New Telegram-abusing Android RAT discovered in the wild

welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

June 18, 2018

Entirely new malware family discovered by ESET researchers

Lukas Stefanko
18 Jun 2018 - 02:58PM

Entirely new malware family discovered by ESET researchers

ESET researchers have discovered a new family of Android RATs (Remote Administration Tools), that has been abusing the Telegram protocol for command and control, and data exfiltration.

Investigating what at first seemed like increased activity on the part of the previously reported IRRAT and TeleRAT, we identified an entirely new malware family that has been spreading since at least August 2017. In March 2018, its source code was made available for free on Telegram hacking channels, and as a result, hundreds of parallel variants of the malware have been circulating in the wild.

One of these variants is different from the rest – despite the freely available source code, it is offered for sale on a dedicated Telegram channel, marketed under the name HeroRat. It is available in three pricing models according to functionality, and comes with a support video channel. It is unclear whether this variant was created from the leaked source code, or if it is the “original” whose source code was leaked.

How does it operate?

Attackers lure victims into downloading the RAT by spreading it under various attractive-sounding guises, via third-party app stores, social media and messaging apps. We’ve seen the malware distributed mostly in Iran, as apps promising free bitcoins, free internet connections, and additional followers on social media. The malware has not been seen on Google Play.

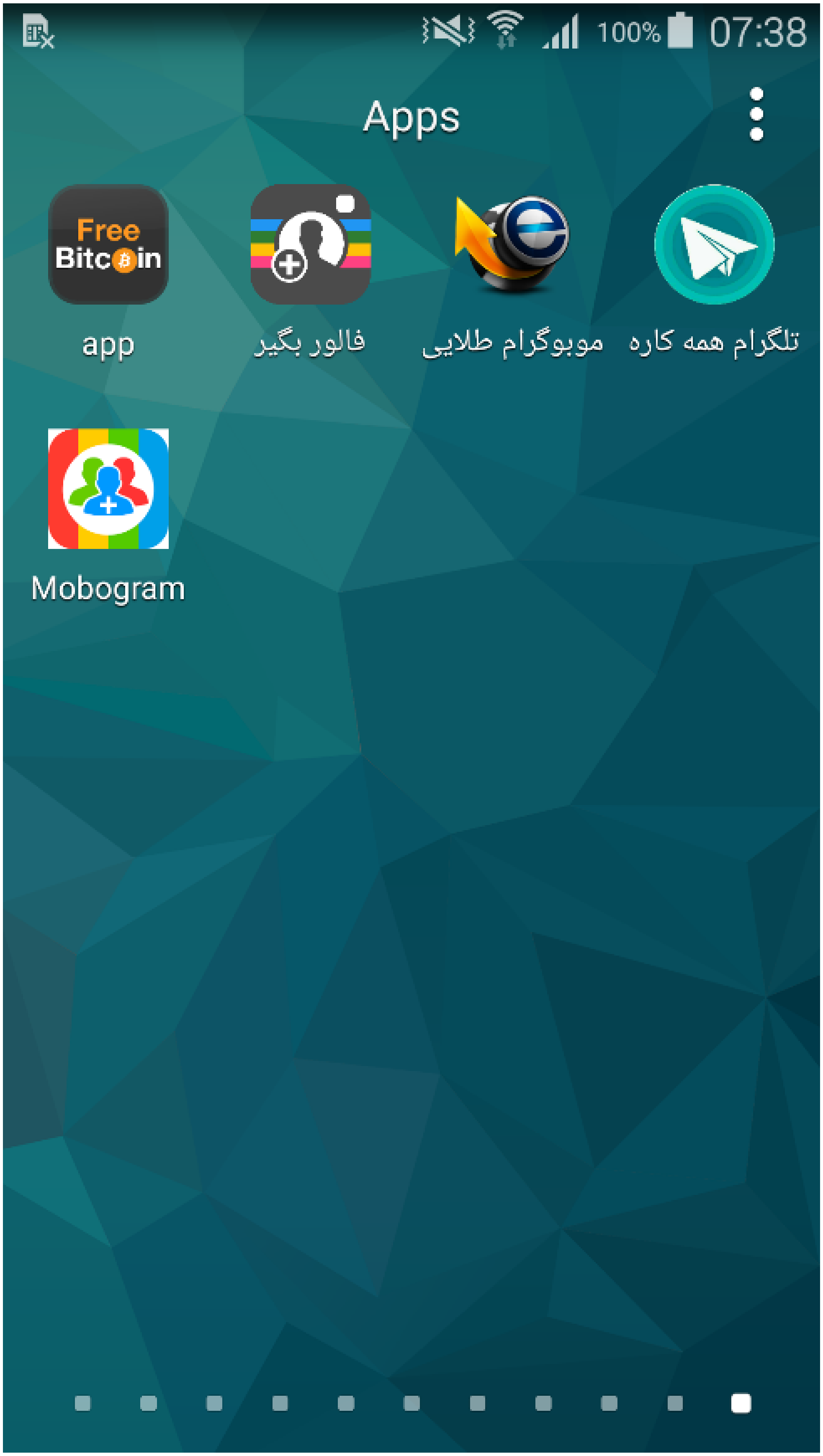
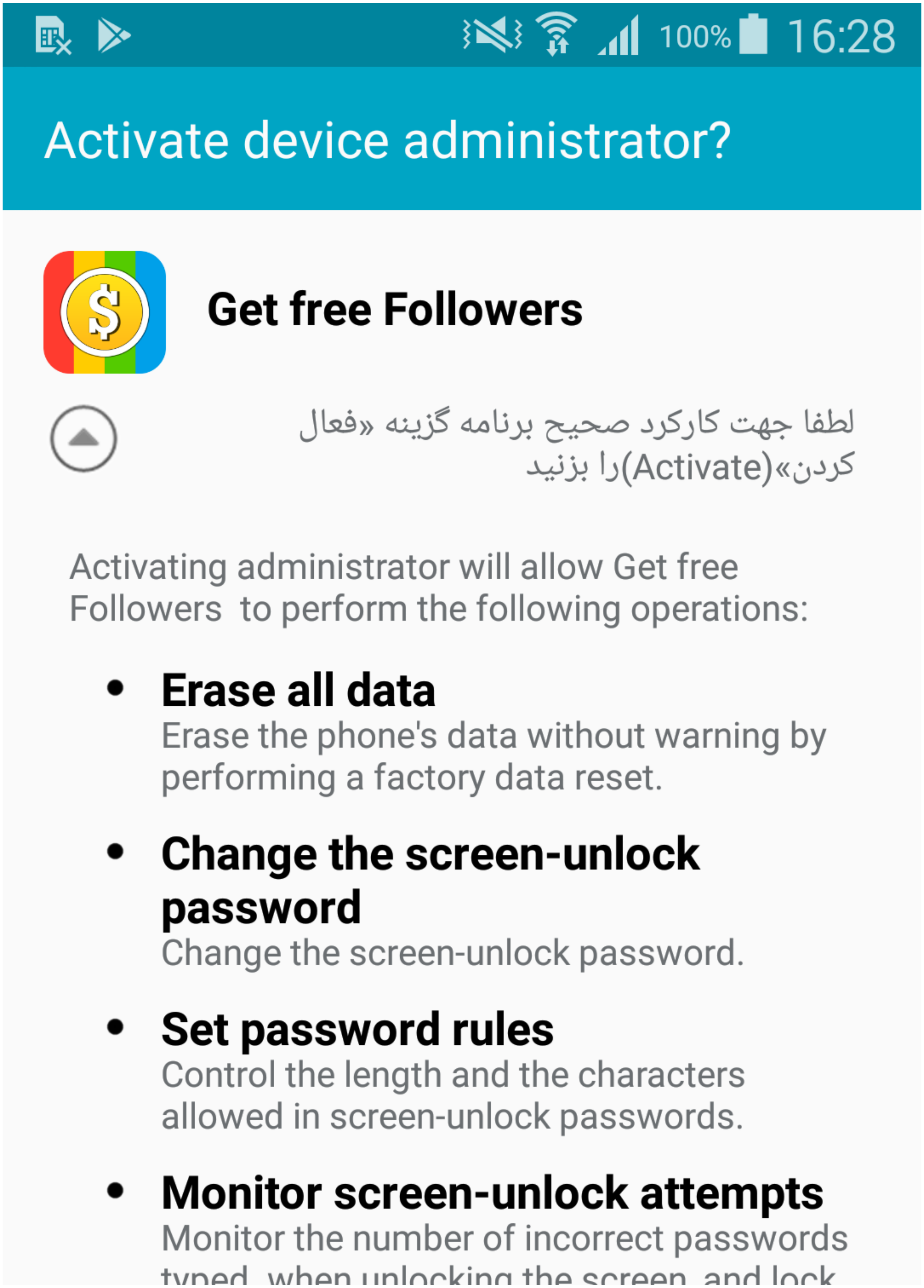


Figure 1 – Some of the guises used to propagate the RAT

The malware runs on all Android versions: however, affected users need to accept permissions required by the app (sometimes including activating the app as device administrator), which is where social engineering comes into play.



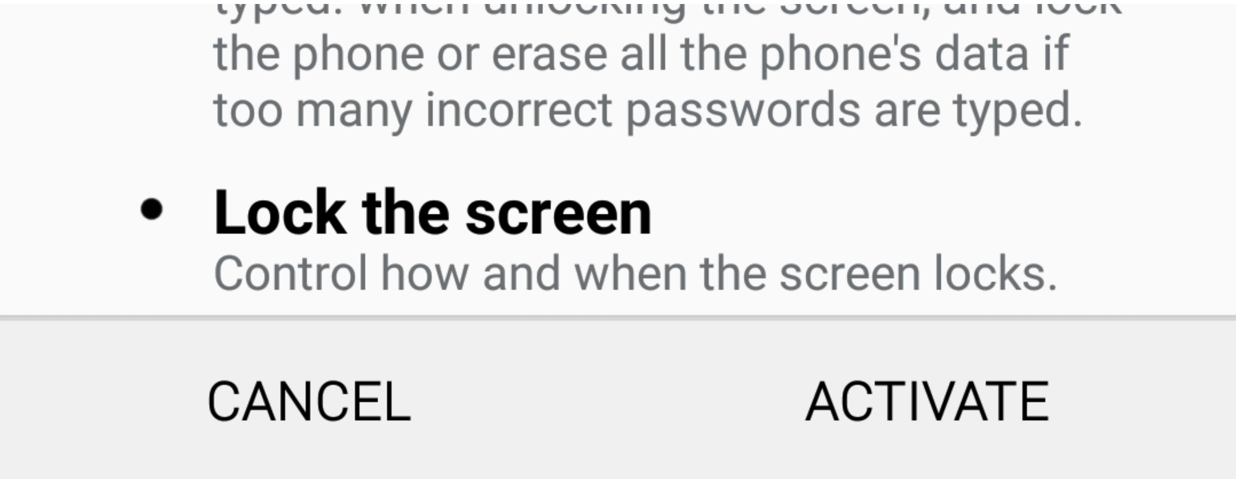
Activate device administrator?

Get free Followers

لطفا جهت کارکرد صحیح برنامه گزینه «فعال
کردن»(Activate)را بزنید

Activating administrator will allow Get free Followers to perform the following operations:

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed, when unlocking the screen, and lock



typed when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.

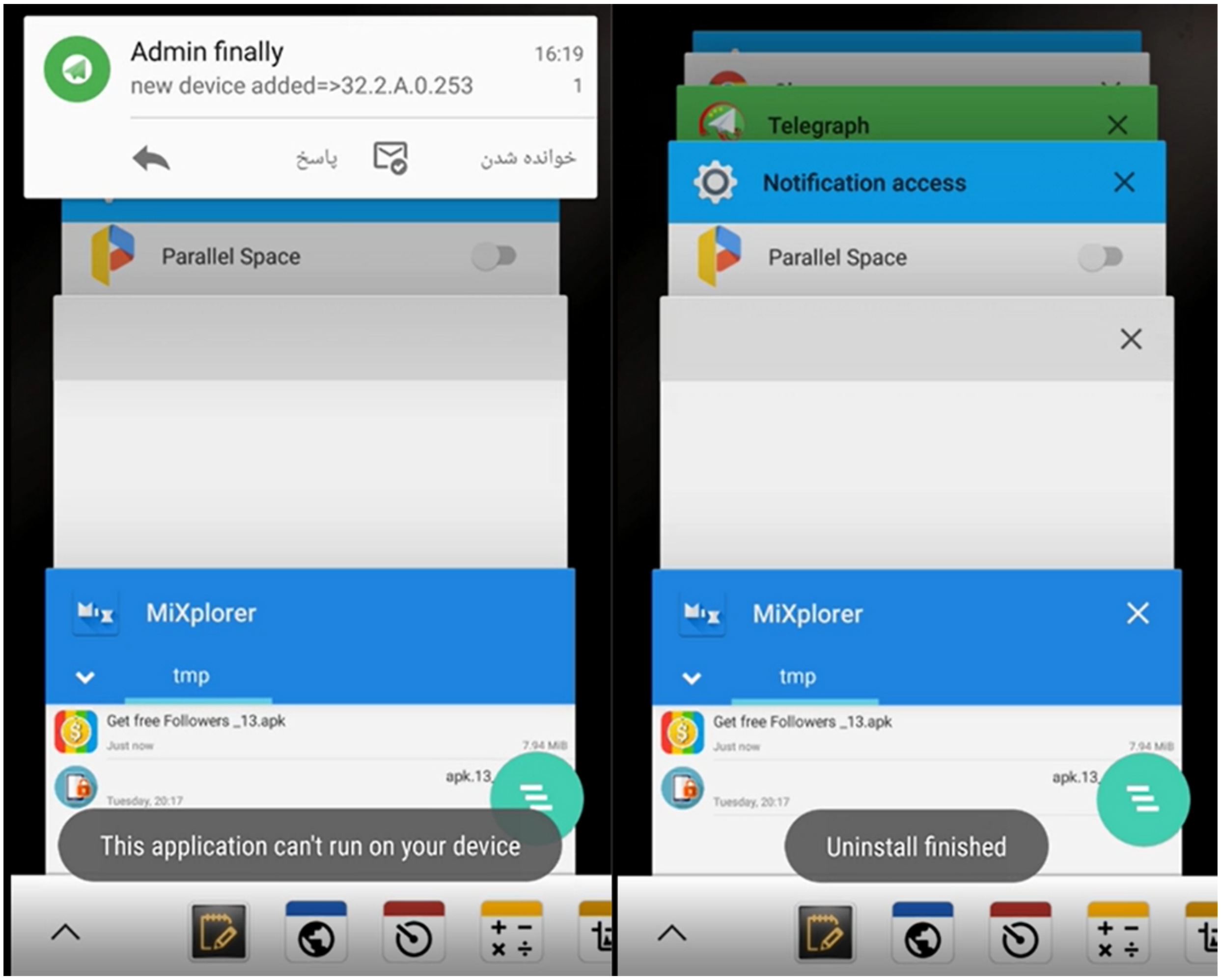
- **Lock the screen**
  Control how and when the screen locks.

CANCEL ACTIVATE

Figure 2 – The RAT requesting device administrator rights

After the malware is installed and launched on the victim’s device, a small popup appears, claiming the app can’t run on the device and will therefore be uninstalled. In the variants we analyzed, the fake uninstall message can be displayed in English or Persian, depending on the target device‘s language settings.

After the uninstallation is seemingly completed, the app’s icon disappears. On the attacker’s side, however, a new victimized device has just been registered.

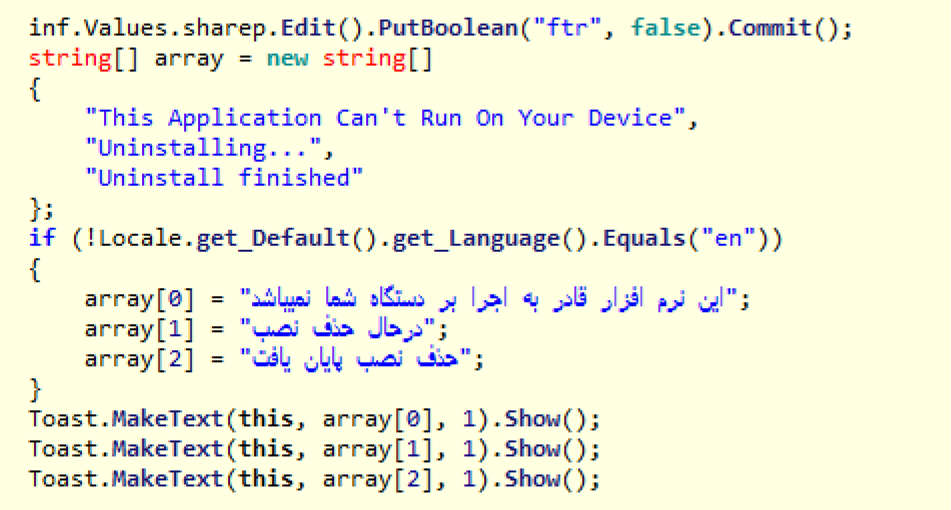


Admin finally 16:19
new device added=>32.2.A.0.253 1

This application can't run on your device

Uninstall finished

Figure 3 – HeroRat author's demonstration of installing the RAT on his own device (screenshots from an instructional video provided by the malware author)



```
inf.Values.sharep.Edit().PutBoolean("ftr", false).Commit();
string[] array = new string[]
{
    "This Application Can't Run On Your Device",
    "Uninstalling...",
    "Uninstall finished"
};
if (!Locale.get_Default().get_Language().Equals("en"))
{
    array[0] = "این نرم افزار قادر به اجرا بر دستگاه شما نمیباشد";
    array[1] = "درحال حذف نصب";
    array[2] = "حذف نصب پایان یافت";
}
Toast.MakeText(this, array[0], 1).Show();
Toast.MakeText(this, array[1], 1).Show();
Toast.MakeText(this, array[2], 1).Show();
```

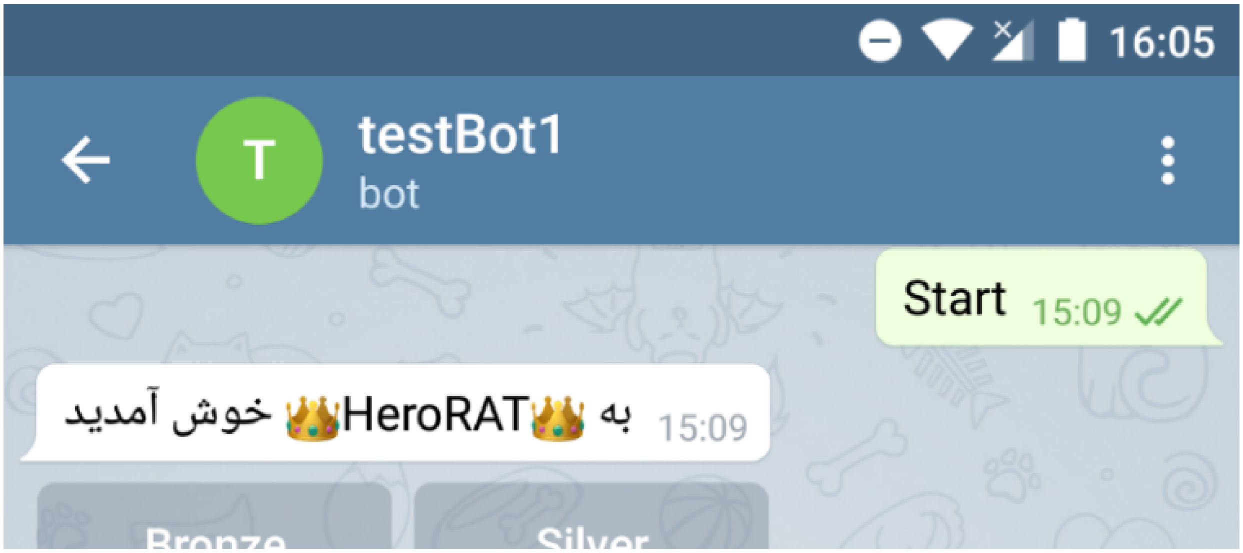
Figure 4 – Malware source code with fake uninstallation messages in both English and Persian

Having gained access to the victim's device, the attacker then leverages Telegram's bot functionality to control the newly listed device. Each compromised device is controlled via a bot, set up and operated by the attacker using the Telegram app.

The malware has a wide array of spying and file exfiltration capabilities, including intercepting text messages and contacts, sending text messages and making calls, audio and screen recording, obtaining device location, and controlling the device's settings.

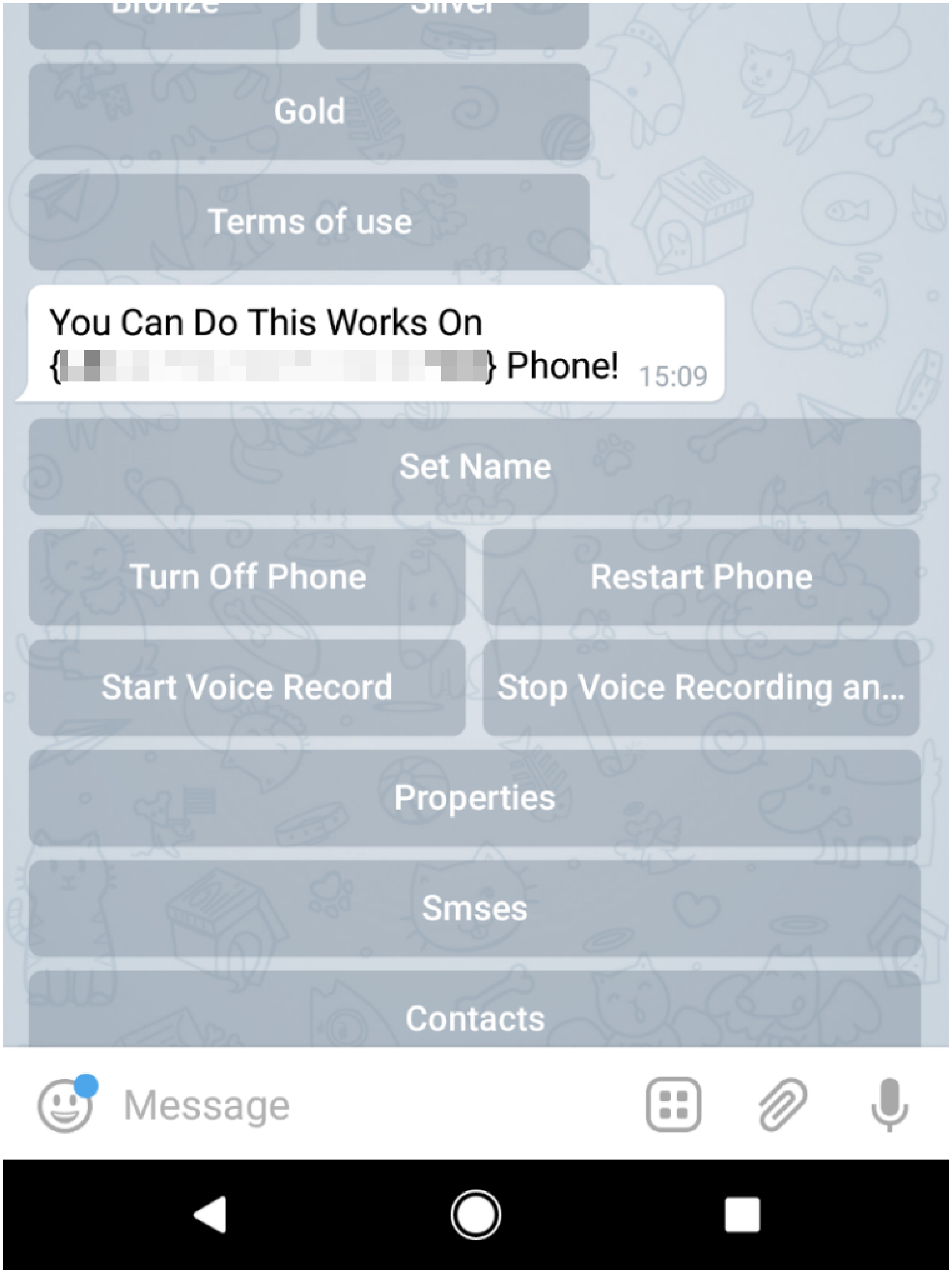
HeroRat's functionality is divided into three "bundles" – bronze, silver and gold panels – offered for sale for 25, 50, and 100 USD, respectively. The source code itself is offered for 650 USD by HeroRat's (ambitious) author.

The malware's capabilities are accessible in the form of clickable buttons in the Telegram bot interface. Attackers can control victimized devices by simply tapping the buttons available in the version of the malware they are operating.



Start 15:09

به 👑HeroRAT👑 خوش آمدید 15:09



You Can Do This Works On {[redacted]} Phone! 15:09

Figure 5 – HeroRat control panel

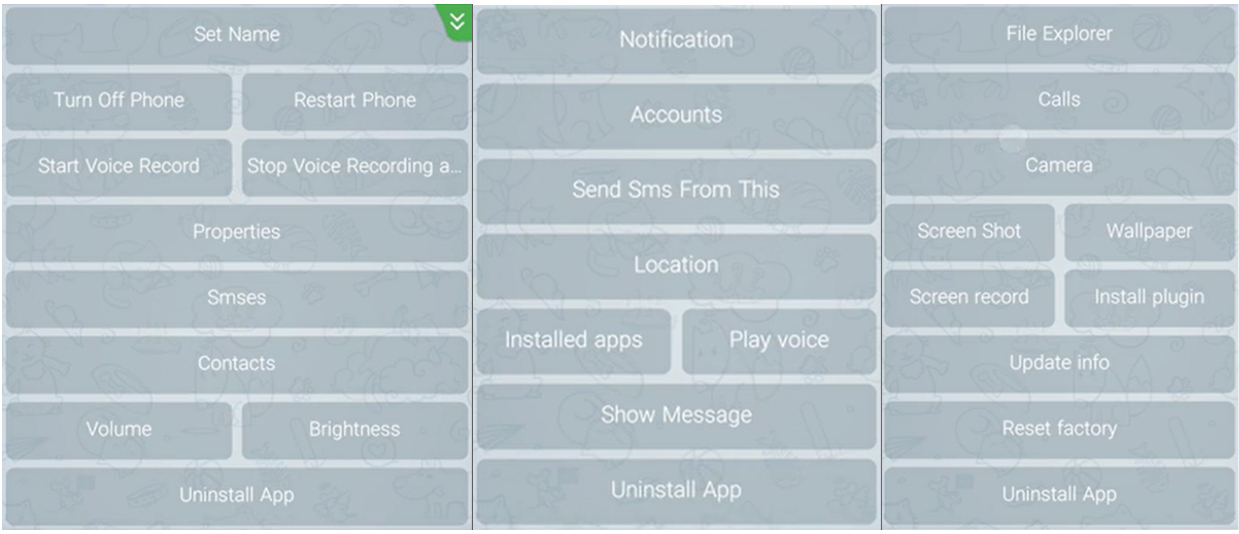


Figure 6 – HeroRat functionality – from left to right, “Bronze panel”, “Silver panel” and “Gold panel” (screenshots from an instructional video provided by the malware author)

Unlike the Telegram-abusing Android RATs previously analyzed, which are written in standard Android Java, this newly-discovered malware family has been developed from scratch in C# using the Xamarin framework – a rare combination for Android malware.

The way the malware communicates via the Telegram protocol has been adapted to its programming language – instead of the Telegram Bot API leveraged by the RATs previously described, this malware family uses Telesharp, a library for creating Telegram bots with C#.

Communicating commands to and exfiltrating data from the compromised devices are both covered entirely via the Telegram protocol – a measure aimed at avoiding detection based on traffic to known upload servers.

How to stay safe

With the malware’s source code recently made available for free, new mutations could be developed and deployed anywhere in the world. Since the distribution method and form of disguise of this malware varies case by case, checking your device for the presence of any specific applications is not enough to tell if your device has been compromised.

If you have reason to believe your device has been compromised by this malware, scan it using a reliable mobile security solution. ESET systems detect and block this threat as Android/Spy.Agent.AMS and Android/Agent.AQO.

To avoid falling victim to Android malware, stick to the official Google Play store when downloading apps, make sure to read user reviews before downloading anything to your device and pay attention to what permissions you grant to apps both before and after installation.

IoCs

Package Name	Hash	Detection
System.OS	896FFA6CB6D7789662ACEDC3F9C024A0	Android/Agent.AQO
Andro.OS	E16349E8BB8F76DCFF973CB71E9EA59E	Android/Spy.Agent.AMS
FreeInterNet.OS	0E6FDBDF1FB1E758D2352407D4DBF91E	Android/Agent.AQO

18 Jun 2018 - 02:58PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion