

Iran steps into US election 2024 with cyber-enabled influence operations

A MICROSOFT THREAT INTELLIGENCE REPORT

Date: August 9, 2024

Foreign malign influence concerning the 2024 US election started off slowly but has steadily picked up pace over the last six months due initially to Russian operations, but more recently from Iranian activity. This third election report from the Microsoft Threat Analysis Center (MTAC) provides an update on what we've observed from Russia, Iran, and China since our second report in April 2024, "[Nation-states engage in US-focused influence operations ahead of US presidential election.](#)"

Over the past several months, we have seen the emergence of significant influence activity by Iranian actors. Iranian cyber-enabled influence operations have been a consistent feature of at least the last three US election cycles. Iran's operations have been notable and distinguishable from Russian campaigns for appearing later in the election season and employing cyberattacks more geared toward election conduct than swaying voters. Recent activity suggests the Iranian regime—along with the Kremlin—may be equally engaged in election 2024.

MTAC continues to examine authoritarian content to detect the malicious use of generative AI. This effort supports Microsoft's commitment to the Tech Accord to Combat Deceptive Use of AI in 2024 Elections. Since our last report in April 2024, MTAC published a [report](#) regarding Russian influence operations to undermine the 2024 Summer Paris Olympics in which Storm-1679 has repeatedly utilized generative AI in its campaigns to little effect. In this installment, MTAC identifies a Russian and a Chinese actor that have employed generative AI—but with limited to no impact. In total, we've seen nearly all actors seek to incorporate AI content in their operations, but more recently many actors have pivoted back to techniques that have proven effective in the past—simple digital manipulations, mischaracterization of content, and use of trusted labels or logos atop false information.

[Iran enters the fold with cyber-influence operations starting June 2024](#)

Iranian actors have recently laid the groundwork for influence operations aimed at US audiences and potentially seeking to impact the 2024 US presidential election. This recent cyber-enabled influence activity arises from a combination of actors which are conducting initial cyber reconnaissance and seeding online personas and websites into the information space.

Cyber-enabled influence operations aimed at US and other global elections have been a persistent target for Iran in recent years. As we noted in our [first elections report](#) last November 2023, "during the 2020 US presidential election, Iran launched multiple cyber-enabled influence operations that impersonated American extremists, and attempted to sow discord among US voters and incite violence against US government officials. Since 2020, Iran extended its track record of election meddling, amplifying cyberattacks with parallel online influence operations in Bahrain and Israel." As seen in Figure 1 below, Iran has

Iran steps into US election 2024 with cyber-enabled influence operations

employed fabricated media, impersonations and in many cases cyberattacks throughout the last four years targeting the US, Bahrain, and Israel.



















Past Iranian election influence efforts						
						
Election Date	NOV 2020	MAR 2021	NOV 2022	NOV 2022	NOV 2022	FEB-MAR 2024
PERSONAS	 	 	 	 	 	 
Operation start	AUG 2020 DEC 2020	DEC 2020 MAR 2021	OCT 2022	JUN 2022 AUG 2022	MAY 2022 JUL 2022	FEB 2024
THREAT GROUP	Cotton Sandstorm	Storm-1660	Cotton Sandstorm	Cotton Sandstorm	Sefid Flood	Storm-0842, 1805, 1084
GOALS	Drive discord Undermine election legitimacy	Drive discord Undermine election legitimacy	Drive discord Reduce voter turnout	Drive discord Undermine trust in authorities	Drive discord, Undermine election legitimacy	Stoke sense of insecurity Undermine Netanyahu
INFLUENCE TTPs	SMS & Email Traditional media Impersonation Coord. amplification Doxing	Fabricated media Impersonation Coord. amplification	SMS & Email Impersonation Coord. amplification	Impersonation Coord. amplification	Fabricated media Impersonation Coord. amplification	SMS & Email Impersonation
CYBER TTPs	Data Theft		DDoS	Data Theft		Spear Phishing Data Theft Wiper malware

Figure 1: Iranian influence actors' election focused tactics, techniques, and procedures

Looking forward, we expect Iranian actors will employ cyberattacks against institutions and candidates while simultaneously intensifying their efforts to amplify existing divisive issues within the US, like racial tensions, economic disparities, and gender-related issues. Here's what we've seen thus far in 2024 from Iranian actors with respect to the upcoming US election.

Sefid Flood prepares for possible influence operations

Sefid Flood, an Iran-linked influence actor, began staging for influence operations in the 2024 US elections following the Iranian New Year in late March. Sefid Flood specializes in impersonating social and political activist groups in a target audience to stoke chaos, undermine trust in authorities, and sow doubt about election integrity. This group's operations may go as far as intimidation, doxing, or violent incitement targeting political figures or social/political groups.

IRGC threat actors enter preparatory stage for likely cyber-enabled influence

In June 2024, **Mint Sandstorm**—a group run by the Islamic Revolutionary Guard Corps (IRGC) intelligence unit—sent a spear-phishing email to a high-ranking official of a presidential campaign from a compromised email account of a former senior advisor. The phishing email contained a fake forward with a hyperlink that directs traffic through an actor-controlled domain before redirecting to the listed domain. Mint Sandstorm similarly targeted a

presidential campaign in May and June 2020 five to six months ahead of the last US presidential election.

On June 13, Mint Sandstorm also unsuccessfully attempted to log in to an account belonging to a former presidential candidate. Mint Sandstorm's target selection and timing—days prior to phishing an active presidential campaign and months ahead of the election—suggest their attempted authentication may also be election-related. Given Mint Sandstorm's [regular targeting](#) of senior political officials for intelligence collection unrelated to elections, additional evidence is required to make a determination. Regardless of the intent, this targeting is a reminder that senior policymakers should be cognizant of monitoring and following cybersecurity best practices even for legacy or archived infrastructure, as they can be ripe targets for threat actors seeking to collect intelligence, run cyber-enabled influence operations, or both.

In May, **Peach Sandstorm** (a.k.a. APT-33)—another group with assessed links to the IRGC—compromised a user account with minimal access permissions at a county-level government in a swing state. The compromise was part of a broader password spray operation from the group, and Microsoft Threat Intelligence did not observe any lateral movement or privilege escalation, making it difficult to determine whether it was election-related. While unclear if related, it is worth noting that the targeted county had undergone a race-related controversy that made national news this year. Since early 2023, Peach Sandstorm's operations have focused on strategic intelligence collection particularly in satellite, defense, and pharmaceutical sectors with some targeting of US government organizations, often in swing states.

Iran-run covert news sites target US voter groups

An Iranian network, **Storm-2035**, comprising four websites masquerading as news outlets is actively engaging US voter groups on opposing ends of the political spectrum with polarizing messaging on issues such as the US presidential candidates, LGBTQ rights, and the Israel-Hamas conflict. This group is part of a broader campaign that has been operating since at least 2020 and includes over a dozen covert news sites targeting French, Spanish, Arabic, and English-speaking audiences with social and political content.

In 2022, [Mandiant](#) reported on one of the news sites, EvenPolitics, noting that the site had published articles discussing the 2022 US midterm elections. An inauthentic amplification network promoting the website was taken down by the X platform in 2022, but the site remains active, publishing around ten articles a week.

A more recently created site, Nio Thinker, first began publishing in late October 2023. The site's early publications focused on the Israel-Hamas conflict, but have increasingly shifted to the US elections in recent months. Its content caters to liberal audiences and includes sarcastic, long-winded articles insulting Trump including calling him an "opioid-pilled elephant in the MAGA china shop" and a "raving mad litigiousaur"¹ (see Figure 2).

Another site, Savannah Time, claims to be a "trusted source for conservative news in the vibrant city of Savannah." The site focuses heavily on Republican politics and LGBTQ issues, particularly gender re-assignment. MTAC has not observed significant social media amplification of these sites as of yet, though it is possible they will begin closer to election day.

MTAC found evidence indicating the sites are using AI-enabled services to plagiarize at least some of their content from US publications. Examination of webpage source code and indicators in the articles themselves suggest the sites' operators are likely using SEO plugins and other generative AI-based tools to create article titles, keywords, and to automatically rephrase stolen content in a way that drives search engine traffic to their sites while obfuscating the content's original source.



Figure 2: June 7 article criticizing Donald Trump published in one of the covert network's outlets, Nio Thinker.

¹ archive.is/Mvf3X

Russian actors sustain influence operations aimed at US audiences

MTAC has observed three Russian influence actors involved in campaigns aimed at the 2024 presidential election. MTAC tracks these as (1) **Ruza Flood** (a.k.a. Doppelganger²), (2) **Storm-1516**, and (3) **Storm-1841** (a.k.a. Rybar). Each has produced election influence campaigns to varying degrees of effectiveness.

As noted in our April 2024 election update, the most impactful of these actors as of late June 2024 is **Storm-1516**, which pivoted in late April from Ukraine-focused operations to targeting the US election with its distinctive video forgeries.³ Storm-1516 consistently launders narratives through videos seeding scandalous claims from fake journalists and nonexistent whistleblowers and amplifying that disinformation via inauthentic news sites. Since April, Storm-1516 has attempted to drive headlines with fake scandals claiming that the US Central Intelligence Agency (CIA) directed a Ukrainian troll farm to disrupt the upcoming US election, the Federal Bureau of Investigation (FBI) wiretapped former US President Donald Trump's residence, and Ukrainian soldiers burned an effigy of Trump. MTAC anticipates the US election will remain this actor's top priority as November approaches. Ruza Flood continues



Figure 3: Storm-1516 created fake whistleblower testimony claiming the CIA instructed a Kyiv troll farm to meddle in the US election (left). In May, Storm-1516 staged a video in which fake Ukrainian soldiers burned an effigy of former President Donald Trump (right).

² disinfo.eu/doppelganger-operation/

³ nytimes.com/2024/05/15/us/politics/russia-disinformation-election.html

its amplification of pro-Kremlin narratives but has not distributed significant US election content since our last report.

Meanwhile, actors associated with the prolific Russian military blogging and content creation collective Rybar—which Microsoft refers to as **Storm-1841**—have set their sights on US immigration issues. Rybar, which until 2022 was associated with the late Russian oligarch Yevgeny Prigozhin’s RIA FAN media empire, also manages US-focused Telegram channels including Topic du Jour (US domestic political news), and Blood Meridian (US southern border immigration news).

More recently, in January and February 2024, Rybar created accounts on Telegram and X using the name “TEXASvsUSA.” TEXASvsUSA posts regularly feature inflammatory news updates, invoke racial dog whistles, and call for mobilization and violence. These posts have most notably included a 30-second AI-generated video titled “Hold the Line,” depicting a horde of immigrant zombies amassing on the southern US border.



Figure 4: This image depicts the TexasvsUSA account manager’s efforts to increase user engagement with a sticker and branding campaign, offering money for user-submitted content.

China

Chinese Communist Party (CCP)-linked influence actors continue to engage US audiences on divisive political issues, expanding to new platforms and evolving their tactics to engage new audience spaces ahead of November. Beginning in late April through late May, the most prolific of these actors, Taizi Flood (a.k.a. Spamouflage), leveraged hundreds of



After Biden turned

Figure 6: Short-form video from Storm-1852 sockpuppet receives over 145K views.

the current administration or mock President Biden, suggesting that he is unfit for office. Some of these videos have garnered hundreds of thousands of views—significantly outperforming Taizi Flood campaigns, but still relatively small in overall scale.

accounts to stoke outrage around pro-Palestinian protests at US universities. Taizi Flood assets appeared to mimic students involved in the protests, reacting in real-time as students clashed with law enforcement across campuses, and lifted text from authentic accounts with directions to demonstration locations. Some of these accounts seeded left-leaning messages into right-wing groups—likely either to further agitate conflict about the protests or misunderstanding which US audiences would be most receptive to their intended message.

Another CCP-linked influence actor, **Storm-1852**, has begun pivoting to short-form video content on political topics to garner audience engagement. These original videos criticize

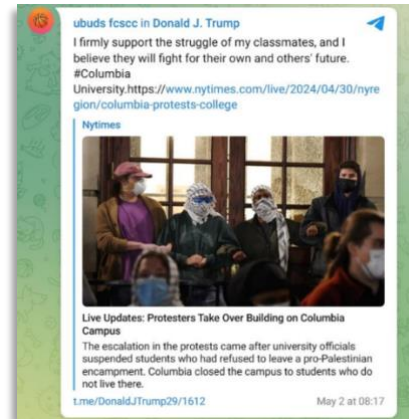


Figure 5: Taizi Flood asset claims to be a student supporting the pro-Palestinian protests on US college campuses.

Appendix A: Iranian actors with assessed links to election interference

Actor	Assessed affiliation	Notable past activity
Cotton Sandstorm <i>a.k.a. Emennet Pasargad</i>	IRGC	Leans heavily on cyber-enabled influence operations to influence elections, but also makes use of influence-only operations. Has targeted US, Bahraini, and Israeli elections.
Lemon Sandstorm <i>Fox Kitten</i>	IRGC	Iranian threat actor known for ransomware hack-and-leak operations, reportedly gained access to a local US election results website in 2020. ⁴ The attack was reportedly thwarted by US Cyber Command, but officials predicted that the group may have sought to tamper with the displayed results to undermine trust in the election outcome. ⁵
Mint Sandstorm <i>Charming Kitten</i>	IRGC	Ahead of the 2020 US presidential elections, they unsuccessfully attempted to log in to accounts of Trump administration officials and Donald J. Trump for President campaign staff. ⁶
Peach Sandstorm <i>APT33</i>	IRGC	Targeted US state government agencies in late September 2022, possibly to gain access ahead of close US Senate elections. While that attempt appeared unsuccessful, it suggests that Peach Sandstorm may be positioned to support elections-related influence operations.
Sefid Flood	Unknown	Targeted Israel during its 2022 election and has been prolific in its operations targeting Israeli activist groups more broadly with influence-only operations. There are indications that this actor conducted reconnaissance on US and Bahraini candidates ahead of their respective 2022 elections.
Storm-1660	Unknown	Actor that conducts influence-only operations responsible for several personas masquerading as "Black Flags" activists opposed to Israeli Prime Minister

⁴ [washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/](https://www.washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/)

⁵ [washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/](https://www.washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/)

⁶ <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/>

		Benjamin Netanyahu. Meta attributes the group to the Iranian IT company Elya Information Technology Research Center (EITRC). ⁷ This actor may be linked to Sefid Flood.
--	--	--

⁷ about.fb.com/news/2020/11/october-2020-cib-report/