

# Rogueware Reborn

A Business Analysis of a Growing  
Fraud in Android

by Rowland Yu

“Rogueware specifically describes programs that pretend to detect and fix problems on your computer and tries to convince you to pay money/add more malware.”

[<http://tek2u.com/what-is-rogueware-and-4-ways-to-avoid-it/>]

## Introduction

Rogueware was a serious security threat in desktop computing from 2008 to 2014. Since then, ransomware and cryptominers have replaced rogueware as the threat du jour and currently dominate the cyber threat landscape.

However, rogueware has been reborn in the Android ecosystem, particularly on Google Play. This research paper reveals that hundreds of antivirus and optimization tool apps on Google Play mislead users into believing that they have a virus or performance problems on their devices to manipulate them to install other fake tools.

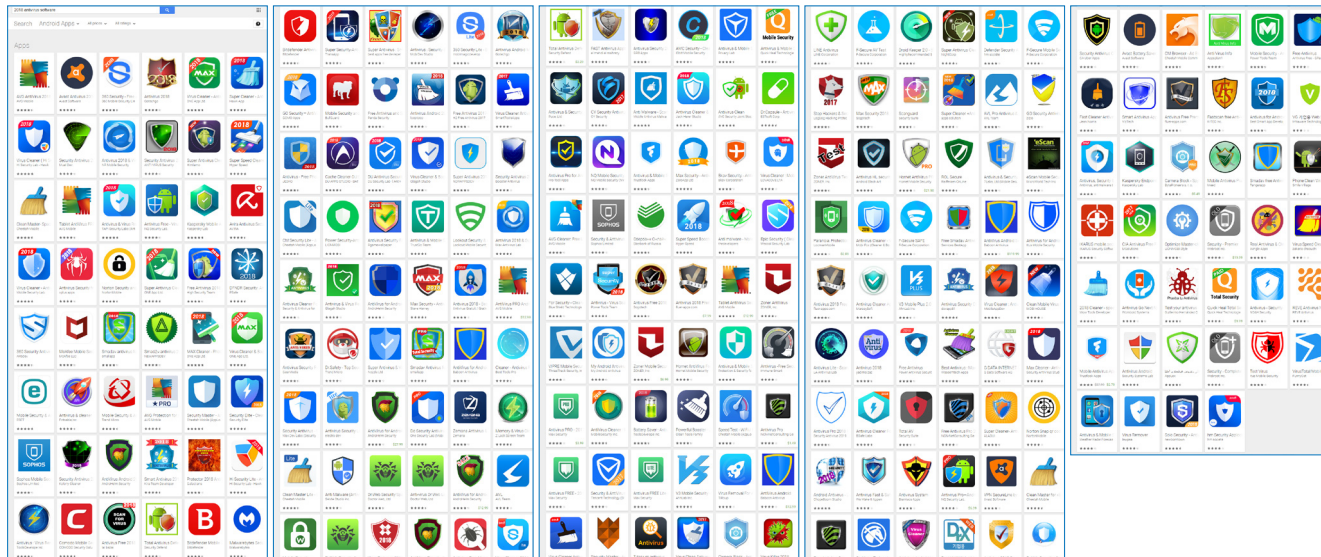
Further investigation shows that all the above-mentioned apps have been downloaded up to 300 – 400 million times. We conservatively estimate that one tenth of active Android devices in the world [<https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users>] [<http://news.pedaily.cn/201707/20170704416455.shtml>] are infected by this kind of new threat.

We will also illustrate a business model based on rogueware and explain how one company took advantage of this new threat and gained revenue of \$68 million USD with nearly \$20 million USD profit in just one year.

## Physiognomic Classification

Our research starts from our recent fake antivirus app discovery on Google Play, SuperClean [<https://news.sophos.com/en-us/2018/01/19/super-antivirus-2018-it-isnt-super-and-its-not-an-antivirus/>]. The fake antivirus app has no proper malware removal feature but uses pop-ups to entice users to download other antivirus or optimization removal tools. After receiving our report, Google Play quickly removed the app.

SophosLabs has found more than 200 antivirus apps available on Google Play when searching keywords “2018 antivirus software” [shown in Picture 1]. We are asking three questions: 1. Do they provide proper protection? 2. Do they entice users to download other apps? 3. Are they malicious or not?



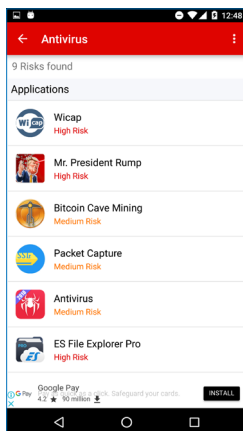
Picture 1: Antivirus apps found by SophosLabs on Google Play

To answer these questions, first all apps were downloaded and tested on a real device to take screenshots of their graphic interface, understand their functionalities, and capture any pop-up alerts. After we investigated and researched this massive amount of data, we developed three criteria to enable us to narrow down these apps and identify potential rogueware:

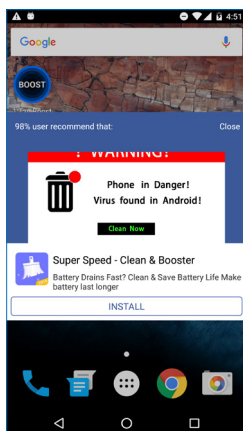
1. Developers use public email addresses such as Gmail, Hotmail or Yahoo (shown in Picture 2).
2. These apps have no antivirus function or an absurd antivirus alert when scanning a large list of the latest Google Play or non-Google Play malware samples (shown in Picture 3).
3. They frequently display scam pop-ups alerts when running (shown in Picture 4).

**Developer**  
Email magniapps@gmail.com  
Privacy Policy  
Fazal Trade Center opposite Chen One Gulberg-III  
Lahore

Picture 2: Criteria 1 example: Public email address in a developer's contact information



Picture 3: Criteria 2 example: "Antivirus" app detected itself as high risk app

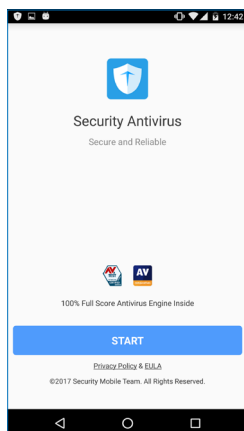


Picture 4: Rule 3 example, scam pop-ups alerts

We also applied supplementary criteria, such as a trademark infringement or fake advertisement [Pictures 5 and 6].

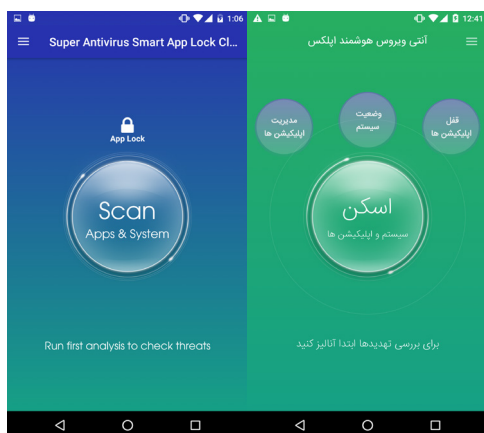


Picture 5: ARSdev copied “360 Security” from the legitimate company “360 Mobile Security”

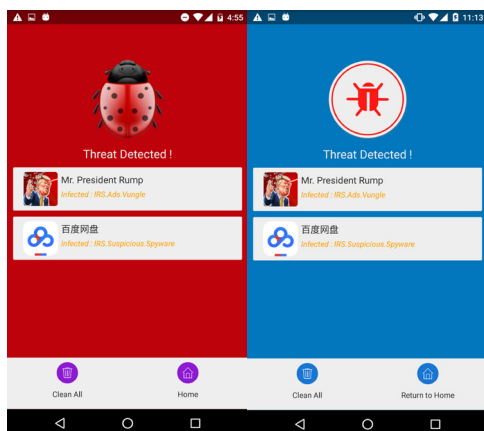


Picture 6: Used AVTest and AVComparative Test for fake endorsement

Grouping the apps into specific categories simplified the comparative study process. Based on the similarities of graphical interface, fonts, functionalities, or scan results, we quickly categorized the suspected rogueware into 12 separate groups. The pictures below show two different grouping examples. In Picture 7, the two apps are from different developers and have different languages and colour in the UI; however, the position of the main button and label is the same. The latter example (Picture 8) displays two apps that return the exact same results when scanning hundreds of malware samples.

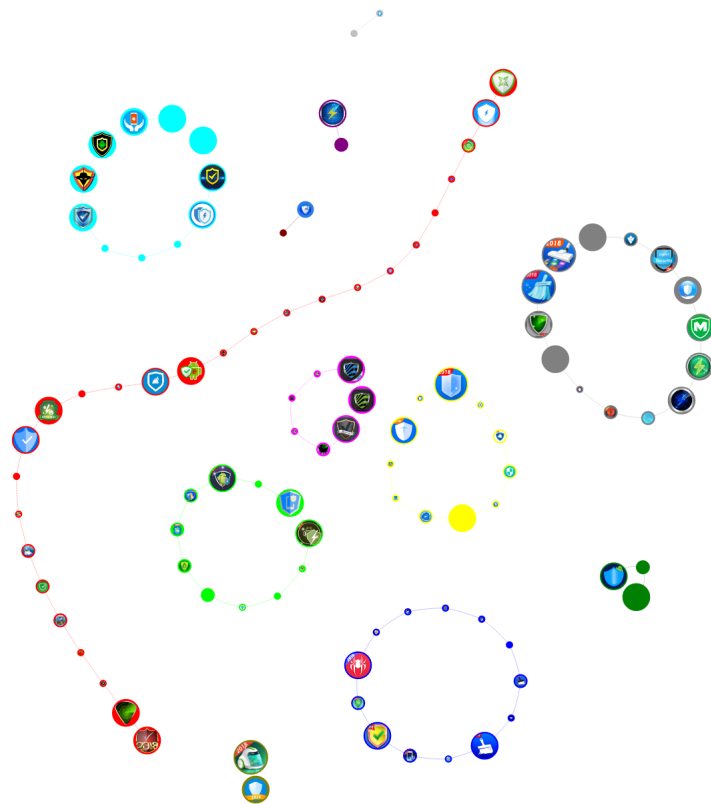


Picture 7: apps with similar GUI



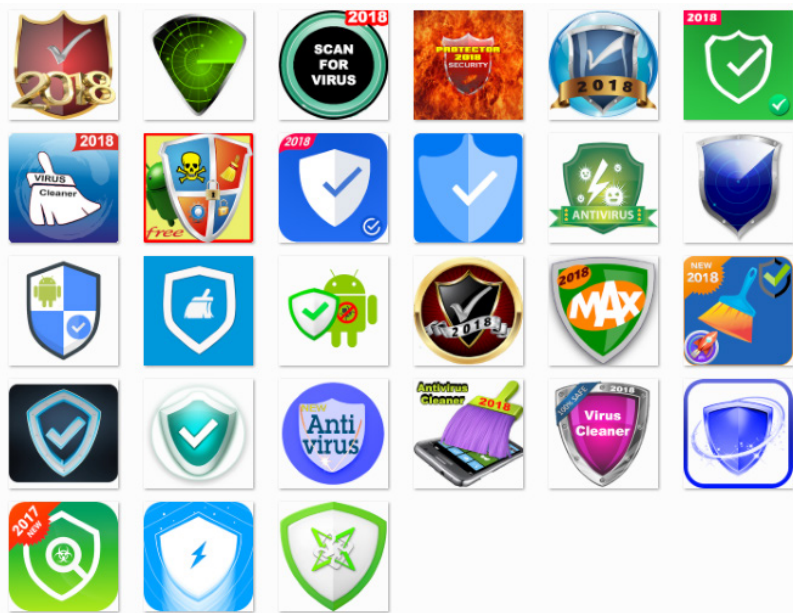
Picture 8: apps with similar GUI and same scan results

We grouped 12 potential rogueware families (Picture 9). Each circle represents an app on Google Play. These circles have five different sizes. The largest-sized circle means that the app has been downloaded more than 10 million times. There are four apps in this category. The second-largest circle means the number of downloads is between 1 million and 9,999,999. The download number of the third category is from 100,000 to 999,999 while the second-last is from 10,000 to 99,999. Any download frequency below 10,000 is included in the smallest circle. Apps in the same family are linked by a dash line. If a circle doesn't have an icon, it means the app was just removed by Google Play, which implies the potential risk and harm the app presents.



Picture 9: Potential rogueware families based on physiognomic classification

Group 1 in Picture 9 is the largest family, in which we identified 27 different apps. The family has different icons (Picture 10), contact emails, or descriptions. However, when running these apps in a real device or testing hundreds of malware samples, they do show very similar UI and scan results (Pictures 11 and 12). When we assess this with our criteria, there is sufficient evidence to label all 27 these apps as rogueware.



Picture 10 : The icons of the 27 apps in Group 1



Picture 11 : The user Interface of the 27 apps in Group 1



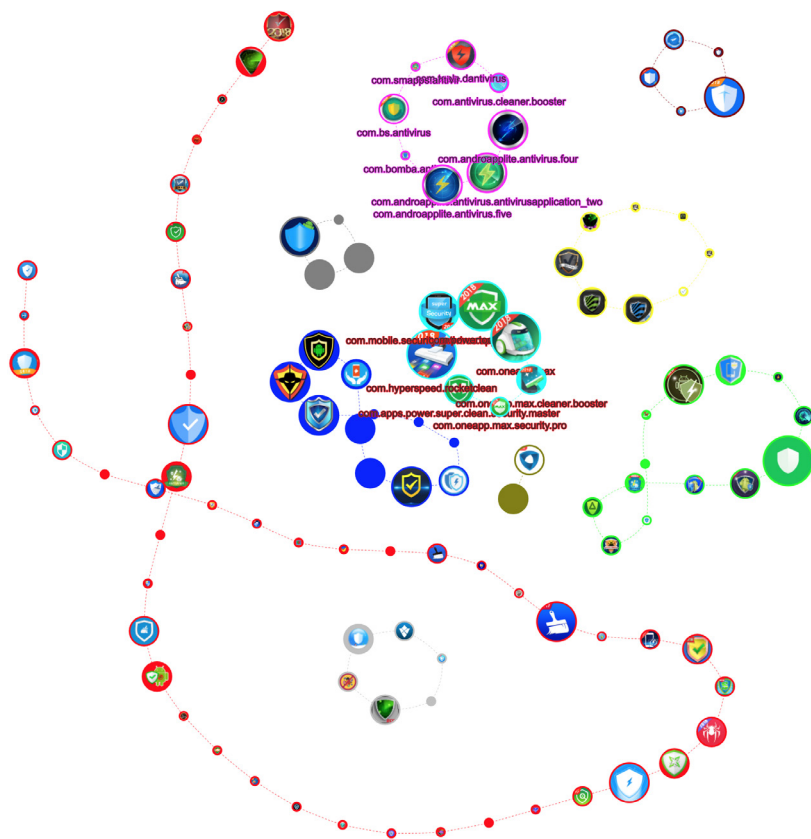
Picture 12 : The scan result of the 27 apps in Group 1

## Anatomic Classification

Classification based on physiognomy is not 100 percent accurate. It is necessary to decompile all the samples in order to fully understand their behaviors and functionalities. Additionally, the grouping based on decompiled codes (anatomy classification ) is much more accurate. As you can see in Picture 13, the total number of groups has been reduced to 10. For example, the number of apps in Group 1 in the previous picture has expanded to 48 apps with up to 23 million downloads on Google Play. The Appendix lists all the package names, file hashes and downloads info for all groups.

The malicious functionalities of Group 2 and Group 3 in Picture 13 are detailed in the table below. Group 4 is confirmed as rogueware due to an app removed from Google Play. However, we will use this Group 4 to illustrate the business model in the next section. Group 1 and the remaining groups can be easily confirmed as rogueware due to apps removed from Google Play for obviously malicious functionalities.





Picture 13: Rogueware families based on anatomy classification

## Rogueware Group 2:

Table 1 below shows the basic information for Group 2. All developers in Group 2 use Gmail as their email contact address. Some addresses show these developers are likely from China.

Package Name	Downloads	Developer Email	Address
com.androapplite.antivirus. antivirusapplication_two	1-5 million	wearmonster.cook@gmail.com	N/A
com.androapplite.antivirus.four	1-5 million	hellocaty412@gmail.com	Dongbeiwang West Road,Haidian District,Beijing
com.androapplite.antivirus.five	1-5 million	zhaominghua31@gmail.com	N/A
com.tools.dantivirus	500,000-1 million	watchfacedev@gmail.com	bei san huan zhong lu ji men li
com.bs.antivirus	100,000 - 500,000	holdthedor748@gmail.com	N/A
com.antivirus.cleaner.booster	50,000 - 100,000	protoolsapp@gmail.com	N/A
com.smapps.antivir	1,000 - 5,000	smiloapp@gmail.com	N/A
com.bomba.antivir	10 -50	update.me.soft@gmail.com	N/A

Table 1: Basic information for Group 2



When checking the code, we find the AndroidManifest.xml files in Group 2 are similar. The AndroidManifest.xml files use the same keywords in Services Broadcast Receivers like “DetectorService” and “PackageAddRemoveReceiver”.

```
<service android:name="com.antivirus.cleaner.booster.app.lock.service.DetectorService" android:priority="1000" />
<receiver android:enabled="true" android:exported="false" android:name="com.antivirus.cleaner.booster.app.lock.receiver.NotificationClickReceiver" />
<receiver android:name="com.antivirus.cleaner.booster.app.lock.receiver.StartupServiceReceiver">
  <intent-filter>
    <action android:name="android.intent.action.BOOT_COMPLETED" />
    <action android:name="android.intent.action.MY_PACKAGE_REPLACED" />
    <action android:name="android.intent.action.USER_PRESENT" />
    <action android:name="android.intent.action.SCREEN_OFF" />
    <action android:name="android.intent.action.SCREEN_ON" />
  </intent-filter>
</receiver>
<receiver android:enabled="true" android:exported="true" android:name="com.antivirus.cleaner.booster.app.lock.receiver.PackageAddRemoveReceiver">
  <intent-filter>
    <action android:name="android.intent.action.PACKAGE_INSTALL" />
    <action android:name="android.intent.action.PACKAGE_ADDED" />
    <action android:name="android.intent.action.PACKAGE_REMOVED" />
    <data android:scheme="package" />
  </intent-filter>
</receiver>
```

When looking deeply into the decompiled JAVA code, the scanning engine has a hard-coded exclusive packageName list such as “elf,” “com.tools.dbattery,” and “com.tools.dsupperclean.” Some of the packageNames can be found and downloaded from Google Play.

```
this.a.runOnUiThread(new Runnable(v2_1, v3) {
  public void run() {
    if(!this.a.b.packageName.contains("elf") && !this.a.b.packageName.contains("com.tools.dbattery") && !this.a.b.packageName.contains("com.tools.dsupperclean") &&
      NewFullScanActivity.a(this.c.a).add(this.a);
    com.androapplite.antivirus.antivirusapplication.antivirus.a.a(this.c.a.getApplicationContext(), NewFullScanActivity.b(this.c.a), this.b, null);
  }
});
```

All eight apps use the same APIKey from the Threatbook cloud engine to scan samples.

```
e.a(arg7).b("threatbook", "扫描APK");
a.a = OkHttpUtils.post().tag("https://x.threatbook.cn/api/v1/file/report?nt=" + i.a(arg7)).url("https://x.threatbook.cn/api/v1/file/report?nt=" + i.a(arg7)).addParams("apikey", "52992f3ae");
a.a.execute(new c(arg7, v2, v3, arg8, arg9) {
  public void a(VirusResponse arg3) {
    this.a.what = 200;
  }
});
```

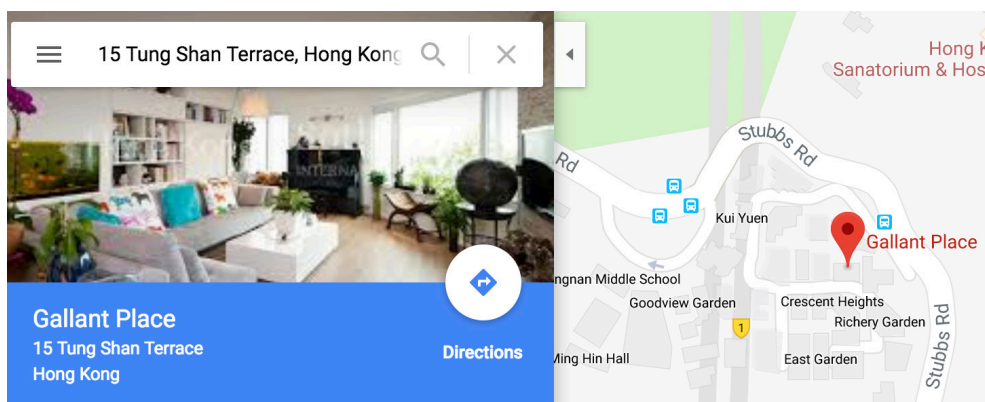
Based on their questionable contact information, plagiarism in the code, and pool scanning techniques, we can confirm these apps are rogueware.

### Rogueware Group 3:

Package Name	Downloads	Developer Email	Address
com.apps.power.super. clean.security.master	100,000 - 500,000	powertoolsapps@ gmail.com	35 Lockhart Road, Wanchai, Wan Chai, Hong Kong
com.hyperspeed.rocketclean	10-50 million	quickcleanerapps@ gmail.com	15 Tung Shan Terrace, Hong Kong
com.mobile.security. antivirus.applock.wifi	1-5 million	quickcleanerapps@ gmail.com	35 Lockhart Road, Wanchai, Wan Chai, Hong Kong
com.powertools.privacy	10 - 50 million	max.support@ oneappessentials.com	Unit 04, Bright Way Tower, No.33 Mong Kok Road, Kowloon, Hong Kong
com.oneapp.max	10-50 million	oneappltd@gmail.com	Unit 04, Bright Way Tower, No.33 Mong Kok Road, Kowloon, Hong Kong
com.oneapp.max.cleaner.booster	500,000 - 1million	oneappltd@gmail.com	Unit 04, Bright Way Tower, No.33 Mong Kok Road, Kowloon, Hong Kong
com.oneapp.max.security.pro	100,000 - 500,000	oneappltd@gmail.com	Unit 04, Bright Way Tower, No.33 Mong Kok Road, Kowloon, Hong Kong

Table 2: Basic information for Group 3

The contact info in Group 3 seems more credible. However, when searching all the above addresses on Google, we find no address for a legitimate company. For example “15 Tung Shan Terrace, Hong Kong” is a residential address.



Picture 14: Google Map of "15 Tung Shan Terrace, Hong Kong"

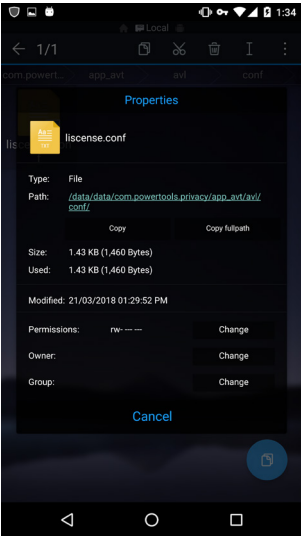
When analyzing the network traffic, these apps use AVLyun to scan samples but share the same AVL license key: sha1 of liscense.conf 3a69cf07cf9c205ffe1ffed36601fc88a25f9c73 (shown in Picture 15 & 16).

```
POST /search HTTP/1.1
Connection: Keep-Alive
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; Nexus 6 Build/MMB29K)
Host: cse.avlyun.com
Accept-Encoding: gzip
Content-Length: 380

{"appid":"handistd","time_stamp":1521590652,"api_version":"1.0","secret":"754F
1B1E899941AA14D9AC97B04FA00F","search_info":[{"keys":["660F1596496A09D9644D33C
78AA3E431","E36BD9ABF491D1E72F7C4FAA209BA0E3","EDCE2FBBF748DF1D1D0CA3D6F00C9BC
3","4549FD74C9FE19DEC6506FF8E97A5A7B","A1A93B57B59CDE8488B54499C683DB65","8226
EE1660ABC597F9608341AE4AB538","88602F958123EE8795ECC25EFAB75B1E"]}]}HTTP/1.1
200 OK
Date: Wed, 21 Mar 2018 00:04:15 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 461
Connection: keep-alive
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
Cache-Control: max-age=600
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, x-requested-with

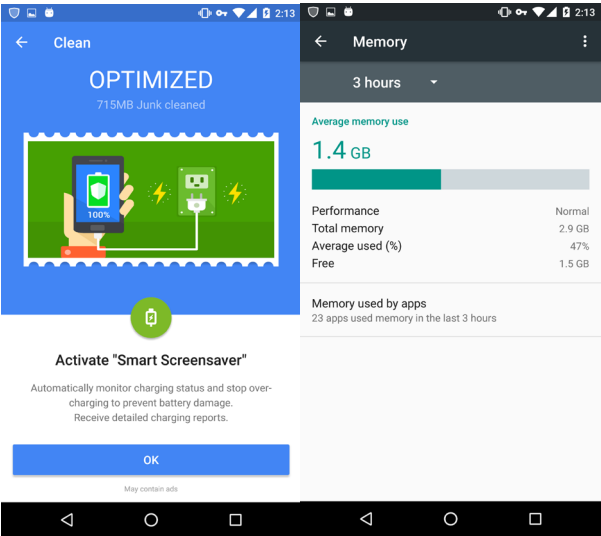
{"cost": 7, "data": {"result": {"app_hash":
{"A1A93B57B59CDE8488B54499C683DB65": "_KNF",
"4549FD74C9FE19DEC6506FF8E97A5A7B": "_KNF",
"E36BD9ABF491D1E72F7C4FAA209BA0E3": "_KNF",
"8226EE1660ABC597F9608341AE4AB538": "_KNF",
"88602F958123EE8795ECC25EFAB75B1E": "White/Android.estrongs.a[app,crt]",
"660F1596496A09D9644D33C78AA3E431": "_KNF",
"EDCE2FBBF748DF1D1D0CA3D6F00C9BC3": "AdWare/Android.Admob.a[ads,gen]}"},
"errCode": 10000, "errInfo": "process succeeded"}
```

Picture 15: Scanning network traffic between AVLyun and rogueware



Picture 16: sha1 of AVLyun license.conf 3a69cf07cf9c205ffe1ffed36601fc88a25f9c73

We also tested their Memory Cache Clean function which claims that more than 700 MB have been cleaned. However, the truth is that there is zero improvement. The memory usage is 1.4 GB, just as it was before cache cleaned [in Picture 17].

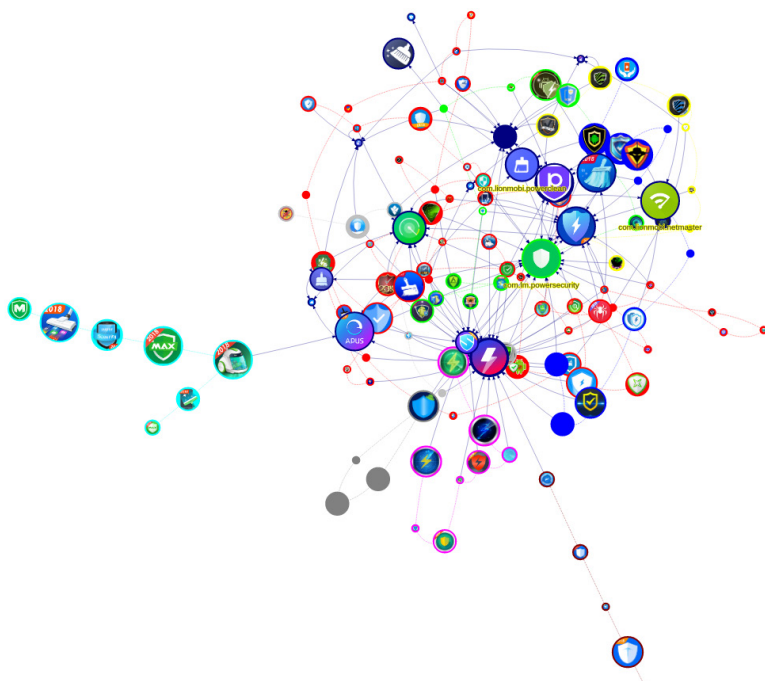


Picture 17: Memory Cache Clean function of Rogueware Group 3

Although these apps can provide very basic protection and detection, we believe they are rogueware due to the poor design, dishonest description, low quality, and fraud functionalities.

## The Business Analysis of Rogueware in Android

When testing these apps on real devices, most of them showed scam pop-up alerts. These alerts attempt to convince users to download more apps to detect and fix non-existent problems. During testing, we ran the apps for about five minutes and then collected all the pop-up alerts with the app links. All rogueware, links, and promoted apps are visualized in the following network Picture 18.



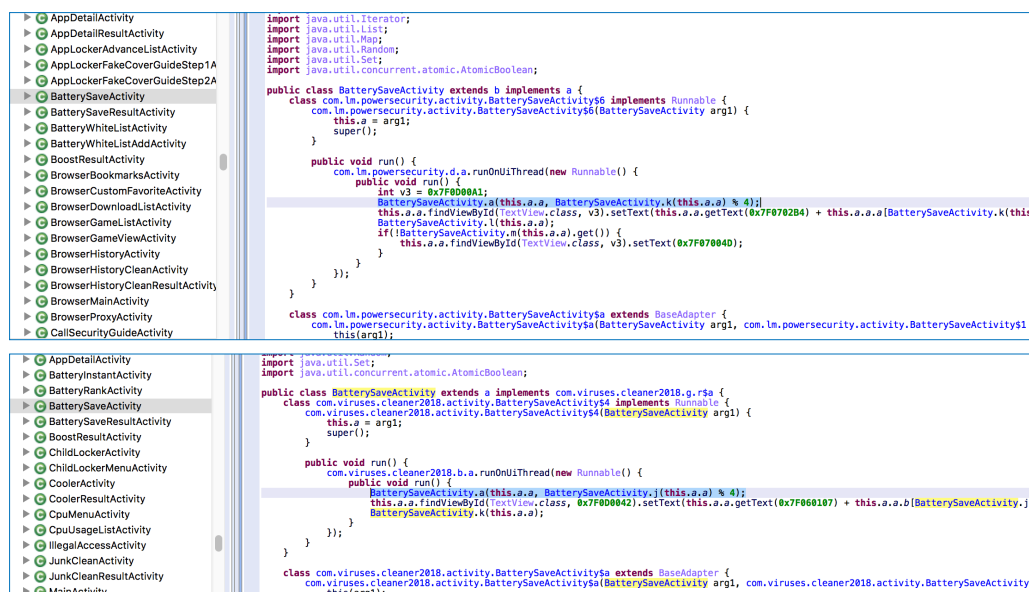
Picture 18: Visualizing network of rogueware, links and promoted apps

From the network picture, several apps stand out, but the most interesting is PackageName “com.lm.powersecurity.” This can be found in both Group 4 (Picture 13) and as a promoted app. Moreover, it shares the same company information with two other promoted popular apps. In this section, we will investigate this company and demonstrate its business model, with more than 100 million active users and an annual revenue of \$68 million USD.

First of all, the malicious code has to be analyzed to prove the relationship between “com.lm.powersecurity” app and the app [PackageName: com.viruses.cleaner2018] removed from Google Play. Below are parts of AndroidManifest.xml and BatterySaveActivity. As you can see, their structures and algorithms are nearly the same.

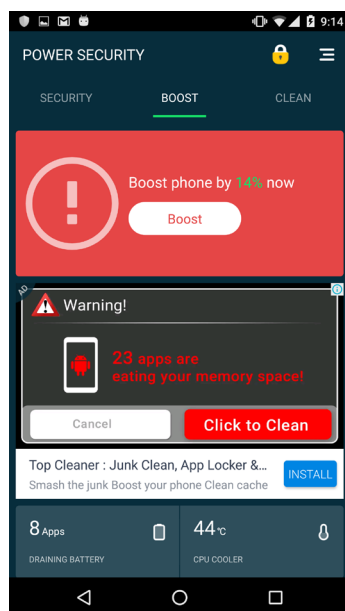
```
</activity>
<activity android:configChanges="0x4a0" android:launchMode="3" android:name="com.lm.powersecurity.activity.AdPostActivity" android:screenOrientation="1" android:theme="@android:style/Theme.Translucent" />
<activity android:configChanges="0x5b0" android:label="@string/app_name" android:name="com.facebook.FacebookActivity" android:theme="@android:style/Theme.Translucent" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.lm.powersecurity.activity.MainActivity" android:screenOrientation="1" android:theme="@style/Transparent" />
<activity android:launchMode="2" android:name="com.lm.powersecurity.activity.ChildLockerActivity" android:screenOrientation="1" />
<activity android:name="com.lm.powersecurity.activity.IllegalAccessActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.lm.powersecurity.activity.ChildLockerMenuActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.lm.powersecurity.activity.SecurityFullScanActivity" android:screenOrientation="1" />
<activity android:launchMode="2" android:name="com.lm.powersecurity.activity.SecurityScanResultActivity" android:screenOrientation="1" />
<activity android:name="com.lm.powersecurity.activity.SecurityResultAdActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.lm.powersecurity.activity.BatterySaveActivity" android:screenOrientation="1" />
<activity android:launchMode="1" android:name="com.lm.powersecurity.activity.SplashActivity" android:screenOrientation="1" android:theme="@style/MainActivityTheme">

<meta-data android:name="channel" android:value="googleplay" />
<activity android:label="InterstitialAdActivity" android:name="com.facebook.ads.InterstitialAdActivity" android:screenOrientation="1" />
<activity android:configChanges="0x5b0" android:label="@string/app_name" android:name="com.facebook.FacebookActivity" android:theme="@android:style/Theme.Translucent" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.viruses.cleaner2018.activity.MainActivity" android:screenOrientation="1" />
<activity android:launchMode="2" android:name="com.viruses.cleaner2018.activity.ChildLockerActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.viruses.cleaner2018.activity.ChildLockerMenuActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.viruses.cleaner2018.activity.SecurityFullScanActivity" android:screenOrientation="1" />
<activity android:launchMode="2" android:name="com.viruses.cleaner2018.activity.SecurityScanResultActivity" android:screenOrientation="1" />
<activity android:configChanges="0x4a0" android:launchMode="2" android:name="com.viruses.cleaner2018.activity.BatterySaveActivity" android:screenOrientation="1" />
<activity android:launchMode="1" android:name="com.viruses.cleaner2018.activity.SplashActivity" android:screenOrientation="1" android:theme="@style/MainActivityTheme">
```



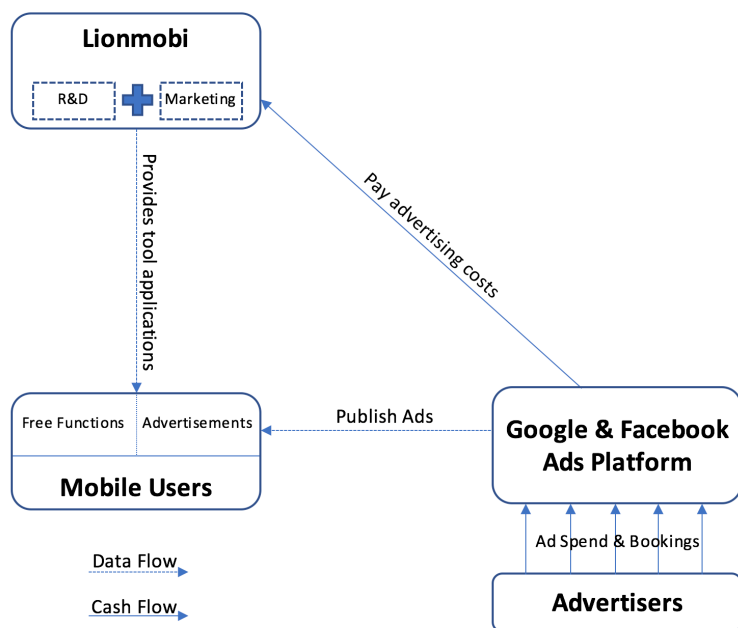
Lionmobi.com developed and published the “com.lm.powersecurity” app. On Google Play, the company address is Unit 24 on 6/F, Topsail Plaza, No.11 on Sum Street, Shatin, New Territories, Hong Kong. Its headquarters are in Chengdu, Western China. The company was established in 2014 and its core products are tool applications, which include Network Master, Battery Boost, Power Clean, and Power Scan [<http://www.lionmobi.com/>].

When running the “com.lm.powersecurity” app on a real device, quite a few pop-up ads are frequently displayed in or out of the app. Some of pop-up alerts are unacceptable and spoof users to install more apps. For example, the message “23 apps are eating your memory space!” as follows is fake because the testing device was reimaged with Google’s official factory Images [<https://developers.google.com/android/images>]. Furthermore, the app detects zero Android malware samples either from Google Play or wild. As a result, we consider the “com.lm.powersecurity” app as a rogueware based on above evidences.



Picture 19: a fake pop-up alert offered by the “com.lm.powersecurity” app

In 2015, the company had only 40 million downloads. However, by the end of 2016 more than 240 million users downloaded their apps, and there were more than 80 million active users every month. By June of 2017, the number of active users had increased to 110 million. Furthermore, the company had a strong annual revenue, exceeding \$68 million US dollars with a profit nearly \$20 million USD in 2016 [<http://news.pedaily.cn/201707/20170704416455.shtml>]. The picture below briefly illustrates the apparent business model of Lionmobi.



Picture 18: The business model of Lionmobi

Ninety-nine percent of Lionmobi's comes from Google and Facebook Ad platforms. Advertisers book and spend on ads via Google and Facebook, while Google and Facebook account for collecting ads, matching ads based on customer preference, and distributing into sub-channels such as Lionmobi apps. It does not appear that their mission is to focus on the protection of their customers worldwide. While they are doing nothing illegal, it does not appear ethical.

## Summary

Rogueware used to be a major threat to cybersecurity. After it all but disappeared from desktop computing for several years, it has developed a new life in the Android ecosystem. The technique has been utilized in a new million-dollar business model which impacts hundreds of millions of users and devices. There is no sign that this threat will go away soon.

This paper has disclosed details of the new threat and its business model. Our findings show that more than 50% of antivirus apps on Google Play can be classified as rogueware. Using three criteria we defined to help researchers narrow down potential rogueware on Google Play, we've established a research methodology to group and investigate the rogueware threat on Android.

However, this is not the end, or even the beginning of the end. Memory clean, battery boost, and junk removal apps constitute another hard-hitting area on Google Play. SophosLabs will continue to research this area to protect our customers.



## Appendix

### Rogueware Group 1:

Package Name	Downloads	SHA1
com.gotechgo.antivirus.mobilesecurity2018	500,000 - 1,000,000	c21f48cf5a76ba755978d6b93d6a465ad345c5e8
muel.security.antivirus	500,000 - 1,000,000	4637539727c133de12b432d3e8bab130724279e2
com.lalbazai.antivirus.mobilesecurity2018	1,000 - 5,000	cbf183c19e35a4cdf2d146e8884c608553294b0e
com.protector2018x.locker	500 - 1,000	751090c944cff114bd3f2c68da2191ff52efb060
com.gotechgo.antivirus.androidmobilesecurity2018	10,000 - 50,000	fe6d9875b1e90e1cc64374a8cb3979fb417baeb8
com.glagahstudio.viruscleaner.booster	10,000 - 50,000	73bdd849239b12325a113f116d6fa3eb63692b2f
com.looptoop.antivirus.android2018	10,000 - 50,000	f1c4775a2a1de01a9b550d1f9767a50a976bd007
us.antivirus.applock.mobilesecurity	1,000 - 5,000	5a25ca0c5ed813c4bdb2ab29cd6619329807fc6e
com.glagahstudio.antivirus.boostercleaner	1,000 - 5,000	f3aad02d8d3fe8333f3fc907051ecf1dda819add
com.superantivirus.mobilesecurity	1,000,000 - 5,000,000	1b6286c57609b5ba37e24e3b3a00c400789088f
com.antivirusforandroid.freeapp	100,000 - 500,000	379e10b09e0a7dcd9106398f64fb64db016fe2c
jts.security	5,000 - 10,000	100cdb1a7ddda091989b3e5ab5ac95272a948210
com.omadev.onecloud.Antivirus	500 - 1,000	55bacdad026475254786b35e8b71b7334858c1bd
com.antimalware.scanvirus1	100,000 - 500,000	63aea18cbf02ad1aaf3bc0e33098cd0abf52f20b
com.mobileapp.virus	500,000 - 1,000,000	9a1b1836f39dfebaeafa8d28e92924fb7233b4b7
com.sogotech.antivirus.security2018	1,000 - 5,000	39eba3de9c468af92285449a315e3bca85f0ab4d
com.sogotech.antivirus.maxsecurity2018	1,000 - 5,000	6be4b9baaf19308fe8e886a4b652bf4f8006333f
com.appssloution.Antivirus.Mobilesecurity	1,000 - 5,000	d772702cd50aad47cf923bea6dc6a202de7ea837
com.androidblackart.antivirus	1,000 - 5,000	7c1bf6dae4759da21534edd150ce4374d7df83b1
com.antivirus.applock.boostercleaner	1,000 - 5,000	15a9f717fae67f103b8d6693a9b847bfe4f93e60
com.techno.antivirus.phonesecurity	100 - 500	d13a86976ed50fbd84623e806d278d67ad3c6675
com.waseemtech.antivirus.maximum2018	100 - 500	c16c6320323acb7f3f800c8f18080494f178c2e7
com.sabirtech.antivirus.mobilesecurity	1,000 - 5,000	f3db8811bbc1d1c4e3e1680e112421fabe7a7293
com.studioninja.antivirus.security	1,000 - 5,000	299e8f974f9788dda7bfeab7f26794936ea12bd2
bunter.cia.antivirus.security.antivirusfree	10,000 - 50,000	37a794756668347c4c2000fd7bb81b1869039c68
com.noah.antivirus	1,000,000 - 5,000,000	fa3a34fe925ffc72a8a7272c5aa1f2bc713f2a99
com.antivirus.applex	100,000 - 500,000	210c320f88255e7f58b8c1ce1d911569926d7e3c
com.xplusapps.antivirus.free	500,000 - 1,000,000	9f35773f313c6c1661fc0a927dba8158b67b22f7
com.smallapp.antivirus	50,000 - 100,000	c345e85b200cfca3d7d5be9d8fa91fd1312542d9
com.rgamewall.anti2018	500,000 - 1,000,000	349ecc00853766fd1e27000d9a2e81faae749b78
com.supersecurity.cleaner	10,000 - 50,000	e45e7a3d5f32cf8640cccf8ba9b5e4fcb49d86f
com.redoulife.antivirus_SecurityMaster	5,000 - 10,000	27fcde09281f9ad328e7d68913e79fc86b0acbfd
com.sta.viruscleaner.antivirus	1,000,000 - 5,000,000	bd8a112c978d47f9dedbc91c6b042cdc2fc29fbd
com.fast.antivirus	100 - 500	ef71edb275a7b62976e26da95cf3a391c09590fc



antivirus.security.antivirus	50 - 100	a070ba7cf243b03f9fa256f49064cca9587939d6
com.stmdefender.viruscleaner.antivirus	10,000 - 50,000	49ee524e88f77df44ce75531cc4d2047dae57e3
hm.defendre.security_removed	100 - 500	959b531ce7af7e5ddced3fe545d169383c54b79d
com.virus.bacteria	500 - 1,000	46da32f176b7dfd16abad64449042ac1bb53f7b8
com.antivirus.freeandbest	500 - 1,000	ee72e6bce44a939890efe95a98bf1bad1c157716
com.mobihouse7.cleanmobilemasternew	5,000 - 10,000	8700b7f0bea6e96643acf8ba1b23f8691b299202
com.rgamewall.antisecure2018	100 - 500	ea9bef2608fa27de930edf70e9f77108de76f53b
com.mssoft.viruscleaner.cleanvirus	10,000 - 50,000	c0392c6095c8e15d611deb1efa2a16a84d57144d
com.myspeed.viruscleaner.clean_remove	100 - 500	07e0fad58c3e43d05dfb9db76b1a43c99181edc8
com.psmlab.tools.antivirusapplock. phonesecurity.antivirus	100,000 - 500,000	65cb4aee106695f8d8299bbb96e84b7509c97c4e
antivirus.threatscannner.security	1,000 - 5,000	270de3e6ec333988e0e7a1c3cc012999f55c0a36
com.stranger.maxsecurity	500,000 - 1,000,000	f59c3ec94d0dea1f5c7a7ebbf2ac5d1eed3aaca0
com.antivirusfree.cleanforandroid	5,000 - 10,000	5e51067443f51b2793d8680a84fcabf786e239eb
com.lempea.antivirus.security.master	10,000 - 50,000	8cc07f88228fec030cde56d098d7ef08a98623b5

#### Rogueware Group 2:

Package Name	Downloads	SHA1
com.androaplite.antivirus.antivirusapplication_two	1,000,000 - 5,000,000	c511aa713ce578fec8658858ce0e0aa16347bab7
com.androaplite.antivirus.four	1,000,000 - 5,000,000	b43c5832153525808850fb1ed6aa20870f091092
com.androaplite.antivirus.five	1,000,000 - 5,000,000	a5f6a6ba48b1d79fcf46f6e3d733d08fb823e9e5
com.tools.dantivirus	500,000 - 1,000,000	45809365efca139f6fb9813581446b9b8c2f4f0d
com.bs.antivirus	100,000 - 500,000	6617524b1ab95817dc7ce8d90ef7c5793994eecd4
com.antivirus.cleaner.booster	50,000 - 100,000	b7c6f45440da78cd73f0cdf5441dc47ca313f3cb
com.smapps.antivir	1,000 - 5,000	ba4d2b3f51fbf53e8ca2e11dad3694873718bf3a
com.bomba.antivir	10 -50	aba0db7a8d6635fc1c9403ea8da1f081ed768742

#### Rogueware Group 3:

Package Name	Downloads	SHA1
com.apps.power.super.clean.security.master	100,000 - 500,000	64c1894962da4cae802eae536f84a8f4a14049bb
com.hyperspeed.rocketclean	10,000,000 - 50,000,000	88709f4f3d24d6089fbb9e4fe6e8b40ca6f362ec
com.mobile.security.antivirus.applock.wifi	1,000,000 - 5,000,000	0508588ea166be85cf94ec6f0f5f4bd80cafbbbc
com.powertools.privacy	10,000,000 - 50,000,000	fc588fa06e1b93ec989c50e3dbc8b4d8e31871e5
com.oneapp.max	10,000,000 - 50,000,000	de993e147b924962dcf6e57dd76a0b2c8110a2c1
com.oneapp.max.cleaner.booster	500,000 - 1,000,000	d94e0772e9b9f065e5a006687341d39bf03bb3d1
com.oneapp.max.security.pro	100,000 - 500,000	1a5b4549f1d5cc44de9e30d4974d90b094c5096a

## Rogueware Group 4:

Package Name	Downloads	SHA1
com.himlamlos.cleaner	100,000 - 500,000	d8fe2279a0df92e6a61b2437d7d4168e5e9cd8b5
antivirus2018.booster.cleaner	10,000 - 50,000	73d5fee29032f4724164a503138f7d85be5604c3
smart.booster.antivirus	10,000 - 50,000	37e444ac6225eabbb6ba80ce89ecba59326cd253
dav.antivirus.smartdv	10,000 - 50,000	c13960f1746776288c9267a4510f204e04ce0804
com.geardots.cleaner	10,000 - 50,000	de140feffbbd76cf72a8f337d84dc755466f08ff
deep.super.guardian	1,000 - 5,000	65a112d3890001d43b353dc4383c26c5bed2c362
com.viruses.cleaner2018	100 - 500	cb663e5085969843d1f04e4028af7aa0599d5852
com.antivirus.antimalware	5,000 - 10,000	0b28443231eb18fe2cbeec4ec8ec327eb222e89a
com.mentokas.cleaner	1,000,000 - 5,000,000	c163195eb470674677219f3e822085cbb0d5d8db
com.mobilesecurity.antivirus.booster.cleaner	100,000 - 500,000	aa104ff3aa4da88b8d489de164ea9220a750ad64
jeanclean.memorybooster.cleaner	500 - 1000	bd495c0d67e0a438e6fd2b24c355476a21cf32ff
protect.privacy.security.app.lock.antivirus.lite	10,000 - 50,000	5bd5c3049dfe342a96207880ae23d1cb34d05eb
com.lm.powersecurity	10,000,000 - 50,000,000	124ac4a2487ce0886d52c3e41170e79b189106a1

## Rogueware Group 5:

Package Name	Downloads	SHA1
com.antiviruspro.security.booster.cleaner	100,000 - 500,000	7b03f35ee2817f1dd9e54a56c31081743d7168b2
com.security.antivirus.remover.scan.removalmx	100,000 - 500,000	1c06eca41b3a2cc226108d5f9e19b04239c65931
com.protoolapps.antivirus.security.android	1,000,000 - 5,000,000	facaf7df3a8432ce4d6e20a39dc931c84368fdb9
com.bit.myandroidantivirus.googleplay	100,000 - 500,000	935a4720c0e0610bb17ae45e0d30b8d914d567e2
com.antivcleaner.speedboost.foranroid	1,000 - 5,000	1dfacd1bca27d2356c3efd207de829adfe2a2325
antivirus.security.cleaner.booster	5,000 - 10,000	49b36d869139fff298187a6e43fa68a06cba8e2f
com.ser.vir.ett	1,000 - 5,000	a673f9df5aa9816ed1a8b564e879b61067901604
com.antivirus.fast.safeboost.wemakeit.googleplay	1,000,000 - 5,000,000	ef845a35b9657213a839da734194503bf28e8ca2
com.antivirussystemforandroid.brainiacs.googleplay	1,000,000 - 5,000,000	1e09085e1f2048164115706c06d59ca8afb59b8b
com.securityantivirusforandroid.uberapps.googleplay	1,000,000 - 5,000,000	a953c91c4316f5b4067f872b690414014850a76d
com.womboidsystems.antivirus.security.android	100,000 - 500,000	b5e7cae7f58504a3d01918507318becc8a62760d
com.benchmark.pro.tool.android	1,000 - 5,000	2c3671f8b57395dfb7713189c266670a638f192f
com.protool.speed.tester.android	50,000 - 100,000	eed888b027a3c8d32d57630355002d89ae12d7fe

## Rogueware Group 6:

Package Name	Downloads	SHA1
smart.antivirus.phone	10,000 - 50,000	e2a3644c1b969b48df9d1bfed31139bb4cadd98c
com.fluerapps.antiviruspremium2018	50 - 100	0258ad052dd341ed58e544fc766a5821b6443ad6
at.ncn.antiviruspro	1,000 - 5,000	5a1686f3c03e86ba83a58529c758d5936acd41e2
com.fluerapps.antivirus2018freepremium	5,000 - 10,000	4fcf7d87e45c926300332063020d684382b2be8d
com.free.antivirus.hoje	1,000 - 5,000	b542004f31c6169a4c77b548add4461f1041899e
at.ncn.freeantiviruspro2014	100,000 - 500,000	a9d0ef8caa32211afd3a445b9547fd7ca057180e
at.ncn.freeantiviruspro	100,000 - 500,000	60f0710e288c6c84033749f134a7a9c91b2390d8
com.fluerapps.antivirus2016premiumfree	100,000 - 500,000	8c6af432971c8880757534ab3d9828a05cb9f045
antivirus.free	1,000,000 - 5,000,000	da5bf77e763f72375e13f169f6f26aca2b5b8649

## Rogueware Group 7:

Package Name	Downloads	SHA1
com.free.security.anti.virus2018	100,000 - 500,000	274cc36c659a0cf78338cf3f059d64b9bbae447a
com.perfectboosterand.cleaner2018.A.Z.R	1,000 - 5,000	15412fcb40c1e59fa8653e69e5f434aaf9d0ca7a
com.antivirus.security.aplock.viruscleaner	100 - 500	05b9b8b0eb5fde8c29d07c09ec7a12c32b0f6221
com.cb.clean.free.optimizer.antivirus.power	10,000 - 50,000	b7a9bb2fedce34c95c577d0a5ebb22dea63741ed
bubble.security.clean.antivirus.master.free	100,000 - 500,000	13e6ba77848479f294a89b60bfae73a18678ca39
com.wingle.real.antivirus	50,000 - 100,000	170f961d94a9de2d4635c92023593561b181af49
com.h2.freeantivirus	500,000 - 1,000,000	d433ca6a12343d51042bd0cce7d63eaefff018e4
ccleaner.clean.boost.battery.pro	5,000 - 10,000	6f9eb5e96b5e4bc482ed39732e87b7c5be2c7d26
com.outthinking.cleanmemory	50,000 - 100,000	b58b8fb87ed714b82f5af6ac60d6191209cce2d2

## Rogueware Group 8:

Package Name	Downloads	SHA1
com.puce.antivirus.mobilesecurity	100,000 - 500,000	eeddc36d5d2e67a85d9d8b5b1c17dfacf6def6c6
com.freeantivirus.cleanvirus	500,000 - 1,000,000	ced049734fe8f0c8ad4b45577f7deb4fa9ae0b11
com.antivirus.security.free	10,000 - 50,000	5d2dfa2cc651038ec8c1ba0b8ddc0073ca5a6e5d
com.gpaddy.free.antivirus	1,000,000 - 5,000,000	6f9af69cf8fa76e2c11ac3514631883dd3a02669

## Rogueware Group 9:

Package Name	Downloads	SHA1
app.free.antivirus.freeantivirus	50,000 - 100,000	431e53b63165b4a2aac6ea24a960d12a5013a556
com.boolmind.antivirus	10,000 - 50,000	942d6f72a322ee1e26947d54d360063e8bbbb6e3
com.freeantivirus.free.antivirus	1,000 - 5,000	095e15ee60997a4a095f356028f026b7c6bf8f36
com.bass.cleaner.security	1,000,000 - 5,000,000	970995ffdee92d769d21f2e5b787e1c37fe039c4
com.bass.max.cleaner	1,000 - 5,000	3f4841b4bc700d38dcfa7562b0fe86266cb10325

### Rogueware Group 10:

Package Name	Downloads	SHA1
com.smail.smile.security.clean.boost	100,000 - 500,000	6de26b8dd9ca96ced35ade6d17b92b862f97334b
com.newborntown.android.solo.security.free	500,000 - 1,000,000	bd2df8cfe973cee7018642be69e5ef05d5426614

### Rogueware Individuals:

Package Name	Downloads	SHA1
com.fasttrack.security	10,000,000 - 50,000,000	2b1535593e4a4daf22911475df9e91442ff84d34
com.antivirus.mobilesecurity.viruscleaner.applock	5,000,000 - 10,000,000	642ba063faf9c04654fcf008a57ad034044587f9
com.fotoable.cleaner	5,000,000 - 10,000,000	a79cc55af60a98b90356dd5c6d62b1c3783145e0
com.cellsoft7.scanner.antivirus.detector. spy.cache.cleaner.malware	10,000 - 50,000	b6776d260780cc9a6a80820297ccb0e939c6e378
com.npv.clean	1,000,000 - 5,000,000	5130250954d07ba51bdfa99876bb2b9027c13a63
app.cleaner.booster.master.antivirus	100,000 - 500,000	a8d3201b7a6e3cc9e7cb183df974ac624cf372f5
com.atvcleaner	50,000 - 100,000	8731c5f3e498f2c30acf66ab3134734a383c2c73
com.fotoable.security	100,000 - 500,000	ac8c8f6a11224b4dbcbd133603593f2a7f2c8c7e
com.immunesmart.security.junkcleaner. cachere mover.power.booster.cleanram.antivirus. memory.master.cooler.fast.speed.free	10,000 - 50,000	490a38795fbcfb04b2ac8e66f87b7f214c91e2ce

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