Hackers Planted Trump Smears—and Pro-Iran Trolls Spread Them

thedailybeast.com/hackers-planted-trump-smearsand-pro-iran-trolls-spread-them

Adam Rawnsley October 19, 2020

Tech

HATERS

Twitter suspended roughly 80 accounts tied to Iran after an investigation by The Daily Beast and Mandiant Threat Intelligence.

Updated Oct. 19, 2020 8:11PM ET / Published Oct. 19, 2020 7:30PM ET

exclusive

Photo Illustration by Kelly Caminero/The Daily Beast/Photo by BRENDAN SMIALOWSKI/Getty

President Trump dying of coronavirus and handing over power to Mike Pence. Black Lives Matter protesters surrounding the Clintons' house in New York and firing gunshots. These are a few of the fake scandals that an Israeli news outlet's hacked Twitter account tried to fool readers into believing for a few brief moments earlier this month. Twitter says the trolls amplifying them are linked to Iran.

The incident ended as quickly as it began and the outlet, *Israel Hayom*, regained control of its account. But the hack wasn't an isolated event. Over the past year, hackers have broken into a number of news organizations' Twitter accounts and at least one website to plant fake stories. A new investigation by The Daily Beast and Mandiant Threat Intelligence suggests that hackers in Iran may be behind the incidents.

Twitter accounts used to amplify the fake *Israel Hayom* stories have been used to hype bogus articles planted by hackers in an Orthodox Jewish news website and a Bahraini news outlet's Twitter account. The Iranian-linked accounts also garnered attention for a fake account impersonating one of America's best-known doctors, Zeke Emanuel.

The Daily Beast shared its findings with Twitter. The social media company then suspended roughly 80 accounts for violating its platform manipulation policies on impersonation, coordinated amplification, and spam.

"At this stage, we're investigating thoroughly but early technical and behavioral indicators suggest that these accounts are interconnected and have their origins within Iran," a Twitter spokesperson said in a statement. "As ever, we disclose every single account and Tweet we can reliably associate with state actors to our public archive — the only one of its kind in the industry."

The Daily Beast was unable to identify the specific hackers responsible for the Twitter account and website breaches. But the coordinated, overlapping amplification of the break-in by Iranian-linked accounts on social media suggests a relationship between the hackers planting stories and the troll accounts publicizing them.

A Trail of Hacks

When hackers broke into *Israel Hayom*'s Twitter account to try and fool users into thinking Trump was on death's door and Black Lives Matter was coming after the Clintons, they slipped in some telling regional content. Next to the fake tweets about U.S. politics, the hackers placed a bogus claim that Israeli authorities had discovered a Hezbollah submarine off the coast of Haifa.

As users pointed out the obviously phoney content, a handful of Twitter accounts leapt to a coordinated defense of the storylines with cut-and-pasted talking points to try and beat back the doubters. Examples included “The word hack is used well to cover the real weakness of the Israeli forces!” and "We must accept the great military capability of Hezbollah which could annihilate the Israel."

The amplification attempts, while lame and unsuccessful, point to a trail of similar hacking incidents involving Iranian-linked propaganda trolls.

The Twitter accounts @fahad_alm1989 and @jessica722225874, the latter of which claimed to be a former ABC News journalist, spent much of their short existence spamming links to a story posted on Hidabroot, an Orthodox Jewish news and TV organization based in Israel.

The story, subsequently deleted and written in clumsy Hebrew, included fake quotes from an Israeli minister likening Arab leaders to easily led donkeys in the wake of Israel’s normalization agreement with the United Arab Emirates.

In an email to The Daily Beast, the site’s administrators said that it had been hacked before the fake story was posted.

@fahad_alm1989 also repeatedly spammed legitimate news organizations’ Twitter mentions with links to hacked tweets from Al Bilad, a Bahraini news organization which briefly lost control of its Twitter account in August and September. Tweets from Al Bilad’s compromised account have since been deleted but, like the fake Hidabroot story, screenshots captured at the time show the account tweeted criticism of the United Arab Emirates for its normalization of diplomatic relations with Israel. In an Instagram post, Al Bilad confirmed that it had been hacked and subject to a series of break-in attempts at the time.

It’s still unclear who was responsible for the account break-ins amplified by Iranian linked trolls. But compromising legitimate news sites to post fabricated news articles is a move cybersecurity researchers are increasingly concerned about, according to Lee Foster, senior manager for information operations analysis at Mandiant Threat Intelligence.

“The compromise of legitimate news websites to post fabricated stories is a tactic we’ve seen from various actors, and is one we’re increasingly concerned about given those sites’ perceived credibility and the direct reach they have with large audiences,” Foster said.

Impersonators

Drawing attention to hacked stories wasn’t the only way the Iran-linked trolls tried to get eyeballs on their propaganda. When hackers couldn’t steal real estate on a legitimate news organization’s website or Twitter accounts, the Iranian-linked trolls simply imitated famous people in an attempt to mimic their way into an audience.

Among the targets of their impersonation campaign was Dr. Zeke Emanuel, the brother of Obama White House chief of staff Rahm Emanuel and the chair of the department of medical ethics at the University of Pennsylvania. The fake Zeke Emanuel account warned that Black and elderly Americans would be forced to receive treatment for COVID-19 at FEMA camps in a racist conspiracy narrative echoed by pro-Iranian troll accounts.

“I did not have a Twitter account before that,” Emanuel told The Daily Beast in an email. “Someone complimented me on getting onto Twitter and that was the first I learned about the account. Frankly the impersonation was pretty damn good.”

The impersonation took place in mid May, just as pro-Iranian trolls pushed a similarly racist narrative about the pandemic, previously reported on by The Daily Beast. At that time, an account in the name of a real World Health Organization executive, mistakenly verified by the social media company, pushed a false conspiracy about the Trump administration testing a coronavirus vaccine on Black Americans, in an apparent callback to the Tuskegee experiments, one of the darkest moments in American medical ethics.

Iranian trolls also impersonated an Israeli hospital executive in an attempt to embarrass the president of Tajikistan and his son. The account posed as the CEO of a private hospital in Herzliya to falsely claim that Rustam Emomali, the chairman of Tajikistan's national assembly and the son of Tajik president Emomali Rahmon, had been treated for rectal cancer in Israel. Emomali and the Tajik government have denied the accusations and called them a “deliberate provocation.”

The real Israeli hospital executive did not respond to requests for comment. Twitter suspended the fake account impersonating him after The Daily Beast reported it to the company.

Relations between Iran and Tajikistan have reportedly been strained after Tajik state television recently broadcast allegations about Iranian-funded militants in the Central Asian country during a civil war in the 1990s.

Endless Mayfly

Twitter suspended an additional four accounts found by The Daily Beast and FireEye but as yet has not linked them to any larger campaign or actor.

The accounts, posing primarily as journalists, used a number of tricks similar to the ones attributed to Iranian actors, including amplifying fake tweets from hacked Twitter accounts used to criticize the U.S. and Saudi Arabia.

In June, hackers took over a long defunct Twitter account, @ArabiaNow, run by lobbying firm Qorvis Communications on behalf of the Saudi embassy in Washington, DC, and used it two tweet fake stories about the Trump Organization getting construction contracts in Saudi Arabia and the Saudi government giving contracts to Israeli cybersecurity firm Check Point.

Qorvis did not respond to a request from The Daily Beast for comment.

The four accounts also tweeted spoofed domains meant to resemble the websites of legitimate news organizations in a manner similar to a disinformation campaign known as Endless Mayfly. The University of Toronto's Citizen Lab first identified Endless Mayfly as an "Iran-aligned" disinformation activity that spoofs real news websites with typo-squatting—registering sites with easy to miss spelling mistakes—to push "narratives critical of Saudi Arabia, the United States, and Israel."

The spoofed sites tweeted out by the four suspended accounts look like something right out of the Mayfly playbook, with spoofed news sites, narratives focused on the U.S., Israel and Saudi Arabia, and amplification of them spammed into the replies of real news outlets' Twitter accounts. The sites—meant to look like real pages for The Independent Australia, Israel National News, and Nouvelobs—used a misspelled URL and copied site addresses registered at differing top level domains to spread fake stories about the son of Israeli Prime Minister Benjamin Netanyahu, a fake U.S.-Israeli coup attempt.

And while Twitter hasn't yet attributed the four accounts to any larger activity or actor, they share some overlap to the suspended accounts recently linked to Iran. In particular, the four accounts amplified both the fake Zeke Emanuel account and the Al Bilad Twitter account hack which featured prominently in the activity of Iranian trolls attributed by Twitter. In other words, they appear to be part of a broader, pro-Tehran disinformation push.