TECH

U.S. Charges Eight With Online-Ad Fraud

Two alleged schemes involved fake websites and infected computers across the world

The Justice Department charged eight people in an indictment unsealed Tuesday. PHOTO: BRENDAN SMIALOWSKI/AGENCE FRANCE-PRESSE/GETTY IMAGES

By Rob Barry and Suzanne Vranica

Nov. 27, 2018 6:32 p.m. ET

The Justice Department charged eight people, most of them in Eastern Europe, with operating two alleged advertising schemes involving scores of faked websites and infected computers across the world, costing advertisers tens of millions of dollars.

In an indictment unsealed Tuesday in New York's Eastern District, prosecutors said the alleged schemes had been going on since at least 2014.

Law enforcement conducted coordinated raids across Europe to take out the networks, followed by successive takedowns of the fake websites. Three of the eight alleged perpetrators were arrested overseas on charges including wire fraud, computer intrusion and money laundering. The others remain at large.

"The defendants in this case used sophisticated computer programming and infrastructure around the world to exploit the digital advertising industry through fraud," said Richard Donoghue, the U.S. Attorney for the district.

One of the operations, named 3ve, was first identified last year by Google, a unit of Alphabet Inc., GOOGL **-0.35%** ▼ which lost millions of dollars in the scam, and ad-fraud-detection firm White Ops. Both companies said they turned their findings over to law enforcement.

The alleged perpetrators used an army of infected computers to fool advertisers into believing they were buying ads on legitimate websites, according to prosecutors and a report by Google and White Ops. In all, advertisers essentially wasted at least $29 million on ads seen by computer programs and not humans.

The other operation, dubbed Methbot, used servers at data centers in Dallas and elsewhere to create fake "bot" traffic to view ads on faked websites—an operation that resulted in at least $7 million in wasted advertising, prosecutors said.

Both alleged schemes primarily targeted video ads, which are especially lucrative because they carry higher rates than other online display ads.

Google joined several other companies last year, including Facebook Inc., Verizon Communications Inc.'s media subsidiary Oath and White Ops, in a secretive effort to unravel the operations.

Tamer Hassan, the White Ops co-founder and chief technology officer, said the charges represent the largest effort by law enforcement to date to disrupt the problem of fraudulent online ads, which have plagued the estimated $280 billion digital-ad industry despite many attempts by the sector to clean up.

Tamer Hassan of White Ops at an event in New York in 2015. PHOTO: ANDREW TOTH/GETTY IMAGES FOR AWXII

"This case sends a powerful message that this office, together with our law-enforcement partners, will use all our available resource to target and dismantle these costly schemes," Mr. Donoghue said.

In recent years, investigators have shut down several ad-fraud operations, including one named ZeroAccess, which cost online advertisers as much as $2.7 million a month.

The new charges could mark a turning point for a largely unpoliced marketplace where actors outside the U.S. have operated with near impunity.

"It has historically been a faceless crime, and having someone like the U.S. government going after the people behind this is a great step," said Scott Spencer, director of product management at Google.

Not only does fake traffic defraud advertisers, but ads that are served to counterfeit sites rather than legitimate ones deprive publishers and other sites of ad revenue.

A study from White Ops and the Associational of National Advertisers in 2017 estimated that advertisers wasted about $6.5 billion in 2017 on online ads served to fraudulent traffic, a slight decline from the $7.2 billion in losses the ANA projected for 2016.

During a single day near its peak in late 2016, the Methbot operators pulled in $56,000 from advertisers who had been fooled into paying for more than 16 million faked ads, prosecutors said.

To mask the operation, the alleged scammers forged internet ownership records of thousands of internet-protocol addresses, making it appear as if they belonged to large American internet-service providers. Like phone numbers, IP addresses are codes assigned to computers connected to the internet.

Once White Ops identified the data centers and forged IP addresses in a December 2016 report, advertisers quickly blocked them, and the operation shut down.

Soon after, investigators spotted 3ve, which they said infected computers around the world with malware that secretly loaded fake websites laced with ads. The malware also faked mouse movements and used a variety of techniques to evade detection. More than 1.7 million computers were used in the scheme, prosecutors alleged.

Google said it had been crediting advertisers for the fraudulent inventory as the company probed the operation.

One of the alleged scheme's participants, Aleksandr Zhukov, sent payments from the operation to a bank account in the Czech Republic and later moved $5.4 million from that account to a bank in New Zealand, prosecutors said.

Mr. Zukhov, a 38-year old from Russia, was arrested earlier this month in Bulgaria and awaits extradition. He couldn't be reached for comment.

Write to Rob Barry at rob.barry@wsj.com and Suzanne Vranica at suzanne.vranica@wsj.com