August 20, 2012, 9:15AM

SMSZombie Malware Infecting Android Devices, Stealing Money (/en_us/blogs/smszombie-malware-infecting-android-devices-stealing-money-082012)

by Dennis Fisher (/author/Dennis Fisher)

(http://threatpost.com/en_us/blogs/smszombie-malware-infecting-android-devices-stealing-money-082012) A nasty new piece of malware that has the ability to steal money from users' via fraudulent SMS payments has shown up in a Chinese Android market and researchers say it's infected more than 500,000 victims. The SMSZombie malware is being hidden inside apps on the app market and once it's on a device it has the ability to prevent users from uninstalling it.

The SMSZombie malware targets Android devices and uses a flaw in the SMS payment system used by China Mobile to forward payments to the attacker without the user's knowledge. Researchers at TrustGo, a mobile security company, found that the malware is hiding inside of various apps on the GFan Android market in China and once users download an infected app, the SMSZombie malware attempts to gain administrator-level privileges on the device.

"The SMSZombie virus has been hidden in a variety of wallpaper apps and attracts users with provocative titles and pictures. When the user sets the app as the device's wallpaper, the app will request the user to install additional files associated with the virus. If the user agrees, the virus payload is delivered within a file called 'Android System Service'," the researchers at TrustGo (http://blog.trustgo.com/SMSZombie/) wrote in an analysis.

Editor's Pick

Zeus Comes to the BlackBerry (/en_us/blogs/zeus-comes-blackberry-080712)

Q&A: Adrian Stone of the BlackBerry Security Team (/en_us/blogs/qa-adrian-stone-

"Once installed, the virus then tries to obtain administrator privileges on the user's device. This step cannot be canceled by the user, as the 'Cancel' button only reloads the dialog box until the user eventually is forced to select 'Activate' to stop the dialog box. These privileges disable users' ability to delete the app, causing the device to return to the home screen even after choosing to uninstall the app."

Mobile malware (https://threatpost.com/en_us/blogs/zeus-comes-blackberry-080712) of

blackberry-security-team-073012)

New OpFake Android Malware Entices Users With Opera Mini Browser (/en_us/blogs/new-opfake-android-malware-entices-users-opera-mini-browser-072412)

Threatpost Newsletter Sign-up (/en_us/node/1690)

this kind is becoming increasingly more common as attackers focus on going after users on whatever device they use the most, and for many people these days, that means mobile phones.

SMSZombie is designed to steal money from users by sending SMS payments to the attackers. The malware has the ability to send payments without the user's knowledge and can send them at random intervals and for whatever amount the attacker chooses. SMSZombie includes a configuration file that the attacker can update remotely, as well.

"Using a configuration file that can be updated by the malware maker at anytime, the malware can intercept and forward a variety of SMS messages. Because these messages often include banking and financial information, users accounts can easily be hacked further," TrustGo said.

"It has been confirmed that this virus has been used to recharge online gaming accounts via the China Mobile SMS Payment system. Commonly, the victim's account is charged a relatively low amount to escape detection."

Commenting on this Article will be automatically closed on November 20, 2012.

Comments

Submitted by Independent (not verified) on Mon, 08/20/2012 - 6:13pm.

This is ANDROID! The NOT READY FOR PRIMETIME rape the users operating system from GOOGLE, the hackers dream OS!

The problem is Google... Haven't we all read the security breaches coming from Google in the past weeks? I'm one who triumps the razors edge of security software especially from KIS, but an OS this stacked against any possibility of securing anything on an Google Android in pretty near imposible. The "perfect" operating system designed to frustrate any user ability to prevent data theft of any kind! In my opinion, the greatest swindle of users world wide in our times.

It's not very hard to see easily what GOOGLE is all about... "ANDROID", the gateway to unlimited users data. IMHO

> **Submitted by Anonymous (not verified) on Mon, 08/20/2012 - 7:26pm.**
>
> Just another personal opinon. There are so many of these types in the world.

Submitted by Anonymous (not verified) on Tue, 08/21/2012 - 7:56am.

Another day and another FUD article from company that makes their money by selling anti virus software.

Post new comment

Your name:

Anonymous

E-mail:

The content of this field is kept private and will not be shown publicly.

Comment: *

(#)

(javascript::)

Path: p (javascript:;) (javasc

Save Preview