Disrupting COLDRIVER: U.S. court orders seizure of domains used in Russian cyberattacks - The Citizen Lab

By Alyson Bruce

Published: 2024-10-03 · Archived: 2026-04-05 17:32:48 UTC

Opens in a new window Opens an external site Opens an external site in a new window

Microsoft's Digital Crimes Unit takes legal action to dismantle Russia-based threat actor COLDRIVER following a joint investigation by The Citizen Lab and Access Now.

In August, The Citizen Lab, jointly with Access Now, in collaboration with First Department, Arjuna Team, and RESIDENT.ngo, published a report that uncovered two distinct spear-phishing campaigns targeting members of Russian and Western civil society. One of the campaigns was attributed to COLDRIVER (also known as STAR BLIZZARD, among other names), a threat group attributed to the Russian Federal Security Service (FSB) by multiple governments.

Today, the United States District Court for the District of Columbia unsealed a civil action aimed at seizing and disrupting the digital infrastructure used by COLDRIVER to target civil society and other actors.

"I welcome this action, and I hope other platforms and governments follow suit. It's already dangerous enough to be a Russian journalist or a Belarusian dissident. Unfortunately, thanks to groups like STAR BLIZZARD, being outspoken about Putin may be a ticket to getting hit with an onslaught of personalized digital attacks," says John Scott-Railton, senior researcher at The Citizen Lab and co-author of the report.

"We shouldn't ask people to be perfectly distrustful of every message in their inbox. They couldn't be effective at their important jobs. Yet a single account compromise of a journalist or dissident can ripple throughout a whole network of people, with consequences for their safety and liberty. This is why it is so important to see platforms taking actions to impose cost on Russian hacking operations."

Microsoft's Digital Crimes Unit (DCU) filed the lawsuit together with the NGO Information Sharing and Analysis Center (NGO-ISAC) and coordinated with the U.S. Department of Justice (DOJ), which simultaneously seized additional domains attributed to STAR BLIZZARD.

Access Now filed a legal statement in support of this civil action, which included statements from Russian civil society victims impacted by this hacking operation.

"Direct action against the ability of the Russian government to carry out these hacking operations is critical. What we observed in our investigation, and the follow-on attacks tracked by Access Now, is that these groups aren't afraid of being discovered. As long as they can continue to fool people with increasingly sophisticated impersonation and personalized attacks, they will. A coordinated disruption of the digital infrastructure used in these attacks will have a significant impact, with the goal of forcing them to stop current operations to rebuild," says Rebekah Brown, senior researcher at The Citizen Lab and co-author of the report.

“Microsoft DCU and the NGO-ISAC have helped protect individuals who are at risk from these continued intrusions. As we get closer to critical election cycles, both in the U.S. and globally, they have also helped build a playbook for how companies and NGOs can respond when, not if, Russian hacking operations resume.”

Read Access Now’s press release here.
Read Microsoft’s blog post here.
Read the U.S. Department of Justice’s press release here.

If you believe you have been targeted by COLDRIVER or other threat actors, follow the digital security recommendations outlined by The Citizen Lab and Access Now and contact Access Now’s Digital Security Helpline.
