FORTALICE CLIENT ADVISORY

Iran Cyber Advisory

January 6, 2020

Fortalice

Fortalice

Executive Summary

Recap of Current Events

This advisory was written in accordance with our desire to keep our clients informed. It contains the information we know so far and, based on the latest DHS Advisory, a few recommendations we believe will be useful to you. It is our hope that this advisory equips you to take the necessary preemptive steps to protect and defend your company from any potential retaliatory attacks by Iran.

There is no immediate intelligence that suggests your firm or firms in your sector will be attacked, but we know from past experience that firms often get caught in the crosshairs of international disputes.

It is important to note that the DHS bulletin from January 5, 2020 states that there is no information indicating a specific or credible threat, physical or cyber, to the USA.

RECAP OF CURRENT EVENTS

On January 2, 2020, the United States conducted operations in Iraq and killed Iranian IRGC-Quds Force commander Qassem Soleimani.

Iran's Supreme Leader, Ayatollah Ali Khemanei, has been quoted as saying Iran will take "forceful revenge" against the United States.

Although Iran's cyber capabilities are widely considered to be less advanced than Russia, China, and N. Korea, it is possible they could band together with other Nation States willing to align with them to support their cause: disruption of the United States' economy and infrastructure. They could also hire sympathizers from cybercriminal syndicates to assist in retaliation via digital tactics.

Our team has been tracking global conflicts and their impact on the way Nation States conduct their affairs. Regarding Iran and their cyber capabilities, we have noted the following unclassified and publicly reported examples.

- There is evidence that Iran units have conducted physical and cyber surveillance of critical infrastructure (energy, transportation, water, banking).
- Iran continues to build out their cyber assets and could launch cyber attacks ranging from Distributed Denial of Service (DDoS), website defacement, and social media account takeovers to more devastating attacks, such as ransomware, extortionware, and data breaches.
- Great social media fanfare may precede an attack, or it could come without warning.

HISTORICAL EVENTS

- Iran was hit with a destructive operation known as "Stuxnet" in 2010 which damaged their nuclear operation capabilities. Since then, they have invested in creating their own cyber force (source: Yahoo! Finance).
- There was a "wiper" strike, referred to as "Shamoon," on Saudi Aramco in 2012. "Wiper" strikes are named for their ability to "wipe," or delete, drives and files. In this case the "wiper" replaced operational files on Saudi Aramco computers with an image of a burning American Flag. They also hit the website of Qatari natural gas firm, RasGas (Source: NY Times).

- **How did they gain access?** Forensics indicates thumb drives, email accounts, unpatched vulnerabilities, and cracked passwords.

- Banking was hit with Distributed Denial of Service, otherwise known as DDoS, attacks from 2010-2012. The attacks were attributed to Iran (Source: NY Times).
- Sand Casinos were hit in 2014. (Source: CNN).
- Nine Iranian hackers linked to Iran's Islamic Revolutionary Guard Corps, also known as the IRGC, were indicted by the DOJ in 2018 for stealing intellectual property from universities located in Canada, the U.S., and several other countries (Source: Vice).
    - **How did they gain access?** Primarily through email accounts.

STEPS TO TAKE THIS WEEK/MONTH

1. Call

Call your technology team and/or web services provider to ask them how prepared your website and client-facing systems are to withstand a DDoS attack. Make sure you have a playbook in place detailing what you will do if your firm is hit by an attack.

2. Practice a Cyber Disaster

Plan to practice your incident response playbook and pay special attention to figuring out how you would respond during a social media account takeover, DDoS attack, ransomware attack, extortionware / destructionware attack, or a data intrusion / exfiltration attack.

3. Practice a Physical Emergency

Conduct a physical safety drill and make sure everyone in your company is aware of the location of all building exits, how to report themselves as safe, and how to reach emergency contacts.

4. Go Old School Offline for Backups

Ensure you have offline backup systems in addition to your online backup systems.

5. Add a Deadbolt to the Cyber Door with Multifactor Authentication

Accelerate plans to institute Multi-Factor authentication on key systems

6. Avoid Dangerous Emails

Links and attachments can be full of boobytraps. Update internet browsers, operating systems, and anti-virus/anti-malware software. Fine tune your email filtering strategies and double check your SPF header records and DMARC. Train staff to use VirusTotal before clicking on a link or opening an attachment. VirusTotal will scan more than 50 sources and notify you if a link or file is bad: www.virustotal.com.

7. Patches and Updates

Make it a priority to keep systems patched wherever possible.

8. Segmentation Strategy

Segment data, user access, and networks. You can start small by setting up more than one domain name to segment your core public facing operations from your back office.

9. Call / Coordinate / Monitor third parties

Often times, the weakest link lies in the vendor access points. Restrict access to common ransomware entry points, like personal e-mail and social media accounts.

10. If You Suspect Surveillance or Witness Suspicious Physical or Cyber Activity:

- Report suspicious activity to local law enforcement.
- Report activity to your FBI Field Office.
- Educate your staff on how to spot and report activities.
- Need a guide? DHS has a publication on how to spot the planning activities: https://www.dhs.gov/publication/suspicious-activity-reporting-indicators-and-behaviors.

11. Stay Informed

- Fortalice will post information updates to our social media accounts as we see them.
- Refer to the January 5, 2020 DHS Advisory: https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-4-2020?fbclid=IwAR13my0Sx4Cu7UCas8eR_-J-Clp3PyzKJGqQyHhWzdpClMAt1EzYhEsK1Mk
- Refer to the Department of State Travel Warnings: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

CONTACT FORTALICE

Contact Fortalice

Fortalice Solutions, LLC. remains the cybersecurity and intelligence operations expert companies and people turn to regarding efforts to strengthen their privacy and cybersecurity. If you'd like to step up your cybersecurity defenses or need help complying with existing or future regulations, give us a call. We are highly skilled in disaster planning and recovery, incident response exercises and cyber risk assessment and we are standing by to aid you and your team.

Contact:
Call **877.487.8160** or email Watchmen@FortaliceSolutions.com