ZeuS-in-the-Mobile for Android

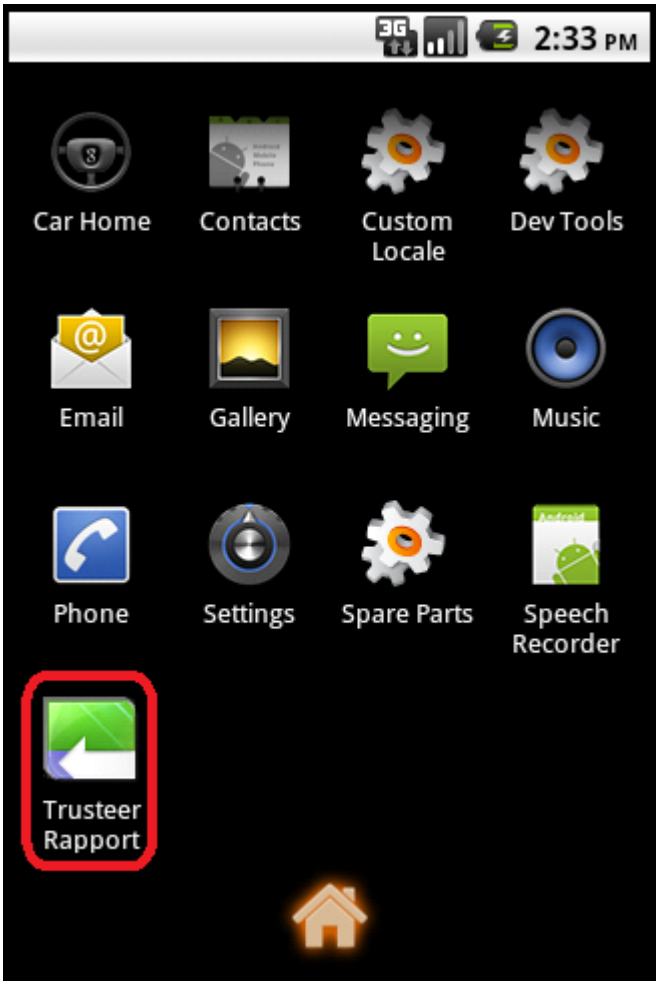
By Denis Maslennikov

Published: 2011-07-12 · Archived: 2026-04-05 14:21:23 UTC

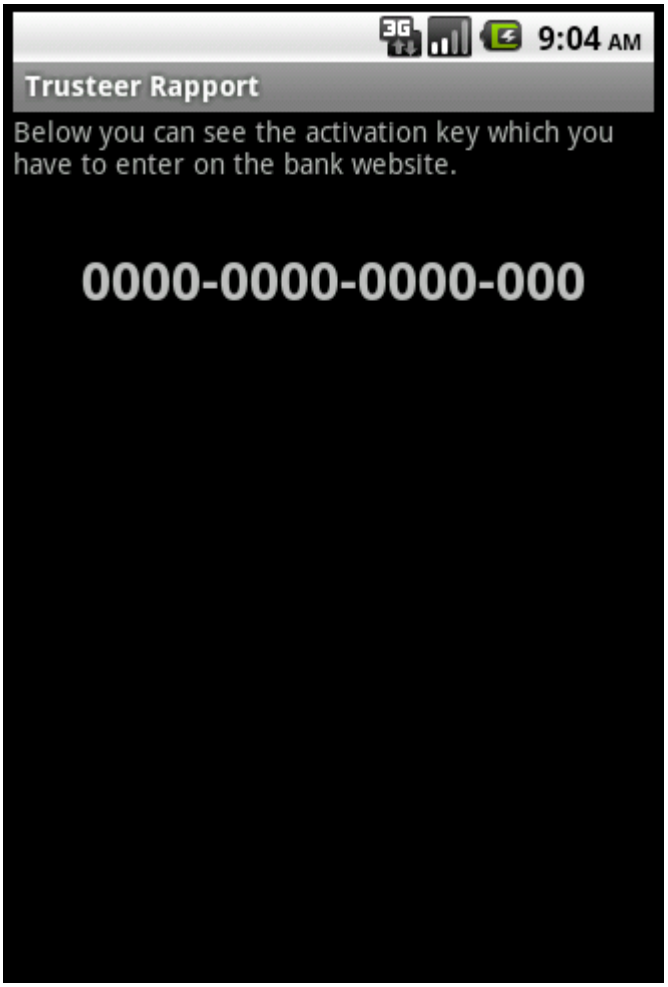
The first version of ZeuS-in-the-Mobile (ZitMo), malware which targets mTANs, was discovered in the end of September 2010. In that case it was targeting Symbian smartphones. Later on, ZitMo versions for Windows Mobile and Blackberry were found. It comes as no surprise that cybercriminals have created new and sophisticated pieces of mobile malware for Symbian and Windows Mobile; more surprising is that Blackberry devices were also targeted; and even more surprising is that until July 2011 there was no evidence of ZitMo for Android's existence. And now please 'welcome' ZeuS-in-the-Mobile for Android.

The first fact that must be mentioned is that ZitMo for Android differs from Symbian, Windows Mobile and Blackberry versions a lot. The functionality and logic of ZitMo for Symbian, Windows Mobile and Blackberry is the same: C&C cell phone number, SMS commands, and the ability to forward SMS messages from a particular number, as well as the ability to change C&C.

The functionality and logic of ZitMo for Android is far more primitive. The APK file itself has a 19k size. It passes itself off as a security tool from the 'Trusteer' company. If a user installs the malicious application then the following 'Trusteer Rapport' icon will appear in the main menu:



And that’s what going to be on the screen after clicking on the application’s link:

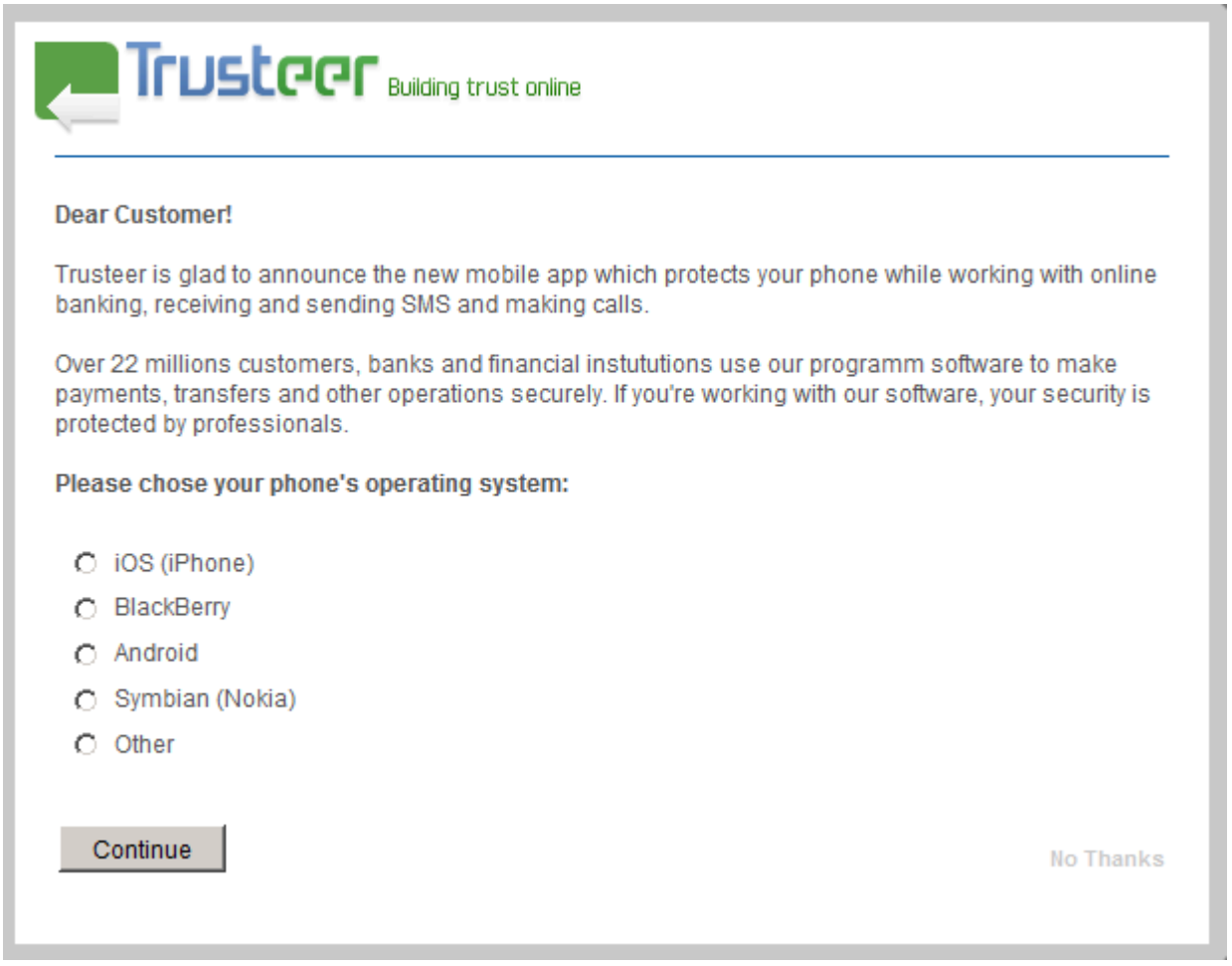


As I said previously, ZitMo for Android is very primitive. Its functionality consists only of the ability to upload all incoming SMS messages (with mTANs also) to a remote web server http://******rifty.com/security.jsp in the following format:

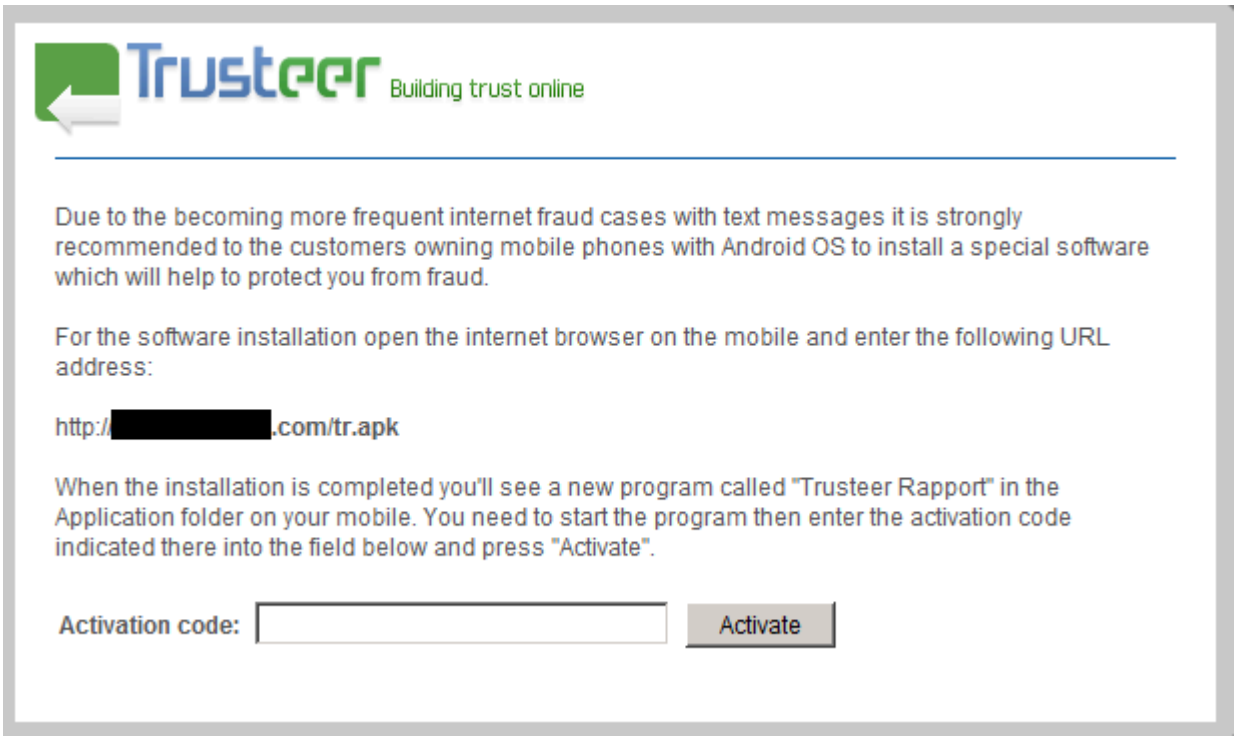
f0={SMS_sender_number}&b0={SMS_text}&pid={infected_device_ID}

The first attacks with ZeuS-in-the-Mobile for Android started probably in early June. But how does ZitMo for Android actually infect devices? Nothing has changed in this area.

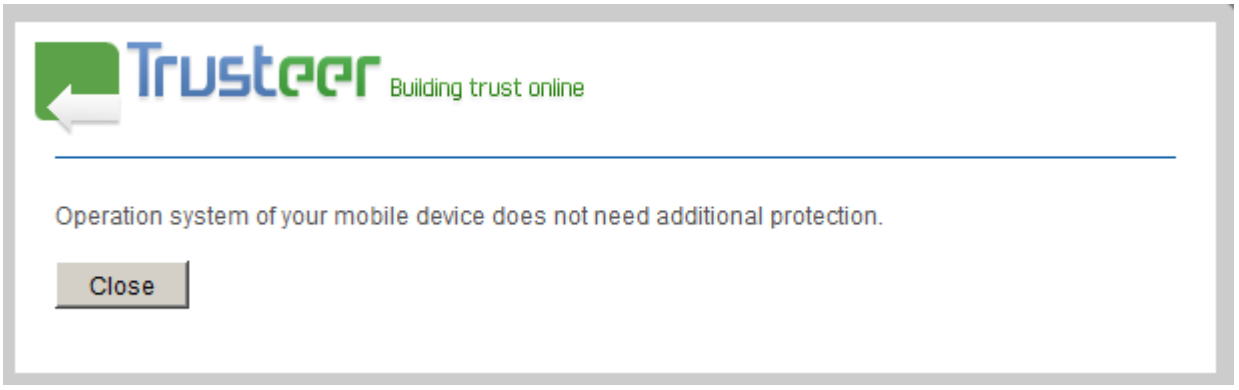
We found one of the *Win32 ZeuS configuration files* which contains following ‘suggestion’:



If the user chooses ‘Android’ and clicks ‘Continue’ he will be redirected to the following page where he is asked to download the ‘security tool’:



If the user chooses any other option (‘iOS (iPhone)’, ‘BlackBerry’, ‘Symbian (Nokia)’ or ‘Other’) they will get… nothing!



In other words this particular attack was targeting only Android devices.

But besides the site http://**********.com/tr.apk cybercriminals have also uploaded ZitMo for Android to the Android Market. The application has already been removed but, as it was in previous cases of malware in the Android Market, there are mirroring websites which save the information about all the programs approved by Google. In the case of ZitMo for Android, the application was uploaded with the ‘TrustMobile’ name probably on the 18th of June.

Security software from Trusteer company

Tweet 2 Мне нравится Buzz 0

TrustMobile was developed for Android by **Gameshastra Publish**

Package name : **com.systemsecurity6.gms**

System permissions : 3 Click here to show/hide list

I am the developer of this Application !

EMAIL

Screenshot(s) available for TrustMobile

Submit a screenshot | Submit a Youtube video

Discussion(s) about TrustMobile in our forum

No discussion found

Be the first to start a discussion about TrustMobile in our forums !

Comments and Ratings for TrustMobile

Price

Free

Version

1.0

Downloads

< 50

Size

19.4 KB

Category

Tools

Website

Official WebSite

Last update

594h ago

Ask for Update

So, now we have ZitMo targeting 4 platforms: Symbian, Windows Mobile, Blackberry and Android. As we wrote in our previous blog about ZeuS-in-the-Mobile ‘cybercriminals are still very far away from stopping their activities’.

Source: https://securelist.com/zeus-in-the-mobile-for-android/29258/