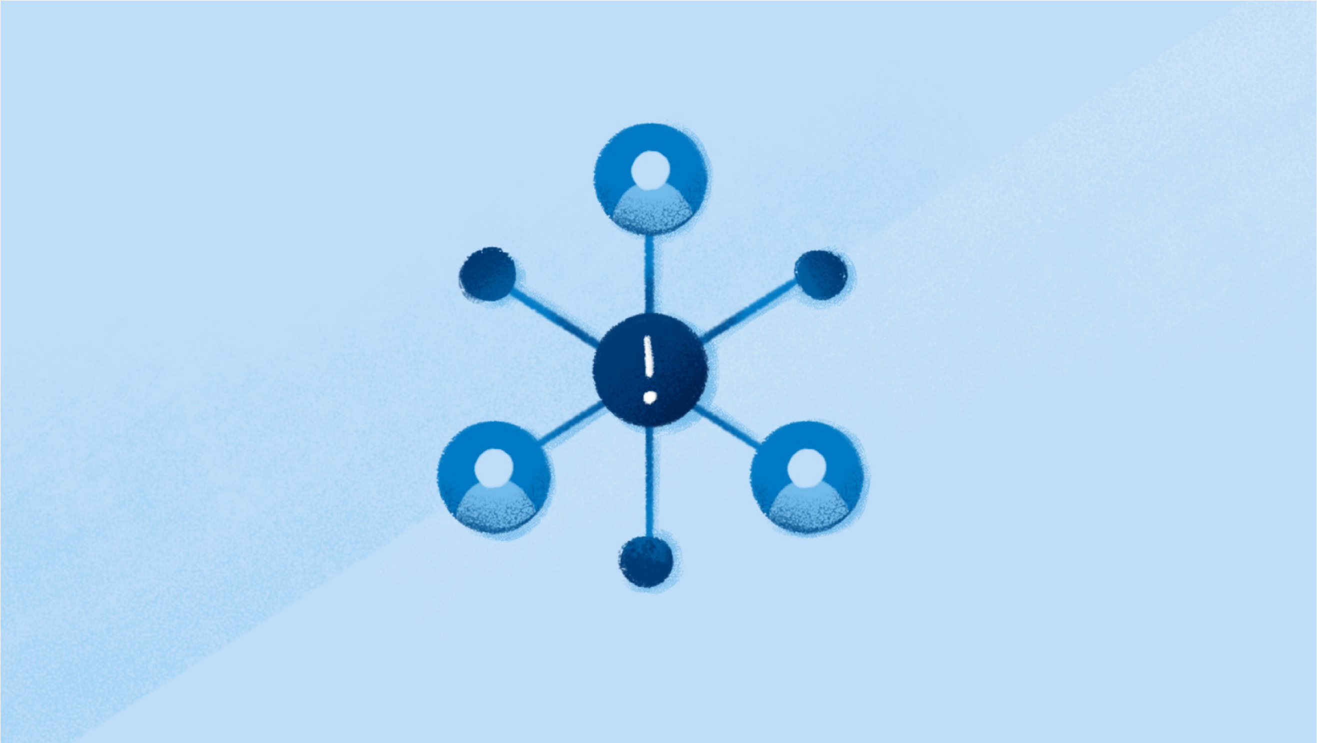
# Meta’s Adversarial Threat Report, First Quarter 2023

April 7, 2022



Today, as part of our quarterly threat reporting, we’re sharing a number of security updates, including our Q1 Adversarial Threat Report and insights into our work against malware campaigns.

Over the past five years, we’ve shared our findings about threats we detect and remove across our technologies. In this threat report, we’re sharing information about six networks we took down for violating our policies against coordinated inauthentic behavior (CIB) and three cyber espionage operations we took action against. We have shared information about our findings with industry partners, researchers and policymakers. Here are the key insights from our first quarter 2023 Adversarial Threat Report:

**We took action against three cyber espionage operations in South Asia**. One was linked to a group of hackers known in the security industry as Bahamut APT (advanced persistent threat), one to the group known as Patchwork APT and another to the state-linked actors in Pakistan. Here is what stood out from our threat research:

- **Diversifying social engineering efforts:** These APTs relied heavily on social engineering and invested in making some of their fake accounts look like more varied and elaborate fictitious personas they created across the internet so they can withstand scrutiny by their targets, platforms and researchers. While we saw them continue using traditional lures like women looking for a romantic connection, they also posed as recruiters, journalists or military personnel.
- **Continued reliance on low-sophistication malware:** This investment in social engineering means that threat actors did not have to invest as much on the malware side. Our investigation into these APTs showed that cheaper, low-sophistication malware can be effective in targeting people when used together with social engineering. In fact, for two of these operations, we observed a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.
- **Impact of public disruptions and threat reporting:** In response to the security community continuing to disrupt these APTs, these groups have been forced to set up new infrastructure, change tactics, and invest more in hiding and diversifying their operations in order to persist, which likely degraded their operations.

**We also took down six covert influence operations** for violating our policy against CIB. These unconnected networks originated in the United States, Venezuela, Iran, China, Georgia, Burkina Faso and Togo. More than half of them targeted audiences outside of their countries. We removed the majority of these operations before they were able to build authentic audiences. Here is what stood out from our threat research:

- **Creating fictitious entities across the internet**: In an attempt to build credibility, nearly all of these operations invested in creating fake entities, including news media organizations, hacktivist groups and NGOs. They operated on many services, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, WordPress, freelancer[.]com, hacking forums and their own websites.
- **Fake hacktivists from Iran**: The operation from Iran posted claims of having hacked organizations in Israel, Bahrain and France, including news media, logistics and transport companies, educational institutions, an airport, a dating service and a government institution. This is not the first time an Iran-origin operation claimed to have hacked government systems; a similar claim was promoted by another CIB network we removed ahead of the 2020 US election.
- **For-hire operations:** As we called out in our past reporting, we continue to see for-hire organizations behind covert influence operations globally, with half of the networks in this report attributed to private entities. This includes an IT company in China, a marketing firm in the United States and a political marketing consultancy in the Central African Republic.

- **The evolution of China-origin operations:** This report brings the total of the China-origin CIB networks we removed since 2017 to six, with half of them reported in the last seven months. These latest takedowns signal a shift in the nature of the China-based CIB activity we've found with new threat actors, novel geographic targeting and new adversarial tactics. However, we continue to find and remove them before they are able to build their audience. These networks experimented with a range of tactics we haven't seen in China-based operations before, although we've observed them elsewhere over the years, including in operations linked to troll farms and marketing and PR firms. The latest behaviors included creating a front media company in the West, hiring freelance writers around the world, offering to recruit protesters and co-opting an NGO in Africa.

We know that adversarial threats will keep evolving in response to our enforcement and that new malicious behaviors will emerge. We'll continue to refine our enforcement and share our findings publicly.

We are making progress in rooting out this abuse; it is an ongoing effort and we're committed to continually improving to stay ahead.

***See the full Adversarial Threat Report for more information.***

Downloads
Meta's Adversarial Threat Report, Q1 2023