

FBI investigates nationwide school-threat 'game'

Suspect in Arizona school-shooting pranks could be linked local school lockdown

By NATALIE ST. JOHN
EO Media Group

LONG BEACH, Wash. — A New York video game enthusiast who is suspected of phoning in shooting threats to at least four schools in Flagstaff, Ariz., could be linked to a rash of similar phone threats that frightened students and staff on the Long Beach Peninsula and elsewhere earlier in the year.

According to court documents, Viktor Lisnyak, 29, has been charged with five counts of making threats in interstate commerce. FBI agents arrested Lisnyak in July, after tracing email accounts associated with the Flagstaff threats to the home where he lived with his parents in Staten Island, N.Y.

According to a Facebook page and other online records that appear to belong to him, Lisnyak is a 29-year-old immigrant from the former Soviet country of Belarus, who has worked as a department store salesman and as a Russian interpreter for AT&T. During a July interview at his home, he allegedly admitted to FBI agents that he had made threatening phone calls to "schools in the United States, including calls made to Flagstaff," and that "he made so many threatening calls that he doesn't remember all of the specific calls."

Lisnyak also told the investigators that the calls were motivated by the online video games he played with others, via his X-Box video game system. In an affidavit, one special agent wrote, "He would gain 'points' for making these calls, and at times had to make the calls if he 'lost' a game."

Similar calls in many schools

Between March and May, numerous schools in Alaska, Washington, Oregon and British Columbia received phone threats of "imminent" school shootings that were very similar to the threats made in Arizona. But so far, Lisnyak has not been linked to any threats outside of Flagstaff.

Saturday, Ayn Dietrich, a spokeswoman for the Seattle FBI office said agents are trying to determine whether there's any possible connection between the events.

"The FBI's Seattle and Portland divisions are working with the FBI's Phoenix Division to review incidents in our states, with consideration of similar ones in Arizona, for which Lisnyak was recently charged," Dietrich said.

The court documents show that eight calls made to Flagstaff schools between April 15 and May 7 shared many of the same characteristics as calls to schools in the Northwest, including the April 16 threats that triggered a roughly two-hour-long lockdown and major police response on Ocean Beach (Wash.) School District campuses.

All of the calls featured a "robotic" sounding voice, usually male, that called from an anonymous, untraceable number. Most of the calls came in between 1 p.m. and 2 p.m., and the caller tended to target numerous campuses within the same district or small community. The exact language of the threats varied, but the themes were consistent: The caller stated that he or she was in or near the school, was feeling suicidal, and was planning an act of violence. In Arizona, each of the calls used phrases like, "I want to kill hundreds of children," or "I'm going to kill your children."

No active threat was ever discovered on any of the campuses.

Attorneys are waiting on a forensic investigation of Lisnyak's iPad, phone and computer. That investigation could reveal new details about the extent of his activities.



Long Beach, Wash., first-graders took shelter in the Chinook Observer's conference room at the outset of a scary hoax mass-shooting threat made against their school last in April.



NAZToday.com/Submitted Photo
Viktor Lisnyak

A break in the case

At first, local police investigated each of the threats in isolation, and had few clues to work with. Employees at many of the schools had tried to trace the incoming calls, but no one succeeded until April 20, when employees at a Flagstaff preschool somehow managed to capture the originating number. Three Flagstaff Police Department detectives subsequently learned that the number was associated with an email account that allowed the account-holder to make phone calls via the Internet, and finally, police had something to work with.

Another lucky break came when police learned that Lisnyak had made a serious oversight while attempting to hide his identity. Lisnyak knew enough to assume aliases when he set up at least 11 new email addresses (and associated phone accounts) that included the phrase "public enemy." However, he apparently did not realize that every computer has a unique — and traceable — identifying number called an "IP Address" that is embedded in virtually all Internet communications. Because he set up all of the emails using technology that was registered to his mother, the Flagstaff detectives and their FBI partners were able to trace the phone threats to the Lisnyak family residence.

In jail, but not for long

After securing warrants, two of the Flagstaff investigators flew to New York, where, on July 15, they met up with an FBI special agent, and went to visit Lisnyak at home. During that interview, Lisnyak allegedly admitted to the Arizona crimes, leading the FBI special agent to seek an arrest warrant. Lisnyak was arrested on Friday July 17, but he spent only a few days in jail. The following Monday, his parents co-signed on a \$150,000 bond. Lisnyak was released after surrendering his passport and promising to report to Arizona for his first court hearing later that month.

If he is convicted at trial, each of the five federal counts is punishable by up to five years in prison and up to \$250,000 in fines, or both, according to the FBI.



A Pacific County, Wash., sheriff's deputy armed with an assault rifle stands posted outside of Long Beach School in April.

Just what is 'swatting'?

Law enforcement officials say that Viktor Lisnyak's alleged hoax-calls to Arizona schools were an example of "swatting", a disturbing type of prank that has flourished in the age of online video-gaming.

In its simplest form, swatting "involves calling 911 and faking an emergency that draws a response from law enforcement — usually a SWAT team," to an unsuspecting victim's door, according to a 2008 article published by the Federal Bureau of Investigations.

"Swatters" tend to be young and technologically savvy, and may use computer hacking skills to make it appear as if a call reporting a bomb scare, hostage situation or school shooting originated inside the victim's home.

Some crime of this type has existed for decades — in the 1970s, "phone phreakers" broke into phone companies' computer systems, and made free long-distance calls. But swatting proliferated after new technology made it possible for "gamers" to connect with their peers all over the globe.

Connected video game systems such as X-Box — the system favored by Lisnyak — allows gamers to access thousands of fellow players' user-profiles. Tech-savvy pranksters can sometimes mine those profiles for home addresses and other personal information, which is then used to orchestrate a police raid on the target's home. If the victim has a computer

camera set up to broadcast live game-play, an audience of hundreds might be able to watch the raid in real-time.

Sometimes, the swatters are seeking revenge. Other times, they're merely after bragging rights. According to a 2014 primer on swatting from the Association of State Uniform Crime Reporting Programs, players are sometimes assigned "points" for perpetrating these pranks, with the point-value of a certain incident depending on "the level of police presence, the type of entry and whether helicopters are called in." Federal affidavits say Lisnyak swatted schools as punish-

ment for losing games, or in order to gain "points."

The FBI says that in addition to being cruel, swatting hoaxes are "dangerous to first responders and to the victims," because they distract emergency responders from dealing with real emergencies, and create the risk that a distressed victim will "defend" himself or herself against the perceived threat.

In several cases, these pranks have caused serious and unexpected consequences. Swatting incidents have delayed sporting events, caused the evacuation of a hotel, led an unsuspecting father to greet a team of respond-

ers with a knife in his hand, caused a responding police officer to be injured in a car accident, and have even so frightened some victims that they had heart attacks.

In 2009, a then 19-year-old Washington man named Matthew Weigman was sentenced to more than 11 years in federal prison for a swatting conspiracy that had gone on for years. According to the FBI, Weigman and a group of co-conspirators harassed and impersonated telecommunications employees and carried out dozens of swatting pranks. His first swatting prank happened in 2004, when he retaliated against a girl who had refused to have phone sex by faking a hostage situation at her Colorado home, prompting a SWAT response.

WANTED

Classified/Inside Sales

The Daily Astorian is looking for an individual with excellent customer service skills, both in person and over the phone. Someone who brings an upbeat and "go get 'em" attitude to the table, works well with a team as well as alone.

This position requires great computer skills, accurate spelling, the ability to receive incoming classified advertising calls as well as calling advertisers back for ad renewals. Manage special monthly projects requiring cold calls.

Must be persistent and be able to handle rejection with ease. This is a full time position, working Monday through Friday. Evenings and weekends off, plus paid holidays!

REWARDING CAREER

Competitive wage plus commissions. Benefits include paid time off (PTO), insurances and a 401(k)/Roth 401(k) retirement plan.

Send resume and letter of interest to
EO Media Group, PO Box 2048, Salem, OR 97308-2048,
by fax to 503-371-2935 or e-mail to:hr@emediagroup.com