U.S. Soldier Charged in AT&T Hack Searched “Can Hacking Be Treason”

Published: 2025-02-27 · Archived: 2026-04-06 03:09:11 UTC

A U.S. Army soldier who pleaded guilty last week to leaking phone records for high-ranking U.S. government officials searched online for non-extradition countries and for an answer to the question “can hacking be treason?” prosecutors in the case said Wednesday. The government disclosed the details in a court motion to keep the defendant in custody until he is discharged from the military.

One of several selfies on the Facebook page of Cameron Wagenius.

Cameron John Wagenius, 21, was arrested near the Army base in Fort Cavazos, Texas on Dec. 20, and charged with two criminal counts of unlawful transfer of confidential phone records. Wagenius was a communications specialist at a U.S. Army base in South Korea, who secretly went by the nickname **Kiberphant0m** and was part of a trio of criminal hackers that extorted dozens of companies last year over stolen data.

At the end of 2023, malicious hackers learned that many companies had uploaded sensitive customer records to accounts at the cloud data storage service **Snowflake** that were protected with little more than a username and password (no multi-factor authentication needed). After scouring darknet markets for stolen Snowflake account credentials, the hackers began raiding the data storage repositories used by some of the world's largest corporations.

Among those was **AT&T**, which disclosed in July that cybercriminals had stolen personal information and phone and text message records for roughly 110 million people — nearly all of its customers. AT&T reportedly paid a hacker $370,000 to delete stolen phone records. More than 160 other Snowflake customers were relieved of data, including TicketMaster, Lending Tree, Advance Auto Parts and Neiman Marcus.

In several posts to an English-language cybercrime forum in November, Kiberphant0m leaked some of the phone records and threatened to leak them all unless paid a ransom. Prosecutors said that in addition to his public posts on the forum, Wagenius had engaged in multiple direct attempts to extort "Victim-1," which appears to be a reference to AT&T. The government states that Kiberphant0m privately demanded $500,000 from Victim-1, threatening to release all of the stolen phone records unless he was paid.

On Feb. 19, Wagenius pleaded guilty to two counts of unlawfully transferring confidential phone records, but he did so without the benefit of a plea agreement. In entering the plea, Wagenius's attorneys had asked the court to allow him to stay with his father pending his sentencing.

But in a response filed today (PDF), prosecutors in Seattle said Wagenius was a flight risk, partly because prior to his arrest he was searching online for how to defect to countries that do not extradite to the United States. According to the government, while Kiberphant0m was extorting AT&T, Wagenius's searches included:

-"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."

"As discussed in the government's sealed filing, the government has uncovered evidence suggesting that the charged conduct was only a small part of Wagenius' malicious activity," the government memo states. "On top of this, for more than two weeks in November 2024, Wagenius communicated with an email address he believed belonged to Country-1's military intelligence service in an attempt to sell stolen information. Days after he apparently finished communicating with Country-1's military intelligence service, Wagenius Googled, 'can hacking be treason.'"

Prosecutors told the court investigators also found a screenshot on Wagenius' laptop that suggested he had over 17,000 files that included passports, driver's licenses, and other identity cards belonging to victims of a breach, and that in one of his online accounts, the government also found a fake identification document that contained his picture.

“Wagenius should also be detained because he presents a serious risk of flight, has the means and intent to flee, and is aware that he will likely face additional charges,” the Seattle prosecutors asserted.

The court filing says Wagenius is presently in the process of being separated from the Army, but the government has not received confirmation that his discharge has been finalized.

“The government’s understanding is that, until his discharge from the Army is finalized (which is expected to happen in early March), he may only be released directly to the Army,” reads a footnote in the memo. “Until that process is completed, Wagenius’ proposed release to his father should be rejected for this additional reason.”

Wagenius’s interest in defecting to another country in order to escape prosecution mirrors that of his alleged co-conspirator, **John Erin Binns**, an 25-year-old elusive American man indicted by the Justice Department for a 2021 breach at T-Mobile that exposed the personal information of at least 76.6 million customers.

Binns has since been charged with the Snowflake hack and subsequent extortion activity. He is currently in custody in a Turkish prison. Sources close to the investigation told KrebsOnSecurity that prior to his arrest by Turkish police, Binns visited the Russian embassy in Turkey to inquire about Russian citizenship.

In late November 2024, Canadian authorities arrested a third alleged member of the extortion conspiracy, 25-year-old **Connor Riley Moucka** of Kitchener, Ontario. The U.S. government has indicted Moucka and Binns, charging them with one count of conspiracy; 10 counts of wire fraud; four counts of computer fraud and abuse; two counts of extortion in relation to computer fraud; and two counts aggravated identity theft.

Less than a month before Wagenius’s arrest, KrebsOnSecurity published a deep dive into Kiberphant0m’s various Telegram and Discord identities over the years, revealing how the owner of the accounts told others they were in the Army and stationed in South Korea.

The maximum penalty Wagenius could face at sentencing includes up to ten years in prison for each count, and fines not to exceed $250,000.
