and Regions Targeted by Iranian Attackers

- Saudi Arabia: APT 33/Elfin, Cleaver, CopyKittens, Magic Hound, OilRig
- United States: APT 33/Elfin, Charming Kitten, Cleaver, CopyKittens
- Israel: Charming Kitten, Cleaver, CopyKittens
- China: Cleaver
- France: Cleaver
- Germany: Cleaver, CopyKittens
- India: Cleaver
- Iran: Charming Kitten
- Jordan: CopyKittens:
- South Korea: APT 33/Elfin
- Turkey: CopyKittens
- United Kingdom: Charming Kitten
- European Union: MuddyWater
- Middle East: LeafMiner, MuddyWater, OilRig
- North America: LeafMiner, MuddyWater

Tactics Favored by Iranian Attackers

- Stolen Credentials: APT 33/Elfin, APT 39/Chafer, Magic Hound, MuddyWater, OilRig, Silent Librarian
- Email Infiltration: Charming Kitten, LeafMiner, Magic Hound, Silent Librarian
- Malware: CopyKittens, Group5, Magic Hound
- Personal Information Gathering: Charming Kitten
- Social Media Targeting: : Charming Kitten, Cleaver
- Phishing: Group5, Magic Hound, Silent Librarian
- Watering Hole Attacks: Group5

Security Recommendations

Sophisticated Iranian state-sponsored and affiliate threats require careful focus internally and externally (in partnership with vendors, suppliers, and others) to improve the overall security posture of an organization—an

elementary approach isn't going to be enough. An immediate and effective action you can take to help protect your organization is mitigating the effects of stolen credentials, particularly those with administrative privileges. Some organizations should consider forcing password resets, including for service accounts.

Be sure to reduce your attack surface, complete security program updates, and make sure employees are trained to identify possible threats. Watch what's coming in and out of the network, and watch what employees are clicking on, opening, and distributing with the company. The smaller the surface, the harder it is for attackers to do anything. Make sure systems are patched because open source tools are available to anyone. We've seen APT groups use public vulnerabilities when they are released because it's low hanging fruit.

And finally, work actively with security leadership to implement a response plan that involves not just your organization but also your employees, vendors, and partners.

Subscribe to the Proofpoint Blog
