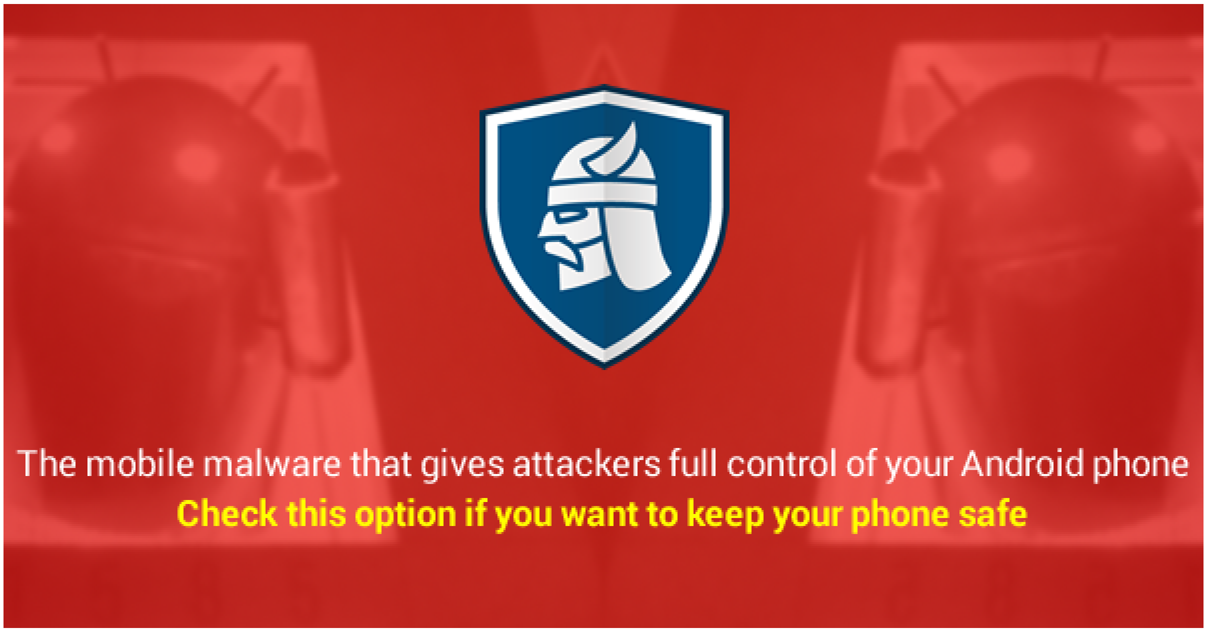
Security Alert: Mazar BOT – the Android Malware That Can Erase Your Phone

heimdalsecurity.com/blog/security-alert-mazar-bot-active-attacks-android-malware/

Andra Zaharia

February 12, 2016


The mobile malware that gives attackers full control of your Android phone
Check this option if you want to keep your phone safe

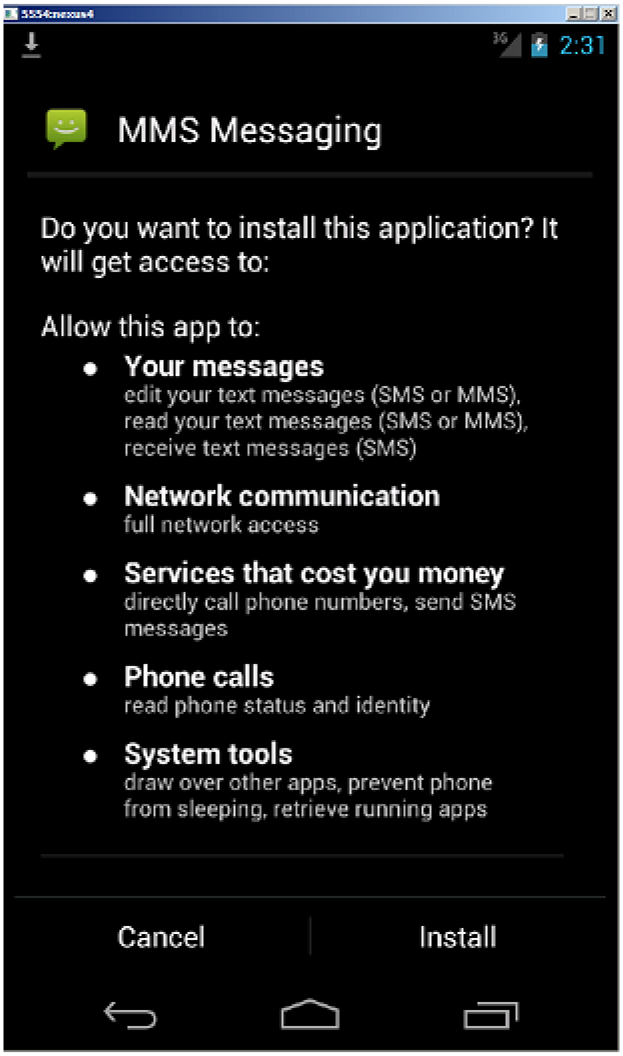
Our team at Heimdal Security has recently analyzed a text message sent to random mobile numbers. The Geographical extent is so far unknown, so please exercise caution. The SMS / MMS in question arrives with the following contents (sanitized by Heimdal Security):

> You have received a multimedia message from +[country code] [sender number] Follow the link http: //www.mmsforyou [.] Net / mms.apk to view the message.

If the APK (which is a program file for Android) is run on an Android-powered smartphone, then it will **gain administrator rights** on the victim's device. This will allow the attackers to:

- SEND_SMS
- RECEIVE_BOOT_COMPLETED
- INTERNET
- SYSTEM_ALERT_WINDOW
- WRITE_SMS
- ACCESS_NETWORK_STATE
- WAKE_LOCK
- GET_TASKS
- CALL_PHONE
- RECEIVE_SMS
- READ_PHONE_STATE

- READ_SMS
- ERASE_PHONE



MMS Messaging

Do you want to install this application? It will get access to:

Allow this app to:

- **Your messages**
  edit your text messages (SMS or MMS), read your text messages (SMS or MMS), receive text messages (SMS)
- **Network communication**
  full network access
- **Services that cost you money**
  directly call phone numbers, send SMS messages
- **Phone calls**
  read phone status and identity
- **System tools**
  draw over other apps, prevent phone from sleeping, retrieve running apps

Our team has identified the malicious APK to be the Mazar Android BOT, a threat also that Recorded Future spotted in November 2015. **The malicious packet (APK) retrieves TOR** and installs it on the victim's phone via the following harmless URLs: https: //f-droid.org/repository/browse/?fdid=org.torproject.android https: //play.google.com/store/apps/details?id=org.torproject.android In the next phase of the attack, the infection will **unpack and run the TOR application**, which will then be used to **connect to the following server**: http: // pc35hiptpcwqezgs [.] Onion. After that, an automated SMS will be sent to the number 9876543210 (+98 is the country code for Iran) with the text message: "Thank you". The catch is that this SMS also includes **the device's location data.**
Mazar BOT – the Android #malware that can erase your phone is on the loose:
Click To Tweet

Insidious mobile malware with crippling options

This specific mobile malware opens the doors to all kinds of malicious consequences for the victim. **Attackers can:**

- Open a backdoor into Android smartphones, to **monitor and control** them as they please;
- **Send SMS messages to premium channel numbers**, seriously increasing the victim's phone bill;
- **Read SMS messages**, which means they can also **read authentication codes sent as part of two-factor authentication mechanisms**, used also by online banking apps and ecommerce websites;
- Use their full access to Android phones to basically **manipulate the device to do whatever they want**.

And it gets worse.

Polipo proxy and Man-in-the-Middle Attack

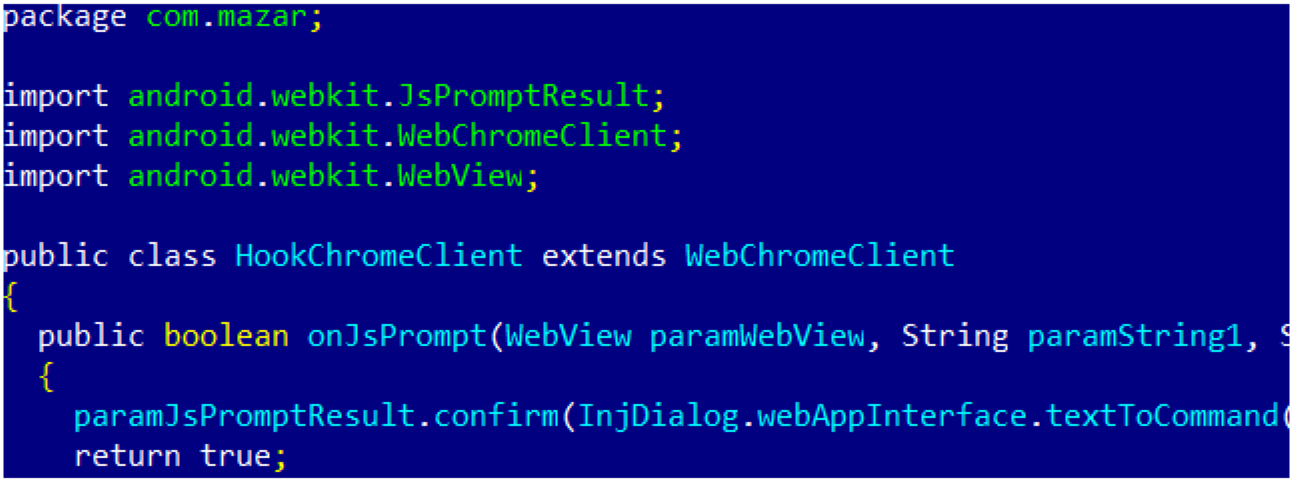
The attackers behind Mazar BOT also implemented the "Polipo proxy", which gives them additional access to even more Android functionalities.

> Polipoid brings the Polipo HTTP proxy to Android. Polipo lets you do useful things such as cache web pages for offline access and should generally speed up browsing a little.

Source: Github Through this proxy, cyber criminals can change the traffic and interpose themselves between the victim's phone and a web-based service. This effectively becomes **a Man-in-the-Middle attack**. **Here's how it happens:** Data is copied to your phone as mp3 files: 122.933 polipo.mp3 1,885,100 tor.mp3 Then, the proxy is configured as you can see below: 174.398 debiancacerts.bks 574 torpolipo.conf 879 torpolipo_old.conf 212 torrc 276 torrc_old For those technically inclined, the configuration of the TOR proxy will seem quite straightforward: proxy address = "127.0.0.1" proxy port = 8118 allowedClients = 127.0.0.1 allowedPorts = 1-65535 proxy name = "127.0.0.1" cacheIsShared = false socksParentProxy = "127.0.0.1:9050" socksProxyType = socks5 diskCacheRoot = "" localDocumentRoot = "" disableLocalInterface = true disableConfiguration = true dnsUseGethostbyname = yes disableVia = true from, accept-language, x-pad link censor referer = maybe maxConnectionAge = 5m maxConnectionRequests = 120 serverMaxSlots = 8 server slots = 2 tunnelAllowedPorts = 1-65535 chunkHighMark = 11000000 object high mark = 128

An even higher degree of compromise: Chrome injects

As if it weren't enough that it **can stop calls and launch other aggressive commands** on the victim's phone, **Mazar BOT is also capable of injecting itself into Chrome**.



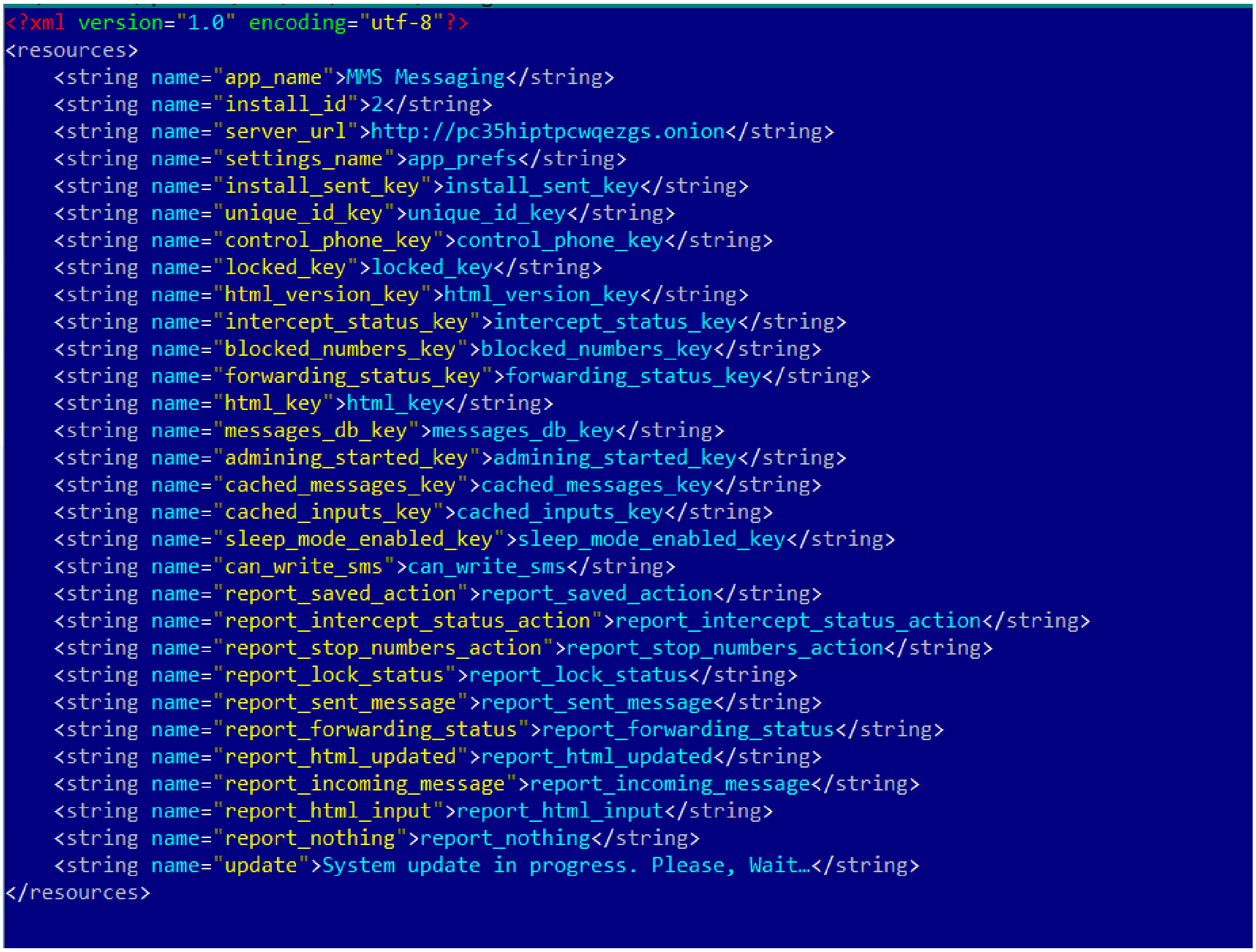
```
package com.mazar;

import android.webkit.JsPromptResult;
import android.webkit.WebChromeClient;
import android.webkit.WebView;

public class HookChromeClient extends WebChromeClient
{
  public boolean onJsPrompt(WebView paramWebView, String paramString1, S
  {
    paramJsPromptResult.confirm(InjDialog.webAppInterface.textToCommand(
    return true;
```

And there are **several other settings and commands that Mazar BOT can trigger**, as showcased below. These include:

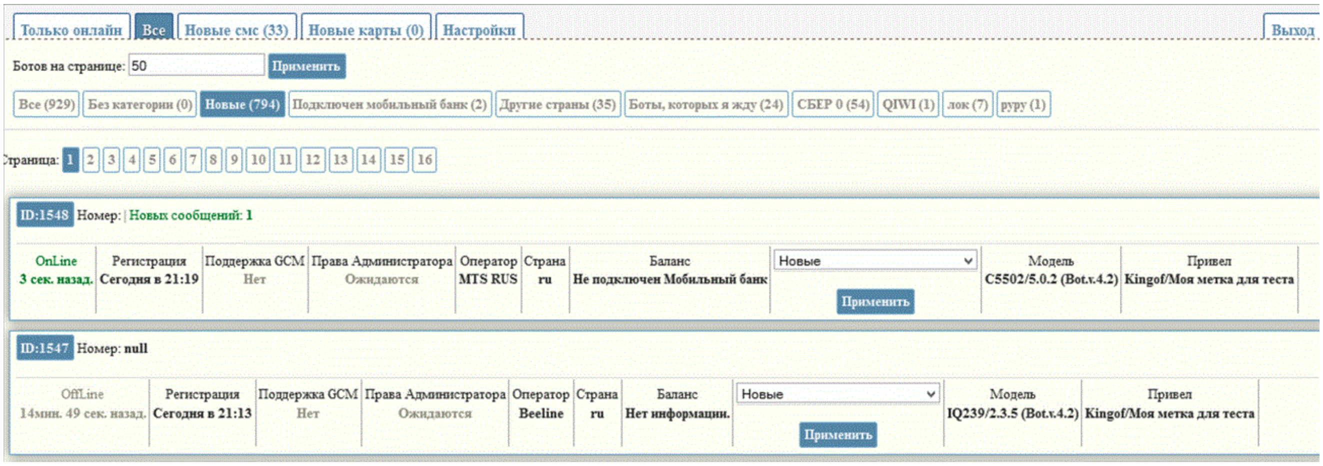
- Controlling the phone’s keys
- Enabling the sleep mode
- Save actions in the phone’s settings, etc.



```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">MMS Messaging</string>
    <string name="install_id">2</string>
    <string name="server_url">http://pc35hiptpcwqezgs.onion</string>
    <string name="settings_name">app_prefs</string>
    <string name="install_sent_key">install_sent_key</string>
    <string name="unique_id_key">unique_id_key</string>
    <string name="control_phone_key">control_phone_key</string>
    <string name="locked_key">locked_key</string>
    <string name="html_version_key">html_version_key</string>
    <string name="intercept_status_key">intercept_status_key</string>
    <string name="blocked_numbers_key">blocked_numbers_key</string>
    <string name="forwarding_status_key">forwarding_status_key</string>
    <string name="html_key">html_key</string>
    <string name="messages_db_key">messages_db_key</string>
    <string name="admining_started_key">admining_started_key</string>
    <string name="cached_messages_key">cached_messages_key</string>
    <string name="cached_inputs_key">cached_inputs_key</string>
    <string name="sleep_mode_enabled_key">sleep_mode_enabled_key</string>
    <string name="can_write_sms">can_write_sms</string>
    <string name="report_saved_action">report_saved_action</string>
    <string name="report_intercept_status_action">report_intercept_status_action</string>
    <string name="report_stop_numbers_action">report_stop_numbers_action</string>
    <string name="report_lock_status">report_lock_status</string>
    <string name="report_sent_message">report_sent_message</string>
    <string name="report_forwarding_status">report_forwarding_status</string>
    <string name="report_html_updated">report_html_updated</string>
    <string name="report_incoming_message">report_incoming_message</string>
    <string name="report_html_input">report_html_input</string>
    <string name="report_nothing">report_nothing</string>
    <string name="update">System update in progress. Please, Wait…</string>
</resources>
```

Mazar BOT won’t run on Russian Android smartphones

Our team was not surprised to observe that **the malware cannot be installed on smartphones running Android with the Russian language option**. Mazar BOT will check the phone to identify the victim’s country and this will stop the malicious APK if the targeted phone turns out to be owned by a Russian user: locale.getCountry () equalsIgnoreCase (“RU”)) Process.killProcess (Process.myPid ());



Ботов на странице: 50

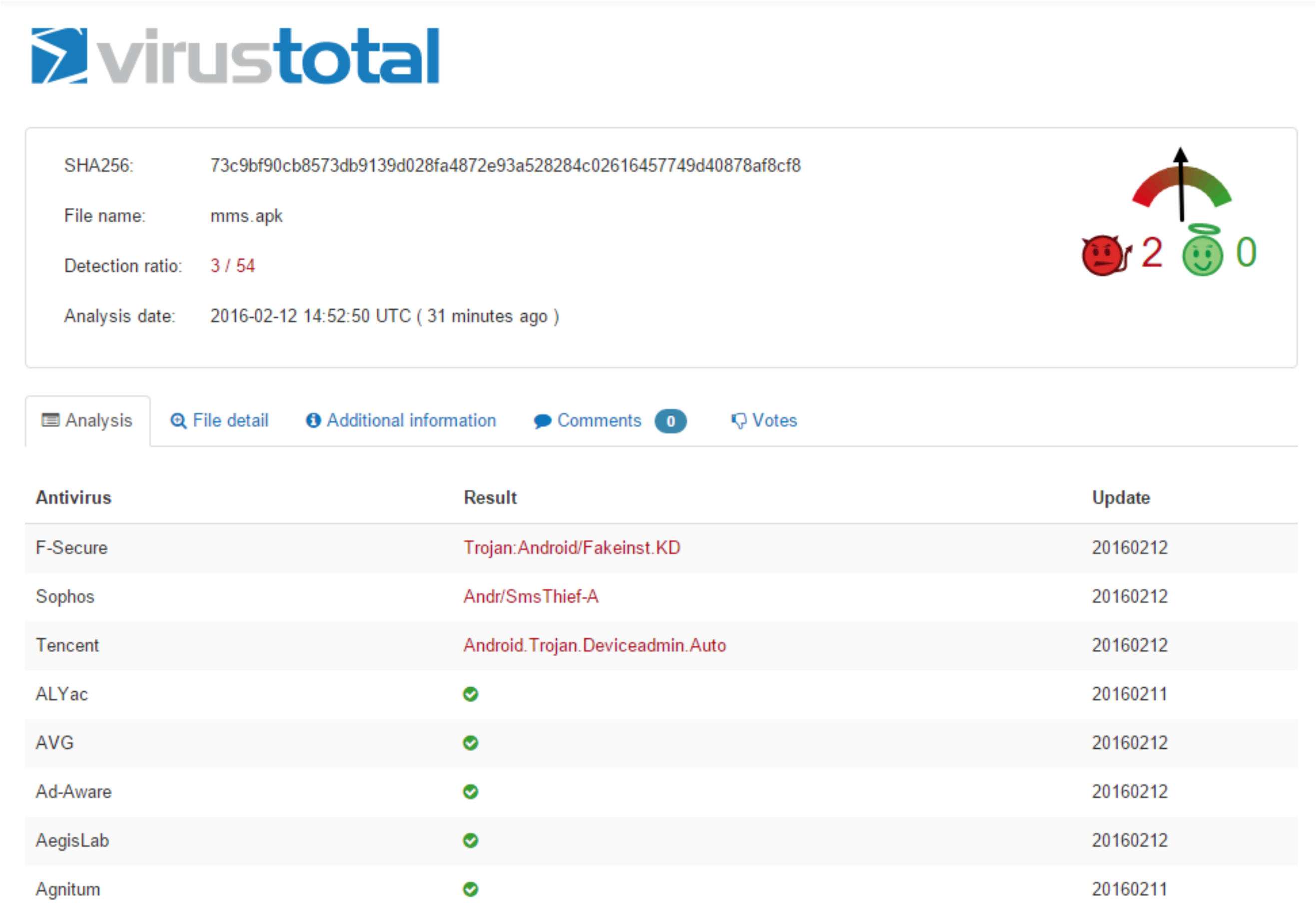
ID:1548 Номер: | Новых сообщений: 1

OnLine	Регистрация	Поддержка GCM	Права Администратора	Оператор	Страна	Баланс	Новые	Модель	Привел
3 сек. назад.	Сегодня в 21:19	Нет	Ожидаются	MTS RUS	ru	Не подключен Мобильный банк		C5502/5.0.2 (Bot.v.4.2)	Kingof/Моя метка для теста

ID:1547 Номер: null

OffLine	Регистрация	Поддержка GCM	Права Администратора	Оператор	Страна	Баланс	Новые	Модель	Привел
14мин. 49 сек. назад.	Сегодня в 21:13	Нет	Ожидаются	Beeline	ru	Нет информации.		IQ239/2.3.5 (Bot.v.4.2)	Kingof/Моя метка для теста

Until now, Mazar BOT has been advertised for sale on several websites on the Dark Web, but this is the first time we’ve seen this code be abused in active attacks. Attackers may be testing this new type of Android malware to see how they can improve their tactics and reach their final goals, which probably is making more money (as always). We can expect this malware to expand its reach, also because of its ability to remain covert by **using TOR to hide its communication**. As you may have anticipated, **antivirus detection of the malicious APK is very low: 3/54 on VirusTotal**.



SHA256: 73c9bf90cb8573db9139d028fa4872e93a528284c02616457749d40878af8cf8

File name: mms.apk

Detection ratio: 3 / 54

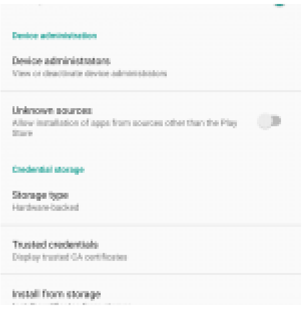
Analysis date: 2016-02-12 14:52:50 UTC (31 minutes ago)

Antivirus	Result	Update
F-Secure	Trojan:Android/Fakeinst.KD	20160212
Sophos	Andr/SmsThief-A	20160212
Tencent	Android.Trojan.Deviceadmin.Auto	20160212
ALYac	✓	20160211
AVG	✓	20160212
Ad-Aware	✓	20160212
AegisLab	✓	20160212
Agnitum	✓	20160211

Click here for the full infection rates at the time the campaign was analyzed.

How to protect yourself from Mazar BOT

There are a few things you can do to keep your phone safe from Mazar BOT, and we recommend you **take a moment now to verify and adjust these settings**. **1.** First of all, **NEVER click on links in SMS or MMS messages on your phone**. Android phones are notoriously vulnerable and current security product dedicated to this OS are not nearly as effective as they are on computers. **2. Go to Settings > Security and make sure this option is turned OFF**: „Unknown Sources – Allow installation of apps from sources other than the playstore."



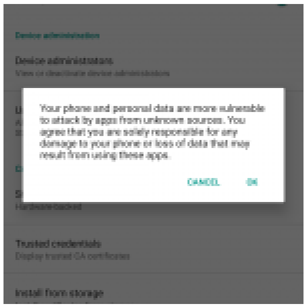
Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from sources other than the Play Store

Storage type
Hardware-backed

Trusted credentials
Display trusted CA certificates

Install from storage



Your phone and personal data are more vulnerable to attack by apps from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these apps.

3. Install a top antivirus for Android. It may not be enough to protect your phone, but it’s certainly good to have. You can find top-rated options in this article. **4. Do not connect to unknown and unsecured Wi-Fi hotspots**. There are plenty of dangers lurking out there, and following some common-sense steps to keep yourself safe from them is the best thing to do. Also, **keep your Wi-Fi turned OFF when you don’t use it**.

Follow these steps to protect your Android phone from the ruthless Mazar BOT #malware: Click To Tweet

5. Install a VPN on your smartphone and use constantly. It’s good for both your privacy and your security. **6. Maintain a cautious attitude at all times.** Android security has not kept up with the high adoption rate of smartphones running the OS, and users may have to wait a long time until better security solutions appear. Until then, a careful evaluation of what happens on your phone is a very good safeguard.

If you liked this post, you will enjoy our newsletter.

Receive new articles directly in your inbox