Foreign actors could sow 'chaos' in the 2024 presidential election, cybersecurity expert says

August 13 2024, by Tanner Stening and Cesareo Contreras

Credit: Pixabay/CC0 Public Domain

Former President Donald Trump says that his campaign was hacked by the Iranian government—a claim that followed news on Friday that Microsoft had evidence suggesting an Iranian hacking group had breached a presidential campaign official's account.

The breach is the result of a "spear phishing" email sent by an individual associated with the Islamic Revolutionary Guard Corps back in June, according to Microsoft. It was one of four examples the tech company provided of Iranian hackers penetrating campaign and election

infrastructure "in an apparent effort to stir up controversy or sway voters—especially in swing states."

Coinciding with Trump's announcement, Politico reported over the weekend that it had received emails from an anonymous account appearing to contain what the news outlet described as "internal communications from a senior Trump campaign official."

The disparate threads—while appearing related—have yet to be corroborated (Microsoft didn't identify which campaign was affected, and Politico hasn't identified the hacker or their motive).

But the developments point to a growing threat of foreign actors seeking to interfere in the U.S. electoral process by obtaining sensitive information that could be used to sow distrust and undermine confidence.

In a tightly contested election, such "hack and leak" campaigns—while not necessarily new—can be hugely "consequential" at the margins, says Ryan Ellis, an assistant professor at Northeastern University whose research focuses on communication law and policy, infrastructure politics and cybersecurity.

"We've invested a lot and learned a lot about election security over the last three elections, and I'm hopeful that the lessons learned and the practices we've developed would be put to good use," Ellis says.

Northeastern Global News spoke to Ellis about the latest threats to election security, and what is being done to counteract them. His comments have been edited for brevity and clarity.

What do we know about the hack?

The reporting from Microsoft last week was that actors affiliated in some way with Iran successfully penetrated one of the presidential campaigns. They have not confirmed which campaign it was, but the Trump campaign has come out and said it was them, but we are still waiting for Microsoft to actually confirm that and it wasn't just an incidental, unrelated leak.

Let's assume for this purpose it was them [the Trump campaign]. Campaigns are large organizations just like universities, businesses and everyone else. The hacking that occurred here could happen to any large organization. It was spear phishing.

So an individual known to the campaign, a "former senior adviser" according to Microsoft, their account was compromised and an email was sent purporting to be from this known intermediary, but it was actually a malicious actor and then the spear phishing campaign had a person click on a link. The link went to a host or website that was under their control, which was then able to promote or steal some unknown amount of data.

This could happen to anybody, any large organization. You see the churn of email, something that comes from a trusted intermediary, or looks to be from a trusted intermediary. I think it's difficult to protect in those cases.

Assuming Iran is behind the Trump campaign hack, what would be the motive?

To cause chaos. We've seen foreign actors do this in the past, and one of the things they want is to cause a lack of confidence and confusion. However, we are just getting the initial news of this hack so until we know more, it's hard to fully assess what the motives are.

Have hackers used this spear phishing method against other political campaigns or public officials in the past?

It's basically exactly what happened in the [Hillary] Clinton campaign in 2016. A malicious link was sent out tailored to John Podesta [then-chairman of her campaign], and information was then selectively leaked strategically via WikiLeaks and other outlets. This is a very common playbook.

Collecting intelligence on foreign actors is as old as time. Collecting intelligence and selectively deploying it—we've seen a lot of that in this environment. Hack and leak campaigns are not new, but in a close election they can be very consequential.

What can presidential campaigns do to protect themselves if they fall victim to a spear phishing attack?

If you assume that these types of compromises may happen occasionally, even despite your best efforts, it's important to make sure that you have sensitive information well segmented.

The way this works is basically through credential theft. We have a trusted intermediary. We got someone inside the campaign to click on a link. Now we've harvested their login information that we can use to login. If you could segment access to information to such a degree that individuals only get access to the information they need, that could reduce risk. For example, if a person is involved in the vetting of VP candidates, they need to make sure that person doesn't also have access to other sensitive areas of the campaign.

So segmenting the data, segmenting access—only allowing credentialed individuals to access the information they need to have—would be a good step. Is that in place? It's impossible to say from the outside.

This story is republished courtesy of Northeastern Global News news.northeastern.edu.

Provided by Northeastern University

Citation: Foreign actors could sow 'chaos' in the 2024 presidential election, cybersecurity expert says (2024, August 13) retrieved 16 August 2024 from https://phys.org/news/2024-08-foreign-actors-chaos-presidential-election.html