blogs.microsoft.com /on-the-issues/2024/08/08/iran-targeting-2024-us-election/

Iran Targeting 2024 US Election

⋮ 8/9/2024

Today we're sharing intelligence about activity we've been tracking that increasingly points to Iran's intent to influence this year's US presidential election. In recent weeks, groups connected with the Iranian government have upped two kinds of activity. First, they've laid the groundwork for influence campaigns on trending election-related topics and begun to activate these campaigns in an apparent effort to stir up controversy or sway voters – especially in swing states. Second, they've launched operations that Microsoft assesses are designed to gain intelligence on political campaigns and help enable them to influence the elections in the future.

We discuss this activity in a new report we released today, which details this activity, and four examples illuminate what we can increasingly expect from Iran as we near November.

One Iranian group has been launching covert news sites targeting US voter groups on opposing ends of the political spectrum. One of the sites, called Nio Thinker, caters to left-leaning audiences and insults former president Donald Trump, calling him an "opioid-pilled elephant in the MAGA china shop" and a "raving mad litigiosaur." Another, called Savannah Time, claims to be a "trusted source for conservative news in the vibrant city of Savannah" and focuses on topics including LGBTQ+ issues and gender reassignment. The evidence we found suggests the sites are using AI-enabled services to plagiarize at least some of their content from US publications.

A separate Iranian group has been setting the groundwork for US-focused influence operations since March. We believe this group may be setting itself up for activities that are even more extreme, including intimidation or inciting violence against political figures or groups, with the ultimate goals of inciting chaos, undermining authorities, and sowing doubt about election integrity.

Yet another Iranian group, this one connected with the Islamic Revolutionary Guard Corps, or IRGC, sent a spear phishing email in June to a high-ranking official on a presidential campaign from the compromised email account of a former senior advisor. The email contained a link that would direct traffic through a domain controlled by the group before routing to the website of the provided link. Within days of this activity, the same group unsuccessfully attempted to log into an account belonging to a former presidential candidate. We've since notified those targeted.

A fourth Iranian group compromised an account of a county-level government employee in a swing state. The compromise was part of a broader password spray operation and Microsoft Threat Intelligence did not observe the actor gain additional access beyond the single account, making it hard to discern the group's ultimate objectives. Since early 2023, the group's operations have focused on strategic intelligence collection particularly in satellite, defense, and health sectors with some targeting of US government organizations, often in swing states.

The Microsoft Threat Intelligence Report we're releasing today is from the Microsoft Threat Analysis Center, or MTAC, which tracks influence operations from specific nation-state groups around the world. MTAC routinely tracks threats to elections as part of Microsoft's broader Democracy Forward work and this builds on work the team did to track threats to recent elections in India, the UK, and France. Today's update also includes activity we have observed by actors advancing the geopolitical goals of Russia and China, each to varying degrees of effectiveness.

We share intelligence like this so voters, government institutions, candidates, parties, and others can be aware of influence campaigns and protect themselves from threats. We've also been training candidates and parties involved in elections this year, building on our longstanding offerings, like AccountGuard. Finally, Microsoft will not endorse a candidate or political party. Our goal in releasing these reports is to underscore the importance of combating election deepfakes and promoting education and learning about possible foreign interference.

Tags: AI, Iran, MTAC