Security Apps under the Looking Glass: An Empirical Analysis of Android Security Apps

Weixian Yao, Yexuan Li, Weiye Lin, Tianhui Hu, Imran Chowdhury,
Rahat Masood, Suranga Seneviratne

THE UNIVERSITY OF SYDNEY

UNSW AUSTRALIA

Motivation

Huge Android Market

75% of 2.6 Billion users

Increasing growth of malware apps

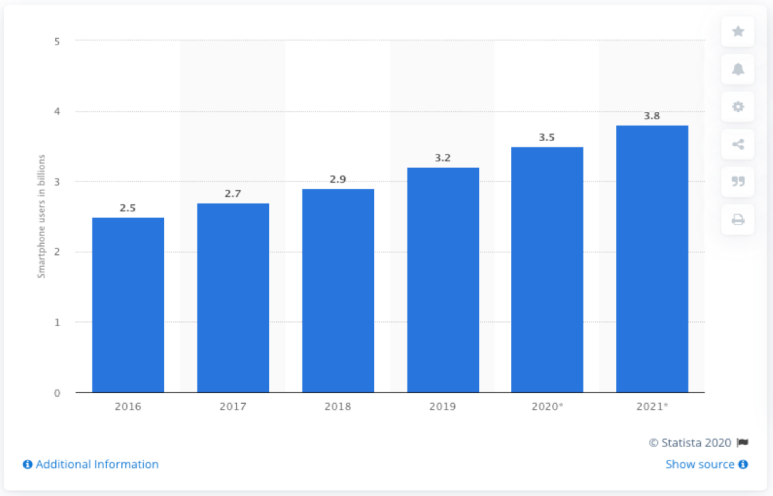
Only in 2015 malware grows 4 times as

Security risks of anti virus apps are overlooked

Not all security apps will make online movement more secure- and some cases they could be worse than doing nothing at all !

Number of smartphone users worldwide from 2016 to 2021

(in billions)



Permission requests of the top 10 Android antivirus, app locker and ad blocker apps

The table below shows the different categories of personal information that a number of top rated antivirus, app-locker and ad-blocker apps request to access when you install them on your device.

	Antivirus	App-lockers	Ad-blockers
Device history	10	9	5
Cellular data info	1	1	0
Identity	10	7	3
Calendar	6	0	0
Contacts	10	7	3
Location	10	1	5
SMS	9	2	0
Phone	10	9	3
Files & media	10	9	7
Storage	10	9	7
Camera	10	9	4
Microphone	6	2	3
Wi-Fi info	10	9	9
ID & call info	10	9	3
Other	10	10	10

Chart: Shelley Hepworth • Source: Google Play • Get the data

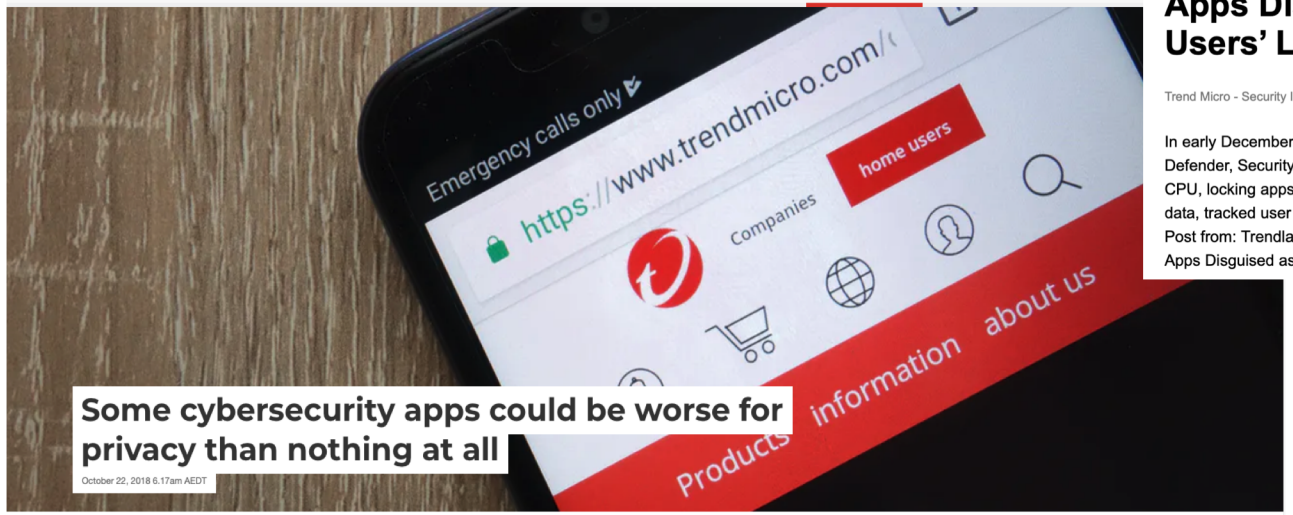
Motivation

THE CONVERSATION

Academic rigour, journalistic flair

Search analysis, research, academics...

COVID-19 Arts + Culture Business + Economy Cities Education Environment + Energy Health + Medicine Politics + Society Science + Technology



Some cybersecurity apps could be worse for privacy than nothing at all

October 22, 2018 6.17am AEDT

Apple has removed several security tools from the Mac app store after they were found to be collecting unnecessary personal data. Shutterstock

CSO

NEWS BREACHES CSOM SECURITY LEADERS NEWSLETTERS RESOURCE LIBRARY FRON

Top IT Security Bloggers

Apps Disguised as Security Tools Bombard Users With Ads and Track Users' Location

Trend Micro - Security Intelligence — 3 Jan 2018, 1:15 p.m.

In early December, we found a total of 36 apps on Google Play that executed unwanted behavior. These apps posed as useful security tools under the names Security Defender, Security Keeper, Smart Security, Advanced Boost, and more. They also advertised a variety of capabilities: scanning, cleaning junk, saving battery, cooling the CPU, locking apps, as well as message security, WiFi security, and so on. The apps were actually able to perform these simple tasks, but they also secretly harvested user data, tracked user location, and aggressively pushed advertisements.

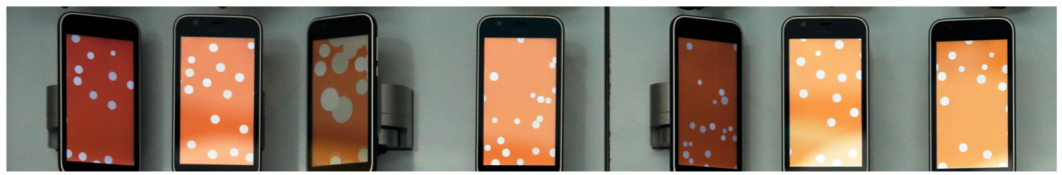
Post from: Trendlabs Security Intelligence Blog - by Trend Micro

Apps Disguised as Security Tools Bombard Users With Ads and Track Users' Location

BRIAN BARRETT SECURITY 03.16.2019 07:00 AM

Most Android Antivirus Apps Are Garbage

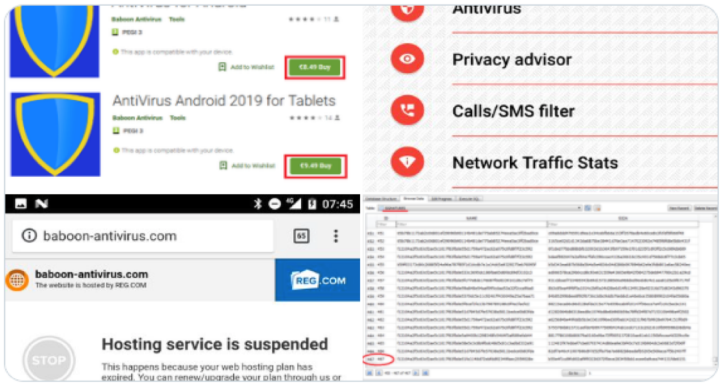
Fraudulent and ineffective antivirus apps persist on the Google Play Store, and it's unclear whether they'll ever totally go away.



Lukas Stefanko
@LukasStefanko

Fake Android AntiVirus for €79,99 available since 2015

-malware database contains only up to 500 static signatures
-can download update database but server is down
-offers different products but all are with the same functionality



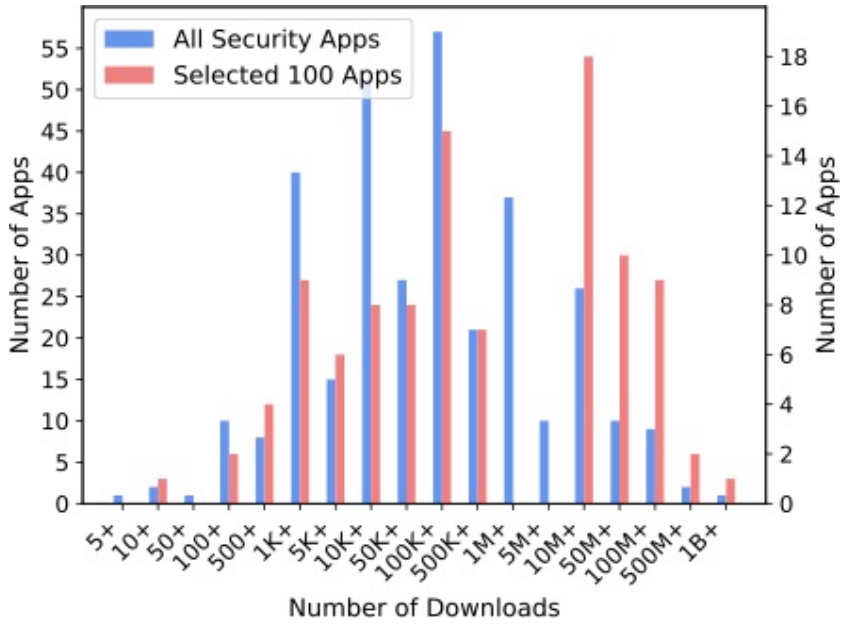
Methodology

- Data Collection & Metadata Analysis
  - Keyword search and APK download & Metadata collection (E.g., No. of downloads, Rating, App description etc.)
- Privacy Policy Analysis
  - Identifying mentions of personal data and what is being done with them
- Effectiveness in Malware Detection
  - Can security apps detect installed/copies of malware?
- Network Traffic Analysis
  - Contacted IPs and domains
  - Identifying personal information transmissions

Dataset & Metadata

- APK & metadata collection
  - 328 potential security apps
  - Meta data includes:
    - App ID, App description, No. of Downloads, No. of ratings (total and rating in each category), Developer information (e.g., Name and Location)
- Selected 100 apps for further analysis
  - By ranking apps according to no. of downloads, average rating, and number of reviews and creating three groups.
  - 40 apps from the top security apps and 30 each from middle and bottom groups

The app "Clean Master" which was downloaded over one billion times was recently removed from Google Play Store under the suspicion of advertisement fraud.



Privacy Policy Analysis

- We read the privacy policies ourselves searching answers for three high level questions
  - What type of data the security apps collect?
  - What are the intended uses of collected data?
  - Is the data being shared with third parties? If yes, who are the third parties with such access

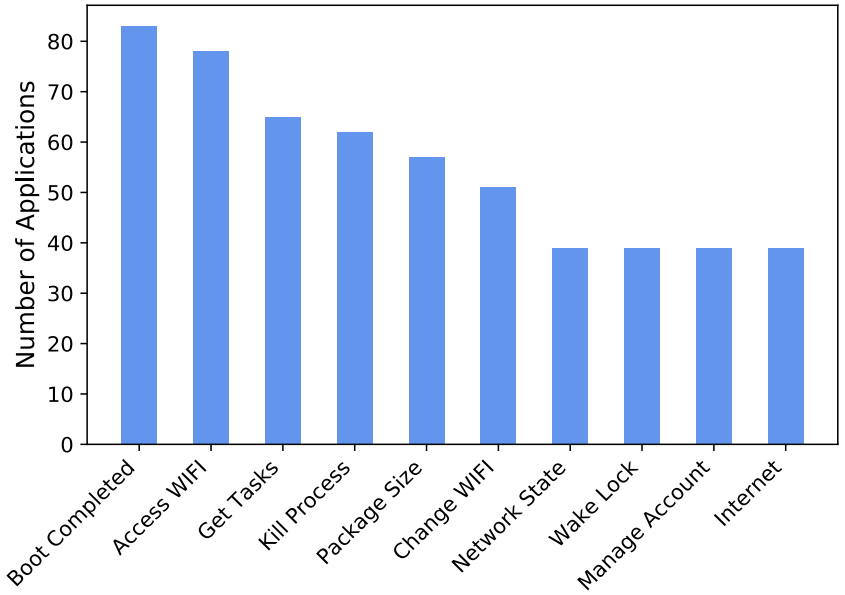
TABLE I: Analysis summary of privacy policies

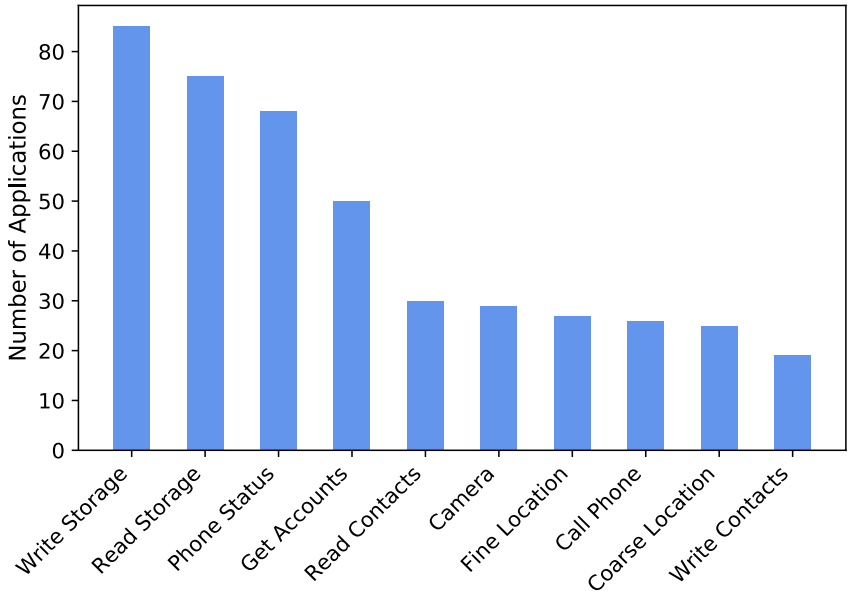
Type of data		Use of data		Data shared with third-parties	
Attribute	**No. of Apps**	**Attribute**	**No. of Apps**	**Attribute**	**No. of Apps**
Personal information	71	Newsletter	53	Legal authorities	55
User behavior	62	Service improvement	77	Business affiliates	48
Hardware information	75	Security services	48	Business partners	55
Upload files to cloud	30			Re-sellers	21
				Others	30

- *55 apps may share data with legal authorities if required.*
- *Almost all the apps had some form of data sharing with their business partners.*
- *Around 70 apps were found to be collecting personal information and hardware information.*

Permission Analysis

- We extracted the permission requests by parsing the *AndroidManifest.XML*
- On average a security app requested 22.09 permissions.
  - Normal permissions ~12.23
  - Signature permissions ~5.52
  - Dangerous permissions ~4.33

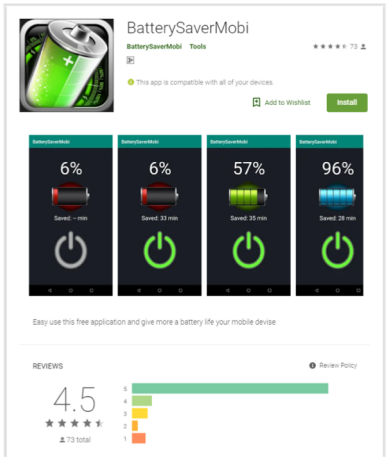




- *The majority of the requested dangerous permissions have an associated legitimate security feature included in the security app. Nonetheless, the security yapp users need to be cautious when granting such permissions and need to carefully evaluate the trade-offs.*

Malware Detection

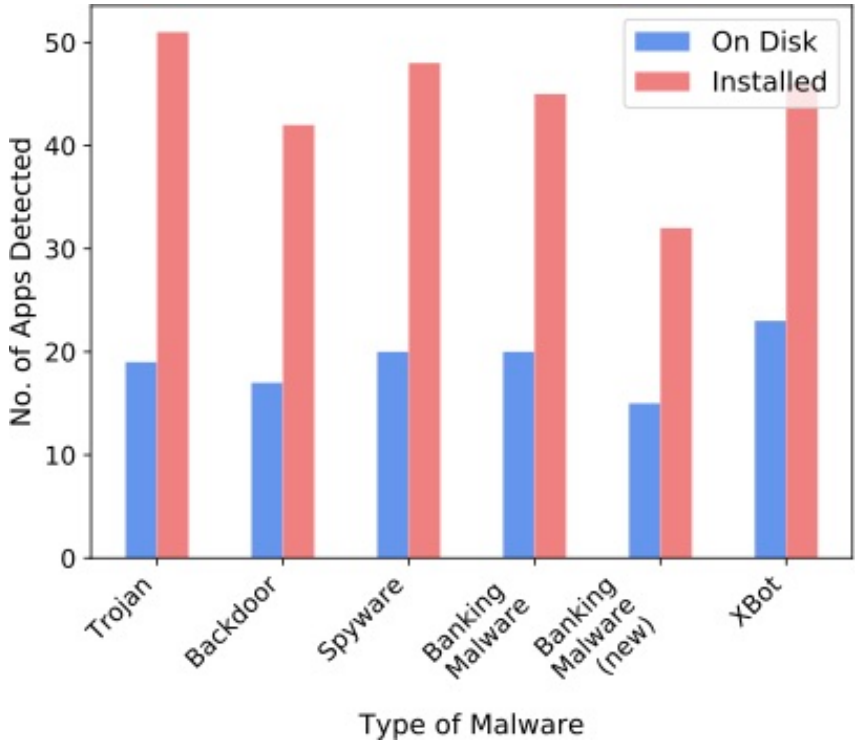
- We selected six malware samples that have been publicly disclosed between 2015 and 2019.
  - Fake Adobe Flash player update (Trojan, 2017)
  - BeNews app (Backdoor, 2015)
  - Banker trojan (Spyware, 2016)
  - Banking malware (Impersonating Sberbank, 2016)
  - Banking malware (BatterySaverMobi, 2019)



Source: TrendMicro

- Using these malware we tested two scenarios;
  - Whether the security apps can detect a copy of malware stored in a phone
  - Whether the security apps can detect malware installed in a phone

Malware Detection

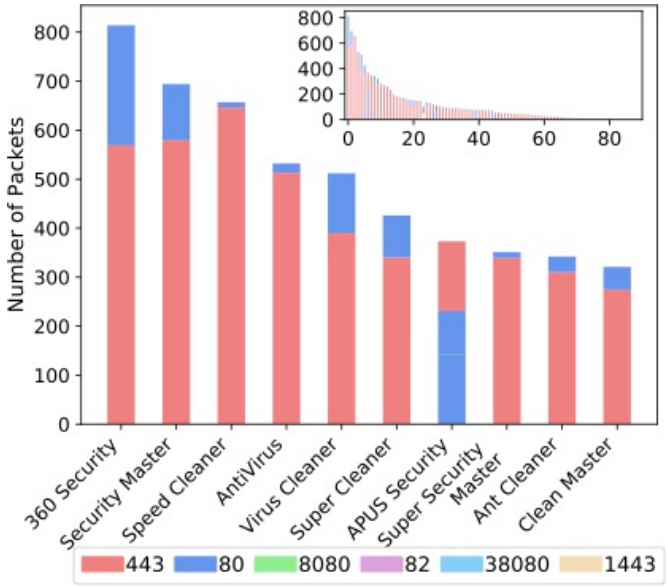


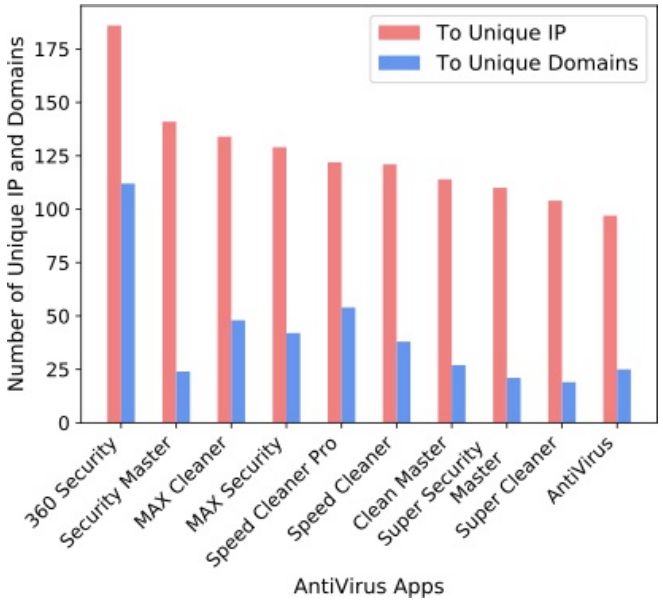
No. of detected malware	No. of detecting security apps
0	30
1 - 3	12
4 - 5	11
6	32

- *For each malware sample, only 15-20 apps could detect them even after running a full system scan*
- *The detection rates of installed malware was high compared to disk copies, yet not perfect.*
- *Only 40-50 were able to identify installed malware except for the case of one new malware that was released in 2019*
- *Only 32 were able to detect all six samples of installed malware.*

Network Traffic

- We used the Lumen privacy monitor which can continuously monitor app traffic.
- Lumen also can identify when personal information is leaked by a particular application





- *Majority of the apps sent encrypted packets with the exception of APUS Security, which had a significant fraction of non-encrypted traffic.*
- *There were nine apps that contacted over 100 IPs and three apps that contacted over 50 domain names.*
- *The top three frequently collected information are device model, build id, and device brand.*
- *We also found a limited number of apps that collect more personal information in nature such as list of installed apps and personally identifiable information such as the Android serial, Android ID, and BSSID.*

Conclusion

- Security apps have access to many sensitive information stored in smartphones
- Privacy policy analysis showed that some apps may share user data with third parties.
- We showed that 30 security apps out of 86 we tested were not able to identify installed malware providing *a false sense of security.*
- Through network traffic analysis we found evidence of security apps indeed collecting and transmitting personal information to their back-end servers.
- The users need to be cautious when selecting security apps, especially given our findings on privacy policies.