DroidJack Uses Side-Load - Backdoored Pokemon GO Android App Found | Proofpoint US

By July 07, 2016 Proofpoint Staff

Published: 2016-11-03 · Archived: 2026-04-06 02:12:55 UTC

Overview

Pokemon GO is the first Pokemon game sanctioned by Nintendo for iOS and Android devices. The augmented reality game was first released in Australia and New Zealand on July 4th and users in other regions quickly clamored for versions for their devices. It was released on July 6th in the US, but the rest of the world will remain tempted to find a copy outside legitimate channels. To that end, a number of publications have provided tutorials for "side-loading" the application on Android. However, as with any apps installed outside of official app stores, users may get more than they bargained for.

In this case, Proofpoint researchers discovered an infected Android version of the newly released mobile game Pokemon GO [1]. This specific APK was modified to include the malicious remote access tool (RAT) called DroidJack (also known as SandroRAT), which would virtually give an attacker full control over a victim's phone. The DroidJack RAT has been described in the past, including by Symantec [2] and Kaspersky [3]. Although we have not observed this malicious APK in the wild, it was uploaded to a malicious file repository service at 09:19:27 UTC on July 7, 2016, less than 72 hours after the game was officially released in New Zealand and Australia.

Likely due to the fact that the game had not been officially released globally at the same time, many gamers wishing to access the game before it was released in their region resorted to downloading the APK from third parties. Additionally, many large media outlets provided instructions on how to download the game from a third party [4,5,6]. Some even went further and described how to install the APK downloaded from a third party [7]:

"*To install an APK directly you'll first have to tell your Android device to accept side-loaded apps. This can usually be done by visiting Settings, clicking into the Security area, and then enabling the "unknown sources" checkbox."*

Unfortunately, this is an extremely risky practice and can easily lead users to installing malicious apps on their own mobile devices.. Should an individual download an APK from a third party that has been infected with a backdoor, such as the one we discovered, their device would then be compromised.

Individuals worried about whether or not they downloaded a malicious APK have a few options to help them determine if they are now infected. First, they may check the SHA256 hash of the downloaded APK. The legitimate application that has been often linked to by media outlets has a hash of 8bf2b0865bef06906cd854492dece202482c04ce9c5e881e02d2b6235661ab67, although it is possible that there are updated versions already released. The malicious APK that we analyzed has a SHA256 hash of 15db22fd7d961f4d4bd96052024d353b3ff4bd135835d2644d94d74c925af3c4.

Another simple method to check if a device is infected would be to check the installed application's permissions, which can typically be accessed by first going to Settings -> Apps -> Pokemon GO and then scrolling down to the *PERMISSIONS* section. Figure 1 shows a list of permissions granted to the **legitimate** application. These permissions are subject to change depending on the device's configuration; for example the permissions "Google Play billing service" and "receive data from Internet" are not shown in the image but were granted on another device when downloading Pokemon GO from the Google Play Store. In Figures 2 and 3, the outlined permissions have been added by DroidJack. Seeing those permissions granted to the Pokemon GO app could indicate that the device is infected, although these permissions are also subject to change in the future.

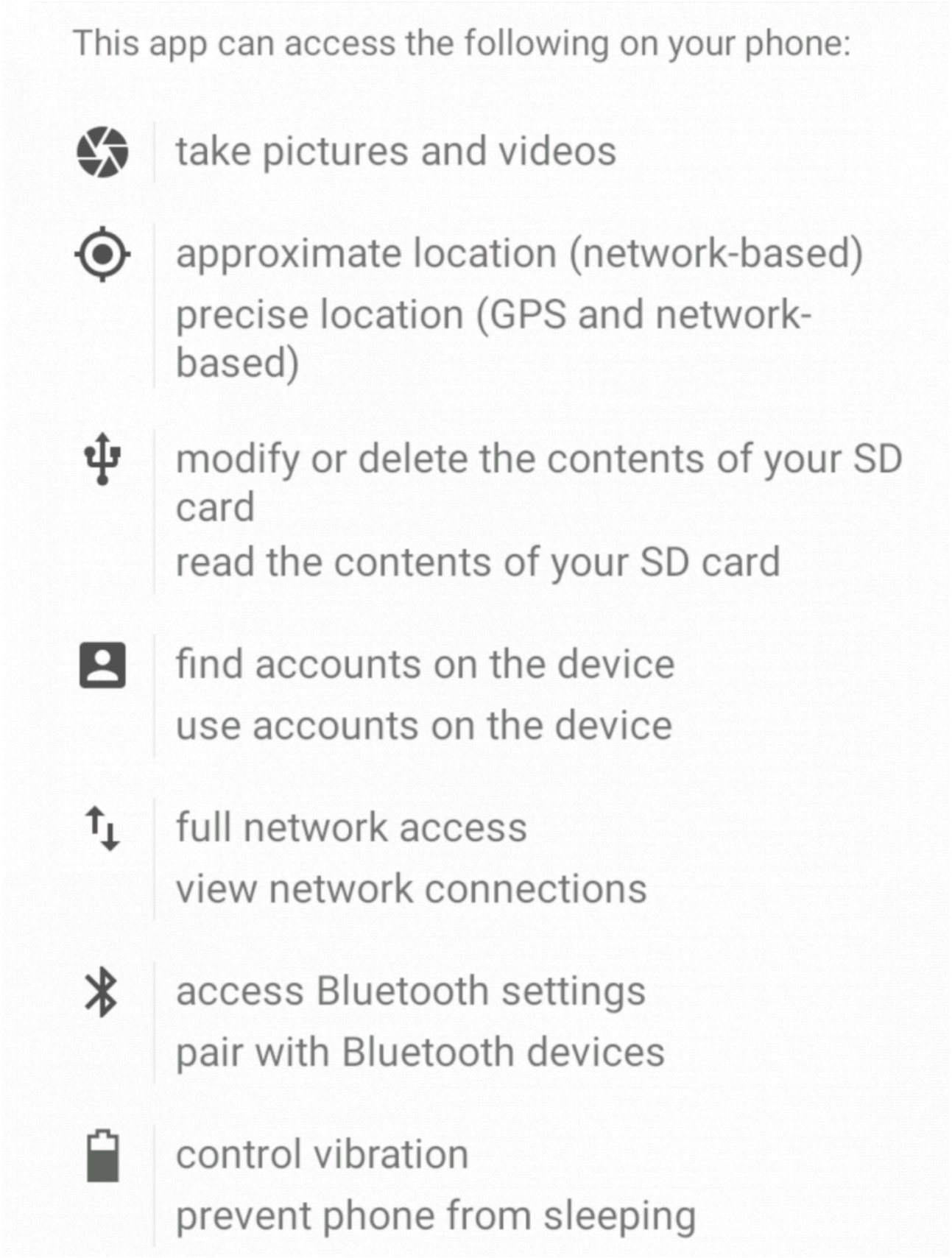

Figure 1: Granted permissions from legitimate Pokemon GO APK

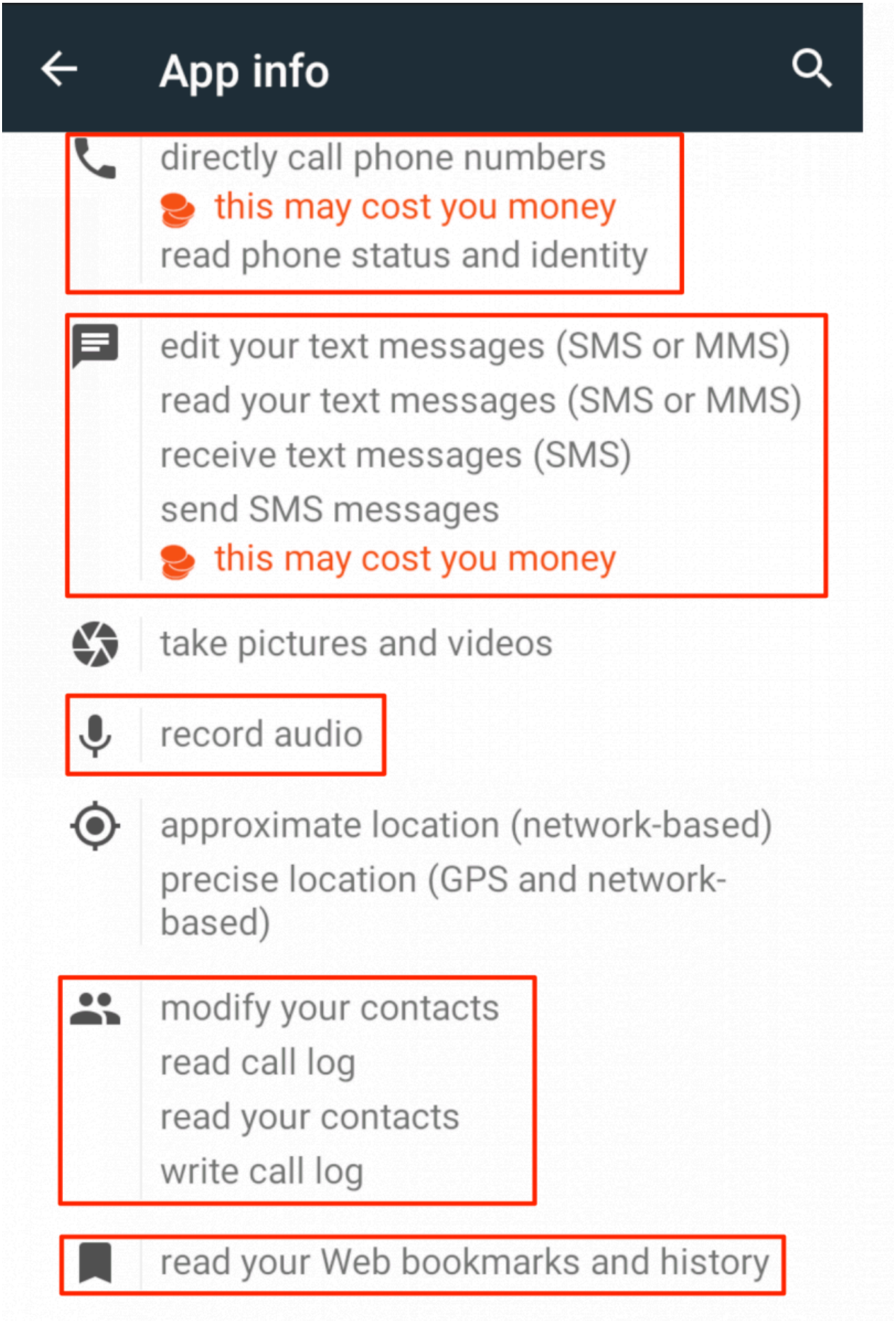
App info
directly call phone numbers
this may cost you money
read phone status and identity
edit your text messages (SMS or MMS)
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money
take pictures and videos
record audio
approximate location (network-based)
precise location (GPS and network-based)
modify your contacts
read call log
read your contacts
write call log
read your Web bookmarks and history

Figure 2: Granted permissions from the backdoored Pokemon GO APK (first screenshot)

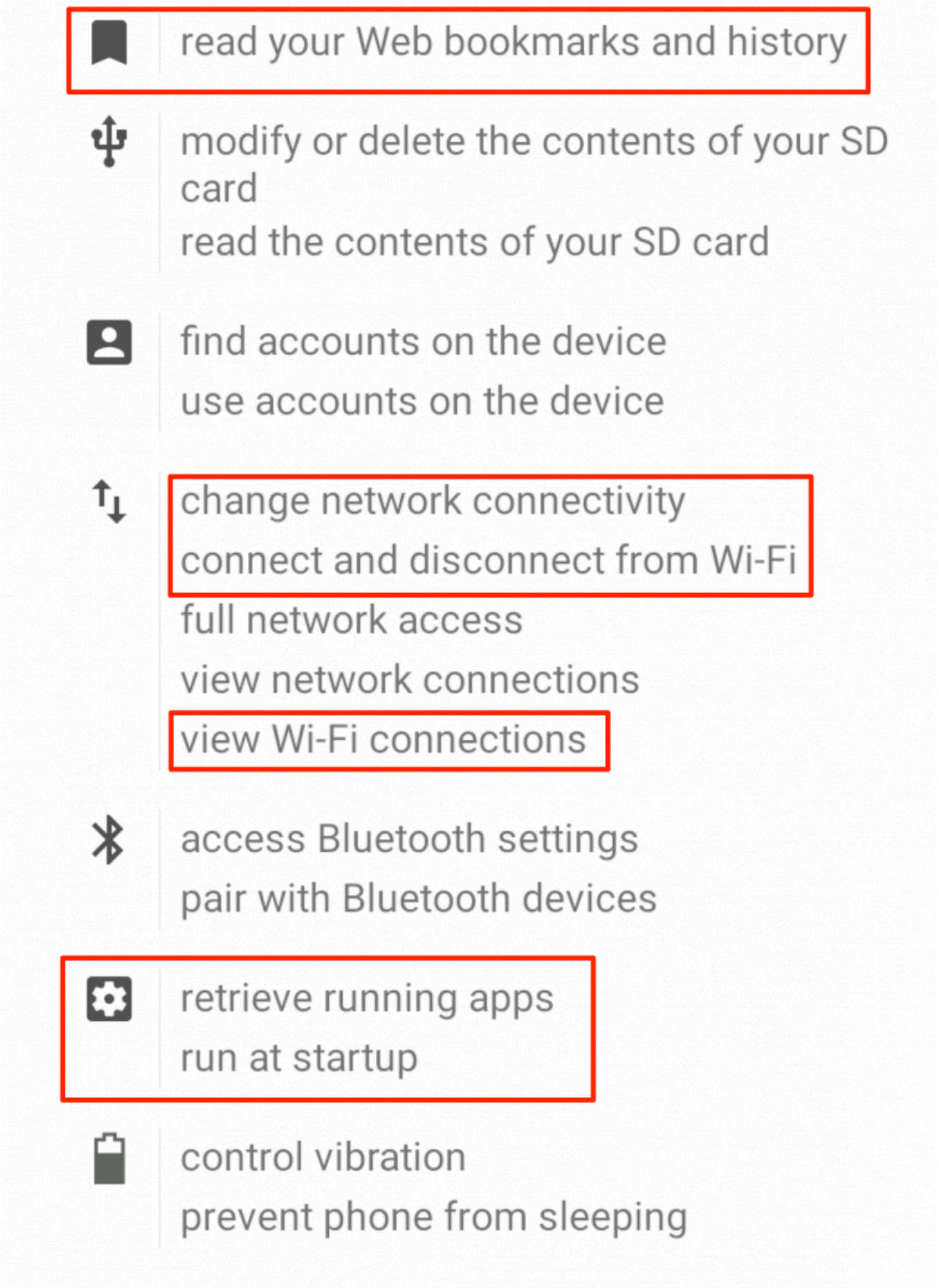

Figure 3: Granted permissions from backdoored Pokemon GO APK (second screenshot)

The infected Pokemon GO APK has been modified in such a way that, when launched, the victim would likely not notice that they have installed a malicious application. Figure 4 shows the startup screen from the infected Pokemon GO game, which is identical to the legitimate one.


Please enter your date of birth.
JAN
1
2016
SUBMIT

Figure 4: Infected Pokemon GO start screen; it appears identical to that of the legitimate application

After inspecting the infected game further, when compared to the legitimate game three classes stand out that have been added by the attacker. Figure 5 shows the classes from the legitimate game while Figure 6 shows the classes from the infected game, including the following added classes:

- *a*
- *b*
- *net.droidjack.server*

Furthermore, this DroidJack RAT has been configured to communicate to the command and control (C&C) domain pokemon[.]no-ip[.]org over TCP and UDP port 1337 (Fig. 7). No-ip.org is a service used to associate a domain name with a dynamic IP address like that generally assigned to home or small business users (as opposed to a dedicated IP address), but is also used frequently by threat actors, along with other similar services like DynDNS. At the time of analysis, the C&C domain resolved to an IP address in Turkey (88.233.178[.]130) which was not accepting connections from infected devices.

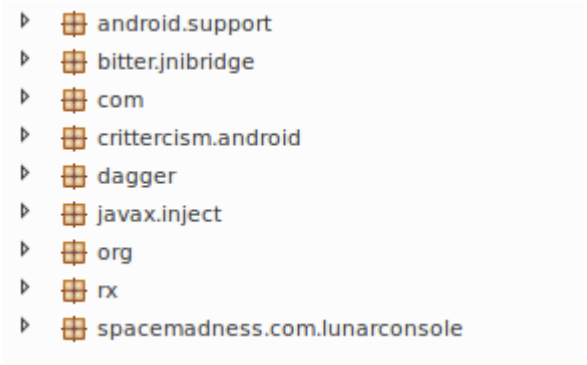

Figure 5: Legitimate Pokemon GO classes

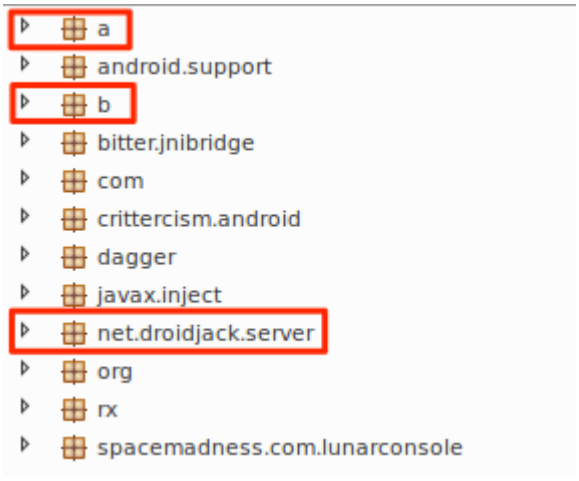

Figure 6: Infected Pokemon GO classes with highlighted malicious classes

```
package net.droidjack.server;

public class br
{
  protected static String a = "pokemon.no-ip.org";
  protected static int b = 1337;
  protected static byte c = -1;
}
```

Figure 7: Hardcoded C&C domain and port

Conclusion

Installing apps from third-party sources, other than officially vetted and sanctioned corporate app stores, is never advisable. Official and enterprise app stores have procedures and algorithms for vetting the security of mobile applications, while side-loading apps from other, often questionable sources, exposes users and their mobile devices to a variety of malware. As in the case of the compromised Pokemon GO APK we analyzed, the potential exists for attackers to completely compromise a mobile device. If that device is brought onto a corporate network, networked resources are also at risk.

Even though this APK has not been observed in the wild, it represents an important proof of concept: namely, that cybercriminals can take advantage of the popularity of applications like Pokemon GO to trick users into installing malware on their devices. Bottom line, just because you can get the latest software on your device does not mean that you should. Instead, downloading available applications from legitimate app stores is the best way to avoid compromising your device and the networks it accesses.

References

1.http://pokemongo.nianticlabs.com/en/

2.http://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime

3.http://www.welivesecurity.com/2015/10/30/using-droidjack-spy-android-expect-visit-police/

4.https://www.theguardian.com/technology/2016/jul/07/how-to-get-pokemon-go-uk

5.http://www.wired.co.uk/article/pokemon-go-out-now-download-ios-android

6.http://www.androidpolice.com/2016/07/07/pokemon-go-now-live-several-countries-including-australia-new-zealand-possibly/

7.http://arstechnica.com/gaming/2016/07/pokemon-go-ios-android-download/

Indicators of Compromise (IOC)

IOC	IOC Type	Description
15db22fd7d961f4d4bd96052024d353b3ff4bd135835d2644d94d74c925af3c4	SHA256	Backdoored Pokemon GO APK
d350cc8222792097317608ea95b283a8	MD5	Backdoored Pokemon GO APK
pokemon.no-ip.org	Domain	DroidJack C&C
88.233.178.130	IP	DroidJack C&C

Select ET Signatures that would fire on such traffic:

2821000 || ETPRO MOBILE_MALWARE Pokemon GO AndroidOS.DroidJack DNS Lookup

2821003 || ETPRO MOBILE_MALWARE AndroidOS.DroidJack UDP CnC Beacon

---