Jan 07, 2020

Categories:

Blockchain and Digital Assets
Blogs
Technology Blog

Authors:

William T. Repasky

Could Banks Be Targeted in Iran's Cyber Retaliation?

Governmental officials and cyber security experts currently anticipate that Iran's responses to recent events in Iraq may include asymmetrical retaliatory acts, including cyberattacks on the United States and against key American domestic industries. *See* Department of Homeland Security's (DHS) most current "Bulletin – Summary of Terrorism Threats to U.S. Homelands." For the present, DHS's Acting Secretary Chad F. Wolf's most current official position is, "While there are currently no specific, credible threats against our homeland, DHS continues to monitor the situation and work with our Federal, State and local partners to ensure the safety of every American."

Bankers should remember that our industry was once the target of Iranian computer meddling. Specifically, many bank CISOs will recall the Iranian cyberattacks in the early part of the last decade, which were directed against several major financial institutions in apparent retaliation for the economic sanctions imposed on the Iranian regime to deter the government's nuclear weapons ambitions. At the time, United States officials attributed those attacks to the Quds Force of Iran's Revolutionary Guard Corps. To connect the historic dots to the present situation, the recently killed Major General Qassem Soleimani was the former commander of the Revolutionary Guard's Quds Force.

Iran has a known history of using computer assaults against domestic businesses in response to actions taken by governments whose policies Iran's leadership finds hostile. Besides the past attack on U.S. banking interests, it is generally accepted that the Quds Force was behind the 2012 Shamoon attack on Saudi Aramco, a "disc wiper" type computer intrusion that resulted in thousands of the targeted systems being wiped clean of all data. And again, in 2014, the computer systems at a prominent Las Vegas casino were disabled by the APT34 variant of a disc wiper protocol, after the casino's owner publicly suggested that the United States should bomb Iran.

FBT Gibbons

Within DHS's most current Bulletin, the commonsense recommendation/reminder is made that all businesses "Implement basic cyber hygiene practices such as effecting data backups and employing multi-factor authentication." Other reputable cyber intelligence sources suggest that enhanced end-user vigilance should include focusing on email subject lines that contain words like "oil" and Iran-related news items, which are intended to cause recipients to click on malicious links and attachments. Another cyber defense recommendation is to pay close attention to all alerts which involve credential harvesting or lateral movement. Past cyber tactics associated with Iranian cyber threat actors include CrackMapExec, LaZagne, Mimikatz, PowerShell, compiled Python executables, and Secure Socket Funneling.

Political tensions are no doubt high. But to be forewarned is to be forearmed, in part. The fact that Iran has targeted U.S. banks and related financial infrastructure in the past suggests that our industry is likely now one of those key industries within Iran's crosshairs for future cyber enabled mischief.

If you have any questions about this post, please contact Bill Repasky P: (502) 77-8184 E: brepasky@fbtlaw.com or any member of our Privacy and Data Security Team.

FBT Gibbons