CLIENT ALERT

Is This the "3ve" of the Digital Ad Fraud Age?

Dec.20.2018

Federal enforcers are increasing scrutiny of criminal digital ad fraud

Digital ad fraud costs advertisers billions of dollars every year. In 2017 alone, digital ad spending reached $209 billion worldwide; however, experts suspect that anywhere from $6.5 billion to $65 billion of that spend was stolen by fraudsters without consequence. But now, the U.S. Department of Justice (DOJ) has issued a warning shot, unsealing last month a 13-count indictment against eight Russian and Kazakhstani individuals for their alleged role in masterminding and operating two large ad fraud schemes—better known as "3ve" and "Methbot." According to the DOJ release, these individuals allegedly stole more than $35 million in ad revenue using "sophisticated computer programming and infrastructure[s] around the world to exploit the digital advertising industry through fraud." Does this enforcement action really signal the death knell for digital ad fraud or merely mark the start of a new phase for ever-evolving cybercriminal strategies?

Bots, bots and more bots

Methbot ran from September 2014 to December 2016 and operated the purported advertising network "Ad Network #2." It had business arrangements with other ad networks to receive payments in return for placing ad tags on websites. Ad Network #2 then rented more than 1,900 servers housed in commercial data centers in Dallas, TX to load ads on fabricated websites spoofing more than 5,000 popular domains. To fool advertisers into believing that real human users were clicking on the ads, the defendants programmed the datacenter servers to act like humans through fake mouse movements, pausing video players, and falsely appearing to be signed into Facebook. They also leased more than 650,000 IP addresses and fraudulently registered them to appear as if they belonged to residential computers subscribed to residential internet providers. As a result, the scheme stole more than $7 million for ads viewed by bots instead of humans.

The second scheme, 3ve, was even more impressive. It rapidly grew from a low-level botnet started in 2016, to one of the most widespread ad fraud operations ever uncovered. 3ve reached these levels through an ever-evolving, three-pronged strategy.

First, instead of using doctored IPs like Methbot, 3ve created fake ad traffic by infecting millions of real personal computers with malware using "malvertising" (malware disguised as "critical" browser or Adobe Flash updates) on popular entertainment sites, giving 3ve access to IP addresses linked to real human users. It then used infected computers to direct fake traffic at counterfeit websites to generate ad views. 3ve also programmed the malware to evade detection by not running if it saw security software or other malware installed on users' computers. At its peak, the malware infected approximately 1.7 million computers.

Next, 3ve combined its malware botnet with data center bots in order to use infected personal computers as tunnels for bots to pass through high volumes of fake traffic on their way to ads on over 5,000 counterfeit websites. 3ve's bots were so sophisticated that they even mimicked human behavior such as mouse movements and clicks to trick anti-bot systems into believing real consumers where playing videos featuring ads.

Finally, 3ve monetized these ad views using over 60,000 accounts selling advertising inventory making more than 3 billion daily requests. 3ve achieved high levels of success as they were able to get ads placed on their site by relying on domain spoofing, tricking advertisers into believing that ads were served to consumers viewing legitimate, premium websites.

This massive online fraud scheme was finally brought down through the collaborative efforts of federal investigators and private stakeholders. 3ve was first discovered in early 2017 when Google and cybersecurity firm White Ops began tracking and sharing information about the botnet's early form. By March 2017, the two firms shared their initial findings with the FBI, and in the summer of 2018, they reached out to industry partners to create an industry-wide alliance to combat the fraud scheme.

By October 2018, the FBI informed the alliance that it was ready to launch a coordinated effort to take down 3ve. Following the arrest of one of the indicted defendants by Malaysian authorities, the FBI, with the aid of the alliance, redirected internet traffic going to the fraud-related domains (an action known as "sinkholing"). The FBI then executed search warrants on 23 internet domains and at 11 different U.S. server providers for 89 servers related to the 3ve botnet-based scheme. (Seizure warrants were also executed on multiple international Swiss bank accounts.)

These indictments arrive as the FBI continues its criminal inquiry into the media buying practices of ad agencies and as U.S. Senators have called on the Federal Trade Commission to investigate ad fraud. As the U.S. Attorney for the Eastern District of New York Richard P. Douglas stated, "This case sends a powerful message that this Office, together with our law enforcement partners, will use all our available resources to target and dismantle these costly schemes and bring their perpetrators to justice, wherever they are."

What can be done about this?

The scope and sophistication of these digital ad fraud schemes highlights the complexity of taking down bad actors perpetrating ad fraud. While dismantling 3ve and Methbot are helpful steps towards cleaning up the digital advertising ecosystem, they are likely only the tip of the iceberg in terms of other schemes infecting the marketplace. Thus, advertisers must continue to be vigilant about how their advertising dollars are spent. As an important first step, advertisers must protect against fraud and ensure transparency with their advertising partners by keeping platforms accountable to identify clicks, impressions, and other programmatic ad measurements that determine advertising expenditures. Existing software applications and verification tools used by many leading advertisers and their agencies do not appear to be enough. Bad actors quickly evolve techniques to evade existing ad fraud technologies such as blacklists. Indeed, ad fraud experts suggest that bad actors may be ordinary employees of reputable companies engaging in lucrative "side gigs" to make money by arbitraging fake traffic.

A dual-pronged attack of effective and informed negotiation of agreement terms and remedies coupled with up-front and forensic assessments of digital media campaigns is likely going to be necessary for advertisers to begin getting a better handle on digital ad fraud risks.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

David Ervin
Partner – Washington, D.C.
Phone: +1 202.624.2622
Email: dervin@crowell.com

Lauren Aronson
Counsel – Washington, D.C.
Phone: +1 202.624.2541
Email: laronson@crowell.com