Poster: Adaptive Data-Driven and Region-Aware Detection for Deceptive Advertising

TonTon Hsien-De Huang and Chia-Mu Yu
Cheetah Mobile
Yuan Ze University

***Abstract*—We find a new trend, called *deceptive advertising* (*deceptive ads*), that some advertisers get paid through pay-per-install schemes. Deceptive ads is the use of false or misleading statements in advertising, which attracts users to click but negatively affects stakeholders. Nevertheless, despite the popularity of deceptive ads, not much research attention has been devoted to the detection. Bad actors use regional advertising, and have a much shorter lifetime than other security threats (e.g., phishing). The fast flux-like behavior of deceptive ads even poses the difficulty in protecting against deceptive ads. Due to the above reasons, we introduce a detection system for data-driven and region-aware detection of deceptive ads with automated feature extraction for further text-mining and pattern recognition. Our proposed system has been deployed in our testbed for intensive analysis and has shown that such hybrid approach yields acceptable results based on our massive real dataset.**

I. Introduction

Deceptive Advertising. Marketing pioneer John Wanamaker said, "Half the money I spend on advertising is wasted; the trouble is, I dont know which half."[1] Deceptive advertising (deceptive ads), a particular type of malicious advertising [1], [2], is the use of false or misleading statements in advertising, and may cause negative impact on stakeholders. Despite its impact on both PCs and mobile devices, deceptive ads causes more impact on mobile devices. Deceptive ads is not a new threat; however, since mobile devices are always on and carried 24/7, such a threat has quickly ascended on the list of everyday Internet threats. Fig. 1 shows an example of deceptive ads whose pop-up ads shows falsified information and instructions. Based on our user base during the past ten weeks, we show in Fig. 2 that the deceptive ads have a stable growth on many countries.

Google has updated its policy that dictates App developers what sort of content their Apps are permitted to display, with a number of rules designed to crack down deceptive ads[2]. In fact, Google is also taking sweeping out deceptive ads in Google Play in consideration[3]. Unfortunately, there have only been few research efforts for detecting deceptive ads on malicious URLs. For example, the pre-defined features or fixed delimiters for feature selection and reactive URL blacklisting can be used for the detection. However, these techniques are inefficient in detecting deceptive ads due to the short lifetime

[1]https://en.wikipedia.org/wiki/John Wanamaker
[2]https://play.google.com/intl/ALL in/about/monetization.html
[3]https://nakedsecurity.sophos.com/2014/04/04/google-takes-aim-at-deceptive-advertising-of-play-store-apps/

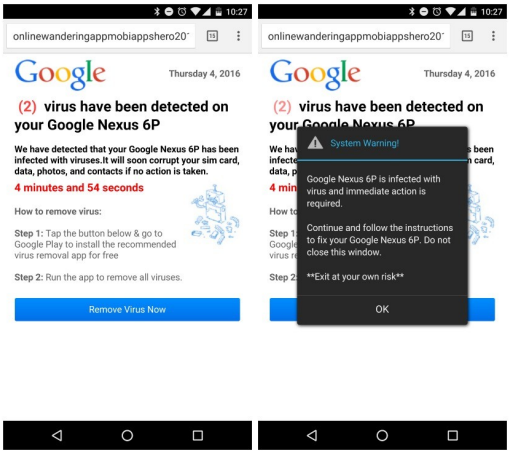


Fig. 1: Examples of deceptive ads.

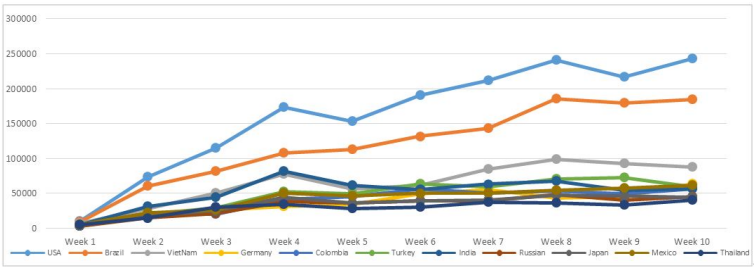
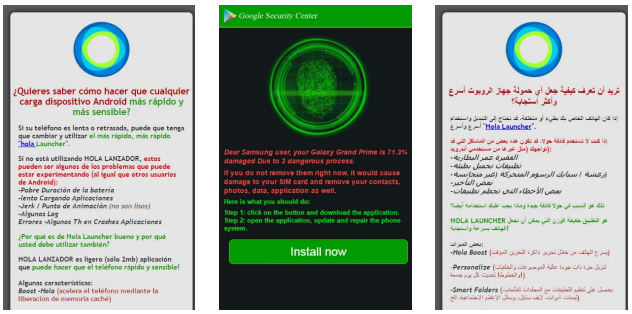


Fig. 2: The growth of the number of deceptive ads in different countries.

of deceptive ads. In fact, we observe that the recent deceptive ads exhibits a fast flux-like and region-aware behaviors. The former means that the URL of the deceptive ads would be valid for only a very short time interval, while the latter means that, by visiting the same deceptive ads URL, the browsers in different countries or even the same browser with different language settings may see different contents (see Fig. 3). These two features makes tracking down the deceptive ads much more difficult.

II. Our Proposed System

Design Idea. The architecture of our proposed system is shown in Fig. 4. In short, our system is a cloud-assisted host-based detection. One may see that once the user device (e.g., smartphone) goes to an URL, the information about the browsing will be sent to the cloud service implemented



(a) (b) (c)

Fig. 3: Multilingual deceptive ads examples.

with our detection core. Afterwards, the cloud will return the detection result to the user device.

Our approach not only collects multilingual deceptive ads from different regions but also generate ontology to represent the semantic of the multilingual text wording. More concretely, we use crawler to collect data from different regions, extract the wordings of deceptive concepts for text mining, extract image features from popular deceptive ads, and then generate the related semantic of behavior. After that, we calculate the weights of extracted wordings and image features under the different regions based on Type-2 Fuzzy Logic, and then store them as JSON format of ontology (*e.g.*, Protégé[4]) to generate OWL for constructing the knowledge base of the ontology.

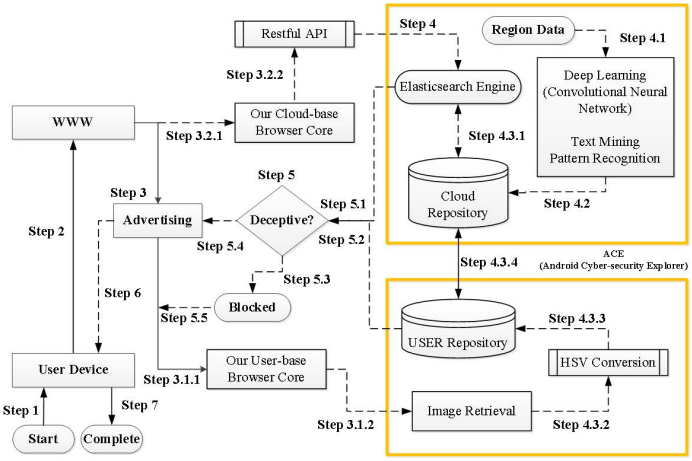


Fig. 4: The architecture of our detection system.

The Detection of Deceptive Ads. Based on our user base and backend system, we collect more than one hundred million advertising URLs everyday, and then capture the advertising figures as the input to our system to learn the difference between benign and deceptive ads. Note that our system has a pre-filter mechanism that uses the blacklist approach to promptly identify the suspicious ads. After that, we adopt machine learning approach to differentiate between benign and deceptive ads. In particular, bad actors use regional and multilingual advertising to generate deceptive ads and have a much shorter lifecycle compared to other cybersecurity problems (as shown in Figure 8 and Figure 9). As a result, we also generate multilingual semantic ontology.

[4]http://protege.stanford.edu

III. Evaluation Results

As the first step toward the detection, our system is implemented by Python language and integrate with some open source projects such as an asynchronous and customizable analysis platform: IRMA[5], Elasticsearch which provides the most powerful full-text search capabilities[6] and Kibana which easily visualizes data[7]. We also provide a simple RESTful API using JSON formatted report over HTTP.

Based on our user base, we have collected a huge dataset of both benign and deceptive ads. Some deceptive ads contains only texts, some shows only a figure, and some others are the combination of texts and figures. For the text part, we extracted the texts first. After that, for non-English texts, we turn them to English texts by taking advantage of translation API. We then do the text mining to classify the ads as either benign or deceptive ads. Note that we have a labelled dataset ("deceptive" and "benign" labels), which is manually constructed by our research team. Thus, we are able to have estimation on the detection accuracy. Our system can accurately identify the deceptive ads with only texts with precision and recall nearly reaching 1. On the other hand, we consider the deceptive ads with figures. For the deceptive ads with figures, Our system can also accurately identify the deceptive ads with precision and recall nearly reaching 1.

IV. Conclusion and Future Work

The proposed detection system is tested in our internal environment. The results show that our detection system works very well to detect deceptive ads. The future work is to reduce the complex task from a huge amount of computation burden.

References

[1] D. Huang, K. Xu, and J. Pei. Malicious URL detection by dynamically mining patterns without pre-defined elements. *World Wide Web*, pp. 1375-1394, 2014.

[2] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang. Knowing your enemy: understanding and detecting malicious web Advertising. *ACMConference on Computer and Communications Security (CCS)*, 2012.

[5]http://irma.quarkslab.com

[6]https://www.elastic.co

[7]https://www.elastic.co/products/kibana