1. Mobile App Squatting

Yangyu Hu (1); Haoyu Wang (2); Ren He (2); Li Li (3); Tyson, G. (4); Castro, I. (4); Yao Guo (5); Lei Wu (6); Guoai Xu (2)

Source: *WWW '20: Proceedings of The Web Conference 2020*, p 1727-38, 20 April 2020; **ISBN-13:** 978-1-4503-7023-3; **DOI:** 10.1145/3366423.3380243; **Conference:** WWW '20: The Web Conference 2020, 20-24 April 2020, Taipei, Taiwan; **Sponsor:** SIGWEB; **Publisher:** ACM, New York, NY, USA

Author affiliation: (1) BUPT, China (2) Beijing University of Posts and Telecommunications, China (3) Monash University, Melbourne, VIC, Australia (4) Queen Mary University of London, United Kingdom (5) Peking University, China (6) Zhejiang University, China

Abstract: Domain squatting, the adversarial tactic where attackers register domain names that mimic popular ones, has been observed for decades. However, there has been growing anecdotal evidence that this style of attack has spread to other domains. In this paper, we explore the presence of squatting attacks in the mobile app ecosystem. In “App Squatting”, attackers release apps with identifiers (e.g., app name or package name) that are confusingly similar to those of popular apps or well-known Internet brands. This paper presents the first in-depth measurement study of app squatting showing its prevalence and implications. We first identify 11 common deformation approaches of app squatters and propose “AppCrazy”, a tool for automatically generating variations of app identifiers. We have applied AppCrazy to the top-500 most popular apps in Google Play, generating 224,322 deformation keywords which we then use to test for app squatters on popular markets. Through this, we confirm the scale of the problem, identifying 10,553 squatting apps (an average of over 20 squatting apps for each legitimate one). Our investigation reveals that more than 51% of the squatting apps are malicious, with some being extremely popular (up to 10 million downloads). Meanwhile, we also find that mobile app markets have not been successful in identifying and eliminating squatting apps. Our findings demonstrate the urgency to identify and prevent app squatting abuses. To this end, we have publicly released all the identified squatting apps, as well as our tool AppCrazy. (0 refs)

Inspec controlled terms: Internet - mobile computing - security of data
Uncontrolled terms: app squatting abuses - identified squatting apps - mobile App Squatting - domain squatting - domain names - mimic popular ones - mobile app ecosystem - app name - app squatters - app identifiers - mobile app markets
Classification Code: C6130S Data security - C7210N Information networks - C6190J Internet software - C6190V Mobile, ubiquitous and pervasive computing
IPC Code: G06F9/44 - G06F21/00
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village