DroidJack isn't the only spying software out there: Avast discovers OmniRat

blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co


Nikolaos Chrysaidos 5 Nov 2015

OmniRat is currently being used and spread by criminals to gain full remote control of devices.

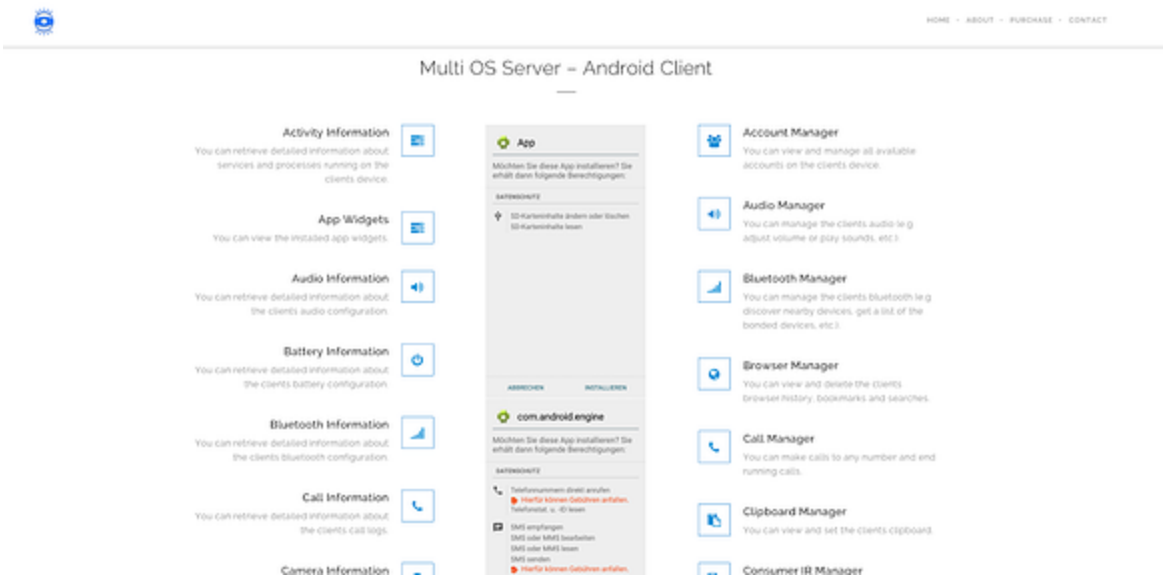
There's more than one RAT

On Friday, I discovered OmniRat, a program similar to DroidJack. DroidJack is a program that facilitates remote spying and recently made news when European law enforcement agencies made arrests and raided the homes of suspects as part of an international malware investigation.

OmniRat and DroidJack are RATs (remote administration tools) that allow you to gain remote administrative control of any Android device. OmniRat can also give you remote control of any Windows, Linux or Mac device. Remote administrative control means that once the

software is installed on the target device, you have full remote control of the device.

On their website, OmniRat lists all of the things you can do once you have control of an Android, which include: retrieving detailed information about services and processes running on the device, viewing and deleting browsing history, making calls or sending SMS to any number, recording audio, executing commands on the device and more.



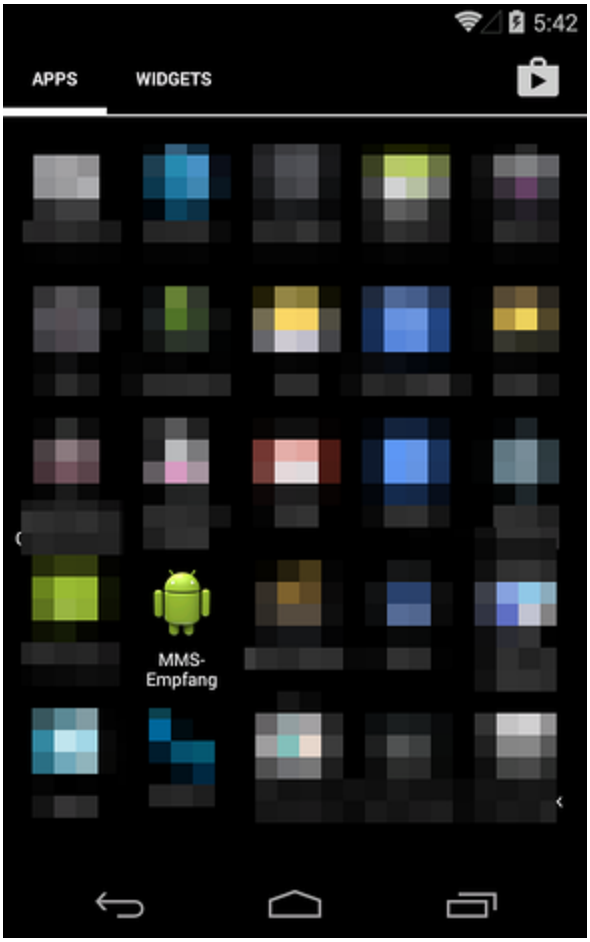
Like DroidJack, OmniRat can be purchased online, but compared to DroidJack, it's a bargain. Whereas DroidJack costs $210, OmniRat costs only $25 to $50 depending on which device you want to control.

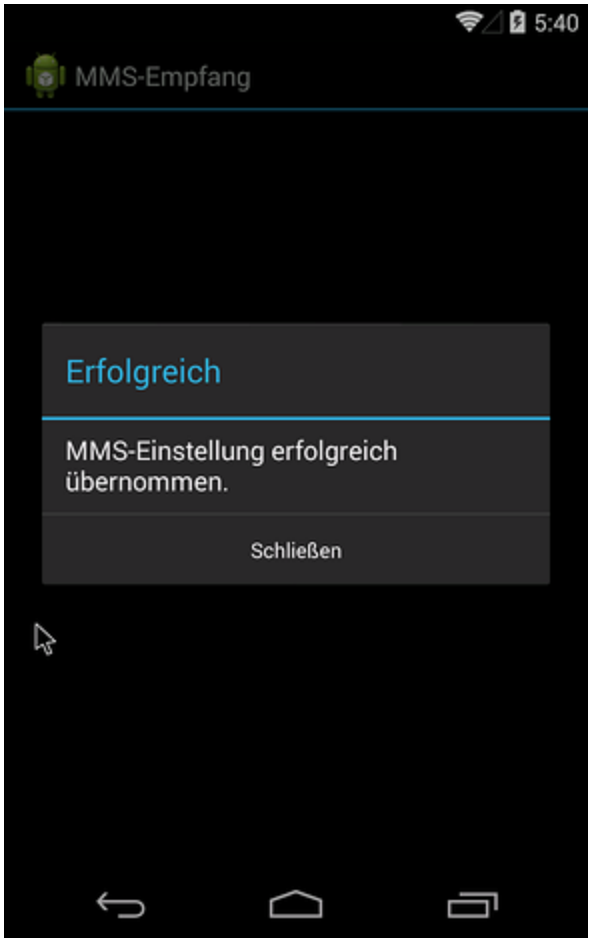
You may be asking yourself, "Why is software like this being sold on the Internet?". According to DroidJack's creator, Sanjeevi, "Droidjack is a parental tool for Android remote administration," but Europol has made it very clear that using software like DroidJack for malicious purposes can have major consequences. In an investigation supported by Europol and Eurojust, law enforcement agencies in Europe and the U.S. arrested users of DroidJack.

OmniRat variant in the wild

A custom version of OmniRat is currently being spread via social engineering. A user on a German tech forum, Techboard-online, describes how a RAT was spread to his Android device via SMS. After researching the incident, I have come to the conclusion that a variant of OmniRat is being used.
The author of the post received an SMS stating an MMS from someone was sent to him (in the example, a German phone number is listed and the SMS was written in German). The SMS goes on to say "This MMS cannot be directly sent to you, due to the Android vulnerability StageFright. Access the MMS within 3 days [Bitly link] with your telephone number and enter the PIN code [code]". Once the link is opened, a site loads where you are asked to enter the code from the SMS along with your phone number.

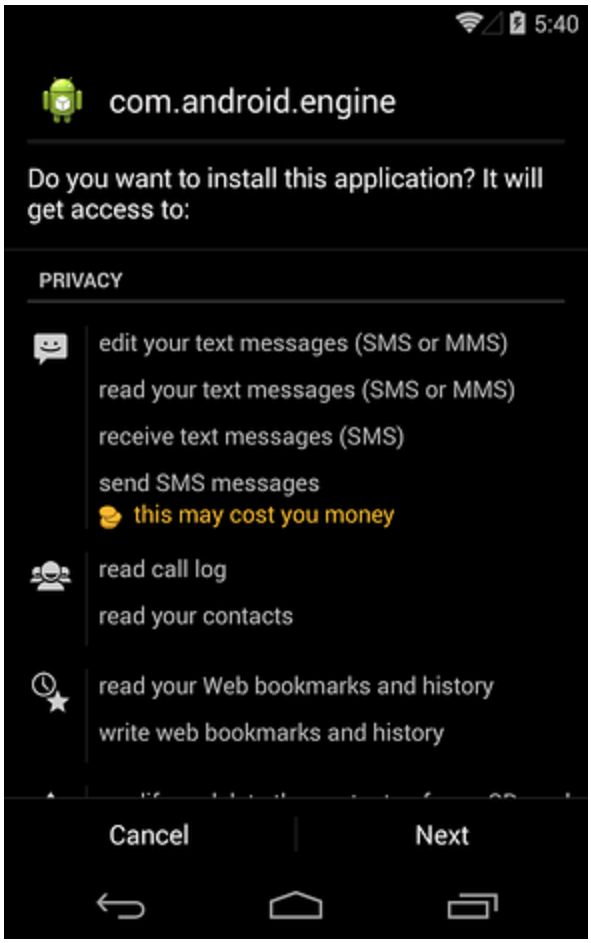
Once you enter your number and code, an APK, mms-einst8923, is downloaded onto the Android device. The mms-einst8923.apk, once installed, loads a message onto the phone saying that the MMS settings have been successfully modified and loads an icon, labeled “MMS Retrieve” onto the phone.





Once the icon is opened by the victim, mms-einst8923.apk extracts OmniRat, which is encoded within the mms-einst8923.apk. In the example described on Techboard-online, a customized version of OmniRat is extracted.

The OmniRat APK requires users to accept and give OmniRat access many permissions, including edit text messages, read call logs and contacts, modify or delete the contents of the SD card. All of these permissions may seem evasive and you may be thinking, “Why would anyone give an app so much access?”, but many of the trusted and most downloaded apps on the Google Play Store request many of the same permissions. The key difference is the source of the apps. I always recommend that users read app permissions carefully. However, when an app you are downloading directly from the Google Play Store requests permissions, it is rather unlikely the app is malicious. I therefore advise you only download apps directly from the Google Play Store. If, like this in case, the app is downloaded from an untrusted source, users should be highly suspicious of the permissions being requested.



Once installed, OmniRat gives full remote administrative control of the device to the attacker. Even if the victim deletes the original “MMS Retrieve” icon installed with the mms-einst8923, OmniRat remains on the infected device. **The victim then has no idea their device is being controlled by someone else and that every move they make on the device is being recorded and sent back to a foreign server.**

Furthermore, once cybercriminals have control over a device’s contact list, they can easily spread the malware to more people. Inside this variant of OmniRat, there is a function to send multiple SMS messages. What makes this especially dangerous is that the SMS spread via OmniRat from the infected device will appear to be from a known and trusted contact of the recipients, making them more likely to follow the link and infect their own device.

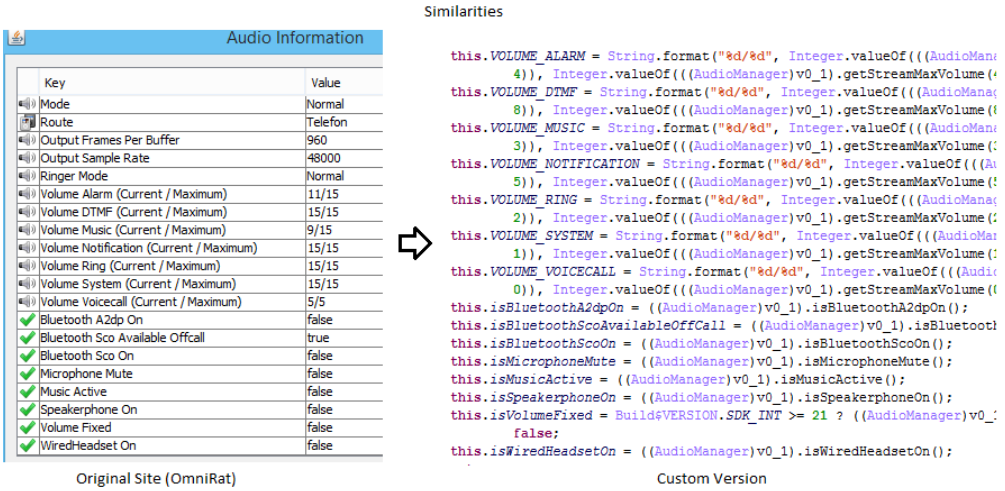
We know that the data collected by the customized version of OmniRat targeting the German person from the Techboard-online forum post is being sent back to a Russian domain, based on the command and control (C&C) server address the data is being sent to.

```
public class MyService extends Service {
    private static final b b;
    private boolean c;

    static {
        MyService.b = new b("[redacted].ru", 1300);
    }

    public MyService() {
```

The ".ru" server address tell us the data is being sent back to a Russian domain.



The left image above was taken from OmniRat's Website and shows the audio data that is being extracted from the victim's device. The right image is of the custom version of OmniRat and shows the similarity of the data (and the order) that it is being gathered in and sent back to a Russian domain.

In the image above, we can see all the dex classes of the second APK file that gather various information about the device and sends it back to the server.

How to protect yourself

- Make sure you have an antivirus solution installed on your smartphone to detect malware, like OmniRat. Avast detects OmniRat as Android:OmniRat-A [Trj].

- Do not open any links from untrusted sources. If an unknown number or email address sends you a link, do not open the link.
- Do not download apps from unknown sources to your mobile device. Only download apps from trusted sources such as the Google Play Store or the Apple App Store.