ANDROIDOS_ANSERVER.A - Threat Encyclopedia | Trend Micro (US)

By Analysis by: Karl Dominguez

Archived: 2026-04-05 14:48:23 UTC

This is the first known Android malware that reads blog posts and interprets these as commands. It can also download and install additional applications, therefore further compromising the affected device.

To get a one-glance comprehensive view of the behavior of this Backdoor, refer to the Threat Diagram shown below.

This malware gathers specific information from the infected device.

It connects to a malicious URL to send the gathered information and get an XML configuration file.

This backdoor may be unknowingly downloaded by a user while visiting malicious websites. It may be manually installed by a user.

Arrival Details

This backdoor may be unknowingly downloaded by a user while visiting malicious websites.

It may be manually installed by a user.

NOTES:

This malware request the following permissions which it could use to perform malicious routines:

- Access network settings
- Access the Internet
- Control the vibrator
- Disable Keylock
- Make a Call
- Read low-level log files
- Read, and write contacts
- Restart applications
- Wake the device
- Write, read, receive, and send SMS

It gathers the following device information:

- Build version
- IMEI
- IMSI
- Manufacturer
- Model
- OS version
- Package name of legitimate application
- SDK version

It connects to the following URL to send the gathered information and retrieves an XML configuration file:

- http://b4.{BLOCKED}r.co.cc:8080/jk.action={information}

The configuration file contains settings of the malware, the package name to be downloaded, and download URL.

As of this writing the package that is installed is *"com.sec.android.touchScreen.server"* and downloaded from the blog post in *http://blog.{BLOCKED}.com.cn/s/blog_8440ab780100t0nf.html*.

The blog post contains encrypted messages that the malware interprets as its commands. It can also download other malicious applications from this blog post.

NOTES:

Trend Micro Mobile Security Solution

Trend Micro Mobile Security Personal Edition protects Android smartphones and tablets from malicious and Trojanized applications. The *App Scanner* is free and detects malicious and Trojanized apps as they are downloaded, while *SmartSurfing* blocks malicious websites using your device's Android browser.

Download and install the Trend Micro Mobile Security App via the Android Market.

Remove unwanted apps on your Android mobile device

To remove unwanted apps on your mobile device:

1. Go to Settings > Applications > Manage Applications.
2. Locate the app to be removed.
3. Scroll and highlight the app to be removed, then choose *Uninstall*.

Did this description help? Tell us how we did.
