10.53477/2668-2028-21-36

MALWARE PROTECTION SYSTEM ON ANDROID

Adriana-Meda UDROIU, PhD
National Institute for Research and Development in Informatics
meda.udroiu@rotld.ro

Mihail DUMITRACHE
National Institute for Research and Development in Informatics
mihail.dumitrache@rotld.ro

Abstract*: At the moment of writing this report (august 2018), the Android has a worldwide market share of 76.88%, being in an ascending slope since 2009, with an increase of 4.14% since the same period on last year and leaving its rival iOS far behind, at 20.38%[1]. Also, Google announced in 2017 that more than 2 billion users are monthly active on devices. These 2 facts make this OS the most important one on the mobile devices and not only smartphones, as nowadays even the smartwatches are using Android (named Wear) being in continuously improving the experience to be as close as the one on phones[2].*

Keywords: *malware; android; security; protection.*

Introduction

A study regarding mobile is against the desktop[3]. As many expected, the mobile takes the lead, with an increase in US traffic from 57% in 2016 to 63% in 2017 (almost ⅔ of it) with adult, tech and gambling applications being the leaders (with percentages from 55 to 86). In each and every aspect, the mobile continues to grow, whereas the desktop still remains important in our daily lives and must not be neglected.

An increasing popular platform needs also some security measures to be taken against all kinds of malware types especially ransomware, which can be painful if taken by a mobile user, that probably has a lot of personal data in his little device: like pictures, videos, applications installed, mobile wallet and also the basic phone call. People were accustomed to have an antivirus installed on their PC (desktop or laptop devices), but nowadays it is necessary to have one also on the smartphone.

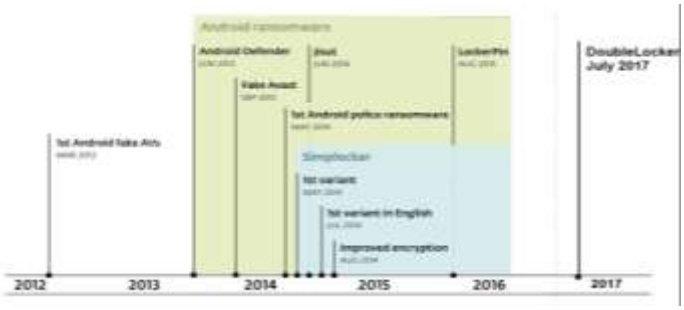

Figure 1. Android ransomware chronology (added also DoubleLocker here)[4]

This paper proposes an application that detects and protects a mobile user against ransomware type of malware. In the next chapters, they are presented some malwares that were analyzed based on the graph from above, starting with the one considered to be the first, Android Defender, continuing with a Fake Avast application, Simplocker and in the end

[1] Mobile Operating System Market Share Worldwide, http://gs.statcounter.com/os-marketshare/mobile/worldwide
[2] The best Wear OS smartwatches: LG, Fossil, Huawei, Polar and more, https://www. wareable.com/smartwatches/ best-android-watch.
[3] Mobile vs Desktop Usage in 2018: Mobile takes the lead, https://www.stone temple.com/ mobile-vs-deskto pusage-study/
[4] The Rise of Android Ransomware, https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of_ And roid_Ransomware.pdf

DoubleLocker (that was described in the report from the 1st semester an here are given more details) and Lockerpin. In the image below there is detailed the setup used for testing these kinds of malwares.

Figure 2. Setup used for testing ransomware

Analysis

Android Defender

This fake antivirus (AV) was found in the mid-2013 and is considered by ESET[5] to be the actual first ransomware to target Android. This application had a very convincing UI that looked like a real security detection software. When the device is scanned using it, there are displayed the actual names of the files plus some malware names which are also real, but they do not exist on the device.

Figure 3. Android Defender UI[6]

After finishing it, there appears a pop-up that says an application is infected with a trojan and it recommended to remove it (of course is all invented there). There are 2 options given here: remove it by paying for the full software or stay unprotected. If the second option is chosen, a new pop-up appears and so on as a service is now displaying this pop-up in an endless loop. As stated here[7] by ESET, after 6 hours of not choosing the first option, the app will go to a more aggressive mode that locks the screen and displays images that are forbidden to minors. In the end, if the user decided to pay the price of USD 89.99 using the credit card, the details of it are in the attacker's hands and could be also sniffed by others as they are sent unencrypted to them and later used by them[8].

Fake Avast

The second fake AV uses a legitimate security software from Avast that is hidden behind wellknown adult website application which has the logo modified a little from the real one (most of the users probably did not see that little change there). When the victim wants to connect to his account, there is displayed a pop-up that requires a scan of the device using Avast (a fake one). After the completion, made up results with are shown and a message that says 'the device is in danger and is locked' is shown. As expected, in order to unlock it there is need to pay a price, in this case for the pro version of Avast. A real AV would never block a device if

[5] The Rise of Android Ransomware, *op.cit.*
[6] *Idem.*
[7] The Rise of Android Ransomware, *op.cit.*
[8] *Idem.*

there are viruses found there, which means that the behavior from here corresponds to a rogue AV. The sum requested to unlock the device and avoid legal consequences is USD 100 and could be paid using Green Dot MoneyPak. After the payment, a voucher code should be sent to unlock the device. There exists a legal notice that notes the payment must be made in the next 48 hours or else "appropriate" legal action will be taken. There are made numerous mistakes there that also demonstrate this is just a scam even for the non-professional users[9].

Simplocker

On 2.1 and 2.2 we had two examples of locker ransomwares, that made the access to the device not possible. A solution to unlock it without paying (as the payment was not sure if it was reliable) is to boot the device to safe mode and uninstall the corrupt application[10].

Here and on 2.4 there are presented two types of crypto ransomware, that encrypt user data. In May 2014 ESET detected[11] the first file-encrypting ransomware from Android which is considered an expected evolution as there were many that appeared for Windows, including Cryptolocker (described in the report from the 1st semester also) or Cryptowall.

After the launch, the application Android/Simplocker[12] variant A scans the files from flash drive with the extensions like: JPEG, PNG, BMP, DOC, MP4 etc.[13] and encrypts them later using the AES algorithm. It also collects valuable information from the device, like model, IMEI (the unique identification code for each mobile device), OS version and producer of the device[14]. The encryption was fairly easy to find as it was "hidden" in the binary code as plaintext, comparing to more complicated ones mentioned earlier. There is believed that this may be only a proof-of-concept (PoC) or an early development version of a malware[15].

Also, this may have been targeted against the people from Ukraine as the ransom message was written in Russian and the payment in Ukrainian hryvnia (not USD as in the last cases) with the value of 260 (with meant at that moment the value of USD 21.84). To make them hard to trace, there were requested vouchers from victims (like QIWI or MoneyXy). There was also found that they were taken pictures of the victim and displayed to "increase the scareware factor"[16].

By digging into more technical aspects, there exists a class called Constants that contains a constant variable called CIPHER_PASSWORD typed String with the hardcoded value 'jndlasf074hr' and an array of string values that contain the extensions of the files (also hardcoded here) called EXTENSIONS_TO_ADD. Also, in the FileEncryptor class there is found that the encrypted files get the extension '.enc'. Encryption is done using AES with cipher 'aes/cbc/pkcs7padding' using the key reminded above. Besides the encryption key, in the Constants class there is also an admin url 'hxxp://xeyocsu7fu2vjhxs.onion/' that is used to connect in C&C mode using Tor as proxy and send to it the IMEI (it gets using getCutImei) or model of the device. There is also created a method that keeps showing the ransom message if the Back key is pressed by the victim[17]. It is believed that the C&C server can send back the instructions to decrypt data, of course after paying the ransom. The scheme from below provides a graphic looking at what was described here.

---

[9] *Idem.*
[10] How to protect your Android device from a ransomware attack, https://blog. avast.com/protect-your-andro idfrom-ransomware
[11] The Rise of Android Ransomware, *op.cit.*
[12] Android/Simplocker [Threat Name], http://virusradar.com/en/Android_Simplocker/ detail
[13] The Rise of Android Ransomware, *op.cit.*
[14] Android/Simplocker [Threat Name], http://virusradar.com/en/Android_Simplocker/ detail
[15] The Rise of Android Ransomware https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of_ Android_Ransomware.pdf
[16] The Rise of Android Ransomware, *op.cit.*
[17] Analyzing Android 'Simplocker' Ransomware, https://www.zscaler.com/blogs/ research/ analyzing-androidsim plocker-ransomware

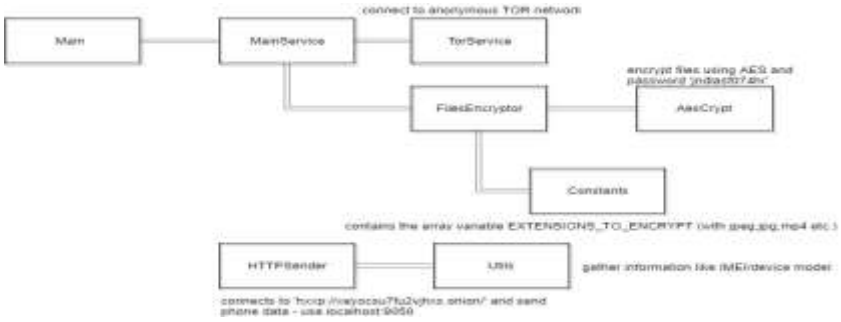

Figure 4. Ransomware main functions

Giving more coding details, there is a function named getFileNames() in FilesEncryptor class that iterates through the files and verifies if the extension is in the list of hardcoded ones. There is also here a method called intuitively encrypt() that encrypts each file found above using another encrypt() method, this time from AesCrypt class and using the cipher and password from above. It requires two parameters: the path to file to be encrypted and the output one, that is just the string path + '.enc'. For example, if the name is picture.jpg, then the output will be picture.jpg.enc. A very important aspect is the obvious deletion of the original file after encryption. There is also found in the AesCrypt the decryption() method which was presumably used when the payment was made by the user. It works in a similar way as encrypt(), using the static encryption key from above.

Now I think is important to detail how to the distribution was made when it appeared back in 2014. According to ESET[18], there were 2 ways of distributing this malware. The first consisted in hiding itself under a popular application, like an adult viewing video, video games (like Grand Theft Auto: San Andreas) or even applications like Adobe Flash Player. The second one consisted in spreading using a trojan downloader that is used, as its name suggests, to download malware. They are not very common on Android, as they are being very popular on Windows OS. Is considered that the second approach has greater odds of success than the first one to bypass the Bouncer on the Google Play app. Fortunately, this was not the case with this downloader.

There are 2 reasons for this statement[19]:

- this trojan downloader simply accesses an URL (which cannot be a malicious behavior, as most apps have this behavior). The analyzed URL did not point to a malicious apk directly. Instead, it was downloaded after it was redirected from there.
- besides access to the storage, there are no other dangerous permissions needed by the application. In most of the cases, users allow this one and do not consider it a potentially harmful one[20].

Only after a month of this discovery, there was found a new version, in English this time that displayed messages from FBI: the user was blocked due to illegal activity like software piracy, child abuse etc. (like a police ransomware). The payment ranged from USD 200 to 500 (a change from UAH) at that time and could have been done using a voucher from MoneyPak (like the fake Avast AV app)[21]. The latest variant contained a message from NSA this time by accusing the victim that he attended forbidden adult sites and asked for USD 500.

There were added here 3 new additions. The first one was the possibility to encrypt also archived files (with extensions like zip, rar or 7z)[22]. There is thought that this was done as many backups are made in this way and the users were left with nothing if this was installed. This is why they should be kept separately, on an external drive or a far better choice, the cloud. The second addition is the usage of XMPP instead of HTTP, which makes the servers to be tracer

[18] The Rise of Android Ransomware https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of_ Andr oid_Ransomware.pdf
[19] The Rise of Android Ransomware https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of_Andr oid_Ransomware.pdf
[20] *Idem.*
[21] *Idem.*
[22] *Idem.*

with difficulty. As stated earlier, from a C&C server there were sent device information and received commands to be executed. The third and most important change is the usage of non-hardcoded, unique encryption keys received directly from a C&C server. This made the decryption harder and marked "the end of trojan's PoC stage"[23].

DoubleLocker/Bankbot

The second crypto ransomware to be analyzed is DoubleLocker, that was built on the trojan Android.BankBot.211.origin[24] and firstly detailed here. Is considered a banking trojan that steals confidential information and execute C&C commands from the server, as happened with Simplocker. After installation there is seen another endless loop behavior, that continuously shows to use Google services. If the user gives up and accepts this, this trojan is added later to the device admin list and reassigns to it the default SMS app and also the screen capturing. The permissions for these exchanges are given by user's consent. Using the example from here[25], we can see that trojan reports this information to the C&C server and receives later some commands:

Figure 5. Info sent to C&C server

In the figure from above there can be seen that there are sent the following: the IMEI of the mobile phone and the operating system version along with build with the action reg (probably register). The next POST request consists in polling the server (action=poll) from the device with the IMEI from above. Using this, the device is registered to receive from the server different kinds of commands like[26]:

- url: open a link;
- server: change the C&C address;
- sms_history: send the SMS messages from device to server;
- call_log: send also details regarding the installed apps on the device, contact list and phone data.

Periodically, this trojan connects to the C&C server found at http://217.***.***.92/jack.zip and sends a post request with header _AUTH being the IMEI. The response is a config file, that contains the applications to be attacked (targeted ones) with the required actions. For example:

- lock-attack (lock_av): presses automatically the button Back when such app is launched;
- window or full screen: to be used to display windows for payment services with input forms for different banks[27] and obtain the credentials.

Moreover, there are made trackings on each app launched and each action performed on it, like menu elements and logging keystrokes. This data is sent to server with the action grabbed_data (also contains the IMEI to identify it) and added the name of the app and what was "grabbed"[28].

Figure 6. Grabbed data sent to C&C server

[23] *Idem.*
[24] *Idem.*
[25] Android.BankBot.211.origin, https://vms.drweb.com/virus/?i=15465665&lng=en
[26] Android.BankBot.211.origin, https://vms.drweb.com/virus/?i=15465665&lng=en
[27] Android DoubleLocker ransomware encrypts data, changes device PIN, https://www. helpnetsecurity.com/ 2017/10/16/android-doublelocker/
[28] *Idem.*

There was even found a keylogger that is using an ingenious way of finding the password of bank accounts: each time the user presses a character of it, the trojan takes a screen capture and sends to server (the char is seen in plain the first second then is censored with * or a filled circle)[29]. The only way to be removed (as it can be easily uninstalled like any other application) is to reboot the device in safe mode, access the list of admins and remove this trojan from it.

More details about DoubleLocker

Comparing with Bankbot, this trojan (called Android/DoubleLocker.A[30]) does not collect banking information, instead it locks the device (by changing the pin number) and also encrypts user data. But, like it is distributed on compromised websites, masked under an Adobe Flash Player update (a disguised program)[31]. After installing and launching it, it requests the accessibility service to be enabled in order for the ransomware to gain admin rights and become a default home application. Being a default home app means that each time the user presses the home button, the malware is activated and prevent the victim to bypass the lock screen. Is considered to be the first ransomware for Android that misuses the accessibility services by having a "a combination that has not been seen previously in the Android ecosystem"[32].

As stated in the first report, the device is locked using a random pin number, stored nowhere on the device or the C&C server and to unlock the phone the ransom has to be paid in order to reset the value by the server. The second step, after locking the device, is to encrypt the data using AES[33].

There were not found tools available to decrypt the data and the only possibility was to do a factory reset. To remove the locker part, a reboot to safe mode had to be done like in the case of Bankbot.

Lockerpin

The last malware that is treated here is Lockerpin (identified as Android/Lockerpin.A[34]), that was discovered in August 2015 and is a step further in comparison with the first 2 fake AVs. There the lock screen functionality was achieved by constantly bringing the window in foreground in an endless loop. The solution the get rid of those was fairly simple and was presented above (safe mode). This is not the case here as the solution to remove it is by having previously rooted the device or has an MDM installed that can reset the pin password[35]. It uses the device admin rights (if provided by the user) to set or reset the pin of the device. This malware has also used the adult app mask to spread on the users.

In the first versions, the request for admin rights was done as earlier, but on the later versions in was overlaid with the trojan's malicious window that says a patch needs to be installed. Under the "Continue" button of this installed stays hidden the "Activate" one for the admin rights. As seen before, after the installation there can be seen the infamous FBI message that requests a ransom of USD 500 for doing fictional "nasty things". After this message appears, the pin is set or reset to a four-digit number and not stored anywhere[36].

---

[29] *Idem.*

[30] DoubleLocker: Innovative Android Ransomware, https://www.welivesecurity.com/2017/10/13/doublelockerinnovative-android-malware/

[31] Android DoubleLocker ransomware encrypts data, changes device PIN, https://www. helpnetsecurity.com/2017/10/16/android-doublelocker/; DoubleLocker: This Android Ransomware Activates Every Time You Press Home Button, https://fossbytes.com/doublelocker-android-ransomware-bitcoin/.

[32] DoubleLocker: Innovative Android Ransomware, https://www.welivesecurity. com/2017/10/13/doublelockerinnovative-android-malware/

[33] DoubleLocker: This Android Ransomware Activates Every Time You Press Home Button, https://fossbytes.com/doublelocker-android-ransomware-bitcoin/

[34] LockerPin Ransomware Resets PIN and Permanently Locks Your SmartPhones, https://thehackernews.com/2015/09/android-lock-ransomware.html

[35] The Rise of Android Ransomware, *op.cit.*; LockerPin Ransomware Resets PIN and Permanently Locks Your SmartPhones, https://thehackernews.com/2015/09/android-lock-ransomware.html

[36] Mobile vs Desktop Usage in 2018: Mobile takes the lead, https://www.stone temple.com/ mobile-vs-deskto pusage-study/

There is also considered here a self-defense mechanism as it wants to keep the acquired admin rights. If the victim wants to remove them for this trojan, this fails as it has a call-back function to reactivate them each time the user does that. Also, this ransomware tries to kill the running AV on the device when the user tries to activate the admin rights for it. There were found 3 types of mobile AV software: Dr.Web, Avast and ESET[37].

```
if(v26.get(v19).processName.contains(((CharSequence)v11))) {
    this.killProc(v26.get(v19));
    this.KickAv(v17, v26, v19);
}
```

Figure 7. Snippet of code that tries to kill the AV running on the device[38]

Another important aspect to be noted here is the fact that most of the affected devices are from USA (~72% of them) which means there is a shift from Ukraine (see Simplocker) or Russia in order to make greater profits from them.

As most users do not have a rooted device, the solution of getting rid of this malware was by doing a factory reset of the device[39].

Solution for protection against ransomware on Android

After analyzing these ransomware attacks that happened during the last 4-5 years, a solution can be provided to protect the mobile devices with Android OS against them. As presented in the first report, there are 2 types of analysis that can be done here:

- **static**: have an updated list of signatures for each ransomware identified until that moment;

- **dynamic** (the most interesting one): based on a known behavior of the last types (some of them reminded here) a behavioral graph can be computed and inserted to the AV. There can be analyzed different paths from it and if one is found on the app that is currently installed a notification can be shown and the user can be advertised. It can also be updated by analyzing new behavior of the newer ransomware malware.

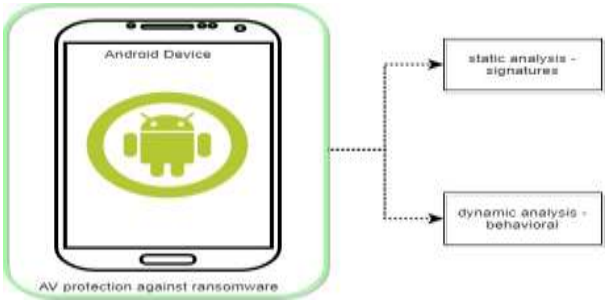

Figure 8. Mechanism of protection for the smartphone against ransomware. Mitigation techniques

As the number of smartwatches with Android Wear increases, they can be considered as a future targeted device[40]. Currently, for this report there was not analyzed this OS model for Android, but I think that some analysis should be made in the next semester to find how they are affected and what mitigation can be done there. This was tested successfully by Symantec in 2015: a paired smartwatch with an infected Android smartphone device resulted in pushing it to the wrist device[41].

---

[37] The Rise of Android Ransomware, *op.cit.*

[38] *Idem.*

[39] LockerPin Ransomware Resets PIN and Permanently Locks Your SmartPhones, https://thehacker news. com/2015/09/android-lock-ransomware.html

[40] Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi Mohammed Ali, Imran, M.,&Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks

[41] The dawn of ransomwear: How ransomware could move to wearable devices, https://www.symantec.com/ connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices

Conclusion

There are many types of ransomware attacks carried out by hackers in the last years, the most important ones being included in this report. A mitigation against them must be provided by using static and dynamic analysis.

Acknowledgements

This research work was supported by a grant on the Romanian Ministry of Innovation and Research, UEFISCDI, project number 8SOL/2018 within PNCDIII, project code: PNIII-P2-2.1-SOL-2017-09-0102, project name: Integrated Information System for Management of Activities (IISMA) (http://siima.pub.ro/en/home/).

BIBLIOGRAPHY

1. *Mobile Operating System Market Share Worldwide*, http://gs.statcounter.com/os-marketshare/mobile/worldwide
2. *Google announces over 2 billion monthly active devices on Android*, https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users
3. *The best Wear OS smartwatches: LG, Fossil, Huawei, Polar and more*, https://www.wareable.com/smartwatches/best-android-watch
4. *Mobile vs Desktop Usage in 2018: Mobile takes the lead*, https://www.stonetemple.com/ mobile-vs-desktopusage-study/
5. *The Rise of Android Ransomware*, https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of_Android_Ransomware.pdf
6. *How to protect your Android device from a ransomware attack*, https://blog.avast.com/protect-your-androidfrom-ransomware
7. *Android/Simplocker [Threat Name]*, http://virusradar.com/en/Android_Simplocker/ detail
8. *Analyzing Android 'Simplocker' Ransomware*, https://www.zscaler.com/blogs/research/analyzing-androidsimplocker-ransomware
9. *How To Dissect Android Simplelocker Ransomware*, https://securehoney.net/ blog/how-to-dissect-androidsimplelocker-ransomware.html#.W4sYmegzbIU
10. *Android.BankBot.211.origin*, https://vms.drweb.com/virus/?i=15465665&lng=en
11. *Android DoubleLocker ransomware encrypts data, changes device PIN*, https://www.helpnetsecurity.com/2017/10/16/android-doublelocker/
12. *DoubleLocker: This Android Ransomware Activates Every Time You Press Home Button*, https://fossbytes.com/doublelocker-android-ransomware-bitcoin/
13. *DoubleLocker: Innovative Android Ransomware*, https://www.welivesecurity.com/2017/10/13/doublelockerinnovative-android-malware/
14. *LockerPin Ransomware Resets PIN and Permanently Locks Your SmartPhones*, https://thehackernews.com/2015/09/android-lock-ransomware.html
15. YAQOOB, I., AHMED, E., REHMAN, M. H. ur, AHMED, A. I. A., AL-GARADI Mohammed Ali, IMRAN, M., & GUIZANI, M. (2017). *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks
16. *The dawn of ransomwear: How ransomware could move to wearable devices*, https://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices