‘Ghostwriter’ Looks Like a Purely Russian Op—Except It's Not

wired.com/story/ghostwriter-hackers-belarus-russia-misinformationo/

Lily Hay Newman

November 16, 2021

For at least four years, the hacking and disinformation group known has Ghostwriter has plagued countries in Eastern Europe and the Baltics. Given its methods—and its anti-NATO and anti-US messages—the widely held assumption has been that Ghostwriter is yet another Kremlin-led campaign. The European Union even declared at the end of September that some member states have “associated” Ghostwriter “with the Russian state.” As it turns out, that's not quite right. According to the threat intelligence firm Mandiant, Ghostwriter's hackers work for Belarus.

Mandiant first took a close look at Ghostwriter in July 2020. The group was then primarily known for creating and distributing fake news articles and even hacking real news sites to post misleading content. By April 2021, Mandiant attributed broader activity to Ghostwriter, including operations to compromise the social media accounts of government officials to spread misinformation and efforts to target politicians with hacking and leaking operations.

The group has long focused on undermining NATO's role in Eastern Europe, and has increasingly turned to stoking political divides or instability in Poland, Ukraine, Lithuania, Latvia, and Germany.

At the Cyberwarcon conference in Washington, DC, on Tuesday, Mandiant analysts Ben Read and Gabby Roncone are presenting evidence of Ghostwriter's ties to Belarus.

“The credential theft activity targeting Eastern Europe and anti-NATO information operations both lined up with what we’ve seen Russia do in the past,” Read told WIRED ahead of the conference. Despite those familiar tactics, techniques, and procedures, Mandiant didn't make an attribution to Moscow at the time, because they hadn't seen specific digital links.

After Belarus' controversial elections in August 2020, longtime president Alexander Lukashenko retained power amid accusations that opposition leader Sviatlana Tsikhanouskaya had actually won. The US denounced the election, and many of Belarus' neighbors, including Poland, made it clear that they support the Belarusian opposition. During this time, Mandiant observed a notable change in Ghostwriter's campaigns.

“We saw a shift to a lot more focus on Belarus-specific issues—targeting Belarusian dissidents, Belarusians in the media, things that really look like they’re conducted in support of the Belarusian government,” Read said. "And then we also stumbled upon technical details that make us think the operators are located in Minsk and some others that hint at the Belarusian military. That gets us to the point now where we’re confident in saying that Ghostwriter has a link to Belarus.”

Shane Huntley, who leads Google's Threat Analysis Group, says that the Mandiant research fits with TAG's own findings. “Their report is consistent with what we have observed,” he told WIRED.

As the group's activity hinted more and more at a specifically Belarusian agenda over the summer, Mandiant worked to untangle who was really behind the campaigns. Since last year's election, 16 of 19 Ghostwriter disinformation operations focused on narratives that disparage the Lithuanian and Polish governments, neighbors of Belarus. Two focused negatively on NATO and one criticized the EU.

A Ghostwriter operation in August focused on Poland and Lithuania pushed a false narrative accusing migrants of committing crimes. Long-simmering tensions between Poland and Belarus have escalated dramatically in recent weeks with the border as a flashpoint. Other recent operations have alleged accidents at Lithuania's nuclear power plants, perhaps because Lithuania has long opposed the proximity of Belarus' Astravyets nuclear plant to its border. State television in Belarus has picked up Ghostwriter misinformation narratives and repeated them, though it's unclear whether this was the result of specific coordination or just part of a general feedback loop of Belarusian pro-government propaganda. Read also points out that Ghostwriter has not focused on Estonia—the one Baltic state that doesn't border Belarus.

Though Mandiant is not publicly releasing details of its evidence, the researchers say that technical indicators connect Ghostwriter activity to the Belarusian government and individuals in Minsk. Additional clues potentially reveal a specific connection to the Belarusian military. The researchers say that they directly observed these connections and also confirmed them with outside sources. Read also notes that among the governments Ghostwriter has targeted, the group most commonly focuses on ministries of defense rather than ministries of foreign affairs, which may suggest a focus on military intelligence.

Lukasz Olejnik, an independent cybersecurity researcher and consultant who has followed Ghostwriter's influence in Eastern Europe, says that some of the group's activity, particularly political leaking operations, have been in significant in countries like Poland. “I do not know what the objectives of these operations were, but I'd risk saying that some of them were achieved successfully,” he says. “It is the most significant politically or militarily motivated cyberoperation targeting the Eastern parts of the European Union.”

Ghostwriter operations are not the most technically sophisticated, Read says, but the group seems fully independent and does not have infrastructure overlap with other known groups from what Mandiant has seen. The hackers use their own malware rather than open source or publicly available tools and seemingly have their own public cloud infrastructure.

The fact remains that the EU and other researchers have attributed Ghostwriter to Russia, but Read says these findings aren't necessarily in conflict, especially given that governments may have different visibility and evidence available to them.

“There is a long political union between Belarus and Russia, so I can’t say Russia is not involved,” Read adds. “But what we have picked up is that we don’t see anything connecting them right now.”

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- Blood, lies, and a drug trials lab gone bad
- *Age of Empires IV* wants to teach you a lesson
- New sex toy standards let some sensitive details slide
- What the new MacBook Pro finally got right
- The mathematics of cancel culture
- 👁️ Explore AI like never before with our new database
- ✨ Optimize your home life with our Gear team’s best picks, from robot vacuums to affordable mattresses to smart speakers