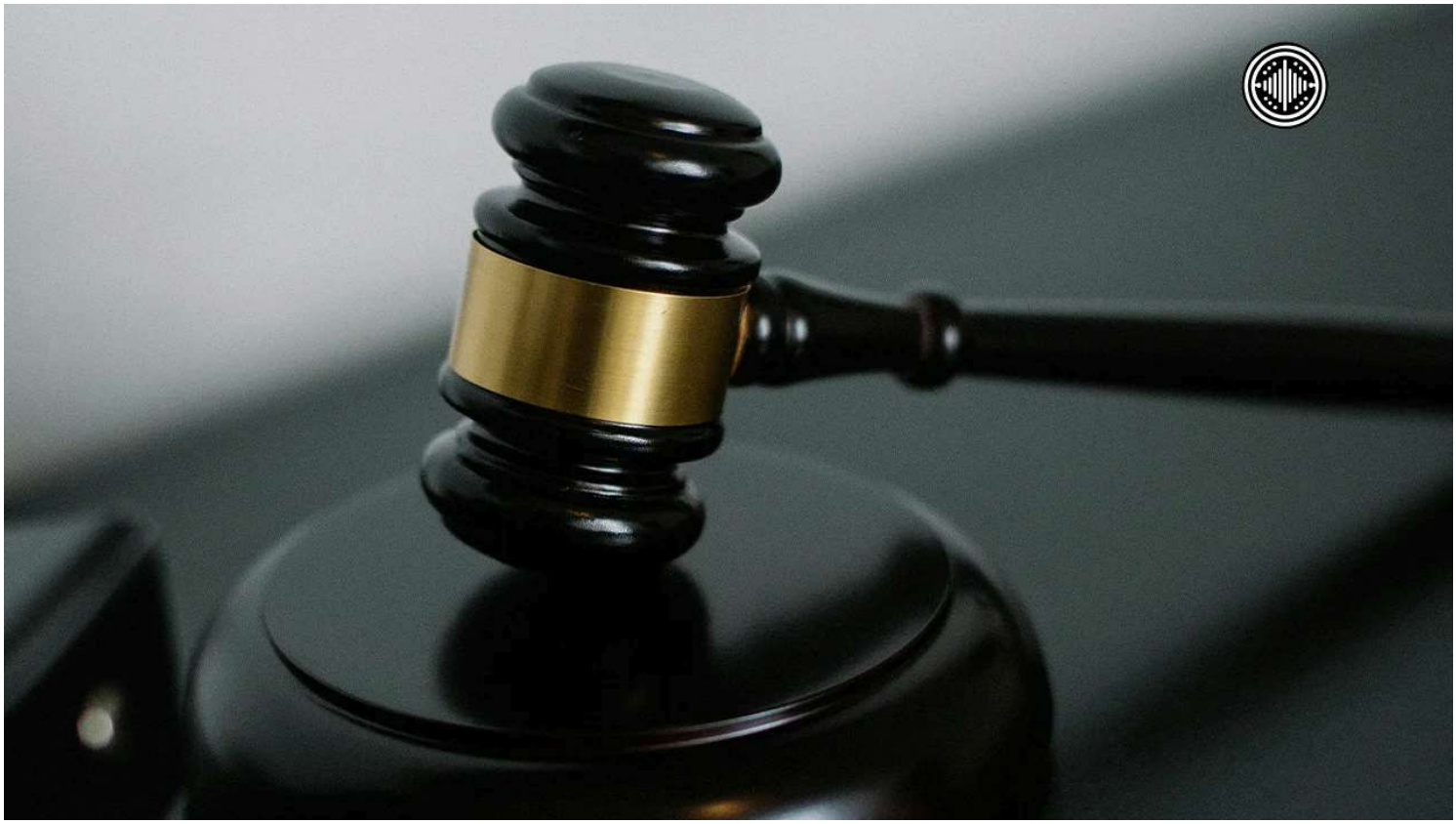
OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

Ex-Soldier Pleads Guilty to Major Telecom Hacks

July 16, 2025
— Categories: Crime



A 21-year-old former U.S. Army soldier has admitted to hacking into the networks of major telecommunications companies, including AT&T and Verizon, and leaking sensitive data such as presidential call logs. The U.S. Department of Justice confirmed that Cameron John Wagenius pleaded guilty to multiple charges, including wire fraud conspiracy, identity theft, and extortion.

According to court documents, Wagenius carried out the cyberattacks while serving on active duty in the United States Army. His guilty plea includes one count of wire fraud

conspiracy, which carries a maximum penalty of 20 years in prison, and one count of extortion, which could lead to an additional five years. He also admitted to aggravated identity theft, which carries a mandatory two-year prison sentence that must be served after any other punishment.

Wagenius is scheduled for sentencing in the coming months.

Between April 2023 and December 2024, Wagenius operated under the online alias "kiberphant0m" and worked alongside co-conspirators to infiltrate at least ten organizations. The hackers gained unauthorized access to internal systems using brute force software and other illicit methods, and later attempted to sell or exploit the stolen data.

Criminal Network

Federal prosecutors say the hackers relied on Secure Shell (SSH) Brute tools to steal login credentials, which allowed them to breach corporate systems. These credentials were then traded and discussed in encrypted Telegram group chats. The stolen data, some of which came from AT&T and Verizon, was reportedly marketed on illicit forums like BreachForums and XSS.is.

Wagenius and his associates didn't stop at selling information. They allegedly threatened victims directly, attempting to extort more than $1 million by leveraging the risk of public exposure. They used private messages and public channels to pressure companies, vowing to leak sensitive information if their demands were not met.

Beyond the extortion, the group engaged in SIM swapping, a scheme that lets criminals take control of a victim's mobile phone number. This often leads to further identity theft and unauthorized access to financial or personal accounts.

Broader Operation

Although the Department of Justice did not name the victim organizations, investigative journalist Brian Krebs has connected Wagenius to a broader hacking campaign involving data stolen from Snowflake, a cloud-based data warehousing company. This campaign has affected hundreds of businesses.

Wagenius was arrested in December 2024 and is the latest in a group of hackers brought to justice. His co-conspirators include Canadian national Connor Riley Moucka, also known as "Judische," who was arrested in October 2024 in relation to the Snowflake breaches, and John Erin Binns, a well-known figure in the cybercrime world who previously claimed responsibility for the 2021 T-Mobile hack. Binns was apprehended in Turkey in May 2024.

The case has raised renewed concerns about national cybersecurity, especially when threats come from those within the military. While the Biden administration has made broader claims about tightening digital security, critics say this incident shows how vulnerable key systems remain. The involvement of a U.S. Army service member adds another troubling layer to an already complex case.