July 5, 2022

Hacking Healthcare

TLP White

This week, Hacking Healthcare begins by trying to untangle how an alleged hacktivist cyberattack in Iran might signal the need for healthcare to start thinking about the possibility of being the target of similar destructive attacks, albeit for different reasons. Next, we look at a Federal Bureau of Investigation (FBI) Public Service Announcement (PSA) on how cybercriminals are using emerging technology to find inventive ways of getting access to an organization’s systems.

Welcome back to *Hacking Healthcare*.

1. Iranian Cyberattack Raises Questions Over Hacktivist Cyber Risk

Last Monday it was reported that several Iranian steel companies had been victimized by a hacktivist cyberattack that may have caused significant physical damage to infrastructure and that reportedly led to a shutdown of some operations. If confirmed, the attack would represent another warning of a particular kind of threat that may be growing, and one that private sector industries may wish to pay more attention to.

On Monday June 27th, Cyberscoop reported that a “hacktivist group calling itself ‘Gonjeshke Darande’” claimed responsibility for a series of cyberattacks against Iran’s steel industry.[1] The hacktivist group posted what it alleges to be screenshots of its access to industrial control dashboards as well as a video of the effects of its attack. The video “appears to show equipment being damaged and a subsequent fire, with firefighters rushing in to extinguish the flames.”[2] There are conflicting reports about the veracity of the attack, with one of the alleged victims apparently stating that no damage was done, but other news sources appear to confirm that some kind of incident had taken place.[3]

The hacktivist group claiming responsibility for the alleged attacks has a history of targeting Iranian entities. It’s been reported that the group was behind a wiper attack on Iranian railway systems last year.[4] The group’s rationale for the attack appears to be overtly political, as it publicly messaged that “[t]hese companies are subject to international sanctions and continue their operations despite the restrictions."[5] The group also claims that its operation was "in response to the aggression of the Islamic Republic" and that it had been "carried out carefully so to protect innocent individuals."[6]

Action & Analysis
Membership required

2. **FBI Sounds Warning Over Deepfake Remote Work Positions**

Emerging technologies always pose new threats for organizations to contend with. While things like quantum computing may yet be a way off from suddenly making current encryption irrelevant, cyber criminals have apparently begun to harness artificial intelligence (A.I.) methods and deepfake tools for a novel approach to getting access to a company's data.

On June 28, the FBI released a PSA to announce that its Internet Crime Complaint Center (IC3) was warning of an apparent increase in "the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions."[7] In particular, it warned of applications for IT and other positions that may have access to "to customer PII, financial data, corporate IT databases and/or proprietary information."[8]

For those with only a passing familiarity with the term, deepfakes "include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said." The IC3 PSA reports that it has received an increasing number of complaints that these fraudulent acts are not limited to just visual forgery but are also using "voice spoofing, or potentially voice deepfakes, during online interviews."[9]

Action & Analysis
Membership required

Congress

Tuesday, July 5th:
- No relevant hearings

Wednesday, July 6th:
- No relevant hearings

July 5, 2022

Thursday, July 7th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness, and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[1] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[2] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[3] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[4] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[5] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[6] https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/

[7] https://www.ic3.gov/Media/Y2022/PSA220628

[8] https://www.ic3.gov/Media/Y2022/PSA220628

[9] https://www.ic3.gov/Media/Y2022/PSA220628