eyeReturn MARKETING

Online fraud

Everything Marketers need to know to protect their media investment

Principal Author
Ian Hewetson
VP Client Services

Online Fraud

Taking Action to Safeguard Your Media Investment

With nicknames like Loveletter, Sobig, Bagle, and Gumblar, it's easy to underestimate the impact of online fraud in the digital media marketplace. And yet, over the past decade or more, cybercrime has evolved from more general trouble-making into a commercial endeavor that's capable of earning big money for fraudsters around the world.

Any time major dollars are being spent in an industry, such as the many billions of dollars invested into digital advertising each year by marketing firms worldwide, there will be networks of people who will attempt to tap into that revenue stream.

Enter online fraud: With an estimated 13% of home networks in North America infected with malware, and up to 95% of the world's Global 5000 enterprises impacted, the issue of online fraud has never been more important than it is today, where the complexity of the digital media industry offers a foothold for fraud to be entrenched at every step in the advertising process.

This paper examines online fraud from several angles. First, we define the issue and look at how it's propagated in the digital media sector. Then, we discuss the magnitude of online fraud and the impact it's having on different groups in the media sector. And finally, we outline practical steps that you can take to safeguard both your brand and your media investment from cybercrime.

What is Online Fraud?

Online criminal activity can take dozens of forms, and is defined in just as many ways by the various agencies and associations tasked with investigating, infiltrating, and shutting down cybercrime worldwide. For the purposes of this paper, we focus on the most prevalent and revenue-impacting type of fraud in the online industry today: digital ad fraud perpetuated by non-human internet traffic.

Because online fraud is so pervasive, and at the same time, so easily camouflaged in the many billions of engagement metrics (like clicks and impressions) achieved on marketing campaigns around the world, it's admittedly difficult to put a real number against the magnitude of its impact. So, while Vivek Shah, chairman of the Interactive Advertising Bureau (IAB) in the US, suggests that a full 36 percent of all web traffic is non-human, some estimates range to as high as 50 to 60 percent – suggesting that non-human web traffic is far more entrenched than industry members generally consider when planning and executing their clients' marketing campaigns.

This type of traffic is usually driven by the introduction of a program – referred to as a "robot" or "bot" – that operates as an agent for a user or another program. When bots are introduced by fraudsters as a means to simulate human activity, as with online click fraud, robot traffic networks ("botnets") have the potential to accelerate cybercrime's scope and depth more than any other tool in the last decade.

How Are Botnets Used in Online Fraud?

Cybercriminals target both personal as well as business networks with malware, and unsuspecting users are persuaded to download virulent software, often via "drive-by downloads," which use exploit kits coded into hacked and/or malicious websites. Once set up, this malware introduces bots into the system's network. Once infected with bots, computers become "zombies" and can be directed to sites that the users themselves would never visit; this happens in the background, and users are often unaware of the activity taking place.

Fraudulent clusters of sites may be set up with the singular intent of hosting real paid ads viewed only by hijacked computers. Botnets are designed to rack up billions of visits to these and other sites, all within a very short period of time. Yet, because of the potential number of computers that can be hijacked in any bot network the resulting inflated metrics don't always trigger warning bells for most ad agency or exchange analyst personnel.

Botnets cross geographic boundaries, so it appears that visitors are coming from a wide range of IPs. The most sophisticated botnets built in the last 5 or 6 years are designed to very closely simulate human activity, by clicking on display ads on many different sites in a matter of minutes or seconds, playing videos, and even moving products into shopping carts.

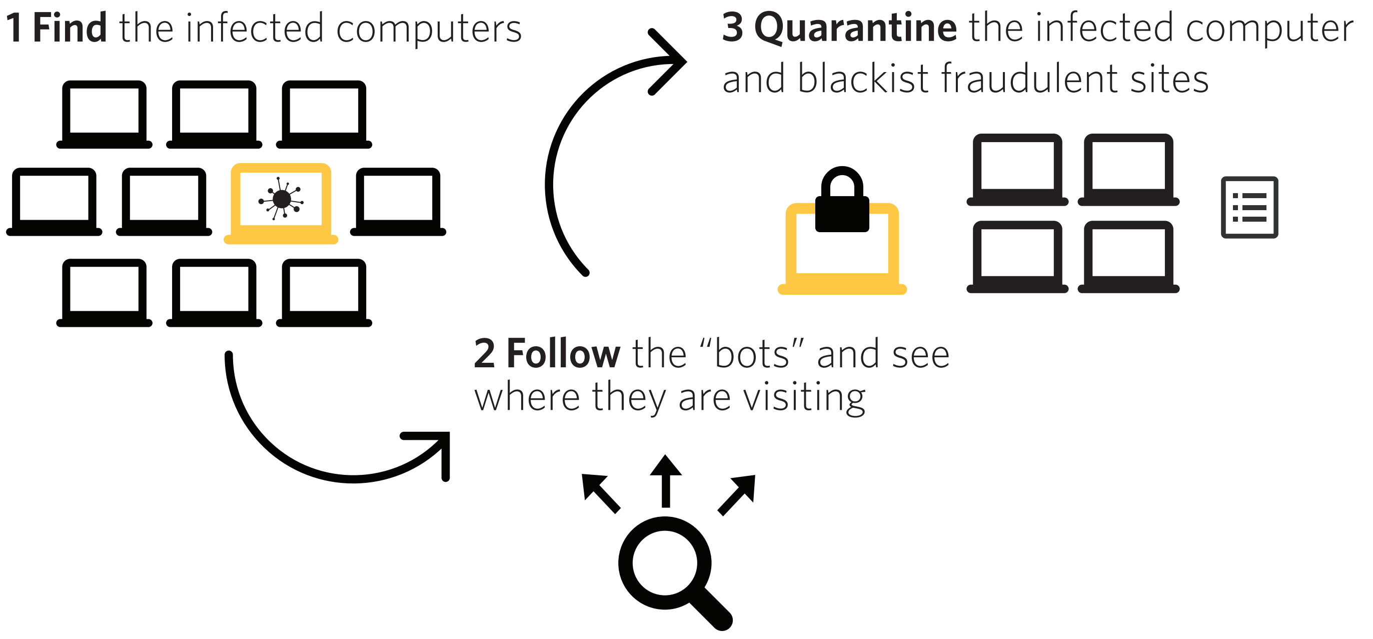
The subsequent engagement statistics from these campaigns are decent but generally not so high that they make advertisers question the performance. The industry is stirring with rumours of more advanced botnets on the horizon, ones that target new software vulnerabilities and can infiltrate Cloud and mobile operating systems.

What Does This Mean For Marketers?

It's estimated that click fraud malware like the ZeroAccess botnet impacts some 2.2 million home networks worldwide. This contributes to a revenue loss of more than $900,000 per day due to faked online traffic engagement. Yet, because digital ad campaigns are mostly booked by volume – that is, the number of impressions, click-throughs, and other measures of engagement an ad can drive for a brand – there's very little incentive for publishers, network owners, and even agencies and ad companies to investigate and quarantine suspicious sources of online traffic. This is especially the case when non-human online traffic so quickly ratchets up those campaign statistics that drive the media spend.

Nevertheless, beyond the massive loss of revenue for brands who invest in faked traffic, there are even more significant and further reaching implications that result from allowing online traffic fraud to continue, including the potential for brands to lose confidence in digital media as an effective engagement tool; diluting media value and chipping away at the credibility of legitimate publishers, networks and exchanges; and perhaps most problematically, undermining the integrity of the digital media industry as a whole.

There have been renewed calls for stakeholders in the digital sector to take a stand and change the way they do business. The next section details what you can do as an industry member to safeguard your advertising dollars against online fraud, while still getting the best return on your digital media spend.



1 Find the infected computers

2 Follow the "bots" and see where they are visiting

3 Quarantine the infected computer and blackist fraudulent sites

What Can Industry Members Do To

Safeguard Their Digital Media Investments?

Not all companies have the capability to update their business practices to continually track and stamp out botnets and other online fraud schemes as they unfold. However, every company – regardless of size or scope – can take proactive measures to reduce risk. The IAB, that represents leading media and digital technology companies in the US and Canada, recommends that industry members consider not just changing their thinking, but also adapting some of the ways they do business, in order to become more aware of potential threats from online fraud.

Stay Informed

As discussed above, cybercriminals continue to adapt to the ever-changing media landscape. Just as quickly as opportunities open up for new and innovative digital engagement for your clients, you can be certain that fraudsters are devising ways to take advantage of the situation to make a cut of the profit, ultimately resulting in losses for you and your clients. One solution: Stay vigilant, and educate yourself on the risks that online fraud poses to your and your clients' businesses.

Take Proactive Measures (even small ones)

Once you apply your knowledge of potential threats to the integrity of your media spend, you'll want to take some steps to protect those campaign dollars. Even small changes can make a difference. A first step is educating buyers and analysts on some of the high-level signs that the media they've paid for isn't adding up to the metrics they're seeing on any given campaign. Also, consider updating business policies to address the impact that fraudulent traffic can have on campaign results, so you can get ahead of conversations that may arise with your clients.

Change the Way You Think about Campaign Delivery Measurements

The industry's long-standing reliance on ad impressions and click-through rates as the main measures of engagement allows click fraud to perpetuate and encourages fraudsters to continue to build schemes to take advantage of these performance metrics. If you're looking for real measures of conversion, look for activities that can't be as easily gamed, such as purchases or subscriptions. By changing the way that you think about campaign results, you'll make it harder for cybercriminals to tap into your ROI, and you'll be able to show even more meaningful conversion rates for your clients.

Know Who You Should Do Business With

As the industry continues to grow and more media sources launch that offer that magic combination of amazingly high impressions for significantly low rates, an important part of vigilance includes performing due diligence on current and potential business partners to ensure that you're investing your ad dollars in reputable, measurable, and verifiable sources.

Ask tough questions of your suppliers and partners, and weigh their abilities to back up their claims with proven results.

Some questions the IAB suggests you ask:

- Do you have your audience measured by credible third-party systems?
- How do you determine which impressions are exposed to real humans?
- How do you ensure that ads are served as reported, and that URLs are visible to advertisers?
- How do you determine whether ads are auto-initiated or user-initiated?
- Do you provide protection from malware?
- Can your partners describe what measures they are taking to combat fraud?

Implement a System for Detecting and Dealing with Fraudulent Traffic

Says Ian Hewetson, VP Client Services of eyeReturn Marketing – the second largest demand-side platform (DSP) in Canada – the trick to combating fraudulent traffic is seeing the signals through the noise.

The solution lies in the intersection between human and machine analysis and intervention. Companies that have a depth of reach across millions of websites are most strategically placed to detect fraud. This bird's eye perspective allows them to tease out relationships between sites that they'd expect would show traffic and user affinities. Any outlying behaviour gets flagged, and the many millions of data points collected by these networks and DSP providers are used to weed out botnet traffic from good traffic.

It takes resources, commitment and market position – to have the scale and scope to drive enough volume of traffic through ad-serving activities to see the malicious patterns emerge.

Stamping Out Online Fraud Starts with You

Several factors come into play when it comes to the pervasiveness of botnet fraud in the digital media industry. Cybercriminals work hard to cover their tracks and hide their activities, and their concerted efforts pay them back many times over when they're able to tap into the billions of dollars spent by marketers on digital media campaigns every year.

For the most part, media professionals are able to turn a blind eye to the infiltration of a certain percentage of fraudulent traffic in their campaigns – in our time-starved and media-frenzied world, who has the time to dig into the data, especially if the impression and click-through rates are hitting required targets? Add to this the common perception that online fraud only really impacts a small percentage of users – the uneducated masses who click on bad links and introduce viruses into their computer system. But the digital media industry is reaching a tipping point: As more news reports shed light on the degree to which cybercrime has infiltrated both personal as well as commercial networks, and major retailers and manufacturers continue to get hit by cyber-attacks that jeopardize not only their reputation but also their revenues, it's incumbent on the media industry to step up and address online botnet fraud.

By taking practical measures to fight fraud – including simple steps like staying current on the latest innovations, looking beyond traditional campaign metrics to see real engagement taking place between your clients and their customers, and working with partners who have the capability to detect fraud and block it from further infiltrating your campaigns – members at every level of the industry can play a part in safeguarding the reputation, revenue, and longevity of digital media in the years to come.

Sources

Baines, Victoria, 2013. "Fighting the industrialization of cybercrime." *UN Chronicle 50(2), August.*
http://unchronicle.un.org/article/fighting-industrialization-cyber-crime (accessed 10.02.14).

Bradley, Tony, 2014. "The top 5 security threats to watch for in 2014." *PC World, January 30.*
http://www.pcworld.com/article/2092226/the-top-5-security-threats-to-watch-for-in-2014.html (accessed 10.02.14).

Canadian Anti-Fraud Centre.
www.antifraudcentre-centreantifraude.ca (accessed 10.02.14).

Canadian Newswire (CNW). (accessed 10.02.14).

Gonsalves, Antone, 2013. "Botnet simulated humans to siphon millions in click-fraud scam." *CSO Online, March 20.*
www.csoonline.com/article/730565/botnet-simulated-humans-to-siphon-millions-in-click-fraud-scam (accessed 10.02.14).

Interactive Advertising Bureau, 2013. Traffic Fraud Best Practices for Reducing Risk to Exposure. *December 5.*
http://www.iab.net/media/file/IABTrafficFraudBestPractices.pdf (accessed 10.02.14).

Interactive Advertising Bureau, n.d. Understanding Online Traffic Fraud.
http://www.iab.net/media/file/IABDigitalSimplifiedUnderstandingOnlineTrafficFraud.pdf (accessed 10.02.14).

Krebs, Brian, 2013. "Microsoft, Symantec Hijack 'Bamital' Botnet." *February 7.*
http://krebsonsecurity.com/2013/02/microsoft-symantec-hijack-bamital-botnet (accessed 18.02.14).

Marshall, Jack, 2014. "IAB chair: Time to take ad fraud seriously." *Digiday, February 10.*
http://digiday.com/platforms/advertising-fraud-iab (accessed 10.02.14).

Mello, John P., 2013. "Malware attacks target home networks." *PC World January: 36.*

Rothenberg, Randall, 2014. "IAB Head: 'The Digital Advertising Industry Must Stop Having Unprotected Sex'." *Business Insider, February 5.*
http://www.businessinsider.com/iab-randall-rothenberg-supply-chain-2014-2 (accessed 19.02.14).

Steward, Christopher S. and Marr, Merissa, 2013. "Inside the effort to kill a web fraud 'botnet'." *The Wall Street Journal, December 5.*
http://online.wsj.com/news/articles/SB10001424052702303722104579240151385337672 (accessed 10.02.14).

Tso, Richard L., 2013. "Special report: Ad fraud and the anatomy of a botnet." *Adotas, December 11.*
http://www.adotas.com/2013/12/special-report-ad-fraud-and-the-anatomy-of-a-botnet (accessed 10.02.14).

For more information please contact Ian Hewetson at:
ihewetson@eyereturn.com | 416.929.4834 ext 223

eyeReturn
MARKETING