The Next Web
Apple now dominates consumer digital video viewing, says new Adobe report

Wall Street Journal
Dish's Finicky CEO is Wild Card in T-Mobile Talks (Subscription may be required)

Associated Press
The consolidation wave sweeping TV providers

Washington Post
Chinese breach data of 4 million federal workers

Associated Press
To stop cyber attacks, NSA expanded US web surveillance

Wall Street Journal
Comcast Has Agreed To Acquire Ad Tech Firm Visible World

Amazon.com's cloud computing service has become a popular conduit for fraudsters looking to create "bot" traffic and disseminate it over the Web, according to new research from advertising fraud detection firm Fraudlogix.

Fraudsters use computer generated bots to mimic the actions of real consumers and trick marketers into paying for ads displayed on Web pages. A number of techniques are used to generate artificial traffic, such as infecting consumers' personal computers with software that loads Web pages without their knowledge, or installing similar software on cloud computing services such as Amazon's to simulate real users.

To get a sense of how non-human or "bot" traffic moves around the Web, fraud detection firm Fraudlogix examined two billion ad impressions over the course of a 30-day period from early March to early April. Those impressions were delivered to nearly 64 million unique IP addresses, which Flaudlogix checked against its own fraud database to categorize them as "good" or "bad."

The research found some of the largest and best-known Internet service providers carried the most fraudulent traffic, which is unsurprising given their scale and market share. Providers such as Comcast and Time Warner were among the companies that racked up the most "bad" IP addresses, for example, but owing to their size they delivered the most "good" IP addresses too.

But topping the list of "bad" ISPs was Amazon's AWS cloud service. Unlike the other companies, AWS doesn't offer high-speed Web access access to consumers. Instead, its cloud computing platform has been twisted by fraudsters to create artificial bot traffic and to disseminate it across the Web.

As a result, Amazon's servers accounted for 7.7% of all the "bad" IP addresses Fraudlogix tracked, and just 0.05% of the "good" ones.

"It's super easy to set up cheap servers in the cloud and to set up scripts and programs to create fake traffic," said Fraudlogix CEO Hagai Shechter. "AWS is a great service for a lot of reasons. The good guys love it and find it easy to work with, and the bad guys do too," he explained.

According to Mr. Schechter, Amazon itself isn't creating the traffic. Rather, it's service is being used by some bad actors for nefarious purposes, but it's a difficult problem for the company to monitor and address.

Amazon said it employs a number of "mitigation techniques," both manual and automated, to prevent the misuse of its services. "Our terms of usage are clear, and when we find misuse we take action quickly to shut it down. Companies that do see malicious activity originating from AWS should contact us immediately," an Amazon spokesperson said.

The good news for marketers, however, is that fake traffic coming from Amazon servers is relatively easy to weed out. Since there's little real or "good" traffic coming from Amazon's servers, marketers should simply block all traffic originating from them, Fraudlogix advised. Doing so could eliminate over 7% of fake traffic affecting online advertising, the company said.

That's unlikely to provide a permanent fix, however. Ad fraud is often described as a "cat-and-mouse" game, and fraudsters can easily migrate their operations to other non-Amazon cloud computing providers if they need to.

Meanwhile, Comcast and Time Warner Cable say they're cracking down as best they can on the fraudulent traffic moving through their own systems, which is often created by infected computers used by their subscribers.

"Online safety is very important to us and it's why we created our Constant Guard Bot Detection and Notification System, which enables us to proactively identify customer accounts that appear to have been compromised," a Comcast spokesperson said.

Similarly, Time Warner Cable said it has a targeted bot detection and notification program in place.

"If it's determined that a customer has been infected by botnets, we make every attempt to notify the customer and provide guidance on cleaning the malware off of their system," a spokesperson for the company said.

Nonetheless, Time Warner Cable said pipe owners shouldn't be the only companies trying to fix the bot problem.

"As a major ISP serving millions of customers, we also believe that more accountability and more action is needed in the broader online ecosystem – including with the ad exchanges and browsers – to better deflect the criminal element where it enters the system," the company's spokesperson said. – ***Wall Street Journal***

BCAP
Broadband
Cable Association
of Pennsylvania
127 State Street, Harrisburg, PA 17101
717.214.2000 • bcapa.com

First in Broadband.
The Future of Broadband.®