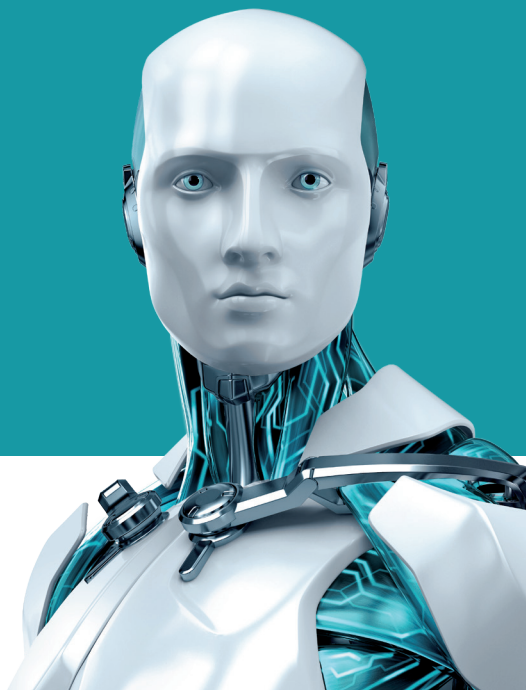
ANDROID RANSOMWARE: FROM ANDROID DEFENDER TO DOUBLELOCKER

Authors:
Robert Lipovský, Senior Malware Researcher
Lukáš Štefanko, Detection Engineer



ENJOY SAFER TECHNOLOGY™

CONTENTS

SUMMARY

2017 was without a doubt the year of ransomware. Users and businesses worldwide had to cope with the fallout of massive campaigns such as Petya or WannaCryptor and had to put up with damages that easily surpassed a billion mark[1].

However, it wasn't just ransomware on PCs that made headlines, as authors of Android malware were also looking for new revenue streams.

One of the most prominent novelties seen over the course of 2017 was the misuse of Android's accessibility services, a functionality designed to help users with disabilities. At first, this kind of abuse was typical of Android banking malware, however, by the end of the year, it spilled over also to the Android ransomware scene.

Probably the most publicly known case of this behavior – found by ESET researchers – was the accessibility-abusing ransomware family dubbed DoubleLocker. A dedicated chapter of this paper details this malicious code, documenting its primary infection vector as well as its unique two-fold extortion method.

Despite these new developments, the most popular attack technique remains screen-locking followed by a ransom demand. According to ESET telemetry, the most frequently detected variants of Android ransomware using this extortion method belonged to the Android/Locker family.

In this paper, readers will also find definition of Android ransomware, data from ESET's detection telemetry as well as

1 WannaCryptor attack losses could reach $4 billion. Publicly admitted damage caused by Petya ransomware also passed a $1 billion mark.

description of the current trends connected to this cyberthreat. The main section details the most noteworthy Android ransomware examples since 2014 with focus on the most recent cases.

As has been a good tradition since we started publishing this report three years ago, the final chapter offers updated advice for Android users detailing best practice helping them to stay secure.

ANDROID RANSOMWARE

Ransomware, as the name suggests, is any type of malware that demands a sum of money from the infected user while promising to "release" a hijacked resource in exchange. On Android, there are three general categories of malware that fall under this label:

- *Lock-screen ransomware*
- *PIN lockers*
- *Crypto-ransomware*

In lock-screen types of ransomware, the hijacked resource is access to the compromised system that is blocked by an image fully covering the screen. PIN lockers work in a similar fashion, only to lock the device, they misuse the built-in protective mechanism of the operating system and change the combination unlocking the device to a value unknown to the user. Finally, in case of file-encrypting "crypto-ransomware", this hijacked resource is user's data that gets encrypted.

While having been around for quite some time, ransomware first became very prevalent on the Windows platform in 2013. Since then, it has been growing and evolving, causing trouble both to individuals and businesses.

The appearance of Android ransomware and its future functionality was well anticipated, as Android malware writers were known to introduce malware that has proven successful on Windows to the mobile platform. Since we've first started observing it in 2013, however, black-hats have also developed an array of techniques that are specific to the Android platform.

Also the amount of ransomware on Androids has grown until 2016. According to ESET LiveGrid®, the largest spike has been observed in the first half of 2016. Past 12 months have brought a change to this trend. Despite the continuously increasing amount of Android malware, the number of ransomware targeting this platform has been in decline.

However, as ESET telemetry shows, the recent drop might have only been temporary as several Android ransomware detection spikes were observed towards the end of the year, including the most interesting case of the period – Android/DoubleLocker.

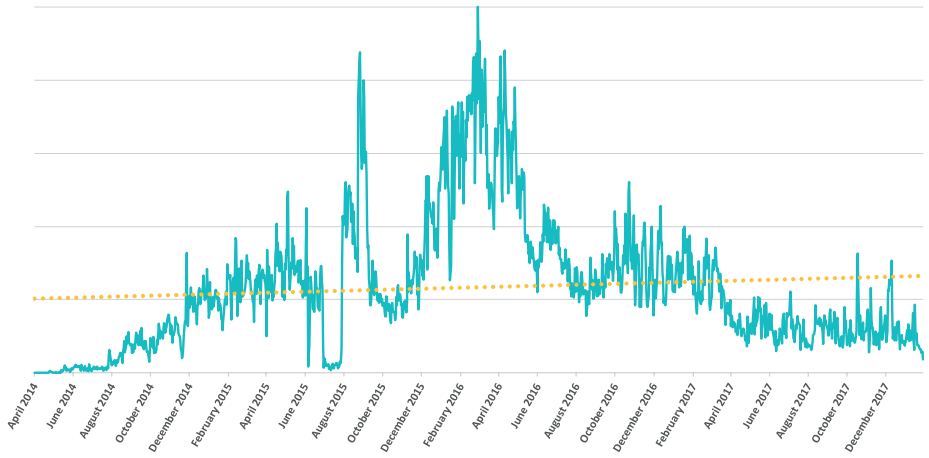


Figure 1 Android ransomware detection trend, according to ESET LiveGrid®

INFECTING AN ANDROID DEVICE

Android ransomware – as well as most other malware types – typically fits the definition of a trojan horse: it spreads by masquerading as a legitimate application. Popular applications, such as trending games or pornography-related apps, are often chosen to increase the likelihood that the victim will download the malware.

In some cases, the malicious APKs bear only the name and icon of the legitimate application, whereas in other cases, malware writers take existing applications and add malicious code, keeping the original functionality. For malware that doesn't inherently rely on a visual manifestation like ransomware does (backdoors or SMS trojans, for example), this increases the chances that malicious behavior will go unnoticed. Of course, since such modifications break the digital signature of the application package, it has to be re-signed and distributed under a different developer account than the original.

ESET experts also documented Android ransomware spreading via email. Attackers have been using social engineering to manipulate victims into clicking on a malicious link in email messages and have been redirecting them to an infected Android application package (APK).

Over the past few years, black-hats have also been putting increased effort into making the infiltration as stealthy as possible. This led them to encrypt the malicious payloads and bury it deeper in the application. A very popular choice for this purpose is the assets folder, typically used for pictures or other legitimate contents. Some of the infected applications seem to have no outside functionality, but in reality work as a decryptor that decrypt and run the hidden ransomware payload. However, using technically more advanced techniques, such as exploit-driven drive-by downloads, is not very common on Android.

Apart from a single exception, none of the ransomware examples described in this paper were found on the official Google Play store. However, there have been numerous cases of malware successfully bypassing Google's ever-improving security measures. ESET researchers have found and reported to Google hundreds of samples of Android malware, including fake apps and fake AV scareware, banking malware, credential-phishing spyware, trojans used for click-fraud, backdoors, and various kinds of PUAs (Potentially Unwanted Applications).

MALWARE C&C COMMUNICATION

After a successful installation, most Android malware "reports home" to a Command & Control (C&C) server. In some cases, the reporting serves only to track the infection, sending back basic device information, such as the device model, IMEI number, and device language. Alternatively, if a permanent C&C communication channel is established, the trojan can listen to and execute commands sent by the malware operator(s). This creates a botnet of infected Android devices under the attacker's control.

Some examples of commands supported by Android ransomware, outside its primary scope of locking the device or encrypting its contents and displaying a ransom message, include:

- *wipe the device*
- *reset the lock screen PIN*
- *open an arbitrary URL in the phone's browser*
- *send an SMS message to any or all contacts*
- *lock or unlock the device*
- *steal received SMS messages*

- *steal contacts*
- *display a different ransom message*
- *update to a new version*
- *enable or disable mobile data*
- *enable or disable Wi-Fi*
- *track the user's GPS location*

The usual communication protocol used is HTTP. In a few cases, we've also seen malware communicating with its C&C via Google Cloud Messaging. This service enables developers to send and receive data to and from apps installed on an Android device. A similar protocol, also used by Android malware, is Baidu Cloud Push. Some malware samples we've analyzed have used Tor .onion domains, or the XMPP (Jabber) protocol.

Alternatively, Android trojans can receive commands, as well as send data using the built-in SMS functionality. The popularity of social-networks has also brought cases where the attackers misused ***Twitter accounts*** to command and control their Android botnet.

MALWARE PERSEVERANCE

Compromising a victim's device with Android malware is not a trivial task for attackers. Even for users without anti-malware solutions like ESET Mobile Security, there are Google's own defensive measures. Naturally, once attackers succeed in overcoming these hurdles, they want to make sure that their malevolent code stays on the device for as long as possible.

Over the years, Android malware authors have developed a number of ways to achieve this.

Some Android malware families, for example, attempt to kill processes that might hamper their further activity. Such processes typically belong to anti-malware applications or are a part of Android's self-defense system.

One of the most universal ways of ensuring persistence on the compromised device is obtaining device administrator privileges. To obtain the privileges, the attackers need to trick the victims into activating the malicious app as device administrator. The techniques we've seen being used to achieve this range from mimicking trustworthy applications to using deceptive overlay techniques, also known as click jacking or tap jacking.

Before any app that has been able to obtain device administrator privileges can be uninstalled, the privileges first need to be revoked. Some malware additionally uses the extra permissions only available to Device Administrator applications to set or change the lock screen PIN.

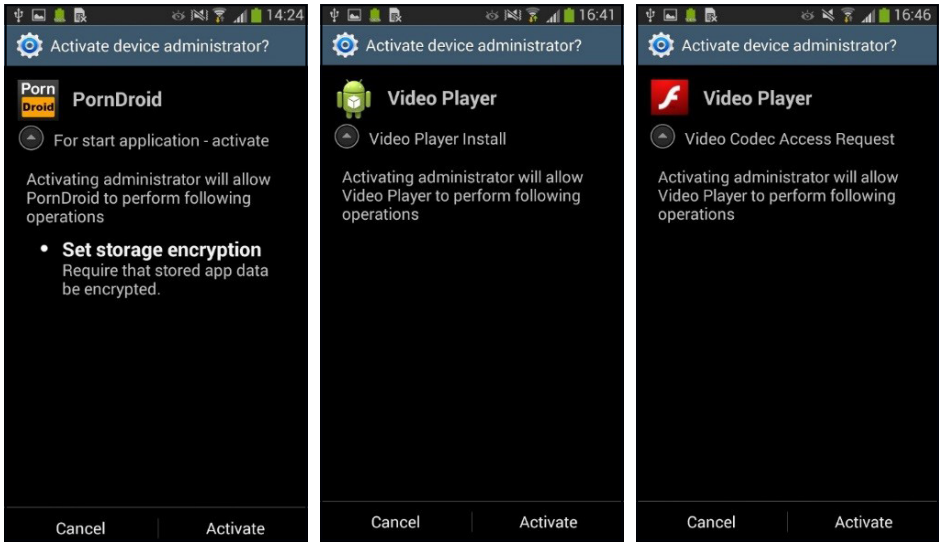


Figure 2 Examples of Android malware requesting Device Administrator privileges

2017 has also seen a rise of a new approach towards gaining control over compromised devices – misusing Android Accessibility services. This native Android functionality was originally designed to help users with disabilities to fully use their devices and apps. Yet, under attackers' control, even a well-meant technology can quickly turn into a dangerous tool fulfilling all kinds of malicious objectives.

By misusing the Android Accessibility services black-hats are able to:

- *activate device administrator rights*
- *set their malicious app as "Home application"*
- *harvest user credentials and sensitive information*
- *intercept victim's data*
- *use layover windows to manipulate victim to harmful actions*
- *download and install malevolent payload, unwanted applications or mobile malware*
- *log user key strokes*

Successful compromise of accessibility services can also allow the attackers to gain control over the victim's device and **intercept SMS messages used as second factor of authentication**, effectively weakening this user-protective measure.

Such attacks have been observed in the wild on multiple occasions over the past 12 months. Most of these campaigns were distributing banking malware, trying to obtain victims' banking credentials, steal credit card numbers, or gain access to victims' bank or PayPal accounts.

However, it wasn't just the "bankers" that misused this mechanism to target mobile device users, as Accessibility services seemed to be interesting for creators of Android ransomware as well. ESET researchers discovered one of the most prominent campaigns misusing the service in the October 2017, naming it DoubleLocker. More details about this ransomware family are provided in one of the following chapters.

PROMINENT ANDROID RANSOMWARE CASES

The Android ransomware scene has transformed a lot since its beginning. The initial appearances on this platform were cases in which extortion functionality was added to fake antiviruses, scaring the victim into believing that their device is infected. Similar tactics was used later by the so-called police ransomware variants.

However, over the years, the cybercriminals have diversified their toolkits and added misuse of the native screen-locking functionality of Android devices as well as data encryption seen in a growing number of Filecoder and Diskcoder families on PCs to their portfolio.

The following section describes the most noteworthy cases of Android ransomware found and analyzed by ESET researchers since 2013, the year of Android ransomware's debut:

Doublelocker

One of the most innovative ransomware families was discovered by ESET researchers in the fall of 2017, dubbed DoubleLocker. While built on the foundations of a previously seen banking trojan, the malware didn't have the functions related to harvesting victims' banking credentials nor did it try to wipe their accounts directly. Instead, it has received two powerful tools for extorting money.

DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data it finds in them – a unique combination that has not been seen previously in the Android ecosystem.

The malware is distributed mostly as a fake Adobe Flash Player through compromised websites. Once launched, the app uses its disguise to request the activation of accessibility services. If accepted by the user, DoubleLocker misuses the permissions to activate device administrator rights and sets itself as the default Home application. This trick allows the ransomware to be activated whenever the home button gets clicked.

DoubleLocker creates two reasons for the victim to pay:
First, it changes the device's PIN to a random value that the attackers neither store nor send anywhere, making it impossible for the user or a security experts to recover it. After the ransom is paid, the attacker can remotely reset the PIN and unlock the device.

Second, DoubleLocker encrypts all files in the device's primary storage directory. It utilizes the AES encryption algorithm, appending the extension ".cryeye". As the encryption is implemented properly, there is no way to recover the files without receiving the encryption key from the attackers.

The ransom has been set to 0.0130 BTC (approximately USD 54 at time of discovery) and the message highlights that it must be paid within the next 24 hours. The only good news is that victims don't have to comply with the attackers' deadline – after the time runs out, the encrypted files are not deleted or damaged in any (additional) way.

Unfortunately, the only way to restore the full functionality of a device after a DoubleLocker infection is via a factory reset. In case of rooted devices, there is a method to get past the PIN lock, but for it to work, the device needs to be in the debugging mode before the ransomware is activated. As for the data stored on the affected device, there is currently no way to recover it.

It is important to note that due to its roots, this malware could easily be turned into what could be called a "ransom-banker" – a two-stage malware that first tries to wipe your bank or PayPal account and subsequently locks your device and data to request a ransom. A test version of similar malware (although not part of DoubleLocker family) was already spotted in May 2017.

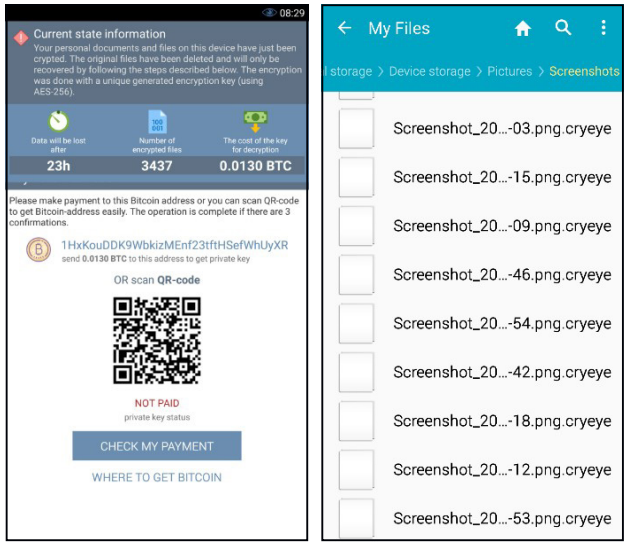


Figure 3 DoubleLocker locks the devices as well as encrypts its contents

Charger

At the beginning of 2017, a remotely controlled backdoor trojan with a device-locking capability was discovered – surprisingly – in the Google Play store. Disguised as an "energy saving" app called EnergyRescue, the malware, dubbed Android/Charger, was trying to steal user data as well as take control of the device in multiple ways.

ESET's analysis of the malware showed that it could harvest contacts and create a list of all installed apps; however, despite possessing this functionality, it seems that Charger never sent the data to the attackers.

On top of that, it could extract and send to the attackers all text messages from the infected device, including those in the inbox, sent and draft folders, send a photo of a victim, update itself and activate administrator rights. Attackers managed these functions using an HTTP protocol to control the infected device.

Based on the commands of the attacker, the malware was also able to lock or unlock infected devices and demand a ransom of 0.2 Bitcoin. This means that Charger has joined an exclusive club as one of the first pieces of lock-screen ransomware that has made it past Google Play's security checks.

Jisut

Jisut was a strange ransomware family first observed by ESET researchers back in 2014. It attracted attention mostly because it locked devices but did not demand any ransom. Their only visible activity was a change of wallpaper or a sound playing in the background, strengthening the presumption it was created mainly as a prank.

Some of the later variants however, have added the "money-making" functionality and asked victims to pay a ransom in exchange for getting their devices unlocked. To make the process simpler and more straightforward, the attackers added a QR code allowing the infected user to either message the attacker or make a direct payment.

One of the Jisut ransomware variants seen in the beginning of 2017 also had a special and curious ability: it demanded ransom by using voice message, making it the first "speaking Android ransomware" detected in the wild. After Jisut was launched on the compromised device, a female voice speaking Chinese "congratulated" the victim and asked for 40 Yuans (approx. 6 dollars) to unlock the screen.

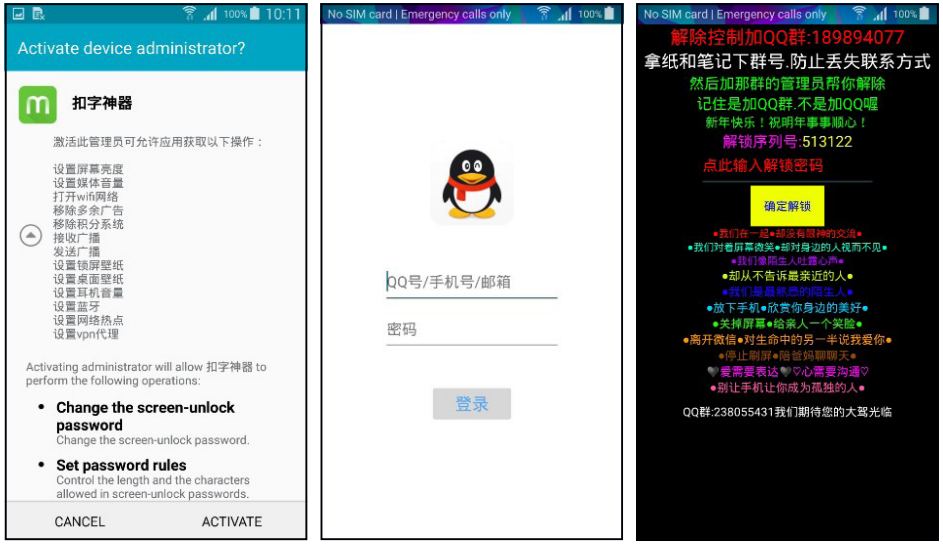


Figure 4 Android/Jisut requests admin rights, harvests QQ credentials and on top of locking the screen demands the ransom by voice message.

The whole Jisut malware family is unlike any other known LockScreen ransomware. One of Jisut behaviors was to create a full screen black overlay that made the device appear locked or switched off. When the

user brought up the menu to shut down or restart the device, a joke message was displayed. Some samples featured a variation to the "talking ransomware" activity: they played music from the famous shower scene from Alfred Hitchcock's Psycho, while vibrating the device in an infinite loop.

Another Jisut variant asked the user to click a button that says "I am an idiot" 1000 times. Even if this condition was met nothing happened; the counter only reset to zero and let the frustrated user click indefinitely.

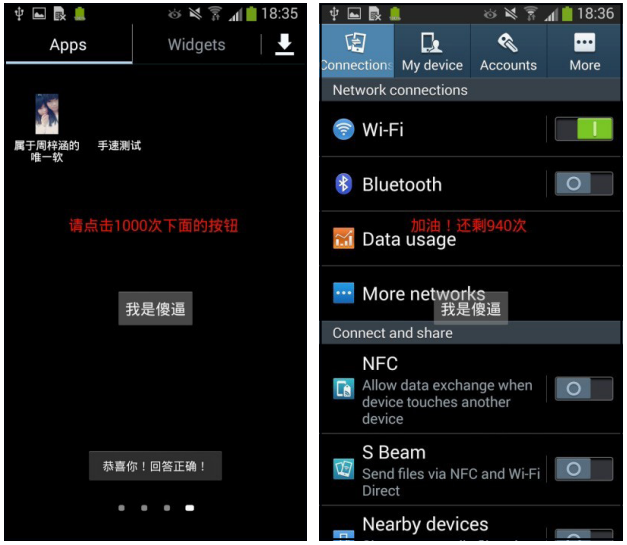


Figure 5 Android/LockScreen.Jisut: "Please click the button below 1000 times"

In addition to the described silly behavior, most Android/LockScreen.Jisut variants also contained harmful functionality. They were able to set or change the device lock-screen PIN or password. Some variants didn't rely on the legitimate built-in Android lock screen functionality but displayed their own full-screen window mimicking the lock screen.

On top of creating an all-around strange ransomware, the gang behind Jisut also took an unusual approach to anonymity – the ransomware nag screens included contact information leading to profiles on Chinese social network QQ. They also urged victims to contact the authors in order to get their files back. If the QQ information was true, the malware operators behind Jisut were Chinese youths of 16 to 21 years old (at the time of discovery).

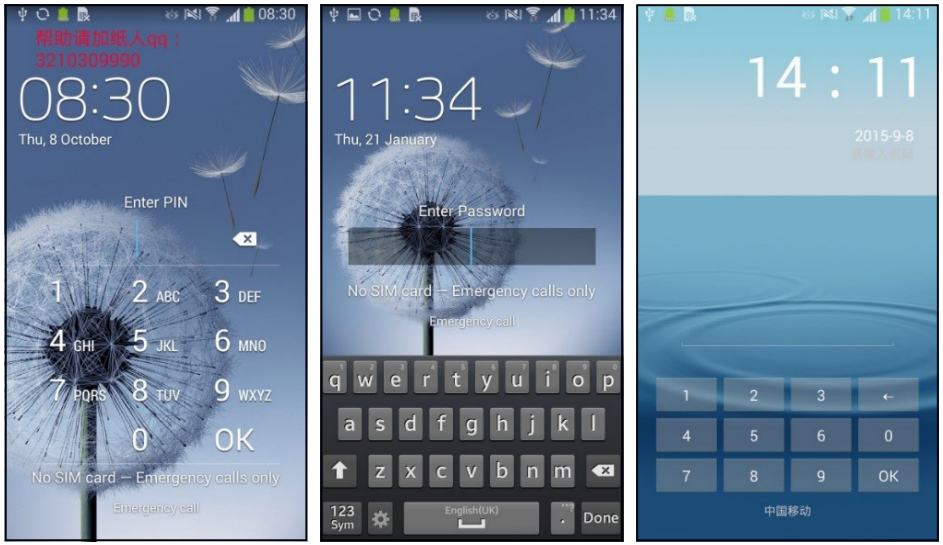


Figure 6 Device locked with PIN or password by Android/LockScreen.Jisut

Figure 7 More vivid custom lock-screens with the malware author's QQ number

In addition to the ransomware aspect, some Jisut variants had an SMS-sending fuctionality, in which a message with a URL link to the malware was sent to all victims's contacts.

As for the prevalence, ESET detected hundreds of Jisut variants shortly after its first appearance in 2014. Although each variant behaved somewhat differently, they were all based on the same code template. A noteworthy spike in activity was observed about two years later (in 2016), when the number of Jisut detections doubled in year over year comparison.

Lockerpin

In early Android lock-screen trojans, the screen-locking functionality was usually achieved by constantly bringing the ransom window to the foreground in an infinite loop. While various self-defense mechanisms were implemented to keep the user locked out, it wasn't too difficult to get rid of the malware and thus unlock the device[2].

With Android/Lockerpin, discovered by ESET in August 2015, malware writers stepped up their game and for the first time leveraged the built-in Android PIN screen locking mechanism. Lockerpin was able to set a PIN on the device, or even change it if it was already set, provided that the victim has granted the malicious app Device Administrator privileges.

If the attackers were successful, it was only possible to remove the PIN lock screen if the device had previously been rooted or had a Mobile Device Management (MDM) solution installed capable of resetting the PIN. Otherwise, the only option was a factory reset, deleting all data on the device.

Lockerpin typically spread disguised as an app for viewing adult videos. Once installed, the malware tried to obtain device administrator status. While earlier versions of the Android/Locker family relied on the user willingly activating the elevated privileges, later versions used a much more covert tap-jacking technique, whereby the system device admin activation window was overlaid with the trojan's window pretending to be an "Update patch installation". The seemingly legitimate Continue button was perfectly placed over the underlying and malicious Activate button was able to grant the malware device administrator privileges.

2 User could use Android Debug Bridge (ADB) or deactivate Device Administrator rights and uninstall the malicious application in Safe Mode.

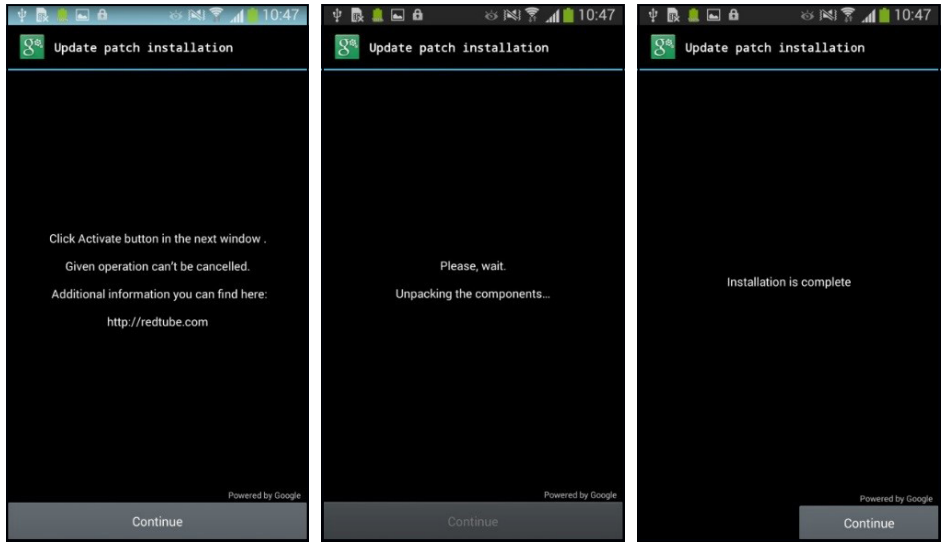


Figure 8 Android/Lockerpin covertly obtaining Device Administrator rights by tap-jacking

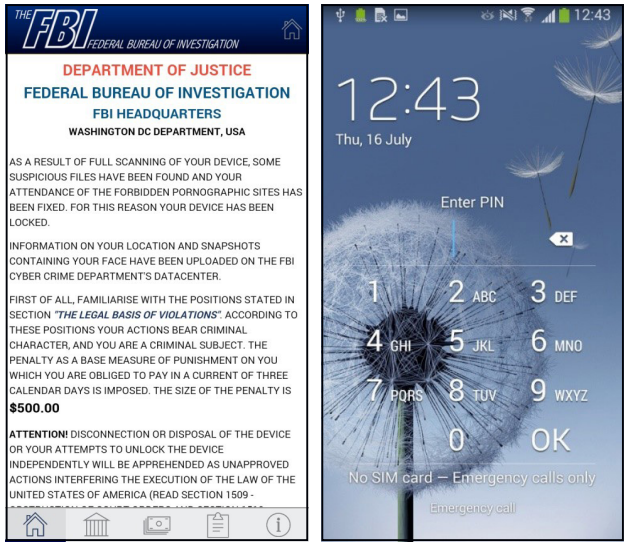


Figure 9 Device locked by Android/Lockerpin

After installation, the user is shown a typical bogus FBI message requesting a $500 ransom for allegedly viewing and harboring forbidden pornographic material. After a specified time delay following the display of the ransom message, the PIN is set (or changed) to a four digit number that's generated randomly and not sent to the attacker. Some variants of Lockerpin have the functionality to remove the PIN lock by resetting it to a zero value.

As for persistence, Android/Lockerpin introduced an aggressive self-defense mechanism to retain its device administrator privileges, using a call-back function to reactivate the privileges immediately after removal is attempted. As an extra layer of self-protection, the ransomware also attempted to kill running AV processes when the user tried to deactivate its device admin rights. The trojan tried to protect itself from three mobile anti- virus applications: ESET Mobile Security and Android solutions by Avast and Dr.Web.

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

com.eset
com.avast
com.drweb
com.android.settings

Figure 10 Android/Lockerpin attempting to kill running AV processes

The malware did not succeed in killing or removing ESET Mobile Security. Lockerpin attempts to kill the com.android.settings process in order to prevent standard uninstallation of the malware through Android's built in application manager.

Simplocker

In May 2014, file-encrypting crypto-ransomware was the only missing kid on the "Android malware block" – until a family that ***ESET dubbed Android/Simplocker appeared***. This was an expected evolution, as at that time, crypto-ransomware had already established itself as a widespread threat on the Windows platform.

The name for the ransomware was inspired by the trivial way in which its damage could be undone – the key needed for decryption of the files was hardcoded inside the binary as plain text. For this reason, we also believed that Simplocker's first variant (detected by ESET as Android/Simplocker.A) was either just a proof-of-concept or an early development version of a more serious threat.

It only took a month before ESET systems detected new and more sophisticated variants.

Android/Simplocker typically tried to trick the user into installing it by using a camouflage of a legitimate and popular application, but was also seen using a more cunning spreading mechanism through trojan-downloaders – small programs whose sole purpose is to download other malware. This way a dangerous malware can avoid the attention of Android market application scanning (such as Bouncer on Google Play).

Furthermore, in the examples we've analyzed, the URL contained within the app didn't point to the malicious Simplocker APK package directly. Instead, the trojan was served after a redirect from the server under the attacker's control. We have not seen Simplocker spreading through the official Google Play store.

The ransom message in the early Simplocker variants was written in Russian and the payment demanded was in Ukrainian Hryvnias, so it's fair to assume that the threat was targeted against Android users in Ukraine.

However, after the first month a new variant detected by ESET as Android/Simplocker.I already displayed ransom screens in English. The victim was led to believe that the device was blocked by the FBI or the NSA after detecting illegal activity – typical behavior of police ransomware. The demanded ransom was between $200 and $500 with victim being instructed to pay it using a MoneyPak voucher.

Like some of the previous Simplocker variants, this one also used the scareware tactic of displaying the camera feed from the device. In addition to encrypting documents, images and videos on the device's SD card, the trojan also encrypted archive files: .ZIP, .7z and .RAR.

Figure 11 Android/Simplocker ransom messages in English

More advanced Simplocker variants also asked to be installed as device administrator, which made them a lot more difficult to remove, since the user first had to revoke the applications' device administrator rights before uninstalling them. And that's rather difficult to do when the ransomware is locking your screen.

Another noteworthy change was that the malware started to use the XMPP (Extensible Messaging and Presence Protocol) protocol (Jabber) for communication with its C&C server, which made the C&C more difficult to trace. A third type of C&C server addressing used by some Simplocker variants were Tor .onion domains.

The most important step in Simplocker's evolution was in the encryption keys used by the malware to encrypt the victim's files. A few months after the initial versions, we spotted Simplocker variants that used unique cipher keys generated and sent from the C&C server. This marked the end of the trojan's proof-of-concept stage and made the decryption of the hijacked files much more complicated, if not impossible.

Back to where it started: fake AVs and police ransomware

This leads us to the beginnings of the Android ransomware. In the early days this scene was dominated mostly by screen-locking malware and malicious code disguised as one of the law enforcement agencies.

The probably first actual ransomware targeting Android platform was spotted by ESET researchers in mid-2013, dubbed Android Defender and detected by ESET systems as Android/FakeAV.B.

The app tried to trick the victims into believing that their device is infected with malware – a critical problem that can only be solved by purchasing the "full version" of its antivirus features. Unlike older fake AV apps that relied on persuasion in demanding payments from their victims, Android Defender renders the affected device unusable by displaying a full-screen window with hardcore pornographic images that can only be removed by proceeding to the payment screen.

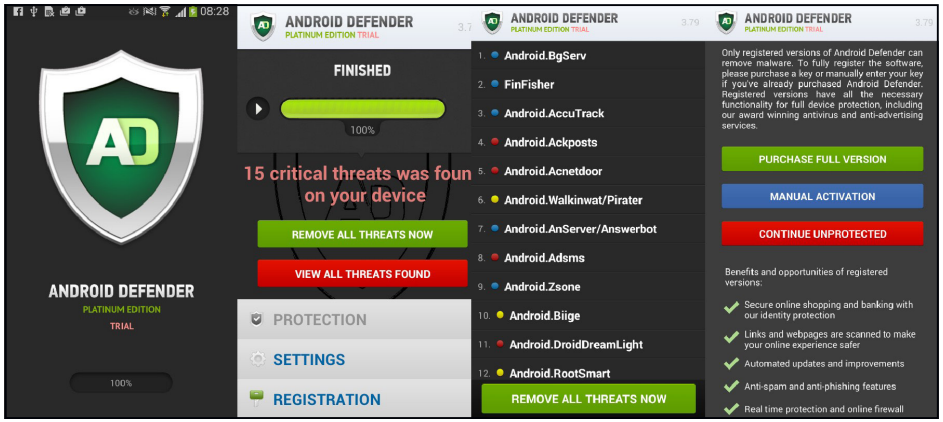


Figure 12 Android Defender locks the screen displaying pornographic images

Another early fake AV ransomware example, detected by ESET as Android/FakeAV.E, attempted to extort money from its victims using a rather odd combination of tricks and disguises.

The ransomware spread by pretending to be a mobile app for the adult video website PornHub, and then moved on to misuse the name of a legitimate Android security application from Avast[3], claiming that a whole barrage of threats has been detected on the device. Again these threats could only be removed by purchasing the "full version" of the app.

3 The fake AV is in no way whatsoever affiliated with Avast Software.

The final part of the fraud, the ransom message screen, completes the confusing narrative of this ransomware: rather than having to pay for the full version of the fake AV, the victim is prompted to pay a $100 fine to unlock the device and "avoid other legal consequences".

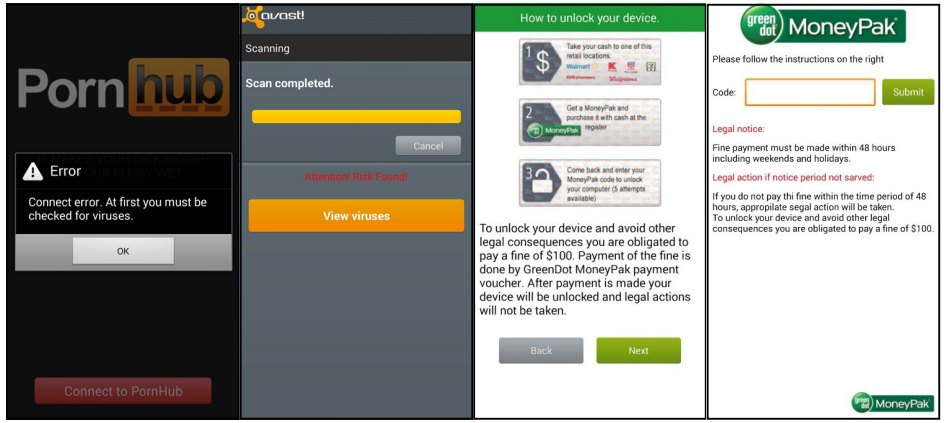


Figure 13 Various disguises and ransom screens of Android/FakeAV.E

Many of ransomware variants seen at that time fell into the category of so-called police ransomware. It claimed that the device has been locked by a local law enforcement agency because illegal content or activity has been detected. The ransom messages sometime quoted Criminal Code articles but said that the user can get away by paying a fee. Police ransomware often used IP-based geolocation in order to "customize" the infection for the user with banners of local law enforcement agencies.

The first samples of police ransomware on Android appeared in the first half of 2014 and were targeted against Russian speaking Android users. Shortly after, location-aware variants appeared, as did variants in the English language. ESET detects the police ransomware examples above as variants of Android/Koler or Android/Locker.

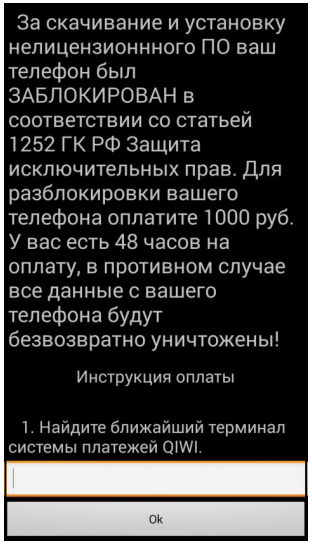


Figure 14 First police ransomware variants were targeting Russian-speaking Android users

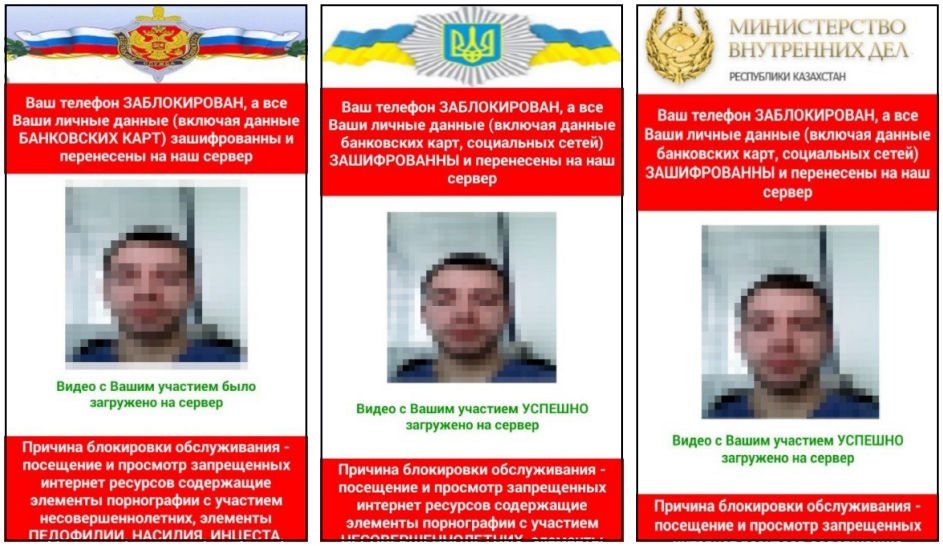


Figure 15 Android/Locker variants capable of displaying a camera shot and adjusting the ransom screen based on the user's location

HOW TO KEEP YOUR ANDROID PROTECTED

For users of Android devices, it's important to be aware of ransomware threats and to take preventive measures. Among the most important active measures to take are:

1. *Avoid unofficial app stores*
2. *Use a mobile security app installed and kept up-to-date*
3. *Have a functional backup of all important data from the device*

Chances are that users who take appropriate measures against ransomware will never face any request for ransom. And even if they fall victim and – in the worst case scenario – see their data encrypted, having a backup turns such an experience into nothing more than a nuisance.

If users do manage to get infected by ransomware, they have several options for its removal, depending on the specific malware variant:

1. *For most simple lock-screen ransomware families, booting the device into Safe Mode[4] – so third-party applications (including the malware) will not load – will do the trick and the user can easily uninstall the malicious application. In the event that the application has been granted device administrator privileges, these must first be revoked from the settings menu before the app can be uninstalled.*
2. *If ransomware with device administrator rights has locked the device using Android's built-in PIN or password screen lock functionality, the situation gets more complicated. It should be possible to reset the lock using Google's Android Device Manager or an alternate MDM solution. Rooted Android phones have even more options. A factory reset, which will delete all data on the device, can be used as the last resort in case no MDM solutions are available.*
3. *If files on the device have been encrypted by crypto-ransomware such as Android/Simplocker, we advise users to contact their security provider's technical support. Depending on the specific ransomware variant, decrypting the files may or may not be possible (as in case of Android/DoubleLocker).*

We also strongly advise affected users **against paying the requested ransom**, for several reasons. While it is true that some established Windows crypto-ransomware gangs have reached the level of professionalism where users will usually get their files decrypted, that is not always the case, especially on Android.

We have seen several variants of ransomware on this platform where the code for decrypting files or uninstalling the lock-screen was missing altogether, so paying would not have solved anything.

Our analyses of crypto-ransomware show that many variants and even families are poorly implemented, which means two things: Firstly, even if users do pay up, their files may not get decrypted. Secondly, it may be possible to decrypt their files without paying.

At the level of a single user or a business being a victim of crypto-ransomware and facing a loss of data, it boils down to a question of trust. Can the cybercriminals be trusted to keep their end of the bargain and decrypt the files after the ransom has been paid? Obviously, there are **no guarantees**. And even if the files are decrypted, there's nothing stopping attackers (the same ones or others) from coming back for more.

Taking a wider view, the entire ransomware economy went as high as ***$1 billion in 2016***, which shows us how giving in to attackers' demands only fuels the problem.

4 The steps for booting into Safe Mode can vary on different device models. Consult your manual, or search for the steps online.

January 2018

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic