Black Rose Lucy

Alireza Arjmand
alirezaarjmandshakoori@gmail.com

Introduction

When you hear "organized crime" you probably think of underground drug dealer companies or thief networks which work together to achieve an illegal goal. In the darknet, however, crime has a different shape. There has been a hot topic in darknet named MaaS or Malware-as-a-service developed by some underground hacker groups and sold to individuals by different prices. A person can use MaaS to infect some victims without much computer knowledge. It is easier and cheaper than finding a group of experienced hackers and asking them to develop your malware from scratch. In this paper, we are taking a closer look at one of these MaaS providers called "Lucy Gang" a Russian group that first seen in 2018 when checkpoint researchers wrote an article about them. Then we will take a closer look at their new software in 2020 and find out about the way it works and its interesting self-protection mechanisms. Finally, we are going to point out some ways to stay safe from these malware programs.

How it worked back in 2018

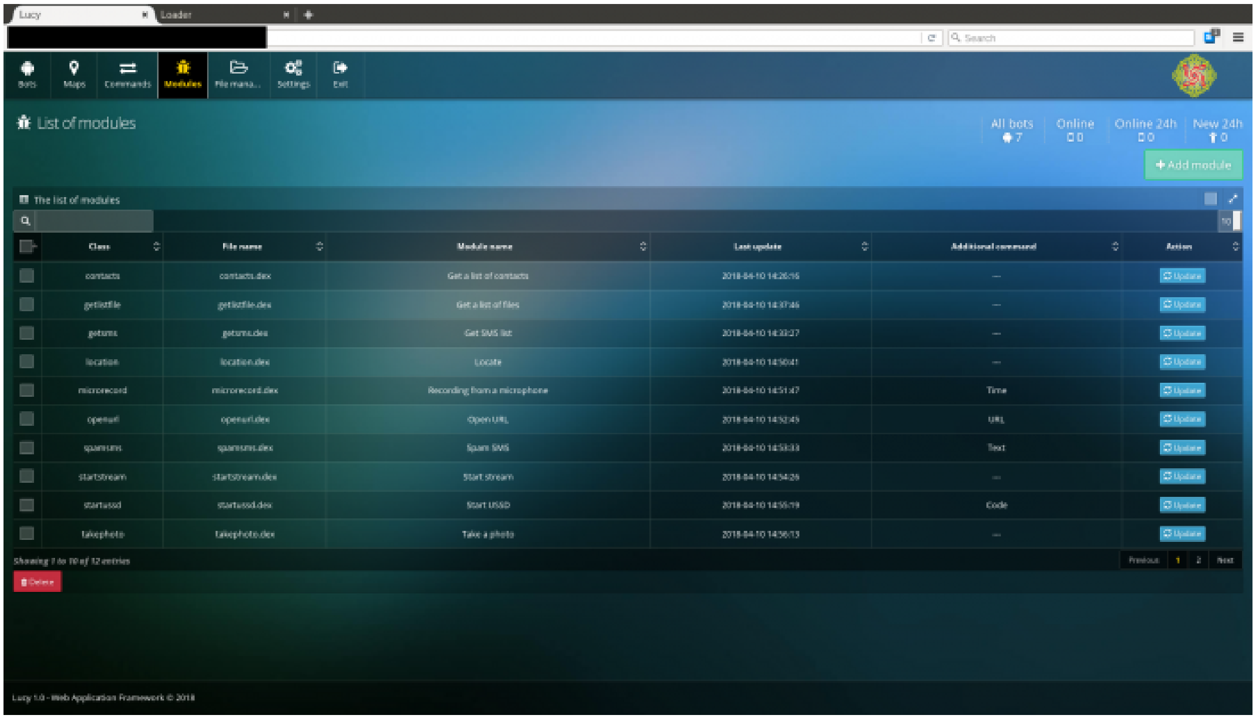
Back in 2018, when their product called "Black Rose" was analyzed, it consisted of two parts, a "Lucy Loader" which was a dashboard for the buyer. The second part was "Black Rose Dropper" that could target android devices and listen to a remote command and control or C&C server to await some commands.

The main exploit they used, according to checkpoint researchers, is through Android Accessibility Service, a service to mimic user's input and automate tasks. Black rose dropper tricked the victim into enabling this service, and then the dropper could give itself admin permission without user consent. While in the usual case user needs to provide an application with admin permission through a predefined set of steps, Android Accessibility Service is used to do this step behind the user's back.

A deeper dive into their 2018 product

First, let us take a look at Lucy Loader; an attacker can use this dashboard to access infected victim devices and do some operations such as installing a new malware or access some of their files. you can see a picture provided by checkpoint researchers in Figure 1.

Second, there is black rose dropper that gets installed on the victim's device and waits for some commands from C&C servers. this dropper needs admin privileges to show dialogs



[redacted]

List of modules

The list of modules

Class	File name	Module name	Last update	Additional command	Action
contacts	contacts.dex	Get a list of contacts	2018-04-10 14:26:16	—	Update
getlistfile	getlistfile.dex	Get a list of files	2018-04-10 14:37:46	—	Update
getsms	getsms.dex	Get SMS list	2018-04-10 14:33:27	—	Update
location	location.dex	Locate	2018-04-10 14:50:41	—	Update
microrecord	microrecord.dex	Recording from a microphone	2018-04-10 14:51:47	Time	Update
openurl	openurl.dex	Open URL	2018-04-10 14:52:45	URL	Update
spamsms	spamsms.dex	Spam SMS	2018-04-10 14:53:33	Text	Update
startstream	startstream.dex	Start stream	2018-04-10 14:54:26	—	Update
startussd	startussd.dex	Start USSD	2018-04-10 14:55:19	Code	Update
takephoto	takephoto.dex	Take a photo	2018-04-10 14:56:13	—	Update

Showing 1 to 10 of 12 entries

Lucy 1.0 - Web Application Framework © 2018

Figure 1: Lucy Loader

on top of other applications and ignore battery life so it can keep its services alive all the time, it tricks user with several steps:

- First, it hides the icon inside application's MainActivity's OnCreate method so the user can't see it.
- Then it starts a monitor service immediately, so it shows the user a message after 60 seconds to enable "Security of System" this message is shown to the user repeatedly until it is activated! When the user activates the Security of System, she is actually activating the Android Accessibility Service for the dropper.
- Finally, with the service enabled, the dropper can go through windows and give itself the admin privilege.

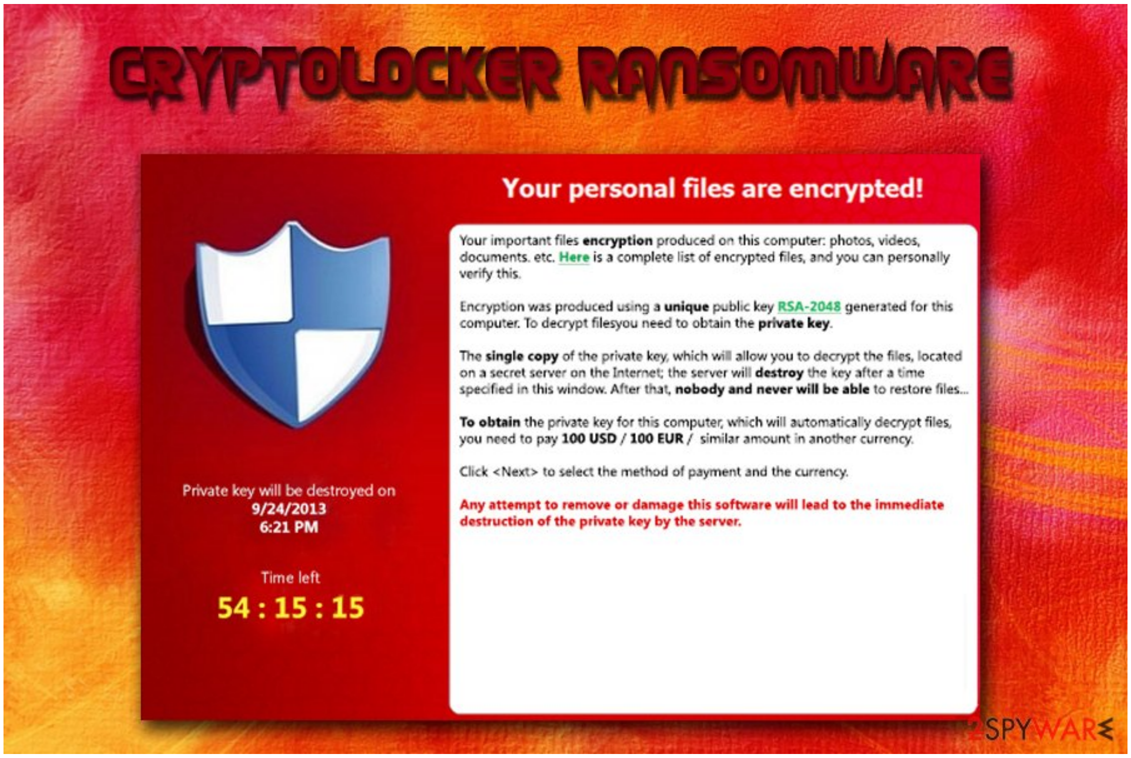
Now that the dropper has admin permissions, it can do a lot of things for its masters; The monitor service restarts itself whenever the screen turns on or off, so it is always running. It then listens to commands from C&C servers and sends log back, which contains the status of the output. On top of all these, black rose dropper has an interesting and effective self-protection mechanism. It actively checks to see if any popular free security tools are launched or not; if one is started, it mimics the press of back or home button, so the user can not use it.

What happened in 2020, First glance

on April 28, checkpoint researchers, Ohad Mana, Aviran Hazum, Bogdan Melnykov, Liav Kuperman published another paper about the new black rose dropper. It seems the Lucy Gang have upped their game, this time it is a ransomware which infects victims device, encrypts their data and asks them for money to give them the key to decrypt data and get their precious data back.

Ransomwares

Before we continue, let us talk about what ransomwares are. Ransomware is a kind of malware developed to infect your device and try to threaten you to give the hackers behind it some money. They usually ask for bitcoin or some other similar cryptocurrency since their transactions are done anonymously. In their most common cases, they use some known cryptography algorithms to encrypt your data and block access to it; then, they ask for money to give you the key to decrypt it. Their early versions had some fatal flaws like storing the key somewhere in the code and the victim could decrypt data without paying any money. Nowadays, they are using some reliable cryptography algorithms, so decrypting the data without the key, after your device is infected is close to impossible. Some famous examples of ransomwares are WannaCry or CryptoLocker; these malware programs made millions of dollars for their developers. You can see a picture of an example of what happens after they encrypt the victim's data in Figure 2.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. **Here** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

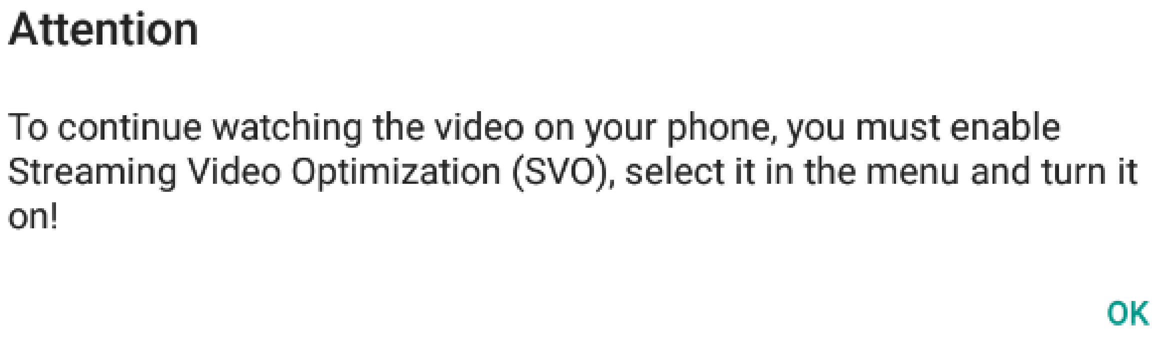
Figure 2: CryptoLocker post encryption message

ransomwares usually follow three steps:

- First is the release phase; the attacker generates a key pair and places the public key hardcoded on the malware.
- Second, the malware uses a randomly generated symmetric key to encrypt data on the victim's device. They encrypt the symmetric key itself with the public key and deletes the plaintext symmetric key, and now only the attacker can decrypt the encrypted key and access the data. This way of encrypting with two keys is also called hybrid encryption.
- Third and last, attacker demands payment, after receiving payment they decrypt the symmetric key and return it to the victim, now they can decrypt their data. There have been some reports of victims making the payment and never hearing back from attackers. Usually, these cases are rare since it is to attacker's benefit to return the key, or further victims will not make any payment.

How lucy does it

This time their application looks like a harmless looking video player, but again they are using the Android Accessibility System to gain all the access they need.
When a user downloads Lucy's new package, they show a pop-up message that asks the user to enable SVO (Streaming Video Optimization) for this application.



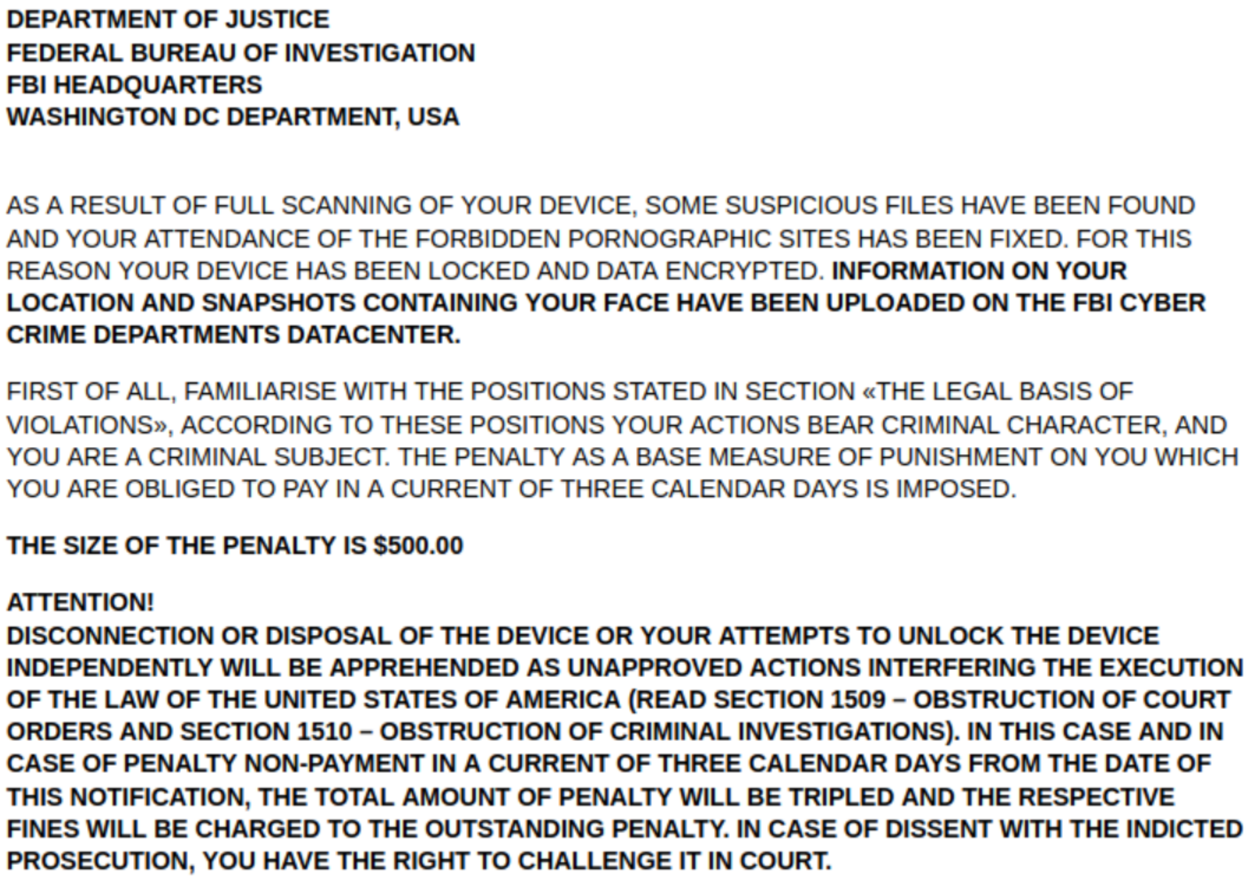
Attention

To continue watching the video on your phone, you must enable Streaming Video Optimization (SVO), select it in the menu and turn it on!

Figure 3: Pop up message

But what really is happening is that the user is giving access to the Android Accessibility Service upon agreeing with this message. Then it can use this service to achieve all of its goals. After that, it starts encrypting data and displays a message, claiming to be an official note from the US FBI, accusing the victim of keeping illegal pornographic on their device and that a snapshot of their face has been uploaded to the FBI servers. you can see the full message in Figure 4.

The weird thing about this ransom is that they are asking for real money instead of some near to untrackable cryptocurrency.



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED AND DATA ENCRYPTED. **INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENTS DATACENTER.**

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS», ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.

THE SIZE OF THE PENALTY IS $500.00

ATTENTION!
DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 – OBSTRUCTION OF COURT ORDERS AND SECTION 1510 – OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

Figure 4: Lucy dropper post encryption message

A deeper dive into their 2020 product

After the Android Accessibility Service got activated, lucy dropper triggers a service in its mainActivity to register a broadcast receiver called by command action.SCREEN_ON and then calls itself; This way, lucy can acquire WakeLock and WifiLock to keep the screen and Wifi on.

Communication with C&C servers

Now Lucy keeps a string of server names hardcoded instead of only IP address; this way, the server name can get resolved into different addresses and can resist against server takedown, which was a point of failure in their previous version. list of their hardcoded servers are :

gapsoinasj[.]in
q9120qwpsa[.]in
ja0h12p14k[.]in
jqeoq0r1hgf03ds[.]in

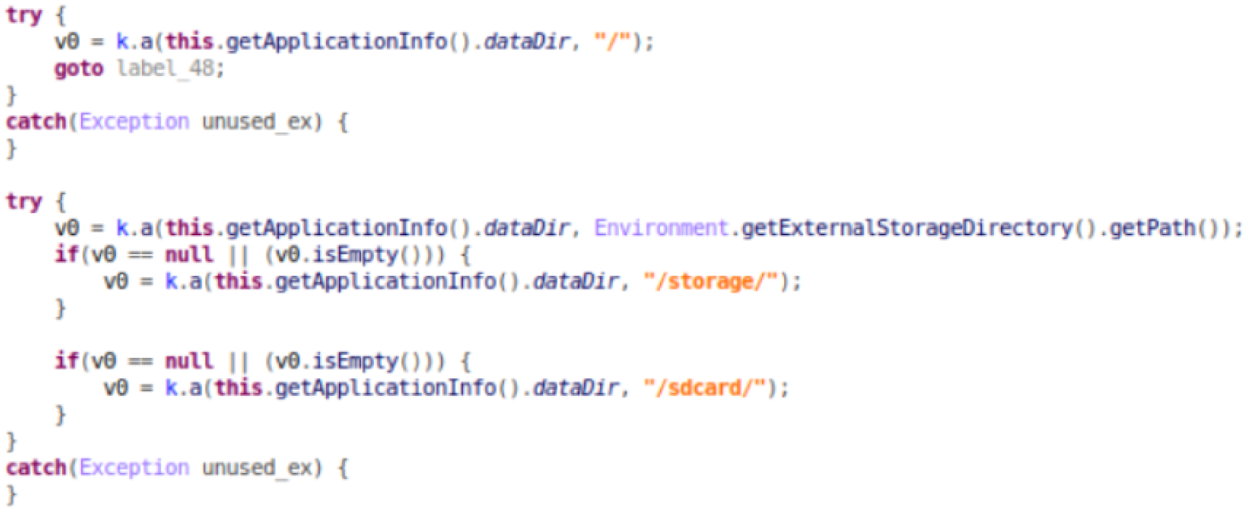
these addresses are concatenated in the code with some unused data; it might be some protection against those who might try and understand it. malware rotates between these servers and listens to them for new commands, a list of valid commands are gathered by checkpoint researchers and shown in Table 1.

Table 1: Valid commands for Lucy dropper

Command	Description
Call	Initiates a phone call to a number it gets from the C&C server.
GetCrypt	Collects a string called “key” from the C&C response.It then calls another service that tries to fetch an array of all the device’s directories.
Decrypt	Similar to ‘GetCrypt’ but used for decryption.
GetCont	Declines previous payment – shows a message that the payment was declined.
GetApp	Sends a list of all installed applications to the C&C server.
Delloc	Empties the variable used in the request to the C&C server.
DelKey	Empties all variables that contain encryption keys.
Deleted	The malware deletes itself from the device.
StartShell	Opens a remote shell on the device with the commands as arguments.

File encryption/decryption

To start the encryption process, malware needs to know about the files in the device. Lucy dropper tries to get access to files array three times; first, it tries to fetch an array of device directories. In case of failure, it tries to get directory/storage, and for the last effort, it tries to fetch /sdcard directory. You can see the code for this part here: Then Lucy dropper uses



```
try {
    v0 = k.a(this.getApplicationInfo().dataDir, "/");
    goto label_48;
}
catch(Exception unused_ex) {
}

try {
    v0 = k.a(this.getApplicationInfo().dataDir, Environment.getExternalStorageDirectory().getPath());
    if(v0 == null || (v0.isEmpty())) {
        v0 = k.a(this.getApplicationInfo().dataDir, "/storage/");
    }

    if(v0 == null || (v0.isEmpty())) {
        v0 = k.a(this.getApplicationInfo().dataDir, "/sdcard/");
    }
}
catch(Exception unused_ex) {
}
```

Figure 5: Code for fetching directory arrays

a key received from the server to concatenate it with a 'Key' pulled from SharedPreferences to build the actual key. To start the encryption, it iterates over the fetched array in the previous step and encrypts files; I am not trying to explain how encryption works since it uses one of the straight forward and known ways, but one interesting point worth mentioning is that there was an encryption function in the code which did nothing! It could be a decoy for the one who was trying to understand the code, we don't know if it is trying to make it harder to understand or it is just a simple mistake from the hackers.
After encryption is over, the dropper checks to see if the encryption is over and done correctly, then it shows the infamous message mentioned above and asks the user for money.
Also, there is a decryption process similar to the encryption, which restores the data using the previous key and then deletes itself.

How can you stay safe from these attacks?

This kind of attacks mostly happen in android devices since android lets application from any source get installed on your phone, but don't get me wrong, these still can occur on any platform, some more than the others. to wrap this paper up, we talk about some simple instructions you can do to stay safe:

- First and foremost, remember that these malware programs encrypt your data and block your access to it, as long as you have a backup on a cloud or another device you can access, you can just use the backup data and delete the malware with a full reset of your device.

- Second, some updates come with critical security updates, so try to keep your device up to date.

- Third, try to stay away from apps from unknown sources since they can have destructive behavior or install other programs without you knowing it.

- Fourth, don't click on suspicious links and stay away from spam.
- Finally, you can achieve a good level of security with a good antivirus program, there are some good known free ones that you can use, or if your safety is essential to you, you can use the paid ones.

References

[1] Feixiang He, Bogdan Melnykov, Andrey Polkovnichenko (September 13, 2018) : Meet Black Rose Lucy, the Latest Russian MaaS Botnet.
https://research.checkpoint.com/2018/meet-black-rose-lucy-the-latest-russian-maas-botnet/

[2] Ohad Mana, Aviran Hazum, Bogdan Melnykov, Liav Kuperman (April 28, 2020) : Lucy's Back: Ransomware Goes Mobile.
https://research.checkpoint.com/2020/lucys-back-ransomware-goes-mobile/

[3] Ransomware, Wikipedia.
https://en.wikipedia.org/wiki/Ransomware

[4] David Bisson (April 29, 2020) : 'Black Rose Lucy' Malware Botnet Returns With Ransomware Capabilities.
https://securityintelligence.com/news/black-rose-lucy-malware-botnet-returns-with-ransomware-capabilities/

[5] Naveen Goud : Black Rose Lucy Ransomware attack on Android Devices.
https://www.cybersecurity-insiders.com/black-rose-lucy-ransomware-attack-on-android-devices/

[6] Tara Seals (September 20, 2018): Lucy Gang Debuts with Unusual Android MaaS Package.
https://threatpost.com/lucy-gang-debuts-with-unusual-android-maas-package/137590/

[7] Tom Spring (April 28, 2020): 'Black Rose Lucy' is Back, Now Pushing Ransomware.
https://threatpost.com/black-rose-lucy-is-back-now-pushing-ransomware/155265/