Dissecting Android Malware : Characterization and Evolution

Yajin Zhou and Xuxian Jiang

Tuesday, February 8, 2016

INTRODUCTION

The notoriety and reception of cell phones has significantly fortified the spread of versatile malware, particularly on the well known stages, for example, Android. As of late, there is an unstable development in cell phone deals and appropriation. By, shipments have tripled in the previous three years (from 40 million to around 120 million). To aggravate matters, the exploration group everywhere is still compelled by the absence of a far reaching versatile malware dataset to begin with. The objectives and commitments of this paper are triple. In the first place, The dataset is aggregated from over one year exertion in gathering related malware tests, including manual or computerized creeping from an assortment of Android Markets. Second, in light of the gathered malware tests, we perform a course of events investigation of their disclosure and altogether describe them taking into account their point by point conduct breakdown, including the establishment, initiation, and payloads. Third, we perform a development based investigation of delegate Android malware, which demonstrates that they are quickly advancing and existing against malware arrangements are genuinely lingering behind.

MALWARE TIMELINE

Malware	Samples	Discoveredmonth	Markets
—FakePlayer	—6—	—2010-08—	—yes—
—GPSSMSSpy—	—6—	—2010-08—	—yes—
—DroidkungFu3—	—309—	—2011-08—	—yes—
—Anserverbot—	—187—	—2011-09—	—yes—
DroidkungFu4—	—96—	—2011-2010—	—yes—

In Table, we demonstrate the rundown of 49 Android malware families in our dataset alongside the time when each specific malware family is found. We get the rundown via deliberately looking at the related security declarations, danger reports, and blog substance from existing portable antivirus organizations and dynamic analysts as thoroughly as could be expected under the circumstances and constantly asking for malware tests from them or effectively slithering from existing official and option Android Markets.

MALWARE CHARACTERIZATION

- Malware Installation.

By physically breaking down malware tests in our accumulation, we order existing ways Android malware use to introduce onto client telephones and sum them up into three principle social designing based strategies, i.e., repackaging, update attack, and drive-by download.

1. Repackaging

Repackaging is a standout amongst the most regular strategies malware creators use to piggyback malignant payloads into famous applications (or essentially applications).

1. Update Attack

The main system commonly piggybacks the whole vindictive payloads into host applications, which could conceivably uncover their vicinity.

1. Drive by Download

The third procedure applies the customary drive-by download assaults to portable space.

- Activation

The framework wide Android occasions of enthusiasm to existing Android malware. By enlisting for the related framework wide occasions, an Android malware can depend on the implicit backing of robotized occasion warning what's more, callbacks on Android to adaptably trigger or dispatch its payloads.

- Malicious Payloads

The premium-rate numbers, some malware moreover influence the same usefulness by sending SMS messages to other telephone numbers. Despite the fact that less genuine than past ones, regardless they bring about certain money related charges particularly at the point when the client does not have a boundless informing arrangement.

MALWARE EVOLUTION

- DroidKungFu

The rise of these DroidKungFu variations unmistakably shows the present fast advancement of Android malware. In the accompanying, we zoom in different parts of DroidKungFu malware.

1. Root Exploits

It is fascinating to notice that in DroidKungFu1, the record name with the scrambled root adventure is "ratc" the acronym of RageAgainstTheCage. In DroidKungFu2 and DroidKungFu3, this record name with the same root misuse has been changed to "myicon", claiming to be a symbol document.

- AnserverBot

AnserverBot was found in September 2011. This malware piggybacks on honest to goodness applications and is by and large effectively appropriated among a couple of outsider Android Markets in China.

MALWARE DETECTION

The quick development and advancement of late Android malware posture noteworthy difficulties for their discovery. In this area, we endeavor to gauge the adequacy of existing versatile hostile to infection programming. To this end, we pick four delegate portable hostile to infection programming, i.e., AVG Antivirus Free (or AVG), Lookout Security and Antivirus (or Lookout), Norton Mobile Security Lite (Norton), and TrendMicro Mobile Security Personal Edition (TrendMicro) what's more, download them from the official Android Market in the to start with week of November 2011.

CONCLUSION

There are some malware families that totally come up short these four versatile security programming. Cases are BeanBot, CoinPirate, DroidCoupon, DroidKungFuSapp, NickyBot and RogueLemon. The portrayal is made conceivable with our over one-year exertion in gathering 1260 Android malware tests in 49 distinctive families, which covers the dominant part of existing Android malware, running from its presentation in August 2010 to late ones in October 2011.