FalseClick: Analyzing Social Engineering Campaigns and Content via Trick Ads

M. Zubair Rafique* and Wouter Joosen*
*iMinds-DistriNet, KU Leuven
{*zubair.rafique,wouter.joosen*}*@cs.kuleuven.be*

I. Abstract

Internet advertising is one of the compelling methods for businesses to advertise their products and to diversify their revenue streams. Because of its pervasiveness, attackers have leveraged Internet advertising as an effective way for distributing malware and unwanted softwares [1], [4]. One well-known class of attacks through Internet advertising is a wide usage of *trick ads* (or trick banners) that manipulate Internet user's perception in order to gain a click on the displayed ad image, potentially leading the user to a malicious domain (e.g., by clicking on an ad that imitates the alert of an infected PC or by clicking on a fake download button).

Prior studies demonstrated that trick banners imposed a significant threat not only to the security of common Internet users, but also to those who are well equipped with technical security knowledge [5]. In general, Internet advertising that tries to deceive/persuade users to perform actions (e.g., installing a malicious browser extension to watch videos online etc.) that they would only carry out for a trusted entity is considered as one of the active and emerging attack vector [3], [4], [7]. To this end, researchers have proposed TrueClick, a supervised learning technique, to automatically identify the trick banners on a webpage in an effort to protect Internet users from such malicious trick banners [1]. However, TrueClick's applicability is limited to a specific type of images that deceive users through disguised download or play images on the webpages. More recently, Google has enhanced its Safe Browsing protection to warn users about the websites that contain deceptive advertisement content. Moreover, the recent work of Terry et. al [4] measures and detect the software (*only binaries*) download attacks through social engineering by passively inspecting network traffic. Their results reveal that the majority of social engineering download attacks are due to Internet advertising supplied through low-tire ad networks.

In the work-in-progress presented here, we seek to perform a first measurement study of trick ads by *infiltrating* the selected ad networks. We strive to develop an infrastructure that (1) facilitates the gathering of diverse and large volumes of trick ad images by reversing and replaying the protocol interaction used by the selected ad networks to display ad images on the websites, (2) use the collected trick ad images as an oracle to automatically identify the displayed trick ads and perform a click while crawling the websites, (3) capture the redirection chain to a final landing domain and analyze the contents offered on the opened ad websites (e.g., malicious binaries [2], unwanted browser extensions, scams, etc.), and (4) utilize the germane DNS information of the ad websites to discover a variety of additional ad websites managed by the same entities. We report initial results of our infiltration on adk2x.com–an ad network that we found responsible of displaying majority of trick ads on the free live streaming websites [6]. Figure 1 shows the work-flow of our approach.

So far, we have stockpiled over 8,000 images, from our brief infiltration of adk2x.com, into our gradually expanding oracle of trick ad images. These images contain a wide variety of multilingual trick ads, fake download and play buttons, banners to get a green card from "trusted sources", fake video players, infection alarms, etc. We intend to make this dataset publicly available to foster further research on trick ads.

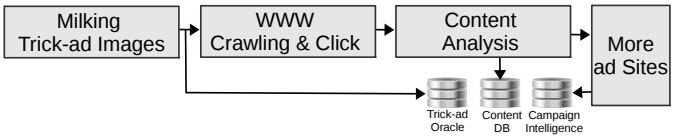

Figure 1: Work-flow of our proposed approach.

By clicking on a *single* trick ad and following the proposed approach, we have identified 48 ad websites hosted on the Google sites offering variety of potentially unwanted Chrome extensions and potentially unwanted binaries. Table I shows the top 25 identified websites and their Alexa rankings. We found that some websites like winrepairpro.com try to trick users to install unwanted binary disguised as antivirus software, while a number of other websites, e.g., safesidetab.com, mynewtabtv.com, try to trick users to install unwanted browser extensions for "better protection" and for "easy access" to online movies and videos. At the time of writing, none of the discovered websites were marked as unsafe in the Google Safe Browsing database.

On further analysis we discovered a new family of *malicious* Chrome extensions that changes the default search-engine page and provides a disguised antivirus software link in the browser to deceive users to install a potentially unwanted binary. Our investigations confirmed Imali.media as the advertiser of all the discovered software programs (binaries and browser extensions).

In this work-in-progress, we propose active infiltration technique to study social engineering attacks launched through trick ads. Our technique provides greater visibility of social engineering attacks through trick ads (beyond executable download attacks), and can be effectively used to minimize the manual effort of updating blacklists of deceptive websites. In the future, we plan to extend our infrastructure to infiltrate a number of carefully selected ad networks that employ deceptive, persuasive, and *coercion* techniques for monetary gains at the expense of Internet users' security.

No.	Web Site	IP	Hosting	Rank
1	newtab-media.com	108.59.81.209	Google Inc	2,249
2	newtab-tv.com	108.59.81.209	Google Inc	5,998
3	medianewtab.com	108.59.81.209	Google Inc	8,819
4	mediatvtab.com	108.59.81.209	Google Inc	12,498
5	mysafetab.com	108.59.81.209	Google Inc	15,870
6	mysafetabs.com	108.59.81.209	Google Inc	18,020
7	emaildefend.com	108.59.81.209	Google Inc	22,554
8	socialnewtabs.com	108.59.81.209	Google Inc	26,947
9	socialnewtab.com	108.59.81.209	Google Inc	31,520
10	socialmedianewtab.com	108.59.81.209	Google Inc	50,339
11	tvnewtab.com	108.59.81.209	Google Inc	98,865
12	downvietnam.com	108.59.81.209	Google Inc	266,932
13	newtabtv.com	108.59.81.209	Google Inc	281,860
14	cooler.video	108.59.81.209	Google Inc	317,422
15	thecoolestmovies.com	108.59.81.209	Google Inc	374,686
16	realcoolmovie.com	108.59.81.209	Google Inc	460,263
17	tv-newtab.com	108.59.81.209	Google Inc	501,403
18	iqabrowser.com	108.59.81.209	Google Inc	608,704
19	internetquickaccess.com	108.59.81.209	Google Inc	631,929
20	mynewtabtv.com	108.59.81.209	Google Inc	737,114
21	safesidetab.com	108.59.81.209	Google Inc	807,209
22	wondrousmovies.com	108.59.81.209	Google Inc	843,724
23	videoplayerclassic.com	108.59.81.209	Google Inc	942,020
24	winrepairpro.com	108.59.81.209	Google Inc	972,422
25	improveyourpc.today	108.59.81.209	Google Inc	990,318

Table I: Discovered ad websites.

REFERENCES

[1] Sevtap Duman, Kaan Onarlioglu, Ali Osman Ulusoy, William Robertson, and Engin Kirda. Trueclick: automatically distinguishing trick banners from genuine download links. In *ACSAC*, 2014.

[2] Platon Kotzias, Leyla Bilge, and Juan Caballero. Measuring pup prevalence and pup distribution through pay-per-install services. In *USENIX Security*, 2016.

[3] Nathan Wyman. Malvertising: When ads go rogue. https://www.webroot.com/blog/2016/03/14/malvertising-when-ads-go-rogue/.

[4] Terry Nelms, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad. Towards measuring and mitigating social engineering software download attacks. In *USENIX Security*, 2016.

[5] Kaan Onarlioglu, Utku Ozan Yilmaz, Engin Kirda, and Davide Balzarotti. Insights into user behavior in dealing with internet attacks. In *NDSS*, 2012.

[6] M. Zubair Rafique, Tom Van Goethem, Wouter Joosen, Christophe Huygens, and Nick Nikiforakis. It's free for a reason: Exploring the ecosystem of free live streaming services. In *NDSS*, 2016.

[7] Warwick Ashford. Social engineering confirmed as top information security threat. http://www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat.