Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm

Published: 2024-07-09 · Archived: 2026-04-05 21:05:47 UTC

Note: View the affidavit for search of 968 X accounts here and affidavit for domains seizure here.

The Justice Department today announced the seizure of two domain names and the search of 968 social media accounts used by Russian actors to create an AI-enhanced social media bot farm that spread disinformation in the United States and abroad. The social media bot farm used elements of AI to create fictitious social media profiles — often purporting to belong to individuals in the United States — which the operators then used to promote messages in support of Russian government objectives, according to affidavits unsealed today.

In conjunction with the domain seizures and search warrant announced today, the FBI and the Cyber National Mission Force (CNMF), in partnership with Canadian Centre for Cyber Security (CCCS), the Netherlands General Intelligence and Security Service (AIVD), Netherlands Military Intelligence and Security Service (MIVD), and Netherlands Police released a joint cybersecurity advisory detailing the technology behind the social media bot farm, including details regarding how the bot farm's creators leveraged their bespoke AI system in furtherance of the scheme. The advisory will allow social media platforms and researchers to identify and prevent the Russian government's further use of the technology. In addition, X Corp. (formerly, Twitter) voluntarily suspended the remaining bot accounts identified in the court documents for terms of service violations.

"With these actions, the Justice Department has disrupted a Russian-government backed, AI-enabled propaganda campaign to use a bot farm to spread disinformation in the United States and abroad," said Attorney General Merrick B. Garland. "As the Russian government continues to wage its brutal war in Ukraine and threatens democracies around the world, the Justice Department will continue to deploy all of our legal authorities to counter Russian aggression and protect the American people."

"Today's action demonstrates that the Justice Department and our partners will not tolerate Russian government actors and their agents deploying AI to sow disinformation and fuel division among Americans," said Deputy Attorney General Lisa Monaco. "As malign actors accelerate their criminal misuse of AI, the Justice Department will respond and we will prioritize disruptive actions with our international partners and the private sector. We will not hesitate to shut down bot farms, seize illegally obtained internet domains, and take the fight to our adversaries."

"Today's actions represent a first in disrupting a Russian-sponsored Generative AI-enhanced social media bot farm," said FBI Director Christopher Wray. "Russia intended to use this bot farm to disseminate AI-generated foreign disinformation, scaling their work with the assistance of AI to undermine our partners in Ukraine and influence geopolitical narratives favorable to the Russian government. The FBI is committed to working with our partners and deploying joint, sequenced operations to strategically disrupt our most dangerous adversaries and their use of cutting-edge technology for nefarious purposes."

“We support all civic engagement, civil dialogue, and a robust exchange of ideas,” said U.S. Attorney Gary Restaino for the District of Arizona. “But those ideas should be generated by Americans, for Americans. The disruption announced today protects us from those who use unlawful means to seek to mislead our citizens and our communities.”

“The disruption announced today is the result of a combined response with our international partners to a serious and unique threat,” said Acting U.S. Attorney Morris Pasqual for the Northern District of Illinois. “Multiple U.S. and foreign governmental components worked closely and efficiently to address the threat and develop and execute a mitigation strategy. Through vigorous enforcement efforts and collaborative international partnerships, the Justice Department works tirelessly to disrupt criminal cyber activity.”

Overview

According to court documents, a bot farm is an enhanced software package which allows for the creation of false personas on social media platforms. Bot farms are enhanced by integrating components which contain artificial intelligence, such as image production or text generation.

As described in the affidavits filed in support of the warrants, development of the social media bot farm was organized by an individual identified in Russia (Individual A). In early 2022, Individual A worked as the deputy editor-in-chief at RT, a state-run Russian news organization based in Moscow. Since at least 2022, RT leadership sought the development of alternative means for distributing information beyond RT’s standard television news broadcasts. In response, Individual A led the development of software that was able to create and to operate a social media bot farm. As planned, the social media bot farm would create fictitious online personas for social media accounts, through which RT, or any operator of the bot farm, could distribute information on a wide-scale basis. The development was executed by Individual B and others, who hid their identities and location (Russia) while beginning to purchase infrastructure for the social media bot farm in April 2022.

In early 2023, with the approval and financial support of the Presidential Administration of Russia (aka the Kremlin), a Russian FSB officer (FSB Officer 1) created and led a private intelligence organization (P.I.O.), as explained in the affidavits. The P.I.O.’s membership was comprised of, among others, employees at RT, including Individual A. The true purpose of the P.I.O. was to advance the mission of the FSB and the Russian government, including by spreading disinformation through the social media accounts created by the bot farm.

According to the affidavits, FSB Officer 1, Individual A, and other members of the PIO had access to the social media bot farm. The following are examples of Russian-government narratives that the bot farm posted on X in October and November 2023:

- A purported U.S. constituent replied to a candidate for federal office’s social media posts regarding the conflict in Ukraine with a video of President Putin justifying Russia’s actions in Ukraine;
- A purported resident of Minneapolis, Minnesota, posted a video of President Putin discussing his belief that certain geographic areas of Poland, Ukraine, and Lithuania were “gifts” to those countries from the Russian forces that liberated them from Nazi control during World War II;
- A purported U.S. resident of a city identified only as “Gresham,” posted a video claiming that the number of foreign fighters embedded with Ukrainian forces was significantly lower than public estimates;

- The same purported individual posted a video of President Putin claiming that the war in Ukraine is not a territorial conflict or a matter of geopolitical balance, but rather the “principles on which the New World Order will be based.”

To register the fictitious social media accounts, the social media bot farm relied on private email servers, which in turn relied on the two domain names seized by the FBI. An individual who controls an internet domain can create email accounts using the domain. For example, an individual controlling the domain name www.example.com can create email accounts using @example.com (e.g., EmailAddress@example.com). Here, the actors obtained and controlled the domain names “mlrtr.com” and “otanmail.com” from a U.S.-based provider. They then used those domains to create the email servers that ultimately allowed them to create fictitious social media accounts using the bot farm software.

The FSB’s use of U.S.-based domain names, which the software used to register the bots, violates the International Emergency Economic Powers Act. In addition, the accompanying payments for that infrastructure violate federal money laundering laws.

The Justice Department commends members of the private sector who coordinated with law enforcement efforts on this disruption, including X for its voluntary efforts to suspend the identified bot accounts from its platform. Prior to the government’s action, X identified and suspended a significant number of the bot accounts.

The Justice Department’s investigation is ongoing.

The National Security Division’s National Security Cyber Section, U.S. Attorney’s Office for the District of Arizona, and U.S. Attorney’s Office for the Northern District of Illinois are prosecuting the case, with valuable assistance from the National Security Division’s Counterintelligence and Export Control Section.
