False clues make it tough to find WADA hackers

September 16 2016, by Raphael Satter

A screenshot of the Fancy Bears website fancybear.net seen on a computes screen in Moscow, Russia, Wednesday, Sept. 14, 2016. Confidential medical data of gold medal-winning gymnast Simone Biles, seven-time Grand Slam champion Venus Williams and other female U.S. Olympians was hacked from a World Anti-Doping Agency database and posted online Tuesday Sept 13, 2016. WADA said the hackers were a "Russian cyber espionage group" called Fancy Bears. (AP Photo/Alexander Zemlianichenko)

Medical data from some of the world's leading athletes has been posted

to the web and the World Anti-Doping Agency says Russians are to blame. Even the hackers seem to agree, adopting the name "Fancy Bears"—a moniker long associated with the Kremlin's electronic espionage operations.

But as cybersecurity experts pore over the hackers' digital trail, they're up against a familiar problem. The evidence has been packed with possible red herrings—including registry data pointing to France, Korean characters in the hackers' code and a server based in California.

"Anybody can say they are anyone and it's hard to disprove," said Jeffrey Carr, the chief executive of consulting firm Taia Global and something of a professional skeptic when it comes to claims of state-backed hacking.

Many others in the cybersecurity industry see the WADA hack as a straightforward act of Russian revenge, but solid evidence is hard to find.

IOC President Thomas Bach said Friday he will ask Russian authorities for help to stop the hackers.

Bach said the IOC will help WADA "including communicating with the Russian authorities, to underline the seriousness of the issue and request all possible assistance to stop the hackers."

"This is an unacceptable and outrageous breach of medical confidentiality that attempts to smear innocent athletes who have not committed any doping offense," said Bach.

This is a Friday, Aug. 12, 2016 file photo of Gold medalist Bradley Wiggins of Britain as he poses on the podium of the Men's team pursuit final at the Rio Olympic Velodrome during the 2016 Summer Olympics in Rio de Janeiro, Brazil. Medical data being leaked, in an alleged criminal attack by Russian hackers on a World Anti-Doping Agency database leaked details of asthma medication used by Bradley Wiggins. "There's nothing new here," a statement issued on behalf of Wiggins said. "Everyone knows Brad suffers from asthma; his medical treatment is BC (British Cycling) and UCI (International Cycling Union) approved."(AP Photo/Pavel Golovkin, file)

What's known is that it was only days after scores of Russian athletes were banned from the Olympic Games that suspicious looking emails began circulating . Purporting to come from WADA itself, the booby trapped messages were aimed at harvesting passwords to a sensitive database of drug information about athletes worldwide. Among other things, the Anti-Doping Administration and Management System carries information about which top athletes use otherwise-banned substances

for medical reasons—prize information for a spurned Olympic competitor seeking to embarrass its rivals.

On Sept. 1 someone registered a website titled "Fancy Bears' Hack Team." A few days later, a Twitter account materialized carrying a similar name. Just after midnight Moscow time on Sept. 13, the Fancy Bears Twitter account came alive, broadcasting the drugs being taken by gold medal-winning gymnast Simone Biles, seven-time Grand Slam champion Venus Williams and other U.S. Olympians. It followed up Thursday with similar information about the medication used by British cyclists Bradley Wiggins and Chris Froome, among many others.

There is no suggestion any of the athletes broke any rules, but Russians seized on the leak as evidence that U.S. and British players were using forbidden drugs with the blessing of anti-doping officials.

"Hypocrisy" Russia's embassy to London tweeted in reaction to the news. Kremlin channel RT broadcast a cartoon showing a WADA official picking up a bulky American player's steroid bottle with a smile. "All good! You're cleared to compete!" he says.

Citing law enforcement sources, WADA said the attacks "are originating out of Russia." Russian officials dismissed the allegation; in an email, WADA said it wouldn't be commenting further.

With little to go on, independent investigators have still made some intriguing connections.

Virginia-based intelligence firm ThreatConnect said that whoever compromised WADA did so using websites registered through an obscure domain name company that also set up the fake sites used in a variety of other hacks blamed on the Kremlin, including the one that hit the Democratic National Committee. In a telephone interview, the

company's chief intelligence officer, Rich Barger said he had been cautious at first about tying the WADA breach to Russian hackers but that "confidence is certainly growing as more and more people weigh in and lend their voice."

This is a Sunday, July 24, 2016 file photo of Britain's Chris Froome, wearing the overall leader's yellow jersey, celebrates with a glass of champagne during the twenty-first stage of the Tour de France in Paris. Three-time Tour de France winner Chris Froome siad Thursday Sept. 15, 2016, has "no issue" with his medical data being leaked, in an alleged criminal attack by Russian hackers on a World Anti-Doping Agency database. (AP Photo/Christophe Ena, File)

Even the meaning of the name "Fancy Bears" is unclear. California-based threat intelligence firm CrowdStrike has long applied that

nickname to an allegedly Russian state-backed group, but the hackers' adoption isn't necessarily a brazen acknowledgement of CrowdStrike's research. It might be an attempt to hold it up to ridicule. Which interpretation the group favors hasn't been made clear. Repeated messages to email addresses associated with Fancy Bears have gone unreturned.

Fancy Bears' website doesn't necessarily provide any more insight. Some its artistry appears to have been lifted from a Russian clip art page. But tech podcaster Vince Tocce also found Korean script in the site's code—characters which vanished shortly after he made his discovery public . In a telephone interview, he said that showed how difficult it was to take anything for granted.

Some pieces of Fancy Bears' infrastructure were almost certainly structured to sow confusion.

The site, for example, appears to be hosted in California but was registered at an address in the town of Pomponne, east of Paris, under the name "Jean Guillalime."

A man residing at that address, Jean-Francois Guillaume, told The Associated Press the registry information was bogus and that he was mystified as to why the hackers had picked on him.

"I have absolutely nothing to do with this," he said, adding that he ran a consulting shop and a flower business and wasn't particularly interested in sports. "I don't know any Russians," he said.