

Forum: [Hack Forums](#)

Thread: [GM Bot \(Android Malware\) Source Code Leaked Online](#)

? Eugtique ? - February 22, 2016, 10:24 am

The source code of a recently discovered Android banking Trojan that has the capability to gain administrator access on your smartphone and completely erase your phone's storage has been LEAKED online.

The banking Trojan family is known by several names; Security researchers from FireEye dubbed it SlemBunk, Symantec dubbed it Bankosy, and last week when Heimdal Security uncovered it, they dubbed it MazarBot.

All the above wave of Android banking Trojans originated from a common threat family, dubbed GM Bot, which IBM has been tracking since 2014.

GM Bot emerged on the Russian cybercrime underground forums, sold for \$500 / €450, but it appears someone who bought the code leaked it on a forum in December 2015, the IBM X-Force team reported.

What is GM Bot and Why Should You Worry about it?

The recent version of GM Bot (dubbed MazarBOT) has the capability to display phishing pages on the top of mobile banking applications in an effort to trick Android users into handing over their financial credentials to the fraudsters.

Besides this, the banking trojan is also capable of forwarding phone calls and intercepting SMS messages to help fraudsters bypass an additional layer of bank security mechanisms, and locking a device's screen.

Cyber criminals could also use the malware to:

- Spy on victims

- Delete data from the infected device

- Gain boot persistence to help survive device restart

- Send and Read your SMS message

- Make Calls to your contacts

- Read the phone's state

- Plague phone's control keys

- Infect your Chrome browser

- Change phone settings

- Force the phone into sleep mode

- Query the network status

- Access the Internet

- Wipe your device's storage (the most critical capabilities of the malware)

However, someone leaked the malware source code only to boost his/her reputation on an underground forum, according to the researchers.

GM Bot Android Malware Source Code for FREE

Yes, the source code for GM Bot and its control panel is now accessible to cybercriminals and fraudsters for FREE.

Here's the Cherry on the Top:

Besides the source code, the leader also posted a tutorial and instructions for server-side installation, which means cybercriminals can create their own versions of the malware strain to conduct online banking frauds.

Though the archive file containing the source code and its control panel is password protected, the leader is offering the password only to active forum members who is approaching him.

"Those who received the password, in turn, passed it on to other, unintended users, so the actual distribution of the code went well beyond that discussion board's member list," IBM cyber security evangelist Limor Kesseem wrote in a blog post.

Online users had started sharing the password to the archive among their friends, and in no time, the GM Bot source code was all over the hacking underground forums.

GM Bot is one of the most dangerous banking trojan in the Android ecosystem and after its source code gets leaked, users are recommended to beware while banking online.

How to Protect Yourself?

As I previously mentioned, online users are advised to follow these steps in order to protect themselves against this kind of threat:

Never open attachments from unknown sources.

Never click on links in SMS or MMS messages sent to your phone.

Even if the email looks legit, go directly to the source website and verify any possible updates.

Go to Settings -> Security -> Turn OFF "Allow installation of apps from sources other than the Play Store" option.

Always keep an up-to-date Anti-virus app on your Android devices.

Avoid unknown and unsecured Wi-Fi hotspots and Keep your Wi-Fi turned OFF when not in use.

Source: <http://geekthe.net/2016/02/22/gm-bot-android-malware-source-code-leaked-online/>

tzuket - February 22, 2016, 11:01 am

Where is the download for the source code

kingfly55 - February 22, 2016, 11:29 am

(Feb 22, 2016 12:01 PM)tzuket Wrote: [\[CITE\]](#) Where is the download for the source code
I would love to know that too

mrnapolean1 - February 22, 2016, 7:18 pm

This is why I don't bank from my phone.

Isley - February 22, 2016, 10:15 pm

Android master race, amirite? Pretty cool looking at the sc though, haven't had the chance to look at such an advanced android malware.

rageSpeed - February 23, 2016, 3:28 am

(Feb 22, 2016 12:01 PM)tzuket Wrote: [\[CITE\]](#) Where is the download for the source code
I'm intrested too ?

Hoodie+ - February 23, 2016, 3:34 am

The most interesting source code to research so far ?

inf2022 - February 23, 2016, 3:48 am

I want the source code too

Hoodie+ - February 23, 2016, 4:07 am

As far as we know, this may be fake.

The sourc code is nowhere avaiable online.

? Eugtique ? - February 23, 2016, 4:35 am

I've searched everywhere for the source of the leaked shit. Not available anywhere... tssssk

kingfly55 - February 23, 2016, 8:09 am

What forum was it sold on??

Wozniak - February 25, 2016, 2:25 pm

On some Russian underground apparently. I sure can't find it :p

Ooze - February 25, 2016, 2:28 pm

I still can't find it

only doing a simple google search though

trilobit - February 25, 2016, 5:50 pm

Its impossible to find this source. Everybody who have it keeps for himself and dont want to leak it :-/ im sure

Ooze - February 25, 2016, 9:41 pm

(Feb 25, 2016 06:50 PM)trilobit Wrote: [\[CITE\]](#) Its impossible to find this source. Everybody who have it keeps for himself and dont want to leak it :-/ im sure

If that were true it wouldn't have been leaked in the first place

zaheer9869 - February 25, 2016, 10:05 pm

As per what I have read it was leaked on underground forum site crdclub DOT ws and is on sale for \$5,000

? Eugtique ? - February 26, 2016, 4:03 am

(Feb 25, 2016 11:05 PM)zaheer9869 Wrote: [\[CITE\]](#) As per what I have read it was leaked on underground forum site crdclub DOT ws and is on sale for \$5,000

That's expensive for some leaked shit

Mcbride - February 27, 2016, 10:22 pm

Leaked yet y'all can't find.

Pablo Emilio Escobar - February 27, 2016, 10:41 pm

(Feb 27, 2016 11:22 PM)Cest La Vie Wrote: [\[CITE\]](#) Leaked yet y'all can't find.

I guess you found it?

leeroy12 - February 29, 2016, 2:46 pm

scares you that people will do that, poverty or greed is a killer these days. so sad

kingfly55 - March 2, 2016, 11:42 am

So, anyone found this yet?

george1 - March 25, 2016, 8:35 pm

Interested as well...supposedly it is on the hell forum in deep web...does anyone have an access code to register??

crimsoncypher - March 25, 2016, 8:37 pm

Title is misleading. Thought you had the source code. Good read though

Andramedia - April 28, 2016, 8:50 am

I have the Mazar Bot.

But I do not know how the setup works .But I need a tutorial step by step

Andramedia - April 28, 2016, 10:41 am

No I did not now sorry man

LlamaZombi - *December 13, 2016, 12:27 am*

Its not availble anymore , but thanks for sharing

ÇdnîS Lu?i? - *December 13, 2016, 5:27 pm*

It's on the Deepwebz, i came across it but i don't intend using it. They charge for the source on some markets.