SOPHOS
Security made simple.

Super Antivirus 2018: A shady app many are downloading on Google Play

By **Rowland Yu**, Senior Threat Researcher

A SophosLabs technical paper January 2018

Contents

Potentially unwanted applications (PUAs) is a term used to classify applications deemed generally unsuitable for end users and customers.

The "generally unsuitable" consideration is quite blurry. While security researchers can clearly see the dangers in PUAs, some users still choose to trust such applications because of their perceived benefits. On the surface, these apps provide a feature they want, like photo editing or performance optimization. But they come bundled with other functions that are poorly explained or not advertised at all, such as adware.

The increasingly blurred line between PUAs and legitimate software is shaping up as a new trend in 2018.

A real-life analogy would be an attempt of criminal groups to legitimize their activities by blending them with normal day-to-day business operations, such as banking, shares, stocks, and real estate.

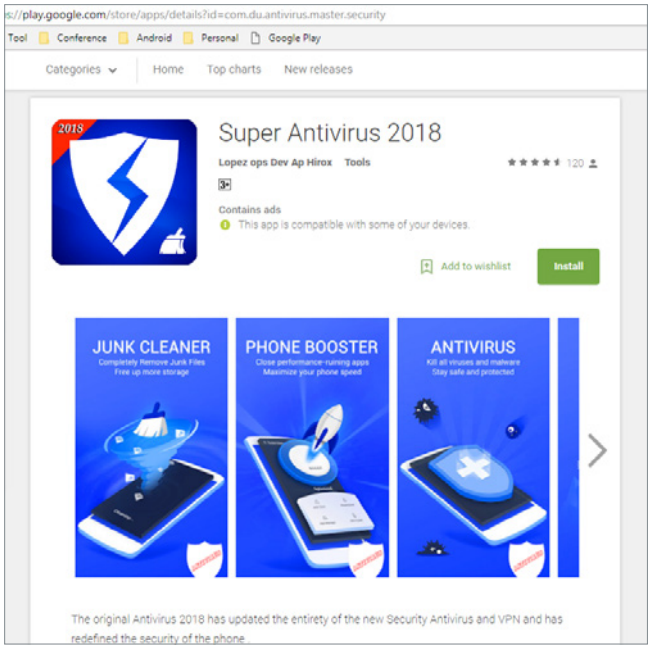
Given that security products still eradicate PUAs by default, the authors choose to throw some legitimate activity into the bag, attempting to confuse researchers and end users.

Enter Super Antivirus 2018

The Super Antivirus 2018 app is a perfect example of that approach. Some legitimate action is added to what is really not an antivirus program at all, in order to throw researchers off the track:

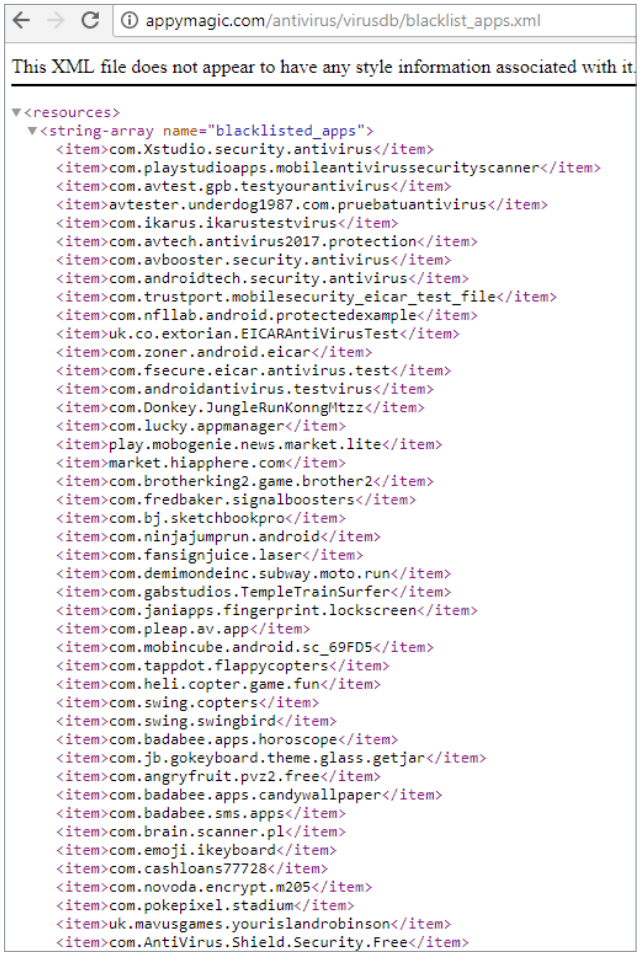
The app was uploaded to Google Play on October 2, 2017 and since then has attracted 10,000 to 50,000 downloads. It claims to "detect 100% of viruses and malware through personalized scanning."

But when SophosLabs analyzed the code of this application, that claim turned out to be not entirely accurate.



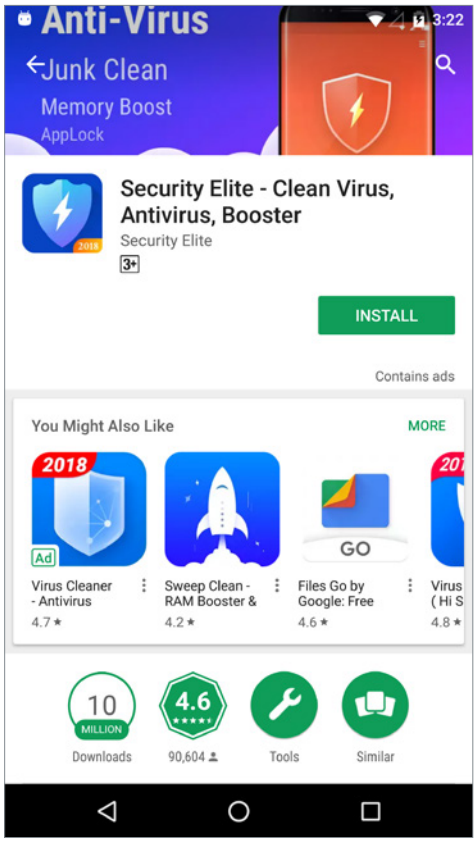
On one hand, it provides no effective protection for end users. On the other hand, it has an online blacklist and even scans and detects nearly 500 apps.

Below is a blacklist of the apps targeted by Super Antivirus 2018:

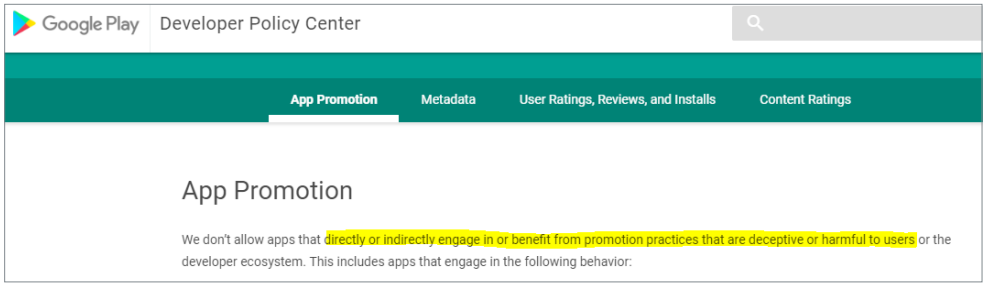


Many of the blacklisted apps are in fact clean and can be found in Google Play. For example, 'Keyboard - emoji, emoticons' (package name – *com.emoji.ikeyboard*).

During the fake virus scan, Super Antivirus 2018 frequently displays a pop-up that the end user may misinterpret as a detected threat. The pop-up advertising promotes an app called 'Security Elite - Clean Virus, Antivirus, Booster.'



Such a promotion is deceptive in nature, and is in clear violation of the Google Play Developer App Promotion Policy:



To summarize the findings, Super Antivirus 2018 app possesses the following characteristics:

- It doesn't provide a proper malware removal feature
- It may mislead users into believing there is a virus on their Android device
- It entices users to download another malware removal tool

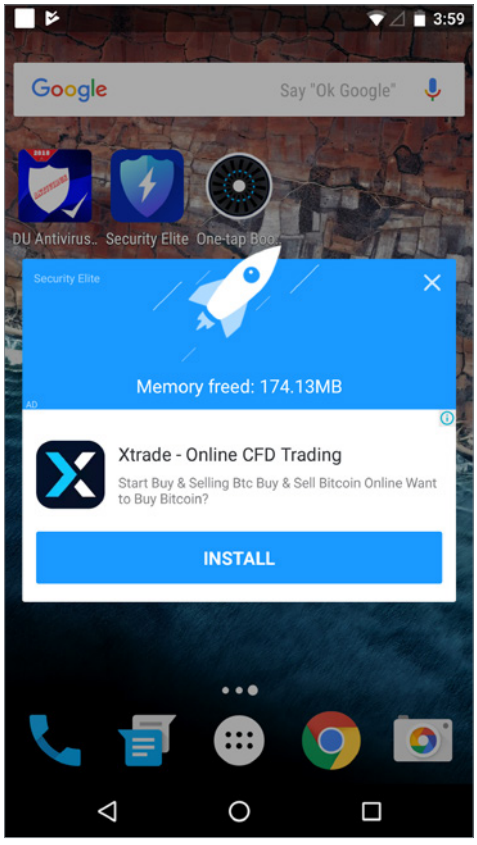
Detection

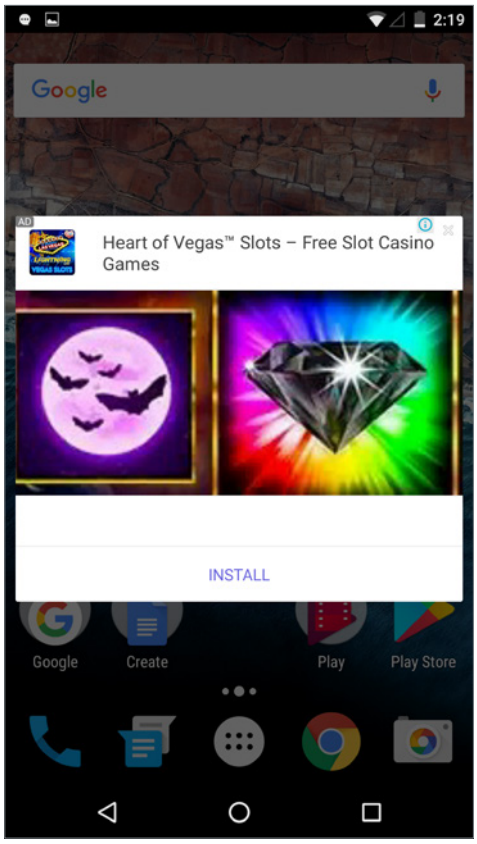
Because of such characteristics, along with the breached Google developer policy, Sophos detects Super Antivirus 2018 as a PUA: Andr/FakeAV-B.

Security Elite - Clean Virus, Antivirus, Booster

Meanwhile, an app promoted within Super Antivirus 2018, named Security Elite – Clean Virus, Antivirus, Booster, was published on Google Play on Oct. 17, 2017. In just three months, it attracted as many as 50 million installs.

During the execution, the app also frequently uses pop-up ads that promote other apps:





Because of this excessive advertising, Security Elite - Clean Virus, Antivirus, Booster is classified by SophosLabs as AdLoad – an adware family of PUA.

Safety Tips

Over the years, Google Play has become a crowded place. While the majority of apps are built by reputable developers and are heavily vetted by Google's security, the number of apps that use shadowy tactics is still growing.

Google claims to be putting effort into making Google Play an ever-safer place to get apps, yet the advertising platforms used by many otherwise legitimate apps are becoming more intrusive, disruptive and invasive.

SophosLabs carefully inspects every analyzed app's functionality and checks if an app is in breach of the Google Developer Policy.

Our advice is to stay vigilant. If an app's claims look too good to be true, then they probably are.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

18-01-15 TP-NA (2904-DD)

SOPHOS