The massive Russian cybercrime operation stealing millions from advertisers - Inside ‘Methbot’

Security experts have uncovered what appears to be the biggest and most profitable advertising fraud scheme known to date.

In a report released Tuesday, cybersecurity firm White Ops mapped out a massive operation through which Russian cybercriminals are stealing millions of dollars from publishers and advertisers in the form of fake video views.

Nicknamed "Methbot" for the frequent references to the drug in its code, the ongoing scheme involves an army of bots whose sole purpose is to watch as many as 300 million video ads per day, thus tricking brand advertisers into paying millions of dollars for fake views.

The company believes it to be the work of a ring of Russian hackers, who researchers say have netted upwards of $180 million in profits since launching the operation in September.

While employing automated users to scam ads is nothing new — it's the foundation of the multibillion-dollar ad fraud industry — the company says the staggering scale and technical intricacy at play here are unprecedented.

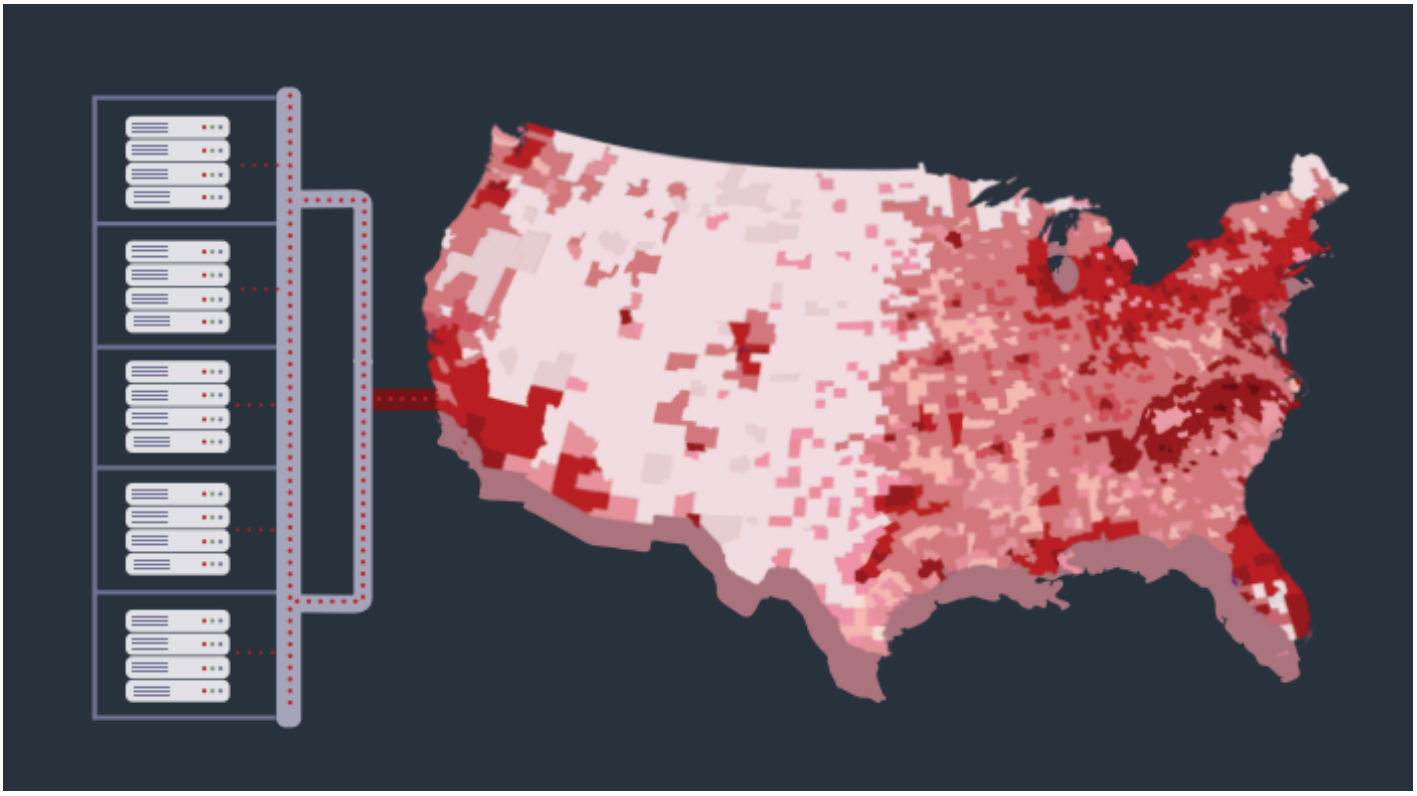
"This is an attack perpetrated against the entire industry," says White Ops CEO Michael Tiffany. "It was robbing both advertisers and publishers, and it was operating at a level of sophistication that's just unheard of."

How it works

The whole operation takes place within a sort of Potemkin Village version of the internet located entirely within the bounds of Methbot's servers.

To populate it, the hackers took over more than half a billion IP addresses — unique strings of characters designed to identify web users — from two major registries and broke them into chunks, which were then assigned to various internet service providers like Comcast and Verizon.

Doing so created the illusion that each of these millions of bots were real web surfers spread across America rather than programs operating out of one of two centralized data centers in Amsterdam and Dallas.



The perpetrators also built custom software designed to make the bots appear convincingly human — they mimicked clicks and cursor movements; installed fake cookies that indicated demographics, online browsing histories and other targetable traits; and even gave them fraudulent social network credentials that made it appear as if they were logged into Facebook or other social media accounts (though no such accounts actually existed).

This elaborate operation goes far and beyond that of your average ad fraudster, Tiffany says. In a typical operation of this kind, bots latch onto the addresses of actual people through malware so that hackers don't have to go through the trouble of creating identities out of whole cloth.

"We've never seen anything like that before," Tiffany says. "It's just astonishing."

But spawning this army of robo-users was just one piece of the puzzle; the cybercriminals also generated more than 6,000 imitation sites designed to resemble major outlets across the web. These include fake versions of publishers like CNN, the New York Times, BuzzFeed and Mashable; platforms like Facebook, Yahoo and Quora; and even some brand websites like those of Air France and Pokémon.

The fake sites allowed the thieves to take advantage of a common form of arbitrage in the ad tech industry in which unsold ad space is bought from an outlet then resold at a higher price.

The criminals would pretend to be reselling space on, say, CNN's website through an automated ad exchange but then instead direct the ad to their shell version of the site that nobody could actually see.

There, the brand would unwittingly pay to have its video ad viewed solely by the millions of bots assigned to visit each of these sites.

As a whole, the operation racked up between 200 to 300 million views per day and bilked advertisers and media companies out of $3 million to $5 million in revenue.

Such intricate attention to detail might seem excessive for a scam that's already considered to have the lowest risk and highest reward of any form of cyber crime.

But the whole plan was put in place in service of making the machine as profitable as possible at every level. Bots imbued with a targetable profile and brand-name outlets are worth much more to advertisers than unknown visitors to a no-name webpage, and video is the most expensive form of online advertising.

"By using these very sophisticated mechanisms to hack some of the architectural systems of the internet, they were then able to unlock much greater profit potential than other operations usually have," Tiffany said.

What's next

White Ops, which specializes in ad fraud detection, first took notice of the operation in October, when its system picked up on some of the bots. The rest of the scheme unraveled from there.

"We had this one thread to pull on, and then as we pulled on it, we uncovered layer upon layer upon layer of complex forgeries," Tiffany said.

Now that the report is out, White Ops is releasing a full list of fake addresses and domains so that ad networks and other fraud detection firms can block accordingly. It is also working with U.S. law enforcement authorities to try to track down the parties responsible.

While the massive scale of Methbot might make other ad fraudsters seem like small-timers in comparison, ad fraud as a whole remains a huge headache for the advertising industry. A research report from an advertiser trade group last year predicted that it could cost digital advertisers around $7.2 billion this year alone.

Tiffany says it's entirely possible that ad fraud rings of comparable scope are currently operating undetected. The murky nature of the crime makes it uniquely hard to suss out.

"It hardy ever leaves traces of the crime behind," he says. "It's such an extraordinarily successful form of theft because nothing goes missing."