ISPs and Ad Networks Against Botnet Ad Fraud

Nevena Vratonjic, Mohammad Hossein Manshaei, Maxim Raya, and Jean-Pierre Hubaux

Laboratory for computer Communications and Applications (LCA), EPFL, Switzerland
{nevena.vratonjic, hossein.manshaei, jean-pierre.hubaux}@epfl.ch, maxim.raya@gmail.com

Abstract. Botnets are a serious threat on the Internet and require huge resources to be thwarted. ISPs are in the best position to fight botnets and there are a number of recently proposed initiatives that focus on how ISPs should detect and remediate bots. However, it is very expensive for ISPs to do it alone and they would probably welcome some external funding. Among others, botnets severely affect ad networks (ANs), as botnets are increasingly used for ad fraud. Thus, ANs have an economic incentive, but they are not in the best position to fight botnet ad fraud. Consequently, ANs might be willing to subsidize the ISPs to do so. We provide a game-theoretic model to study the strategic behavior of ISPs and ANs and we identify the conditions under which ANs are likely to solve the problem of botnet ad fraud by themselves and those under which the AN will subsidize the ISP to achieve this goal. Our analytical and numerical results show that the optimal strategy depends on the ad revenue loss of the ANs due to ad fraud and the number of bots participating in ad fraud.

Keywords: Ad Fraud, Botnets, ISP, Ad Network, Security, Game Theory.

1 Introduction

Today, botnets are a very popular tool for perpetrating distributed attacks on the Internet. Botnets are a serious threat for a number of entities: end users, enterprises with online businesses, websites, Internet Service Providers (ISPs), advertisers and ad networks (ANs). Botnets usually consist of compromised end users’ PCs. Thus, depending on the malware, the consequences for end users can be severe (e.g., stolen credentials). Very often botnets are used for sending spam, which creates problems for ISPs, enterprises and end users. Botnet operators (aka bot masters) also use botnets to extort money from websites’ owners under the threat of Distributed Denial of Service Attacks (DDoS). Lately, it is becoming more and more popular to use botnets for ad fraud [4], which creates a loss of ad revenue for advertisers, associated websites and ad networks and security threats for end users (e.g., fraudulent ads that lead to phishing attacks).

Consequently, thwarting botnets would benefit everyone and would reduce the level of online crime on the Internet. However, the problem of botnets in general cannot be solved exclusively by users (lack of know-how), ISPs (too expensive to fight botnets alone), ad networks, advertisers, websites and enterprises (lack of tools and resources).

Recent initiatives propose that ISPs should perform the detection of botnets and remediation of the infected devices [20] [24]. Indeed, it is the ISPs that are in the best
position to detect the presence of a botnet and to take measures against it. Yet, the revenue of ISPs are not (directly) affected by the botnets and ISPs would probably welcome some external funding in the efforts to fight botnets. One possible approach is a government-sponsored program, as in Australia [7] and Germany [10]. In the case governments are unwilling to fund these initiatives, ISPs need to find a way to make them, at the very least, cost neutral if not cost positive.

Over the last decade, online advertising has become a major component of the Web, leading to annual revenues expressed in tens of billions of US Dollars (e.g., $22.4 billion in the US in 2009 [5]). The business model of a fast growing number of online services is based on online advertising and much of the Internet activity depends on that source of revenue. Unsurprisingly, the ad revenue has caught the eye of many ill-intentioned people who have started abusing the advertising system in various ways. In particular, click fraud has become a phenomenon of alarming proportions [4]. Recently, a new type of ad fraud attack has appeared, consisting in the on-the-fly modification of the ads themselves. A prominent example is the Bahama botnet, in which malware causes infected systems to display altered ads, as well as altered results for Google or Yahoo searches to the end users [17]. Another example of such a botnet is Gumblar [16]. If the modification of ads is successful, users see ads that are different from what they would otherwise be. Consequently, users’ clicks on the altered ads generate a revenue for the bot master instead of the AN. Thus, the modification of the ads negatively affects the revenues of the “legitimate” advertisers and undermines the business model of the ANs.

Considering the increasing trend of botnet ad-fraud attacks and the consequently increasing loss of ad revenue for ad networks, ANs have economic incentives to fight botnets. However, ANs are not in the best position to thwart botnets themselves and thus ANs might be willing to subsidize the ISPs to achieve that goal. In this paper, we investigate whether ad fraud botnets alone are cause enough for ISPs and ANs to cooperate. Such cooperation would help ISPs deploy detection and remediation mechanisms and would be a first step towards fighting all botnets.

The contributions of our paper are threefold. First, we identify two potential countermeasures that ANs could use to address the problem of botnet ad fraud and we propose a cooperation scheme in which ISPs and ANs jointly fight botnets. Second, we provide a game-theoretic model to study the interactions between ISPs and ANs, as well as to identify an optimal countermeasure strategy of ANs and ISPs under different conditions. Finally, we apply the results to a real data set to study the practical impact. To the best of our knowledge, this paper is the first to model the behavior of ISPs and ad networks facing botnet ad fraud.

The rest of the paper is organized as follows. After a brief presentation of the state of the art in Section 2, we describe the impact of botnets on the online advertising business in Section 3. We then address the various threats and countermeasures in Section 4 and provide a case study of a botnet ad fraud in Section 5. In Section 6, we present a game-theoretic model with two players, the ISP and the AN, and identify optimal equilibrium outcomes of that game. We provide a numerical example to study the practical impact of the obtained results in Section 7 and conclude the paper in Section 8.