Report: Russian cybergang scored millions in fake-ad scam (Update)

December 20 2016, by Tali Arbel

A Russian criminal group is running a massive fraud that has been siphoning off millions of digital advertising dollars a day for a couple of months, a firm that specializes in detecting online-ad fraud says.

The scam may have cost brands, and potentially media companies, hundreds of millions of dollars.

The New York-based firm White Ops said in a Wednesday report that the "Methbot" scam made it appear that hundreds of thousands of people, mostly in the U.S., were watching real video ads from real companies on more than 6,000 fake websites that mimicked well-known publishers, including CNN, ESPN, Vogue and The New York Times. Nobody was actually watching.

The criminal ring's gains come out of the pockets of companies paying for digital ads and also, potentially, of the websites that could have hosted those ads.

White Ops President Eddie Schwartz said he can't put a total value on the amount the Russian group has stolen, because it's not clear when the scam began. But the firm estimates that the scammers were getting $3 million to $5 million per day since roughly early October, and the fraud is still going on.

The revelation of the fraud and ongoing anxiety about where ad dollars are going could make it harder for legitimate web publishers to make

money from ads if brands become more suspicious, said Forrester digital publishing expert Susan Bidel.

"It's the advertiser's money that's being stolen, it's the publisher's reputation. It punishes all of publishing," she said.

Brands need to insist that advertising-technology platforms and ad agencies show them exactly what they are paying for—where ads end up, Bidel said. Right now, that's difficult to determine because of the number of companies and networks involved in automatically placing digital ads on sites that have ad holes to fill.

Fraud has long been a problem in the roughly $187 billion global digital-ad market. White Ops, which sells anti-fraud software to ad agencies and other advertising players, estimated in January that "bot" ad fraud would amount to $7 billion globally this year. The company will put out a 2017 estimate in May.

Methbot is "a novel, new approach" to digital-ad fraud that seemingly allowed the scammers to go undetected for longer and make more money, said Cameron Camp, a researcher for IT security firm ESET.

Schwartz said that while ad fraud often relies on individual computers infected by malware, the scammers bought or "somehow compromised" in another way more than half a million IP addresses, strings of numbers that identify computers, and controlled them from two data centers—one in Amsterdam, one in Dallas.

They made it look like these were actual households that had internet service from legitimate providers like Comcast, AT&T and Verizon to help trick advertisers using automatic ad exchanges into accepting them as real people.

Schwartz said White Ops knows what group is behind the "Methbot" fraud and has passed information on to law enforcement, although he wouldn't name the group or say which law enforcement agency is working on the case.