U.S. Intelligence: Russia Tried to Con the World With Bogus Missile

Ankit Panda
Daily Beast, 02.18.19

The Russians hyped a cruise missile launch earlier this year. But a briefing by the CIA and a second agency determined that it was essentially a hoax.

The top secret treason trial of a cybercrime analyst wrapped up this week after months of testimony behind the closed doors of a Moscow military court, with prosecutors reportedly demanding 20 years in a penal colony for the crime of allegedly snitching on Russian cybercriminals to American investigators. A verdict is expected on February 27.

Ruslan Stoyanov is a one-time cybercop who went on to head the computer incidents investigation team at the cybersecurity firm Kaspersky Lab. He stood trial with Col. Sergei Mikhailov, who was second in command in the cybercrime division of Russia's federal security service, the FSB, until December 2016, when his fellow agents ended an internal meeting by abruptly shoving a black bag over his head and dragging him off to prison.

The men are accused of passing confidential material from a 2010 cybercrime and spam investigation to an analyst at a U.S. security firm. But the trial ended without the court hearing from a key figure in the prosecution's theory: the analyst herself, who says the Russian military appears to be on the verge of convicting Stoyanov for treason he didn't commit.

"I formally requested to testify, and they said no," said Kimberly Zenz, a veteran cybercrime threat analyst who was caught up in the Russian intrigue while working for Verisign's iDefense threat intelligence division. "You'd think the opportunity to interrogate a 'spy' would be exciting for them, but they don't even bother to pretend."

The treason case has been closely watched, if seldom observed, since the high-profile arrests in the final days of 2016. The entire matter is considered a state secret in Russia, and with few hard details to go on initial speculation linked the arrests to Russia's election interference campaign.

Over time, a clear and consistent account of the case has emerged from court leaks and people connected to the events. And it turns out the charges have nothing to do with election interference. Instead they're uniquely a product of Vladimir Putin's kleptocratic justice system: the defendants are on trial because eight years ago they allegedly shared confidential documents about a convicted Russian cybercriminal with an American colleague.

Stoyanov's arrest shocked the computer security community. The Kaspersky analyst is well respected internationally, and has no obvious connection to the swamp of corruption and backstabbing synonymous with Russia's intelligence agencies. But

in a country that routinely protects its criminal hackers, and sometimes conscripts them into state service, cross-border cooperation can evidently amount to high treason.

“Things are going very badly,” said Zenz, a longtime friend of Stoyanov. “Ruslan is an honest guy, he’s a good guy. He does not deserve this.”

The treason charges are rooted in allegations first leveled against Stoyanov and other defendants in 2010 by one of the Russian cybercriminals they were tracking: Pavel Vrublevsky, founder of the credit card payment processor ChronoPay.

Vrublevsky is notorious for, among other things, allegedly running a black market pharmaceutical business that hired hackers and spammers to send billions of marketing emails. His misadventures have been chronicled in some detail over the years by independent journalist Brian Krebs, who wrote a book about Vrublevsky called *Spam Nation*.

In 2013, a Russian court sentenced Vrublevsky to two and a half years in prison for ordering a sustained denial-of-service attack against a competing payment processor, an attack that shut down e-ticket sales for the airline Aeroflot for two weeks. Vrublevsky was granted early release after serving one and a half years.

To this day, Vrublevsky insists on his innocence. He blames his legal woes on the FSB officer who led the case, and says that same officer colluded for years with outside security researchers to smear and scapegoat him. In his account, it’s all part of an American conspiracy to paint Russia as a hotbed of global cybercrime. (Note: Russia *is* a hotbed of global cybercrime).

Today that conspiracy theory is at the root of the remarkable treason prosecution. In its broad strokes, Vrublevsky believes that defendant Sergey Mikhaylov, while serving as the deputy chief of the FSB’s anti-cybercrime unit, routinely passed confidential information from the FSB’s ChronoPay probe to the corporate cybercrime analyst Kimberly Zenz.

That’s where Ruslan Stoyanov enters the theory. Stoyanov worked in the Ministry of Interior's cybercrime unit from 2000 to 2006, when he left to begin a cybersecurity startup. He no longer had access to government secrets, but he was a mutual friend of both Zenz and Mikhaylov, the FSB colonel. Vrublevsky has a hunch that Stoyanov served as a middleman in the information transfer.

The information passed to Zenz, he said, informed a series of damning iDefense reports that Zenz wrote about the Russian cybercrime landscape in general, and ChronoPay and Vrublevsky in particular.

Acquired by Accenture in 2017, iDefense was an early player in what today is called the “threat intelligence” marketplace. The firm’s business model involved monitoring

cybercrime groups and tracking security vulnerabilities, then producing detailed reports for its clients—largely Fortune 500 companies and the finance industry, as well as U.S. government agencies.

Zenz worked as an analyst at iDefense for a decade beginning in 2006, about a year after it was acquired by Verisign. She specialized in Russian hacker groups, and divided her time between her home in Northern Virginia, where iDefense was based, and a rented apartment in Moscow.

Zenz freely admits a longtime friendship with Stoyanov. “If you deal with Russian cybercrime he was the guy,” she said. “Everybody knows Ruslan.” She showed him around when he visited the States for a week, and, yes, she did frequently discuss Russian cybercriminals with him, including Vrublevsky. But he was out of government service and had no access to secret information, she said. In that respect Stoyanov was no different from any other smart, informed computer security analyst, except that he happened to be Russian. “I asked him all about it, but I didn’t ask him for any material, any secrets,” she told the Daily Beast.

She said it’s understandable that Vrublevsky would harbor some resentment for her. She considered him a significant figure in the world of Russian cybercrime, and made no secret of it. “I talked publicly about him in conferences, so he was very aware that I was out there,” she said. “I was publicly trying to get him arrested, so he’s not wrong. That’s what I wanted.”

But she’s dismayed that the case has swept in Stoyanov, who she’s known for over 10 years. On multiple occasions, she said, she tried to lure Stoyanov into taking a job with her at iDefense, and he always rebuffed her. “He turned down multiple opportunities to make much more money as an anti-cybercrime rockstar in the West because he wanted to serve his country,” she said. “And all of that is being used against him and it’s just wrong.”

Even taking Vrublevsky’s allegations as true, they sound less like espionage and more like the kind of cross-border information-sharing routinely practiced among national law enforcement agencies. But Vrublevsky has more. Much more. He feels strongly that Zenz’s iDefense position was just a cover story for her real job as an undercover spy. ”We investigated Kimberly and saw clear signs of CIA affiliation,” he said. That evidence of Zenz’s double life includes her home address in Virginia. “She lived in the same village where CIA is—McLean,” Vrublevsky noted.

Vrublevsky presumably said the same thing during the three hours of testimony he gave recently in the secret treason trial of Mikhaylov and Vrublevsky—he can’t confirm that because the details of his testimony are also considered a Russian state secret.

To that stew of alleged information-sharing and suspicious street addresses, prosecutors have sprinkled new specifics of their own atop Vrublevsky’s original claims, according to press reports and accounts of people involved in the trial. They

charge that the defendants didn't just share information with Zenz and possibly other Americans, but that they passed along government documents, for which they were collectively paid an astounding $10 million.

The key thread, as alleged by prosecutors, conveniently weaves through three of the defendants back in 2010. That's when Mikhaylov allegedly loaded up a CD with confidential material from the ChronoPay probe, then gave that CD to his subordinate, Dmitry Dokuchaev, who in turn gave it to Ruslan Stoyanov. Stoyanov allegedly brought the disk with him when he attended Microsoft's invitation-only Digital Crimes Consortium conference in Montreal, Canada, where he supposedly slipped the disk to Zenz.

Zenz calls this claim ludicrous, and late last year she made a bold offer to the panel of military judges overseeing the trial. From her new home in Germany—she took a new job and left Russia in 2016—she wrote a letter asking to testify at the treason trial. In the letter she affirmed that she didn't receive documents, on CD or in any other fashion, from her friend Stoyanov, nor did she see him pass a disk to anyone else at the Montreal event. "I was literally with him all day at that conference," she said. "I was with him all day every day and he didn't give anyone a CD."

Zenz wrote the court that she wanted to testify at the trial—a gutsy move for an American now regarded a cunning spymaster by the Russian government. "I requested the option to testify at the embassy here because it's a lot safer and you're allowed to do that in the court system there," she said. "But if I had to, I'd go. I had a big fight with my husband over it."

To her surprise, the military judges ignored the letter, and she says they also rejected a request from Stoyanov's lawyer to call Zenz as a witness. "Instead, the main witness is a Russian criminal convicted of breaking Russian laws in Russia, and coincidentally the accused happen to be the people who put him in jail for those crimes," she said.

Zenz thinks the entire case is a manifestation of infighting between different units of the FSB, and between the FSB and the Russian military intelligence unit, the GRU. Stoyanov himself has cast the prosecution as payback, because he'd been stirring up trouble by criticizing the FSB's practice of granting effective immunity to hackers willing to do some espionage on the side. "The essence of the deal is that the state gets access to the technologies and information of 'cyberthieves,' in exchange for allowing them to steal abroad with impunity," he wrote in a letter from jail made public in 2017.

Ironically, one of Stoyanov's co-defendants, a black hat hacker turned FSB officer named Dmitry Dokuchaev, has been indicted in the U.S. for doing just that—allegedly letting a well-known hacker go free in exchange for a massive hack into Yahoo that was useful to the FSB's domestic spying. Dokuchaev and another co-defendant have taken plea deals in the treason case.

Vrublevsky says he finds it “weird” that prosecutors want the 20 year maximum for Stoyanov. “While I am not aware of case details I find it hard to believe that Ruslan indeed was such a self-motivated betrayer,” he said. And he can’t explain why the conspiracy he’s been complaining about since 2010 is suddenly being taken so seriously by the Russian government.

“Nobody knows why they took so long,” Vrublevsky said. “It’s the biggest mystery of them all.”