Janeth Jepkogei
Comp 116: Introduction to Computer Security
Mentor: Ming Chow

Digital Ad Fraud through use of "bots" to create False Traffic

Abstract

Advertisers worldwide are spending billions of dollars on digital ads with the expectation that their content will be displayed on the web and viewed by human beings who will potentially buy their products and services. The growth of this industry has however been met with the reality of digital ad fraud. Advertisers are loosing money to digital ad "bots" that create impressions and appear to be serving real audiences, but are actually "seen" only by computers. Fraudulent ad "bots" are responsible for visiting these sites and performing the clicks hence creating false traffic on the site. In this paper we will be looking at how digital ad fraud is executed, why this is a real concern that needs to be addressed, ways in which we can prevent this kind of attack from happening and then conclude with what the next steps are.

Introduction

According to a study done by the Interactive Advertisement Bureau (IAB), more than 36% of all web traffic is fake due to digital ad fraud [1]. There are two main types of digital ad fraud: impression fraud and search click fraud[2].

Impression fraud involves uses of fake websites that load tones of ads on the page without the intention of clicking through them[3]. This increases the number of times a web page is viewed but almost none of these ads are actually viewed by humans. Bots are used to repeatedly load pages so as to generate fake ad impressions. This kind of attack is common in the Pay per click advertisement[4].

Search click fraud involves putting up fake websites and participating in search networks. This kind of fraud uses bots as well to type keywords that cause search ads to load, and then to clicks on the ad so as to generate search ad revenue. Once the fraudster's bot clicks on the real ad, an advertiser gets a report that makes it look like the click came from a real, respected website. The money the advertiser pays however goes to the bot master.

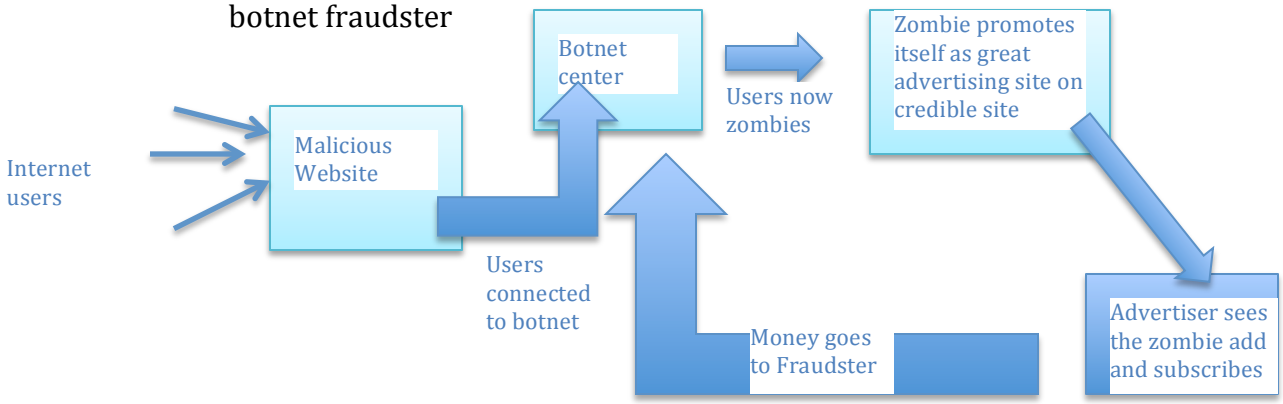
Digital ad fraud is carried out across all platforms. It affects computers, tablets and even mobile devices. The process by which this fraud is carried out is non-trivial too. To avoid being caught and to continue making money, fraudsters use lots of tricks in executing this attack.

Here is how a digital ad fraud process works:

---

[1] "Digital Ad Fraud."
[2] "Digital Ad Fraud and Bots Stories from the Front Line"
[3] "The Bot Baseline: Fraud in Digital Advertising | ANA."
[4] "Pay Per Click."

1. An innocent user clicks on a compromised link on his computer after visiting a random website that happened to be malicious.
2. On visiting the website, a malicious bot is immediately installed on his computer
3. The installed bot then begins to communicate with the botnet center and the user's computer is turned to a Zombie
4. The zombie is then programmed to execute requests, visiting different websites, mostly high-value audience sites, at certain frequencies and sequences so as to market the zombie computer as an ideal candidate for advertisers.
5. In addition to visiting websites, the bot also promotes itself as an "advertising impression storefront driving real unique visitors" which makes it look really attractive to advertisers
6. Due to need for website owners to increase traffic, they purchase impressions from the storefront site and the money goes to the botnet fraudster



This same process happens to millions of other computers, tablets and mobile devices all over the world increasing the intensity of the attack.

To the Community

Due to digital ad fraud, many advertisers have paid for millions of false ad impressions. These are ads "seen" by only computers not humans. According to the 2016 ANA/White Ops Bot Fraud study[5], it was estimated that advertisers could lose approximately $7.2 billion globally to bot-generated, non-human traffic in 2016[6]. This is a lot of money that companies are losing. Another study on an advertisement

[5] "The Bot Baseline: Fraud in Digital Advertising | ANA."
[6] "Eliminate Fraudulent Traffic."

run by Mercedes-Benz showed that 57% of the advertisement was viewed by bots. A news article on Financial Times reported, "In a sample of 365,000 ad impressions brokered by Rocket Fuel over three weeks, Telementry found that 57 per cent were "viewed " by automated computer programs rather than real people."[7] Digital fraud ad leads to huge losses of money especially in the advertisement industry and should therefore be called to the attention of everyone.

In addition to loss of money, digital ad fraud also destroys the credibility of a website. If a websites keeps buying impressions from a fraud storefront, then with time its credibility goes down as the advertisers will not be receiving as much returns from what they are spending advertising on that website.

Digital ad fraud also messes up analytics. Due to false traffic and lots of false impressions it is hard to get a true picture of what is going on in the industry. This could be really costly as it causes lots of false positives, which could lead to false confidence on how a company is doing for instance. Data analysis and predictions will also be skewed making it even more difficult to use the data.

Action Items:

Digital ad fraud is extremely profitable and the fraudsters won't stop doing it. However, there is need to protect ourselves from this form of attack. Below are some of the action items on how to protect oneself from digital ad fraud:

- **Monitoring traffic sources coming to your site**
  Digital ad fraud is automated and operated at certain frequencies and sequences. Bots traffic tends to be almost constant or in a certain predictable sequences which could be detected. In addition, bots tend to operate at all times of the day since they are programmed. Traffic on most websites is however low at night between 2-5am. Such patterns on the network traffic could be used to detect instances of digital ad fraud.

- **Sign up for the TAG Certified Against Fraud Program**
  This program provides additional tools to prevent digital ad fraud attacks, which include[8]:
    - **The Payment ID Protocol:** enables companies to ensure that payments made in the digital ad ecosystem are going to legitimate companies.
    - **The Data Center IP List** is a database of data centers from which fraudulent non-human ad traffic originates.
    - **The Domain Fraud Threat List:** A database of domains identified as known sources of fraudulent bot traffic for digital ads

---

[7] "Mercedes Online Ads Viewed More by Fraudster Robots than Humans."
[8] "Eliminate Fraudulent Traffic."

- **The Publisher Sourcing Disclosure Requirements** (PSDR): Fosters trust in the marketplace by disclosing the amount of sourced traffic for a given publisher

- **Get some knowledge about ad traffic frauds**
  Education is the most important piece. Everybody should be aware of digital ad frauds especially because your computer or device is likely to be the one executing this kind of attack. People should be aware of the websites they are visiting so as to also reduce the risk the being infected with the malware.

Conclusion

Despite the recommendations above, it is still very difficult to detect and prevent digital ad fraud from happening. None of the measures stated above are accurate. There is therefore need for more research to be done on this field so to come up with more effective ways of combating this attack. There is also need to educate more people on how they are vulnerable to such an attack. People should know how their devices could easily be turned into zombies that fraudsters use to execute attack. Most importantly, don't just visit any random websites.

References

"Digital Ad Fraud: The Seedy Underbelly of Online Advertising." *Ahead Of The Curve Blog*. Accessed December 15, 2016. http://www.inma.org/blogs/ahead-of-the-curve/post.cfm/digital-ad-fraud-the-seedy-underbelly-of-online-advertising.

"Digital Ad Fraud and Bots Stories from the Front Line" February 2016, Augustine Fou, Marketing Science consulting Group Inc. Accessed December 15,2016. http://rsquareedge.com/wp-content/uploads/2016/02/Stories-from-the-Front-Lines-2016-02-19-1.pdf

"Eliminate Fraudulent Traffic." *Trustworthy Accountability Group*. Accessed December 15, 2016. https://tagtoday.net/traffic/.

"Impression Fraud in On-Line Advertising via Pay-Per-View Networks | USENIX." Accessed December 15, 2016. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/springborn.

"Mercedes Online Ads Viewed More by Fraudster Robots than Humans." *Financial Times*. Accessed December 15, 2016. https://www.ft.com/content/788d6d42-da6c-11e3-8273-00144feabdc0.

"Pay Per Click." *Every Market Media*. Accessed December 15, 2016. http://everymarketmedia.com/glossary/pay-per-click/.

"The Bot Baseline: Fraud in Digital Advertising | ANA." Accessed December 15, 2016. http://www.ana.net/content/show/id/botfraud-2016.