CYBERWARFARE: A SPECIAL REPORT ON IRANIAN CYBER THREAT

January 2020

TABLE OF CONTENT

703.786.8884

sales@appguard.us

www.appguard.us

Cyberwarfare: A Special Report on Iranian Cyber Threat

Threat Timeline

On 3 January 2020, the United States assassinated General Qassim Suleimani, head of the Islamic Revolutionary Guards Corps (IRGC). A Pentagon statement said, "General Suleimani was actively developing plans to attack American diplomats and service members in Iraq and throughout the region. This strike was aimed at deterring future Iranian attack plans."

The death of Suleimani led to increased tensions between the U.S and Iran. This could potentially cause wide-scale cyber-attacks by Iran and its proxies against the United States.

On 4 January 2020, hackers claiming to be linked with Iran targeted the website of the U.S. Federal Depository. The new page displayed images of Iran's supreme leader, Ayatollah Ali Khamenei, the Iranian flag, and a promise of revenge against the United States. With escalating tensions between Tehran and the United States, this attack was not a surprise.

On 6 January 2020, the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security (DHS), offered insights into how Iran could potentially launch cyberattacks against the U.S and its allies and harm critical infrastructure.

On 7 January 2020, the U.S. Army issued a warning about "fraudulent text messages," telling people they have been selected for a military draft. The texts falsely advise recipients to "report to the nearest branch" and warn that the recipient would be "fined and sent to jail for a minimum of 6 years" if they don't comply.

On 9 January 2020, industrial control system security firm Dragos detailed a broad campaign of so-called password-spraying attacks that it tracked and attributed to a group of hackers known as APT33, Refined Kitten, or Elfin, and has previously been linked to Iran.

Iranian Threat Analysis

Iran Sponsored Cyber Activities

Iran and its sympathizers have a history of leveraging cyber-attacks to cause information warfare, disruption, espionage, intellectual property theft, and more.

- **Disruptive and destructive cyber operations** against strategic finance, energy and telecommunications organizations, and other high-value targets.
- **Espionage and intellectual property theft** targeting a variety of industries and organizations to enable a better understanding of strategic direction and policymaking.
- **Information warfare** promoting pro-Iranian narratives and anti-U.S. sentiments.

Past Iranian Cyber Attacks

Cyber theft campaign on behalf of the IRGC: A series of thefts targeted academic institutions, intellectual property data, and email account credentials. Between 2014 and 2017, the attacks targeted 144 U.S. universities, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund.

Sands Las Vegas hacked: In February 2014, cyber threat actors hacked the Sands Las Vegas Corporation in Las Vegas, Nevada, and stole customer data, including credit card data, social security numbers, and driver's license numbers. The hackers also wiped several computer systems harming critical infrastructure and causing reputational damage.

Unauthorized access to Bowman Dam: In August and September 2013 and on behalf of the IRGC, one Iranian threat actor illegally accessed the supervisory control and data acquisition (SCADA) systems of the Bowman Dam in Rye, New York. The access allowed the actor to obtain information regarding the status and operation of the dam.

DDoS attacks targeting the U.S. financial and banking sector: Between late 2011 and mid-2013 and on behalf of the IRGC, Iranian threat actors conducted a number of distributed denial of service (DDoS) attacks, primarily on public-facing websites of U.S. banks. This attack prevented thousands of customers from accessing their accounts and cost the banks millions of dollars in remediation efforts.

Known Iranian Cyber Threats

- APT33: https://malpedia.caad.fkie.fraunhofer.de/actor/apt33
- APT34: https://malpedia.caad.fkie.fraunhofer.de/actor/apt34
- APT35: https://malpedia.caad.fkie.fraunhofer.de/actor/apt35
- Chafer: https://malpedia.caad.fkie.fraunhofer.de/actor/chafer
- Charming Kitten: https://malpedia.caad.fkie.fraunhofer.de/actor/charming_kitten
- Cleaver: https://malpedia.caad.fkie.fraunhofer.de/actor/cleaver
- Clever Kitten: https://malpedia.caad.fkie.fraunhofer.de/actor/clever_kitten
- Copy Kittens: https://malpedia.caad.fkie.fraunhofer.de/actor/copykittens
- Cyber fighters of Izz Ad-Din Al Qassam: https://malpedia.caad.fkie.fraunhofer.de/actor/cyber_fighters_of_izz_ad-din_al_qassam
- Flying Kitten: https://malpedia.caad.fkie.fraunhofer.de/actor/flying_kitten
- Greenbug: https://malpedia.caad.fkie.fraunhofer.de/actor/greenbug
- Infy: https://malpedia.caad.fkie.fraunhofer.de/actor/infy
- Iridium: https://malpedia.caad.fkie.fraunhofer.de/actor/iridium
- Madi: https://malpedia.caad.fkie.fraunhofer.de/actor/madi
- Magic Kitten: https://malpedia.caad.fkie.fraunhofer.de/actor/magic_kitten
- Magnallium: https://malpedia.caad.fkie.fraunhofer.de/actor/magnallium
- MuddyWater: https://malpedia.caad.fkie.fraunhofer.de/actor/muddywater
- OilRig: https://malpedia.caad.fkie.fraunhofer.de/actor/oilrig
- Rocket Kitten: https://malpedia.caad.fkie.fraunhofer.de/actor/rocket_kitten
- Sands Casino: https://malpedia.caad.fkie.fraunhofer.de/actor/sands_casino
- Sima: https://malpedia.caad.fkie.fraunhofer.de/actor/sima

Best Practices to Secure Critical Infrastructure

AppGuard strongly recommends that organizations use this checklist to prevent the most common attacks. While a determined, persistent group of attackers may prove challenging to defeat, all businesses, institutions, and government agencies can improve their security practices by taking specific steps to harden their cyber presence.

- Evaluate your existing security solution and practices, don't assume your systems are secure.
- Periodically engage third party pen testers to do in-depth vulnerability testing.
- Employ a system of layered defenses involving complementary new technologies.
- Develop an understanding of the current threat environment and take appropriate measures to protect yourself from attacks.
- Don't underestimate simple attacks vectors that are easy to miss, as they can use significant harm to the infrastructure.
- Make sure you have a robust and tested incident response plan in place that is updated continuously.
- Practice constant vigilance and heightened awareness – prepare employees, so they don't fall for any future attacks. Train employees to monitor and report any unusual activities.
- Monitor insider threats; restrict access to crucial information on a need to know basis.
- Assume your security parameters are already compromised, don't rely on detect and response, instead utilize a preventative solution.
- Constantly monitor new attack and threat vectors, share new findings with industry peers.
- Look at history and learn from past attacks (attack on Sony Pictures by North Korea, 2014, and others) – the typical detect and response solution didn't work in the past.
- Use prevention methods that can stop zero-day and other known and unknown attacks.

About AppGuard

AppGuard is an award-winning cybersecurity solution that secures enterprises by enforcing the integrity of OS Design through a zero-trust framework. AppGuard protects the OS through kernel level policy enforcement. AppGuard's adaptive policy enforcement (APE) prevents viruses, fileless malware, botnets, polymorphic malware, weaponized documents, targeted attacks, in-memory attacks, ransomware, phishing, watering-holes, drive-by-downloads, and other advanced threats. AppGuard doesn't rely on scanning known signatures or patterns to identify good from bad files. AppGuard's lightweight agent sits low at the kernel level and blocks unacceptable actions like code injection or registry override at the process level.

References

"APT Groups." MITRE: https://attack.mitre.org/groups/.

"A government website was 'defaced' with pro-Iran messaging and an image of a bloodied Trump. Hackers claimed responsibility." The Washington Post 6 January 2020. https://www.washingtonpost.com/nation/2020/01/06/american-government-website-defaced- iran-hackers-bloodied-trump/.

"Increased Geopolitical Tensions and Threats." CISA Insights 6 January 2020. https://www.cisa.gov/sites/default/files/publications/CISA-Insights-Increased-Geopolitical- Tensions-and-Threats-S508C.pdf.

"Industrial control system security firm Dragos detailed a broad campaign of so-called password-spraying attacks." Wired. https://www.wired.com/story/iran-apt33-us-electric-grid/

"Designation of the Islamic Revolutionary Guard Corps." U.S. Department of State 8 April 2019. https://www.state.gov/designation-of-the-islamic-revolutionary-guard- corps/.

"URGENT NEWS: Army Recruiting discredits military draft texts." U.S. Army Recruiting Command 7 January 2020. https://recruiting.army.mil/News/Article- Display/Article/2051787/urgent-news-army-recruiting-discredits-military-draft-texts/.

A Blue Planet-works Company

VA Office

14170 Newbrook Drive
Suite LL-01
Chantilly, VA 20151
USA

NY Office

141 West, 36th
Street, 17th Floor
New York, NY 10001
USA

Tokyo Office

(Blue Planet-works, Inc.)
Daiwa Jingumae Bldg.,
3Fl2-4-11 Jingumae
Shibuya-Ku Tokyo,
150 - 0002
Japan

Los Angeles Office

530 Wilshire Blvd., Suite
206 Santa Monica, CA
90401
USA