

## ANDROID MALWARE ACTS AS AN SMS RELAY

Just the Tip of the Iceberg for *Android* Malware

*Android's popularity and the Android Market's "open" nature are causing mobile devices running on the mobile OS to be targeted by several noteworthy malware. In this article, we will look at the different Android malware we have recently seen, particularly those that steal information from users and that monitor mobile activities.*

### MALICIOUS ANDROID APP ACTS AS AN SMS RELAY



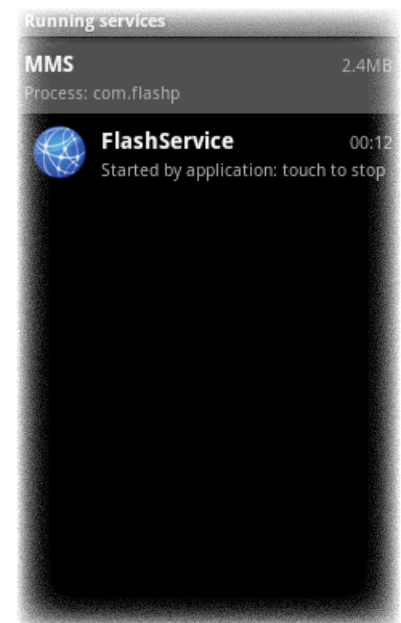
What made ANDROIDOS\_CRUSEWIN.A notable was the fact that it was not injected into legitimate *Android* apps to spread unlike most of the malware we have discovered so far.

Trend Micro researchers came across an *Android* malware that was later on found to have the capability to act as a **short message service (SMS) relay**. Detected as **ANDROIDOS\_CRUSEWIN.A**, the malware uses an infected mobile device as an agent to send and receive malicious text messages. What made this notable was the fact that it was not injected into legitimate *Android* apps to spread unlike most of the other malware we have discovered so far.

Upon execution, ANDROIDOS\_CRUSEWIN.A installs *FlashService* in infected devices. This service has two receivers—*FlashReceiver* and *SMSReceiver*—that run once triggered such as when a device receives a text message. When this occurs, all of the functions that are supposed to run when a certain event occurs do so.

*FlashService* runs every time an infected device boots up or each time it receives a text message. If the first instance occurs, *FlashReceiver* runs then starts *FlashService*. This allows the device to communicate with a remote server and to download its .XML configuration file. If the second instance happens, *SMSReceiver* checks if the text message's sender is indicated in the configuration file it downloaded. If so, it sends the text message to other users then monitors related replies. The content of these messages' SMS body is then replicated and sent to a remote server. To cover its tracks, it deletes the related text messages it sends and receives.

Cybercriminals can take advantage of *FlashService's* malicious routines to abuse premium services, to forward text messages to others without the affected users' knowledge, or to use infected devices as proxies. Despite the dangers this app poses, however, it can very well be just the tip of the iceberg as far as *Android* malware are concerned.



**Figure 1.** *FlashService* using the multimedia message service (MMS) icon



**ANDROIDOS\_CRUSEWIN.A** performed several malicious routines, including downloading a configuration file from a malicious site, sending text messages without the affected users' knowledge, and monitoring the text messages affected users sent and received.

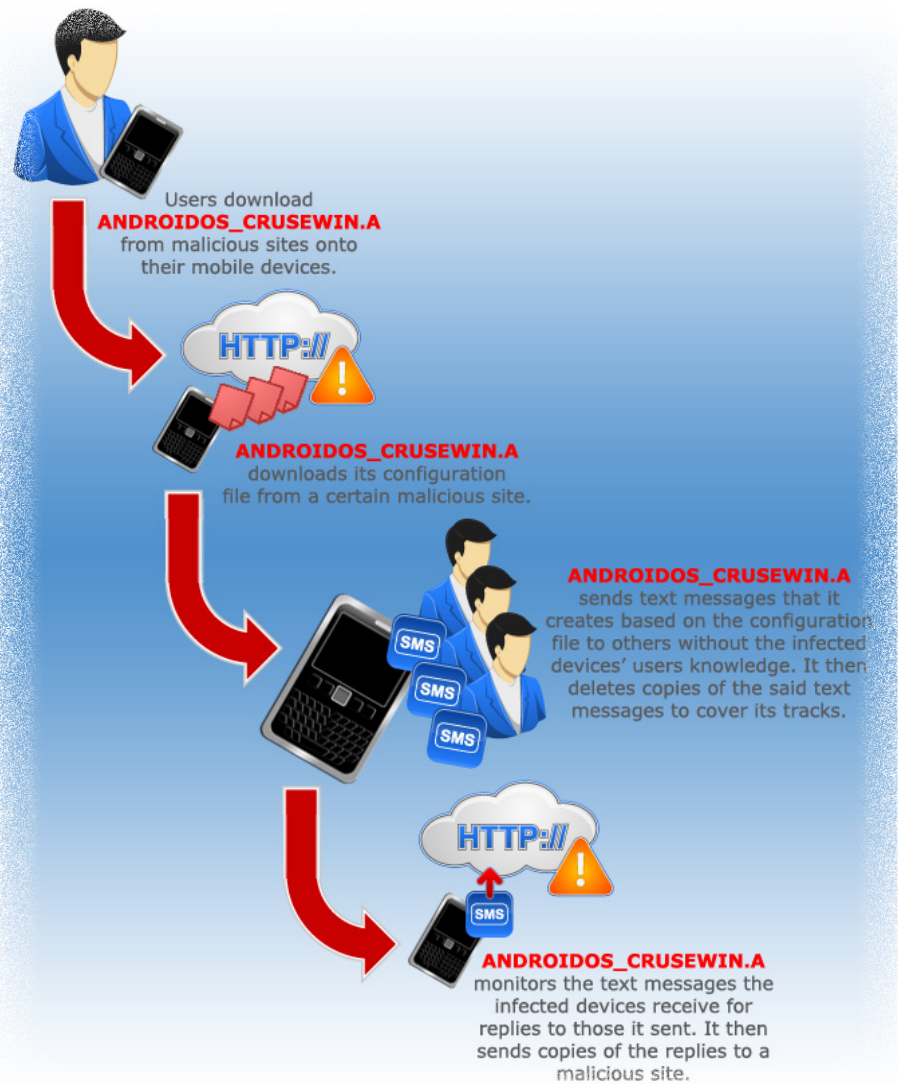


Figure 2. ANDROIDOS\_CRUSEWIN.A's infection diagram

## SPOTLIGHTING *ANDROID* MALWARE IN THE WILD

In the past few months, TrendLabs<sup>SM</sup> engineers have come across several *Android* malware, some of which monitored the activities of users of infected mobile devices and stole and sent the data these steal to remote users via HTTP POST. Certain malware even went as far as stealing device-related information or had the capability to root infected devices.

The following sections discuss some of the *Android* malware types we have seen in the past few months categorized based on their routines and on their possible payloads.



### Mobile Device Data Stealers

Data stealers are probably the most common *Android* malware today. These usually acquire various kinds of information like OS version, product ID, International Mobile Equipment Identity (IMEI) number, and International Mobile Subscriber Identity (IMSI) number from infected devices that may be used for future attacks. Stolen data is then encrypted and sent via HTTP POST.

Some of the most noteworthy information stealers targeting *Android*-based mobile devices include legitimate apps that have been injected with *DroidDreamLight*, aka *ANDROIDOS\_DORDRAE.L*. This malware accesses certain URLs to upload the data it steals for possible use in future attacks.

We have yet to determine what the real motivation behind information theft is, as Trend Micro researchers have yet to see stolen data sold in underground markets. Trend Micro senior threat researcher Joey Costoya believes cybercriminals may still be checking out what kinds of information they can get from mobile devices.

### Rooting-Capable Malware

Rooting-capable *Android* malware infect mobile devices in order to gain so-called root privileges, which give malicious remote users access to files and the devices' flash memory. Rooting helps malware drop copies of themselves onto devices or onto their flash memory so they can't be detected and consequently deleted by antivirus products. This leaves infected devices more open to threats that can have even more damaging effects.

A Trojanized app, aka *ANDROIDOS\_GONFU.A*, for instance, was able to root a device by installing a malicious package called *LEGACY*. This allowed the malware to stay in infected devices even if the apps that dropped it have been removed and rendered manual app removal ineffective. The malware also starts *SearchService*, which is responsible for executing all of its backdoor routines. Just like other *Android* malware, it steals information from infected devices, too.

### Premium Service Abusers

*Android* malware that abuse premium services are known for sending text messages to predetermined premium numbers. These can also sign affected users up for costly services that they may not even be remotely interested in. Affected users then end up being charged huge fees for useless stuff, causing them grief.



We at Trend Micro categorized the *Android* malware we have seen so far into at least four types—mobile device data stealers, rooting-capable malware, premium service abusers, and mobile device spies.

One of the more recent examples of this malware is ANDROIDOS\_ADSMS.SMA, which targeted China Mobile users and arrived via a link that spread via text messages. Its routines include accessing specific URLs to download its configuration file, which contains preset premium numbers like China Mobile's service number, 10086. It then monitors infected devices for messages originating from these numbers and prevents affected users from seeing them.

### Mobile Device Spies

Some *Android* malware secretly monitor varied kinds of information stored on infected devices, including affected users' Global Positioning System (GPS) location, saved text and email messages, and call logs. Like data stealers, these also send stolen data to specific URLs via HTTP POST. Unlike data stealers, however, these focus more on obtaining more personal data.

One particular mobile device spy, for instance, ANDROIDOS\_FSPY.A, gives malicious users the capability to remotely listen in to affected users' personal calls and to gain control of their devices via the simple act of sending a text message.

A more recent case involving such an *Android* mobile device spy is GoldDream, aka ANDROIDOS\_SPYGOLD.A. This malware Trojanized the legitimate app, *Fast Racing*, which allowed it to monitor and to copy the content of affected users' text messages as well as to record calls made and received via infected devices. It also communicates with a command-and-control (C&C) server to send and receive commands from remote users.

## ANDROID MALWARE CONTINUE TO SHAPE-SHIFT

Analyses of previously discovered *Android* malware made us realize that some use various techniques at once. In essence, a mobile spy can also be a data stealer; a premium service abuser can also be either a data stealer or a mobile spy. Affected users are then subjected to several payloads that may cost them more than just money; they may lose their personal information or, worse, their identities.

The threats plaguing *Android*-based devices, however, do not end with those mentioned in this article. The mobile OS's popularity and the *Android Market's* open nature will continue to entice cybercriminals to milk the platform. In fact, Trend Micro senior threat researcher Ryan Flores believes that the number of *Android* malware increased by 800 percent from February to May of this year alone.



The number of *Android* malware increased by 800 percent from February to May of this year alone.

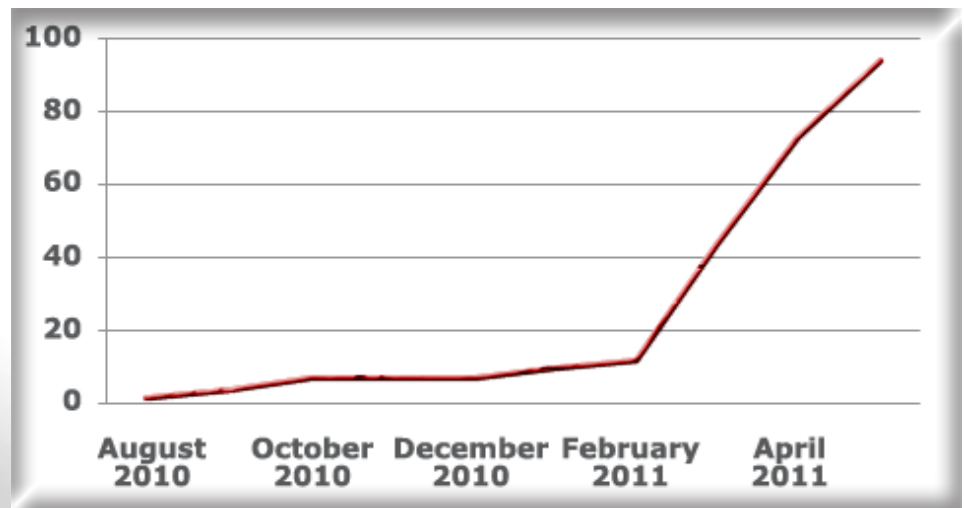


Figure 3. *Android* malware volume trend from August 2010–May 2011



According to a Nielsen report, 38 percent of the total number of consumers in the United States have smartphones. In the same study, the research firm noted that 55 percent of the total number of users who bought new mobile phones chose smartphones over feature phones.

Google estimates that there are currently 100 million active *Android*-based mobile devices, which is expected to continue increasing at an estimated 400,000 more devices per day.

*Android*'s larger market share compared with other mobile OSs may be due to its more open nature. Note, however, that this seeming advantage can also very well be a disadvantage in that it can bring about more security issues. In fact, Trend Micro threat analyst Mark Balanza believes that *Android*-based device users are likely to encounter more and more malware posing as legitimate apps on both the *Android Market* and in third-party app stores. Unlike other OS-specific app stores that screen every app before this can be uploaded and offered to users, virtually anyone, including cybercriminals, can easily create malicious apps and upload these to the *Android Market*. In fact, this only requires them to register as developers and to pay a very small fee. Those who cannot develop apps on their own can also just as easily download, modify or Trojanize, and reupload any legitimate app to the *Android Market* in order to victimize unknowing users.

Third-party app stores pose another problem. *Android*-based device users are not restricted from going to third-party app stores for their app needs. Though this does give them more choices and is probably one of the selling points of *Android*-based devices, this same lack of constraint is also putting them at greater risk.

As has often been said, cybercriminals flock to where the money is. As such, the more popular a platform is, the more they will target it. Popularity does come at a price, after all.



As has often been said, cybercriminals flock to where the money is. As such, the more popular a platform is, the more they will target it.

### CONSCIENTIOUS MOBILE PHONE USE CAN PREVENT DEVICE INFECTION

Though it is hard to ensure the legitimacy of the apps you download onto your *Android*-based mobile devices, there are still ways to mitigate the threats Trojanized apps pose. Take a look at just some of the many ways by which you can keep your mobile devices, your personal data, and even your identity safe from harm:

- Maximize your mobile device's built-in security features. Configure its security and location settings via the *Location & security* option found under *Settings*.
- Consider blocking access to third-party app stores and only download apps from the *Android Market*. Though this does not guarantee that the apps you will download are totally nonmalicious, it still minimizes the probability of downloading Trojanized apps.
- Be very wary of the permissions you give to apps. Trojanized apps typically seek access to more information than these actually require.

For more details on how you can protect yourself from the threats Android malware pose, take a look at our e-book, “[5 Simple Steps to Protect Your Android-Based Smartphones](#).” For added measure, installing an app like [Trend Micro™ Mobile Security for Android™](#) is also a good idea. Solutions like this can act as your safety net in case wily cybercriminals trick you into doing something you normally would not do.

## REFERENCES

- Dave Lee. (May 9, 2011). *BBC Mobile*. “Is ‘Open’ Killing the Android?” <http://www.bbc.co.uk/news/uk-13284156> (Retrieved August 2011).
- Google Inc. (May 10, 2011). *The Official Google Blog*. “Android: Momentum, Mobile, and More at Google I/O.” <http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html> (Retrieved August 2011).
- Kervin Alintanahin. (July 7, 2011). *TrendLabs Malware Blog*. “New Android Malware on the Road: GoldDream ‘Catcher.’” <http://blog.trendmicro.com/new-android-malware-on-the-road-golddream-catcher/> (Retrieved August 2011).
- Mark Balanza. (May 12, 2011). *TrendLabs Malware Blog*. “Android Malware Targets China Mobile Subscribers.” <http://blog.trendmicro.com/android-malware-targets-china-mobile-subscribers/> (Retrieved August 2011).
- Mark Balanza. (June 1, 2011). *TrendLabs Malware Blog*. “Analysis of DroidDreamLight Android Malware.” <http://blog.trendmicro.com/analysis-of-droiddreamlight-android-malware/> (Retrieved August 2011).
- Mark Balanza. (June 24, 2011). *TrendLabs Malware Blog*. “Android Malware Acts as an SMS Relay.” <http://blog.trendmicro.com/android-malware-acts-as-an-sms-relay/> (Retrieved August 2011).
- The Nielsen Company. (June 30, 2011). *nielsenwire*. “In U.S., Smartphones Now Majority of New Cellphone Purchases.” [http://blog.nielsen.com/nielsenwire/online\\_mobile/in-us-smartphones-now-majority-of-new-cellphone-purchases/](http://blog.nielsen.com/nielsenwire/online_mobile/in-us-smartphones-now-majority-of-new-cellphone-purchases/) (Retrieved August 2011).
- Trend Micro, Incorporated. (June 2011). “5 Simple Steps to Secure Your Android-Based Smartphones.” <http://about-threats.trendmicro.com/ebooks/5-simple-steps-to-secure-your-android-based-smartphones/#/1/> (Retrieved August 2011).
- Trend Micro, Incorporated. (March 2011). *Threat Encyclopedia*. “ANDROIDOS\_FPSY.A.” [http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS\\_FSPY.A](http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_FSPY.A) (Retrieved August 2011).
- Trend Micro, Incorporated. (May 2011). *Threat Encyclopedia*. “ANDROIDOS\_ADSMS.A.” [http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS\\_ADSMS.A](http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_ADSMS.A) (Retrieved August 2011).
- Trend Micro, Incorporated. (June 2011). *Threat Encyclopedia*. “ANDROIDOS\_CRUSEWIN.A.” [http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS\\_CRUSEWIN.A](http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_CRUSEWIN.A) (Retrieved August 2011).
- Trend Micro, Incorporated. (June 2011). *Threat Encyclopedia*. “ANDROIDOS\_DORDRAE.L.” [http://about-threats.trendmicro.com/malware.aspx?language=us&name=ANDROIDOS\\_DORDRAE.L](http://about-threats.trendmicro.com/malware.aspx?language=us&name=ANDROIDOS_DORDRAE.L) (Retrieved August 2011).
- Trend Micro, Incorporated. (June 2011). *Threat Encyclopedia*. “ANDROIDOS\_GONFU.A.” [http://about-threats.trendmicro.com/malware.aspx?language=us&name=ANDROIDOS\\_GONFU.A](http://about-threats.trendmicro.com/malware.aspx?language=us&name=ANDROIDOS_GONFU.A) (Retrieved August 2011).
- Trend Micro, Incorporated. (July 2011). *Threat Encyclopedia*. “ANDROIDOS\_SPYGOLD.A.” [http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS\\_SPYGOLD.A](http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_SPYGOLD.A) (Retrieved August 2011).
- Wikimedia Foundation, Inc. (July 20, 2011). *Wikipedia*. “Rooting (Android OS).” [http://en.wikipedia.org/wiki/Rooting\\_\(Android\\_OS\)](http://en.wikipedia.org/wiki/Rooting_(Android_OS)) (Retrieved August 2011).