ISPs and Ad Networks Against Botnet Ad Fraud

Nevena Vratonjic, Mohammad Hossein Manshaei and Jean-Pierre Hubaux
School of Computer and Communication Sciences, EPFL, Switzerland
{ nevena.vratonjic, hossein.manshaei, jean-pierre.hubaux}@epfl.ch

1. Botnet Ad Fraud

Today, botnets (collections of software agents running autonomously and automatically, typically on compromised end users' PCs) 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). 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 [1, 2]. Indeed, it is the ISPs that are in the best position to thwart the botnets. Yet, the revenues of ISPs are not (directly) affected by the botnets and ISPs would probably welcome some external funding in the efforts to fight botnets (e.g., government-sponsored programs in Australia [2]). 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 [3]). 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, people started abusing the advertising system in various ways. Lately, it is becoming more and more popular to use botnets for ad fraud [4, 5], which creates a loss of ad revenue for advertisers, associated websites and ANs and security threats for end users (e.g., fraudulent ads that lead to phishing attacks). Therefore, 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. We investigate whether ad fraud botnets are a strong enough reason 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.

2. System Model

We consider a system consisting of an *online advertising system*, a number of *bots* that attempt to exploit the online advertising system and an *ISP*, as depicted in Figure 1.

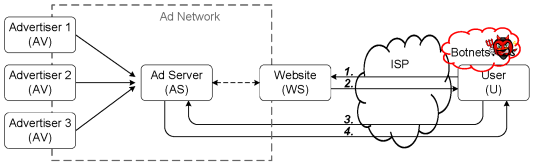

Figure 1. System Model: Online Advertising System, ISP and bots exploiting the advertising system.

The most prevalent model of serving online ads to end users is depicted in Figure 1. To have their ads appear with the appropriate web content, Advertisers (AV) subscribe with an ad network (AN) whose role is to automatically embed ads into web pages. Ad networks have contracts with Websites (WS) that want to host advertisements. When a User (U) visits a website (step *1*) that hosts ads, while downloading the content of the web page (step *2*), the user's browser will be directed to communicate with one of the Ad Servers (AS) belonging to the AN (step *3*). The AS chooses and serves (step *4*) the most appropriate ads to the user, such that users' interests are matched and the potential revenue is maximized.

We consider the types of ad fraud: (i) in which malware causes infected devices to display altered ads, which have been the most prominent lately [4, 5] and (ii) in which subverted users' routers modify ad traffic on-the-fly between a web server and a user [6]. When users click on the altered ads, the clicks generate revenue for

the bot master instead of the AN. Thus, the bots divert a part of the ad revenue from the AN.

3. Countermeasures

One possible approach for ANs to protect their revenue is to improve the security of the online advertising systems, thus making it more difficult for an adversary to successfully exploit those systems. For example, ad fraud can be reduced if webpages and ads are served over HTTPS instead of HTTP. The cost of implementing HTTPS at a web server includes the cost of obtaining a valid X.509 authentication certificate. Usually, website owners are not willing to bear this cost. Thus, if an AN wants the secure protocol to be deployed, it should cover the costs itself [7]. The AN may decide to selectively secure only the websites that generate sufficient ad revenue that compensates the costs.

Another possible approach for ANs to protect their revenue is to cooperate with ISPs and eliminate the major cause of the revenue loss, namely botnets. They can do so by funding the existing initiatives for ISPs to detect and remove botnets, since ISPs are in a privileged position to fight botnets. As removing botnets would benefit ANs, they have economic incentives to subsidize ISPs to thwart botnets.

4. Game-Theoretic Model

We introduce a static game to analyze the interaction between an ISP and an AN. In our model, the ISP can choose between the two actions: *Abstain* (*A*) and *Cooperate* (*C*). The AN can choose one of the following four actions: *Abstain* (*A*), *Cooperate* (*C*), *Secure and Cooperate* (*S+C*), and *Secure* (*S*). The *Abstain* models the ISP that is not willing to fight botnets and the AN not willing to perform any countermeasures. When cooperating, the ISP first detects the bots and then remediates infected devices, for which it receives a reward from the cooperative AN. The AN can secure the websites by choosing the action *S*. Finally, the AN can choose to simultaneously secure some of the websites and cooperate with the ISP to remediate some of the infected devices. The analytical results of our game-theoretic analysis are presented in details in [8].

In order to understand the implications of the analytical results in reality, we simulate the game using the real data on the ad traffic generated on the 1000 most popular websites obtained from *Compete.com*. We compute numerically the payoffs of the static game and identify the resulting equilibria. We represent the outcomes of the game for 10^4 bots in the system in Figure 2 and Figure 3. Figure 2 shows the number of secured websites depending on the fraction λ of the revenue that bots divert from the AN. When the AN cooperates with the ISP, the fraction of remediated devices depending on the level of threat λ is shown in Figure 3. We consider three scenarios, for three different efficiencies P_D of the detection system employed by the ISP.

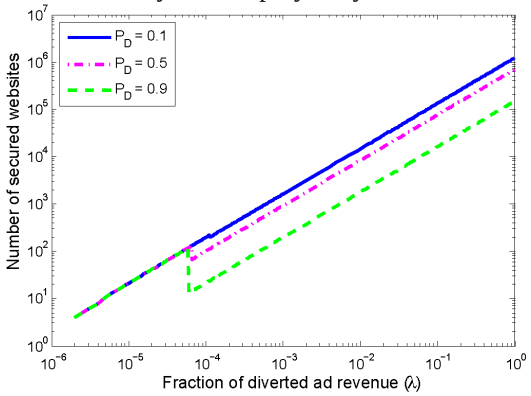

Figure 2. Number of the most popular websites to be secured

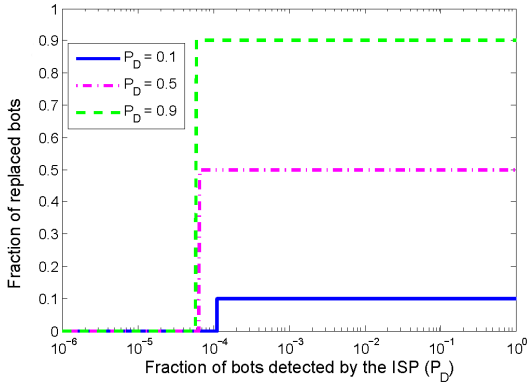

Figure 3. Fraction of infected devices remediated by the ISP

The obtained results illustrate that: (i) For a very low level of threat ($\lambda<2\cdot10^{-4}$) no countermeasures will be taken (no websites are secured and no infected devices are remediated); (ii) When the fraction λ of the diverted revenue increases, the AN secures a number of websites that depends on λ; (iii) Securing websites is not sufficient for an even higher level of threat (e.g., $\lambda>10^{-4}$ for P_D=0.1), thus the AN will in addition cooperate with the ISP to remediate infected devices.

4. Conclusions

The game-theoretic analysis of the behavior and interactions of the ISPs and ANs facing botnet ad fraud shows that cooperation could emerge under

certain conditions that mostly depend on: (i) the number of infected devices (ii) the aggregate power with which bots divert revenue from the AN and (iii) the efficiency of the botnet detection system. The cooperation is a win-win situation where: (i) users benefit from the ISP's help in maintaining the security of users' devices; (ii) the AN protects its ad revenue as the botnet ad fraud is reduced; (iii) it is at least cost neutral, if not cost positive for the ISP to fight botnets. Cooperation between the AN and the ISP would help to reduce the level of online crime and improve the Web security in general.

References

[1] Jason Livingood, N. Mody, Michael O'Reirdan and Comcast Communications. Recommendations for the Remediation of Bots in ISP Networks. IETF, 2009.

[2] Jason Livingood, N. Mody, Michael O'Reirdan and Comcast Communications. ISP Voluntary Code of Practice for Industry Self-regulation in the Area of e-security. Internet Industry Code of Practice, 2009.

[3] Internet Advertising Revenue Report. Interactive Advertising Bureau, 2009.

[4] Click Forensics Discovers Click Fraud Surge from New Sophisticated Bahama Botnet. http://www.clickforensics.com/newsroom/press-releases/144-bahama-botnet.html

[5] Viral Web Infection Siphons Ad Dollars from Google. http://www.theregister.co.uk/2009/05/14/viral_web_infection

[6] Nevena Vratonjic, Julien Freudiger and Jean-Pierre Hubaux. Integrity of the Web Content: The Case of Online Advertising. In Usenix CollSec '10: Workshop on Collaborative Methods for Security and Privacy, Washington, DC, USA, 2010. ACM.

[7] Nevena Vratonjic, Maxim Raya, Jean-Pierre Hubaux and David C. Parkes. Security Games in Online Advertising: Can Ads Help Secure the Web? In WEIS '10: Workshop on Economics of Information Security, Cambridge, MA, USA, 2010.

[8] Nevena Vratonjic, Hossein Manshaei, Maxim Raya, and Jean-Pierre Hubaux. ISPs and Ad Networks Against Botnet Ad Fraud. In GameSec' 10: Proceedings of the First Conference on Decision and Game Theory for Security, Berlin, Germany, 2010.

Nevena Vratonjic is a PhD student in the Laboratory for Computer Communications and Applications (LCA) at EPFL. Prior to pursuing a PhD degree, she completed one year of the Master Program in Computer Science at EPFL in 2007. She obtained a MSc degree in Communication Systems and a BSc degree in Electrical Engineering from University of Belgrade, Serbia in 2006. Her research interests are in the area of network and system security. Her current research work focuses on online advertising frauds and security of online ad serving systems. For more details, see http://people.epfl.ch/nevena.vratonjic

Mohammad Hossein Manshaei earned his B.Sc. degree in electrical engineering and his M.Sc. degree in communication engineering from the Isfahan University of Technology (IUT), Iran, in 1997 and 2000, respectively. He earned another M.Sc. degree in computer science and his Ph.D. in computer science and distributed systems from the University of Nice Sophia-Antipolis, France, in 2002 and 2005, respectively. He completed his thesis work at INRIA Sophia-Antipolis. He currently works as a senior researcher and lecturer at the Laboratory for Computer Communications and Applications (LCA) in EPFL. His research interests include wireless networking, security and privacy, social networks, cognitive radios, and game theory. For more details, see **http://people.epfl.ch/manshaei**

Jean-Pierre Hubaux has been a faculty member at EPFL since 1990. His current research activity is focused on privacy preservation mechanisms in pervasive communications. He has authored and co-authored more than 150 publications in networking, network security and privacy. In 2008, he completed a graduate textbook entitled "Security and Cooperation in Wireless Networks", with Levente Buttyan. He held visiting positions at the IBM T.J. Watson Research Center and at UC Berkeley. He is a Fellow of both ACM and IEEE. For more details, see http://people.epfl.ch/jean-pierre.hubaux