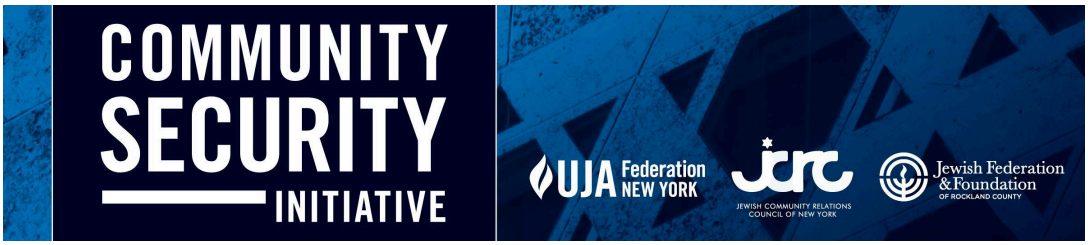


The Iranian Cyber Security Threat to Jewish Organizations

August 20, 2024

Context:

The Iranian regime has a robust cyber warfare capability contained within the praetorian guard branch of their armed forces known as the Iranian Revolutionary Guards Corps (IRGC). Nefarious Iranian cyber activity is a persistent threat, as the regime uses these capabilities to target their perceived enemies.

According to U.S. intelligence officials, as recently as two weeks ago, on August 10, 2024, Donald Trump's campaign was highly likely the target of an Iranian hack, resulting in a large data leak of campaign information to the media. This is in line with prior announcements by the Iranian government declaring intentions to interfere in the U.S. elections.This is in line with prior announcements by the Iranian government declaring intentions to interfere in the U.S. elections.

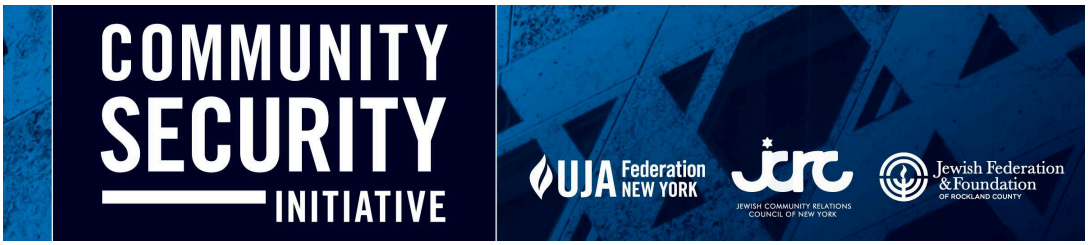
Previous Iranian cyber efforts have included both attacks on Israeli made software used in the water and wastewater systems and the energy, food and beverage, banking and healthcare sectors in the US.

While Iran and their proxies are culpable in planning, attempting, and carrying out physical terror attacks at Jewish and Israeli entities around the world cyber-attacks provide the regime with a modicum of plausible deniability. Considering the current tensions between Iran and Israel and given their cyber prowess, we assess that it is quite likely that Iran will conduct a cyber attack against a Jewish organization.

What Kind of Attacks Can Be Expected?

The most likely cyber attacks are as follows:

1. Website defacement: The intentional defacement of a website through obtaining login credentials used to alter the website content.
2. Distributed Denial of Service (DDoS) attacks: Shutting down a website by using bots to inundate the site with requests for access and thereby overloading the system and crashing the site.
3. Phishing: Emails designed to make the recipient download malware or disclose login credentials. Once the malware and/or the credentials are obtained, this could allow the bad actor to gain access to critical data such as bank account information.



4. Ransomware extortion: A type of malware that encrypts all data on a network and directs you to a "ransom" payment site to obtain the encryption key. This is often paired with downloading critical data to extract later payments.

What Should You Do?

1. Reinforce your authentication procedures:
    a. Implement multifactor authentication (MFA) whenever able. MFA is an authentication system where you input the usual ID and password and are then prompted to further authenticate your account with a one-time password sent to your email, phone, or a third-party application.
    b. Insist on strong passwords: These must be at least 8 characters long and complex (at least one upper case character, one lower case character, a number, and a special character). This lowers the probability of your password will be hacked if bad actors utilize password guessing programs.
2. Social Media:
    a. Reduce your footprint on social media by limiting who can view your social media posts. Check your settings on social media to limit who has access to your information.
    b. Make sure your social media accounts are secured with passwords that are at least 8 characters long and complex. Change them at the first indication the account has been improperly accessed.

For more information:

CISA:
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

CSI has built a substantial cybersecurity program for Jewish Organizations. The program includes cybersecurity assessments, cybersecurity assessments, support for grants and cyber-attacks. All these services are at no cost to your organizations. Visit https://csiny.org/cybersecurity/ to learn more.