SpyNote RAT posing as Netflix app | Zscaler Blog

By Shivang Desai

Published: 2017-01-23 · Archived: 2026-04-05 21:52:52 UTC

Watch on Fox News: Hackers may use fake Netflix app to spy on users

As users have become more attached to their mobile devices, they want everything on those devices. There's an app for just about any facet of one's personal and professional life, from booking travel and managing projects, to buying groceries and binge-watching the latest Netflix series.

The iOS and Android apps for Netflix are enormously popular, effectively turning a mobile device into a television with which users can stream full movies and TV programs anytime, anywhere. But the apps, with their many millions of users, have captured the attention of the bad actors, too, who are exploiting the popularity of Netflix to spread malware.

Recently, the ThreatLabZ research team came across a fake Netflix app, which turned out to be a new variant of SpyNote RAT (Remote Access Trojan).

SpyNote RAT is capable of performing a variety of alarming functions that includes:

- Activating the device's microphone and listening to live conversations
- Executing commands on the device
- Copying files from the device to a Command & Control (C&C) center
- Recording screen captures

- Viewing contacts
- Reading SMS messages

The screenshot below shows part of the sandbox's report on the SpyNote RAT's signature and detected functions:

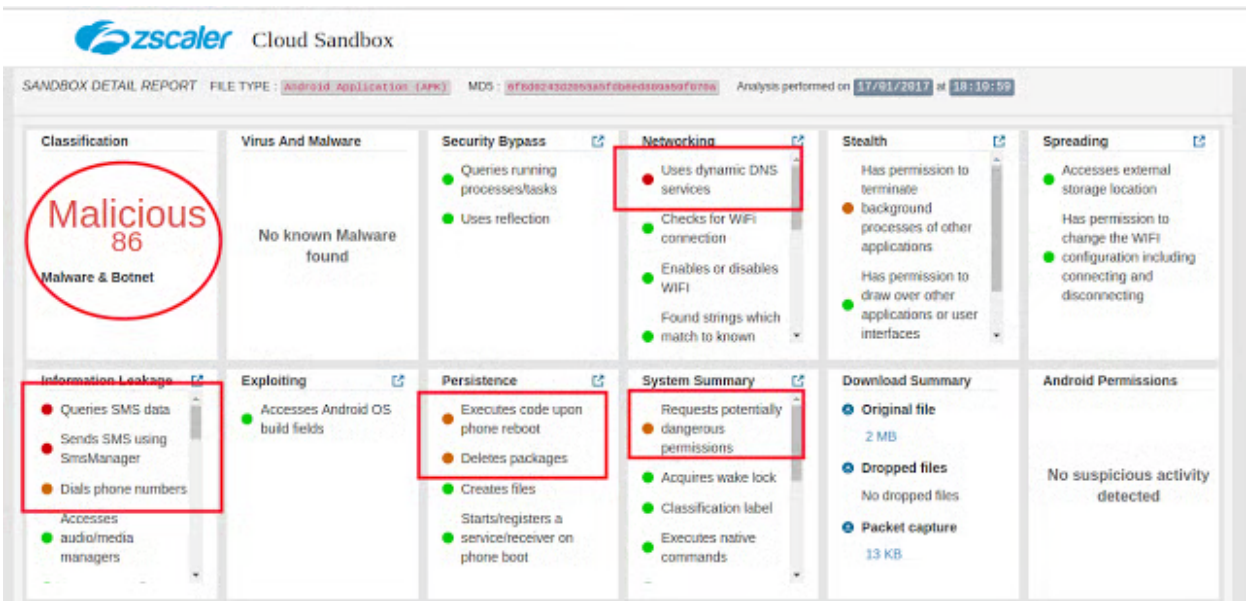

Figure 1 : Zscaler Cloud Sandbox Detection

The fake Netflix app we are analyzing in this blog appears to be built using an updated version of SpyNote RAT builder, which was leaked last year.

Technical details

Please note that our research is not about the legitimate Netflix app on Google Play.

The spyware in this analysis was portraying itself as the Netflix app. Once installed, it displayed the icon found in the actual Netflix app on Google Play.

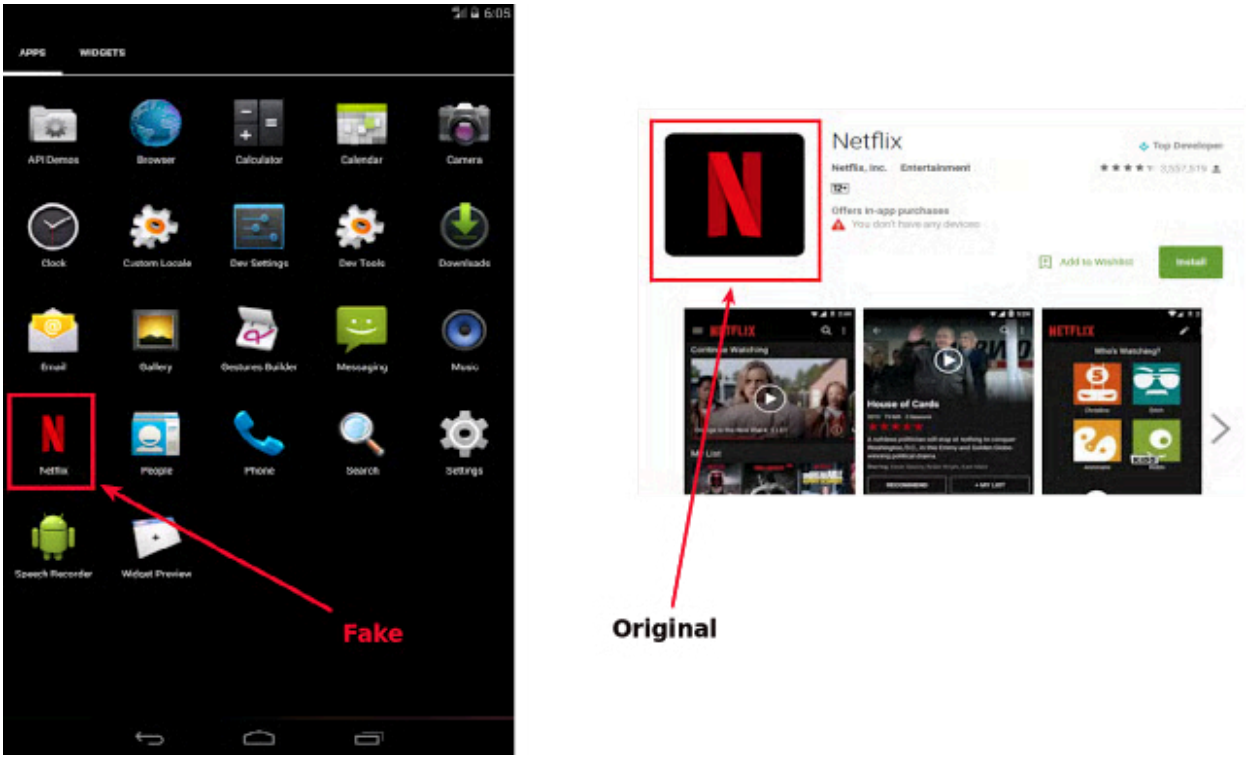

Figure 2: Fake Netflix vs. legitimate Netflix

As soon as the user clicks the spyware's icon for the first time, nothing seems to happen and the icon disappears from the home screen. This is a common trick played by malware developers, making the user think the app may have been removed. But, behind the scenes, the malware has not been removed; instead it starts preparing its onslaught of attacks.

For contacting C&C, the spyware was found to be using free DNS services, as shown in the screenshot below:

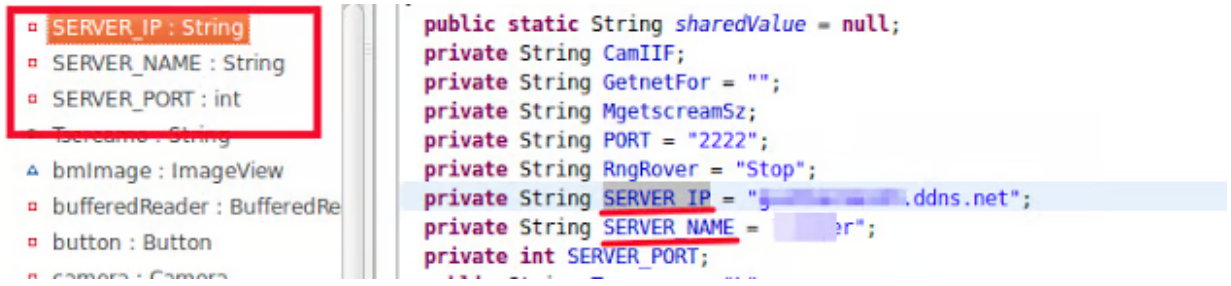

Figure 3: Server details

SpyNote RAT uses an unusual trick to make sure that it remains up and running and that the spying does not stop. It does so using the Services, Broadcast Receivers, and Activities components of the Android platform.

Services can perform long-running operations in the background and does not need a user interface. Broadcast Receivers are Android components that can register themselves for particular events. Activities are key building blocks, central to an app's navigation, for example.

The SpyNote RAT registers a service called AutoStartup and a broadcast receiver named BootComplete.

MainActivity registers BootComplete with a boot event, so that whenever the device is booted, BootComplete gets triggered.

BootComplete starts the AutoStartup service and the AutoStartup service makes sure that MainActivity is always running.

What follows are some of the features exhibited by SpyNote RAT.

Command execution

Command execution can create havoc for victim if the malware developer decides to execute commands in the victim's device. Leveraging this feature, the malware developer can root the device using a range of vulnerabilities, well-known or zero-day.

The following screenshot shows the command execution functionality in action:

```
public String Executer(String paramString)
{
  StringBuffer localStringBuffer = new StringBuffer();
  try
  {
    paramString = Runtime.getRuntime().exec(paramString);
    paramString.waitFor();
    paramString = new BufferedReader(new InputStreamReader(paramString.getInputStream()));
    while (true)
    {
      String str = paramString.readLine();
      if (str == null)
        break;
      localStringBuffer.append(str + "n");
    }
  }
  catch (Exception paramString)
```

Figure 4: Command Execution

The paramString parameter shown in the above screenshot can be any command received from C&C.

Screen capture and audio recording

SpyNote RAT was able to take screen captures and, using the device's microphone, listen to audio conversations. This capability was confirmed when the Android permission, called android.permission.RECORD_AUDIO, was being requested along with code found in the app.

SpyNote RAT captured the device's screen activities along with audio using the MediaProjectionCallback functionality (available with Lollipop, the Android 5.0 release, and later) and saved the output in a file named "video.mp4" as shown in the following screenshot:

Figure 5 : Output File

SMS stealing

SpyNote RAT was also observed stealing SMS messages from the affected devices, as shown in screenshot below:

Figure 6: Reading SMS messages

Stealing contacts

The ability to steal contacts is a favorite feature for spyware developers, as the stolen contacts can be used to further spread the spyware.

The following screenshot shows the contacts being stolen and written in a local array, which is then sent to C&C:

```
private void writeContact(String paramString1, String paramString2)
{
  ArrayList localArrayList = new ArrayList();
  localArrayList.add(ContentProviderOperation.newInsert(ContactsContract.RawContacts.CONTENT_URI).withValue("account_type", null).with
  localArrayList.add(ContentProviderOperation.newInsert(ContactsContract.Data.CONTENT_URI).withValueBackReference("raw_contact_id", 0).
  localArrayList.add(ContentProviderOperation.newInsert(ContactsContract.Data.CONTENT_URI).withValueBackReference("raw_contact_id", 0).
  try
  {
    MainActivity.this.getApplicationContext().getContentResolver().applyBatch("com.android.contacts", localArrayList);
    return;
  }
  catch (RemoteException paramString1)
  {
    paramString1.printStackTrace();
    return;
```

Figure 7: Stealing and writing contacts

Uninstalling apps

Uninstalling apps is another function favored by developers of Android spyware and malware. They tend to target any antivirus protections on the device and uninstall them, which increases the possibility of their malware persisting on the device. Following screenshot shows this functionality in action:

```
private void Uninst()
{
  try
  {
    Intent localIntent = new Intent("android.intent.action.DELETE");
    localIntent.setData(Uri.parse("package:" + getPackageName()));
    startActivity(localIntent);
    return;
  }
  catch (Exception localException)
  {
    localException.printStackTrace();
  }
}
```

Figure 8: Uninstalling functionality

Other functions

In addition to the functionalities we've described, the SpyNote RAT was exhibiting many other behaviors that make it more robust than most off-the-shelf malware.

SpyNote RAT was designed to function only over Wi-Fi, which is the preferable mode for Android malware to send files to C&C.

The screenshot below shows SpyNote RAT scanning for Wi-Fi and enabling it if a known channel is found:

Figure 9 : Scanning Wi-Fi

Additional features

- SpyNote RAT could click photos using the device's camera, based on commands from C&C.

- There were two interesting sub-classes found inside Main Activity: Receiver and Sender. Receiver was involved in receiving commands from the Server and the main functionality of Sender was to send all the data collected to the C&C over Wi-Fi.

- SpyNote RAT was also collecting the device's location to identify the exact location of the victim.

SpyNote RAT builder

The SpyNote Remote Access Trojan (RAT) builder is gaining popularity in the hacking community, so we decided to study its pervasiveness. What we found were several other fake apps developed using the SpyNote builder, which should come as a warning to Android users. Some of the targeted apps were:

- Whatsapp
- YouTube Video Downloader
- Google Update
- Instagram
- Hack Wifi
- AirDroid

- WifiHacker
- Facebook
- Photoshop
- SkyTV
- Hotstar
- Trump Dash
- PokemonGo

With many more to come.

Furthermore, we found that in just the first two weeks of 2017, there have been more than 120 such spyware variants already built using the same SpyNote Trojan builder as SpyNote RAT and roaming in the wild. A complete list of sample hashes is available here.

Conclusion

The days when one needed in-depth coding knowledge to develop malware are long gone. Nowadays, script kiddies can build a piece of malware that can create real havoc. Moreover, there are many toolkits like the SpyNote Trojan builder that enable users to build malware with ease and few clicks.

In particular, avoid side-loading apps from third-party app stores and avoid the temptation to play games that are not yet available on Android. Yes, we are talking about SuperMarioRun, which was recently launched by Nintendo only for iOS users. Recent blogs by the Zscaler research team explain how some variants of Android malware are exploiting the popularity of this game and tricking Android users into downloading a fake version. (Have a look here and here.)

You should also avoid the temptation to play games from sources other than legitimate app stores; such games are not safe and may bring harm to your reputation and your bank account.

Zscaler users are protected from such attacks with multiple levels of security.
