# Threatpost | The first stop for security news

- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - The Kaspersky Lab News Service

### Featured Posts

All

IoT' s Day of Reckoning on the…

Modern Defenders Share, Visualize and Succeed

- Podcasts

### Latest Podcasts

All

Threatpost News Wrap, February 5, 2016

Threatpost News Wrap, January 29, 2016

Jon Callas on Securing Our Private…

Threatpost News Wrap, January 22, 2016

Threatpost News Wrap, January 15, 2016

Threatpost News Wrap, January 8, 2016

### Recommended

The Kaspersky Lab Security News Service

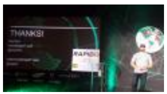
- Videos

### Latest Videos

All

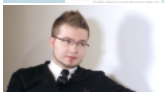
Vitaly Kamluk on the Adwind RAT

Kris McConkey on Hacker OpSec Failures


Trey Ford on Mapping the Internet…

Christofer Hoff on Mixed Martial Arts,…

Twitter Security and Privacy Settings You…


The Biggest Security Stories of 2013

## Recommended

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

- 🇬🇧
- 🇷🇺

Welcome > Blog Home>Malware > Mazar Bot Actively Targeting Android Devices

f 57 g+ 81 in 65 0 0

# Mazar Bot Actively Targeting Android Devices

Follow @mike_mimoso by Michael Mimoso February 15, 2016 , 8:00 am

Nearly three months after it was spotted for sale in a Russian hacker forum, the Mazar bot has been put to use in active attacks targeting Android devices.

Researchers at Heimdal Security said on Friday the bot is being sent to Android users via SMS and MMS messages and if the victim executes the APK, the bot roots the phone and gives the attacker extensive capabilities on the compromised device.

## Related Posts

Metel Bank Robbers Borrowing from APT Attacks

February 8, 2016 , 7:20 am

WordPress Infections Leading to TeslaCrypt Ransomware

February 5, 2016 , 7:00 am

Critical Wi-Fi Flaw Patched on Android

February 1, 2016 , 2:00 pm

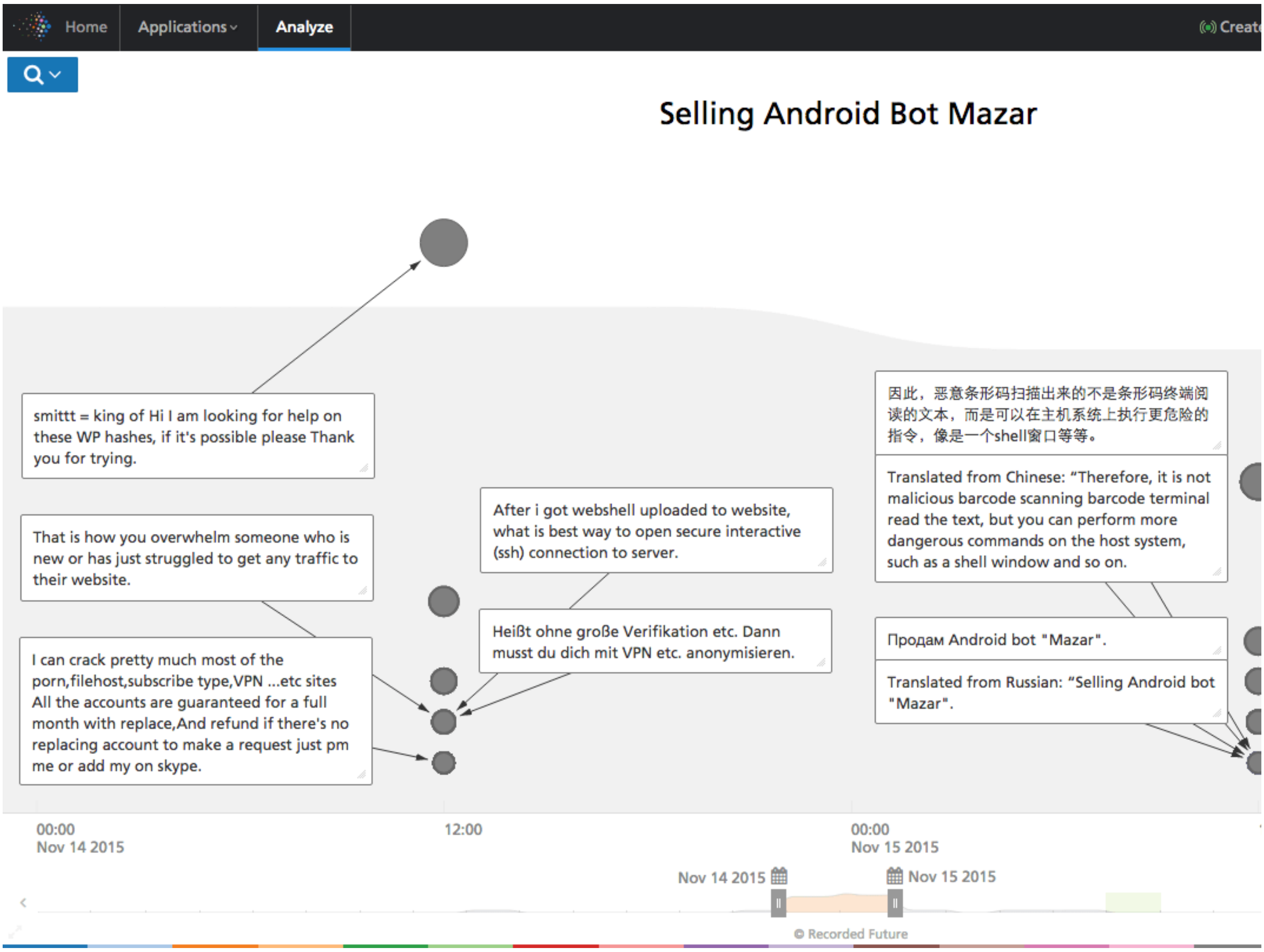
The malware allows the attackers to spy on almost every activity capable on an Android device, including establishing a backdoor connection, sending premium SMS messages, reading texts sent to the device, including bank authentication PINs. Heimdal researchers said the attackers’ root access can also allow them to erase the phone.

The researchers added that the malware won’ t install on devices set to the Russian language option.

“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,” Heimdal said in its report. “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).”

The attackers’ original SMS tries to entice the user to click on an embedded link which leads the victim to http://www[.]mmsforyou[.]net/mms[.]apk. The APK starts by installing Tor—grabbed from legitimate sources—on the device and then tries to connect to a .onion server. It then sends an automated SMS to a number in Iran with a benign message and the device’ s location data, Heimdal said.

In addition to rooting the phone, Mazar also installs the Polipo HTTP proxy, which exposes the device to man-in-the-middle attacks, putting the attacker between the phone and a web-based service, Heimdal said. It can also infect a version of the Chrome browser installed on the device, allowing the attackers to control the phone’ s keys, turn on sleep mode or save actions in the phone’ s settings.



Selling Android Bot Mazar

smittt = king of Hi I am looking for help on these WP hashes, if it's possible please Thank you for trying.

That is how you overwhelm someone who is new or has just struggled to get any traffic to their website.

I can crack pretty much most of the porn,filehost,subscribe type,VPN ...etc sites All the accounts are guaranteed for a full month with replace,And refund if there's no replacing account to make a request just pm me or add my on skype.

After i got webshell uploaded to website, what is best way to open secure interactive (ssh) connection to server.

Heißt ohne große Verifikation etc. Dann musst du dich mit VPN etc. anonymisieren.

因此，恶意条形码扫描出来的不是条形码终端阅读的文本，而是可以在主机系统上执行更危险的指令，像是一个shell窗口等等。

Translated from Chinese: “Therefore, it is not malicious barcode scanning barcode terminal read the text, but you can perform more dangerous commands on the host system, such as a shell window and so on.

Продам Android bot "Mazar".

Translated from Russian: “Selling Android bot "Mazar".

Researchers at Recorded Future saw the bot advertised, above, on a Russian forum known for selling malware used by cybercriminals, and panels make mention of a prominent Russian financial services company Sberbank. At the time, they were not sure of the bot’ s authenticity and whether it was in the wild. Heimdal said last week this is the first time the malware had been spotted in active attacks.

57 81 65 0 0

Categories: Malware, Mobile Security

## Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email

Post Comment

☐ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

## Recommended Reads

f 74 g+ 301 in 158 2 0

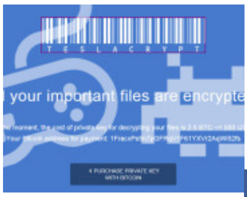
February 8, 2016 , 7:20 am
Categories: Hacks, Malware, Security Analyst Summit

### Metel Bank Robbers Borrowing from APT Attacks

by Michael Mimoso

At the Security Analyst Summit, Kaspersky Lab researchers unveiled three cybercrime outfits—Metel, GCMAN, and Carbanak 2.0—targeting Russian banks with APT-style tactics.

Read more...



f 70 g+ 211 in 103 0 0

February 5, 2016 , 7:00 am
Categories: Malware, Web Security

### WordPress Infections Leading to TeslaCrypt Ransomware

by Michael Mimoso

A massive string of WordPress compromises are redirecting victims to the Nuclear Exploit Kit and Teslacrypt ransomware.

Read more...

f 106 g+ 531 in 128 1 1

February 1, 2016 , 2:00 pm
Categories: Mobile Security, Vulnerabilities

### Critical Wi-Fi Flaw Patched on Android

by Michael Mimoso

Google’ s monthly Android Security Bulletin includes a patch for a critical flaw in the Broadcom Wi-Fi driver and another set of exploitable issues in Mediaserver.

Read more...

## Top Stories

Threatpost News Wrap, February 5, 2016

February 5, 2016 , 10:00 am

Metel Bank Robbers Borrowing from APT Attacks

February 8, 2016 , 7:20 am

Apple’ s ‘Targeted’ Gatekeeper Bypass Patch Leaves OS X Users Exposed

January 15, 2016 , 8:00 am

Google Challenges Number of Android Devices Affected by Linux Flaw

January 21, 2016 , 11:45 am

Critical Wi-Fi Flaw Patched on Android

February 1, 2016 , 2:00 pm

Data Theft Hole Identified in LG G3 Smartphones

January 29, 2016 , 3:13 pm

OpenSSL Patches Serious Flaws in Library

January 28, 2016 , 11:16 am

Israeli Electric Authority Hit by ‘Severe Cyber Attack,’ Likely Ransomware

January 27, 2016 , 12:55 pm

## The Final Say

From Kaspersky Blogs

3-in-1: history, innovation and business travel….

I find myself in many different far-flung places on this planet, but quite often they’re… predictable: world capitals, business hubs, Must-See places… But occasionally I also get to less o...

Read more…

Experts: what ATM jackpotting malware is

Kaspersky Lab security researchers Santiago Pontirol and Roberto Martinez explain how ATM malware works in Latin America and why it's difficult to discover 'jackpotting' malware.

Read more…

7 bad tricks used to trick people online

Sooner or later each user of the internet will face a trick or trap. Here’ s the list of the most widespread ones. Forewarned is forearmed!

Read more…

A bug in the grid: about an incident with Israel E...

Israel's Electric Authority - an agency in charge of regulating and overseeing the distribution of electricity in Israel - had to mitigate what officials there called a "severe cyber attack."...

Read more…

How to protect a contactless bank card...

The appearance of contactless bank cards came as no surprise. Near Field Communication (NFC) technology allows you to simply touch a payment terminal with your wallet without having to take your bank ...

Read more…

Threatpost | The first stop for security news The Kaspersky Lab Security News Service
CategoriesBlack Hat | Cloud Security | Critical Infrastructure | Cryptography | Featured | Government | Hacks | Malware | Mobile Security | Podcasts | Privacy | Security Analyst Summit | Slideshow | Uncategorized | Videos | Vulnerabilities | Web Security

- RSS Feeds
- Home
- About Us
- Contact Us

## Authors

Michael Mimoso
Christopher Brook

- | Terms of Service
- | Privacy