

Hackers—hope to defect to Russia? Don't Google “defecting to Russia.”



The next day, December 7, he... bought himself a new laptop, installed a VPN, and hopped right back online. Wagenius evaded scrutiny only until December 12, when the new laptop was also seized under orders from a military magistrate judge.

On December 20, Wagenius was arrested and charged with several federal crimes, and the feds have since resisted his efforts to get free on bail while his case progressed. (Due, in part, to the laptop episode mentioned above.)

Last week, Wagenius pleaded guilty to several of the charges against him. The documents in his case reveal someone with real technical skills but without a more general sense of opsec. The hacked call logs, for instance, were found right on Wagenius' devices. But it was all the ways he kept *saying explicitly what he was up to* that really stood out to me.

For instance, there were numerous explicit Telegram chats with conspirators, along with public posts on boards like BreachForums and XSS. (In related news, the alleged admin of XSS was arrested yesterday in Ukraine.) In one representative chat with a “potential co-conspirator,” for instance, Wagenius outlined his various schemes in October 2024:

*whats funny is that if i ever get found out
i cant get instantly arrested
because military law
which gives me time to go AWOL*

(Narrator voice: “Military law did *not* give him time to go AWOL.”)

Then there were the emails in November 2024, all of them sent to “an e-mail address [Wagenius] believed belonged to Country-1’s military intelligence service in an attempt to sell stolen information.” These were all traced back to Wagenius and used as later evidence that he should not be released on bail.

Finally, there were his online searches. The government includes “just a subset” of these from 2024, including:

- “can hacking be treason”
- “where can i defect the u.s government military which country will not hand me over”
- “U.S. military personnel defecting to Russia”
- “Embassy of Russia – Washington, D.C.”

None of this shows impressive data/device security or even much forethought; the only real plan seems to have been: “Don’t get caught.” Once Wagenius’ devices were seized and searched, the jig was up.

Allison Nixon is chief research officer at the investigative firm Unit 221B. She helped expose Wagenius’ identity, and in

an article last year for Krebs on Security, she shared a message to young men like Wagenius who “think they can’t be found and arrested.”

“You need to stop doing stupid shit and get a lawyer,” she said.

<https://arstechnica.com/security/2025/07/hackers-hope-to-defect-to-russia-dont-google-defecting-to-russia/>