COMPUTERS & SECURITY 76 (2018) 92–100

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Experimental large-scale review of attractors for detection of potentially unwanted applications

Vlasta Stavova [a], *Lenka Dedkova* [b], *Vashek Matyas* [a,*], *Mike Just* [c], *David Smahel* [a], *Martin Ukrop* [a]

[a] *Faculty of Informatics, Masaryk University, Czech Republic*
[b] *Faculty of Social Studies, Masaryk University, Czech Republic*
[c] *School of Mathematical & Computer Sciences, Heriot-Watt University, United Kingdom*

ARTICLE INFO

Article history:
Received 22 December 2017
Received in revised form 21 February 2018
Accepted 25 February 2018
Available online 12 March 2018

Keywords:
Usable security
Potentially unwanted application
Attractor
Security software
User decision

ABSTRACT

While malicious software (malware) is designed to disrupt or damage computer systems, potentially unwanted applications (PUAs) combine useful features with less desirable ones, such as adware or spyware. Unlike anti-malware solutions, removing PUAs can be controversial, for both the PUA owners and also the users who might wish to accept the PUA features. Thus, solutions for removing PUAs require users to make their removal decisions. In this paper we investigate the effectiveness of 15 screen variants that use different "security warning attractors" designed to encourage users to enable PUA detection when they are installing a security software solution from the online security software company ESET. Our live field study with close to 750,000 software installations by end users in 222 countries shows that a small change of switching the order of the options presented using radio buttons and offering the "enable detection" option first was the most effective (and was later set as the option of choice by ESET). The chosen approach led to a significant reduction of non-consenting users from 17.9% to 11.1%. Other features, such as the use of colours and pictorials, which have previously demonstrated their effectiveness with more traditional SSL security warnings, did not yield significant improvements for enabling PUA detection.

1. Introduction

Potentially unwanted applications (PUAs, a.k.a. potentially unwanted programs, PUPs), cover several arguably malicious families of software such as adware, spyware, pornware, bundleware or junkware. Differing from malicious software (*malware*), PUAs often combine a potentially useful feature with arguably less desirable features that deliver unwanted ads, monitor users' behaviour or collect their data (Stavova et al., 2016).

Many online security software solutions (e.g., endpoint antivirus with some additional features) include a service to detect and alert users about PUAs targeting their devices. However, automatically classifying an application as a PUA can be challenging, in part due to the different perceptions of what constitutes an "unwanted" application. For example, some PUAs might be knowingly installed by users, such as with browser

* *Corresponding author.*
E-mail addresses: vlasta.stavova@mail.muni.cz (V. Stavova), ldedkova@fss.muni.cz (L. Dedkova), matyas@fi.muni.cz (V. Matyas), m.just@hw.ac.uk (M. Just), davs@mail.muni.cz (D. Smahel), mukrop@mail.muni.cz (M. Ukrop).
https://doi.org/10.1016/j.cose.2018.02.017
0167-4048/

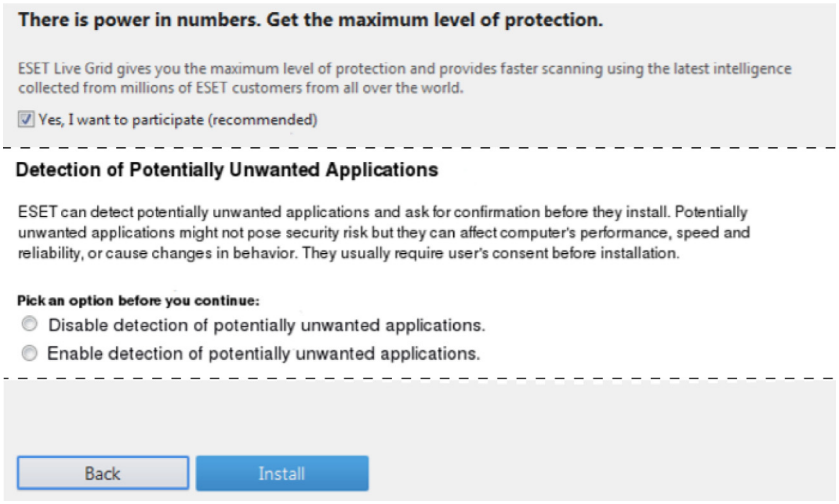

Fig. 1 – The control variant (A1) with highlighted area of PUA inquiry.

toolbars that are sometimes packaged with software. Even benign applications (such as remote desktop controllers or various registry cleaners) can contain functions that would be identified as unwanted by some users. However, automatically classifying such software as "unwanted" for all users can create confusion that could cause users to lose trust in PUA classification decisions. Further, as several example encounters have shown, well-established adware companies do not hesitate to sue security software vendors for automatically classifying their software as adware (Masnick, 1998).

These circumstances pose a unique challenge for security software vendors who want to protect their users and facilitate PUA detection, but who might be legally restricted from automatically removing a PUA. The approach chosen by vendors has been to involve users in the decision of labeling applications as unwanted, before removing them from their system. In this way, the approach to involve the user in PUA decisions is similar to what is done for security warnings, for example for phishing (Egelman and Schechter, 2013), SSL warnings (Fahl et al., 2012) or malware (Akhawe and Felt, 2013). While there has been much recent focus on such security warnings, there has surprisingly been little research undertaken so far in user decisions for PUA warnings.

There are two stages of user involvement with PUAs. First, there is a choice about whether or not to enable the detection of PUAs in users' security software. Second, if PUA detection is enabled, there are decisions about whether or not to accept or reject an individual application identified as a PUA. In this paper, we focus on the first stage.

A 2016 survey (AV Comparatives, 2016) with 2022 participants found that 73% of people who changed default security software settings (from 41.2% of all research participants) also enabled PUA detection. However, the study used users' self-reports, which may lead to inaccurate estimation of PUA detection enablement.

In our previous study (Stavova et al., 2016) we collected system installation data from a large set of beta testers and found out that overall, 74.7% of beta testers enabled PUA detection. Since beta testers may differ from standard end users in terms of their IT abilities, and consequently their ICT related behaviour, repeating research with standard end users is necessary (Stavova et al., 2018).

In this paper, we present the results of our study of the effectiveness of 15 variants with different "attractors" that were designed for encouraging users to enable the detection of PUAs. The attractors consist of different interface modifications, similar to those studied for security warnings.

Each of the 748,795 end users was presented with a single randomly chosen variant when installing an online security software solution from security software company ESET. We report the decisions of our end-user participants to enable the detection of PUAs, as well as the time they spent on each screen to make their decision.

The following section describes the dataset, introduces our data cleaning and analytical strategy, and presents the 15 designed variants. Section 3 reports on the effect of the attractors on users' decisions to enable the detection of PUAs. In Section 4, the issue of time spent on the variants' screens is examined. Study limitations and related research on PUAs are discussed in Sections 5 and 6. Section 7 then concludes our article.

2. Methods

Our study was conducted in cooperation with ESET, an online security software company with over 100 million users in more than 200 countries and territories[1]. During the installation process, ESET presents a screen dialog that asks users to either enable or disable the detection of PUAs. This step cannot be skipped and thus each user has to choose one option or the other, although it is possible to change this decision later in the software settings.

For our experiment, we prepared 15 different screen variants (14 new approaches and 1 control variant (A1) – see Figs 1 and 2) of the PUA enable/disable screen with various attractors. One variant was randomly selected for display to each user

[1] https://www.eset.com/int/about/.