Office of External Affairs

Cyber and Emerging Threats Spot Report

June 23, 2025

Open-Source Review of Iranian Cyber Threats

Iran has emerged as a significant cyber threat actor over the past two decades, developing asymmetric capabilities in cyberspace as a counterbalance to its conventional military limitations. Iran's cyber warfare program has evolved from rudimentary defacements to highly targeted operations. This Spot Report provides an open-source overview of Iran's cyber capabilities, notable incidents, threat actor groups, and the current state of the Iranian cyber threat based on publicly available sources.

Historical Evolution of Iranian Cyber Capabilities

Early Activity (2000s–2010)

- Operation Cleaver (2009–2014): Attributed to the Iranian group "Cleaver" (also known as APT33), this campaign targeted critical infrastructure worldwide, including aviation and energy sectors.
  Source: Defense News, "Iranian Hackers Infiltrated Airlines, Energy, Defense Firms," 2014
- Stuxnet Fallout (2010): The U.S.-Israeli cyberattack on Iran's Natanz nuclear facility using the Stuxnet worm reportedly spurred Iran to invest heavily in cyber capabilities as a form of retaliation and self-defense.
  Source: The New York Times, "Obama Order Sped Up Wave of Cyberattacks Against Iran", 2012

2011–2015: Retaliation and Expansion

- Shamoon (2012): The destructive malware attack on Saudi Aramco erased data on over 30,000 machines. While direct attribution to Iran remains circumstantial, U.S. officials have long suggested Iranian involvement as retaliation against Gulf adversaries.
  Source: The New York Times, "Cyberattack on Saudi Oil Firm Disquiets US."
- DDoS Attacks on U.S. Banks (2011–2013): A group widely believed to be Iranian-backed, disrupted online services of major U.S. banks in retaliation for sanctions, and purportedly also accessed a dam in New York.
  Source: Politico, "US Indicts Iranians in Cyber Attacks"

3. Key Iranian Threat Actors

APT33 (Elfin)

- Focuses on aerospace, defense, and petrochemical industries.

FEMA

- Known for campaigns involving spear-phishing and malware like DropShot and TurnedUp.
- MITRE Assessment
- CrowdStrike Assessment

APT34 (OilRig)

- Conducts cyber-espionage primarily in the Middle East.
- Uses custom tools such as PowBAT and BONDUPDATER.
- MITRE Assessment
- CrowdStrike Assessment

APT35 (Charming Kitten/Phosphorus)

- Targets academics, journalists, and dissidents.
- Notorious for phishing operations and impersonating journalists or think tanks.
- MITRE Assessment

APT42 (UNC788):

- Identified by Mandiant in 2022 as a cyberespionage arm of the IRGC.
- Highly targeted attacks on healthcare, academia, and government sectors.
  Source: Mandiant, "APT42: Crooked Charms, Cons and Compromises," 2022
- Mitre Assessment

4. The Current Threat Landscape

Recent Cyber Incidents

- Cyberattack on Israeli made PLCs targeting water and gas infrastructure.
  Source: Wired, "CyberAv3ngers Hacking Water and Gas Industrial Systems," 2025
- Ransomware-as-a-cover operations: Iran has increasingly used ransomware tactics to mask espionage or sabotage efforts.
  Source: CrowdStrike 2024 Global Threat Report
- Attacks on U.S. Infrastructure (2024): The FBI warned of Iranian attempts to breach U.S. ports and logistics firms using the Botnet infrastructure built from compromised routers.
  Source: The Hacker News, "US and Allies Warn of Iranian Cyber Attacks," 2024

5. Tactics, Techniques, and Procedures (TTPs)

Iranian groups frequently rely on:

- Credential harvesting and phishing.
- Webshells and PowerShell-based backdoors.
- Destructive malware (e.g., Shamoon, Dustman, ZeroCleare).
- Exploitation of unpatched VPNs and Microsoft Exchange vulnerabilities.
- Social engineering via LinkedIn and WhatsApp.

Iran also favors long dwell times, establishing persistent access to networks before acting.

Source: CrowdStrike 2024 Global Threat Report

Conclusion

Iran's cyber warfare program has grown significantly in scope and sophistication over the past two decades. While it remains behind top-tier adversaries in raw capability, Iran's willingness to conduct disruptive and politically motivated operations makes it a volatile and persistent cyber threat actor.