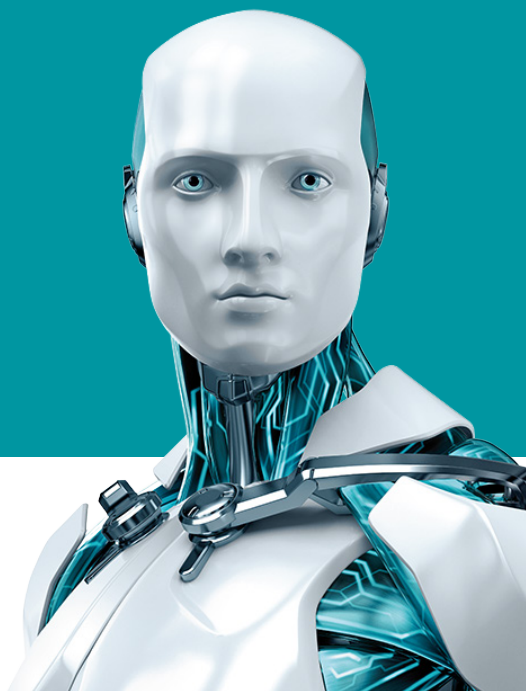
TRENDS IN ANDROID RANSOMWARE

Authors
Robert Lipovský – Senior Malware Researcher
Lukáš Štefanko – Detection Engineer
Gabriel Braniša – Malware Researcher



ENJOY SAFER TECHNOLOGY™

Contents

SUMMARY

2016 brought some interesting developments to the Android ransomware scene. Ransomware is currently one of the most pressing cybersecurity issues across all platforms, including the most popular mobile one.

Authors of lock-screen types as well as file-encrypting "crypto-ransomware" have used the past 12 months to copycat effective techniques from desktop malware, as well as develop their own sophisticated methods specialized for targets running Android devices.

In addition to the most prevalent scare tactics used by lock-screen "police ransomware", cybercriminals have been putting an increased effort into keeping a low profile, by encrypting and burying the malicious payload deeper into the infected apps.

In 2015, ESET observed that the focus of Android ransomware operators shifted from Eastern European to US mobile users. However, last year demonstrated a growing interest by the attackers in the Asian market, as evidenced by the Jisut lock-screen, which began using a localized Chinese ransom message. This increased activity can also be seen in the growing prevalence of this now notorious malware family, doubling in the previous 12 months.

In the first part of this paper, we provide a definition of ransomware, take a look at ESET's detection telemetry to see the current trend for this cyber threat, and analyze malware specifics that apply to ransomware on Android. The main section details the most noteworthy Android ransomware examples since 2014. The final chapter offers advice to Android users.

RANSOMWARE ON ANDROID

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. There are two general categories of malware that fall under the "ransomware" label:

- Lock-screen ransomware
- Crypto-ransomware

In lock-screen types of ransomware, the hijacked resource is access to the compromised system. In file-encrypting "crypto-ransomware" that hijacked resource is the user's files.

Both types have been a very prevalent problem on the Windows platform since 2013, when ransomware started to increase in popularity among cybercriminals, even though it had been around for many years before. Ransomware infections have been causing trouble both to individuals and to businesses.

Since one of the most noticeable trends in regard to Android malware is that malware writers have been bringing to this platform malware techniques that have proven to be successful on Windows, the appearance of ransomware on the most popular mobile platform was anticipated and has been observed for several years now.

According to ESET LiveGrid®, the number of Android ransomware **detections has grown in year on year comparisons by more than 50%, with the largest spike in the first half of 2016**.

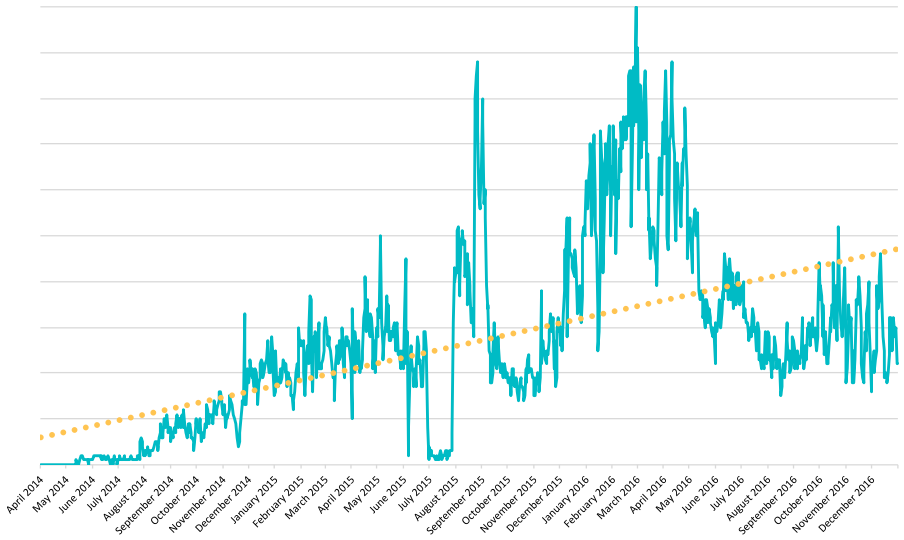


Fig. 1: Android ransomware detection trend, according to ESET LiveGrid®

With more and more consumers switching from PC to mobile, increasing amounts of valuable data is stored on the devices we all carry, making Android ransomware ever more worthwhile for attackers.

Common infection vectors

In 2016, ESET experts documented an emerging trend, 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).

However, Android malware – ransomware as well as most other types – typically fulfils 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 in order 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 would break the digital signature of the package, it has to be re-signed and submitted under a different developer account than the original.

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's researchers have found and reported to Google hundreds of samples of Android malware, including fake apps and fake AV scareware, credential-phishing spyware, trojans used for click-fraud, backdoors, ad-displaying PUAs (Potentially Unwanted Applications), and other PUAs, etc.

Malware writers have also begun to use more sophisticated methods to spread their infected apps. To avoid the unwanted attention, attackers have started to encrypt malicious payloads, burying them deeper in the application – often moving them to the assets folder, typically used for pictures or other necessary contents. Infected applications often seem to have no outside functionality, but in reality work as a decryptor able to 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.

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, device

language, and so on. 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 and displaying a ransom message, include:

- wipe device
- reset 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 user's GPS location

The usual communication protocol used is HTTP. But 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 the 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.

Malware self-protection

Infecting 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 they succeed in overcoming these hurdles, they want to make sure that their malevolent code stays on the device for as long as possible.

Several self-preserving techniques have been observed in the case of Android/Lockerpin, including attempts to kill processes belonging to anti-malware applications.

One of the most universal techniques that we're starting to see in more and more Android malware is obtaining Device Administrator privileges. Note that Device Administrator privileges are not the same as root access, which would be even more dangerous if acquired by malware.

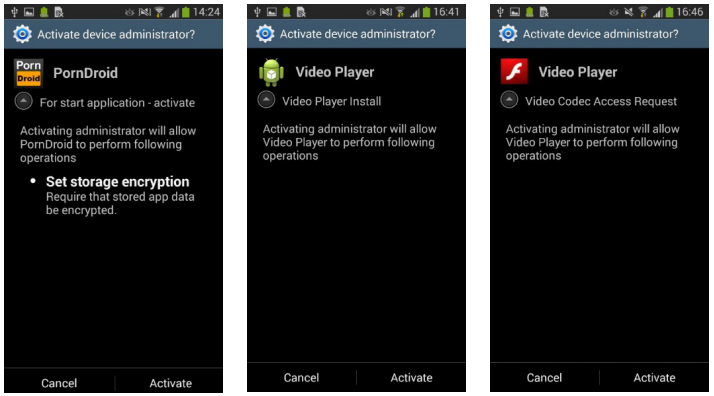
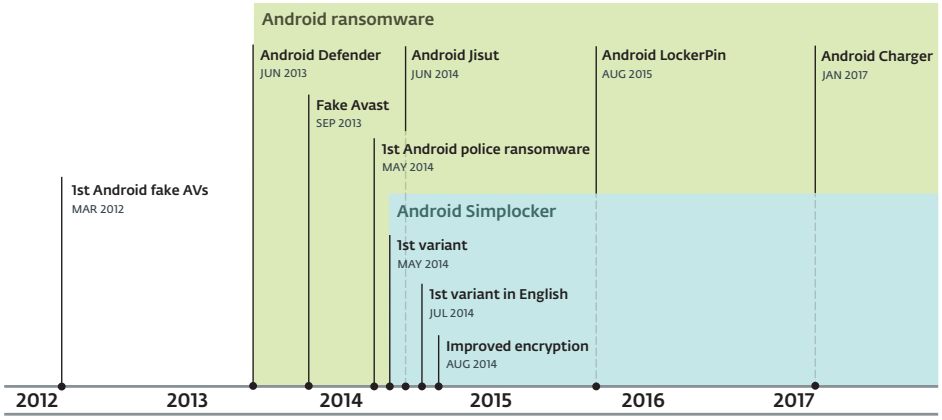


Fig. 2: Examples of Android malware requesting Device Administratorojan privileges

To obtain them, malware uses click jacking or tap jacking technique that creates two overlying layers – a fake one displayed to the user and an underlying one activating Device Administrator rights. By clicking on the foreground activity, victim unknowingly taps also on the one in the background broadening the privileges for the malicious code.

Legitimate Device Administrator applications use these extended permissions for various (mostly security-related) reasons. Malware, on the other hand, uses this Android feature for its own protection against uninstallation. Before such an app can be uninstalled, its Device Administrator rights must first be revoked.Some malware, such as Android/Lockerpin, additionally uses the extra permissions only available to Device Administrator applications to set or change the lock screen PIN.

ANDROID RANSOMWARE CHRONOLOGY



The first appearances of ransomware on Android were cases in which extortion functionality was added to fake (rogue) antiviruses.

Fake AVs are a malware type that has been around for a long time – on Android since 2012 and on desktop platforms since at least 2004. As the name implies, they display a fake antivirus scan of files on the device

and then try to trick users into paying money to remove the threats with which the files are supposedly infected. They're also referred to as "scareware", because they extort payment from the victim after scaring them into believing that their device is infected.

Rogue AVs are generally not considered ransomware – while they also attempt to get money from the victim, they typically rely on persuasion rather than extortion and the tricked users usually believe

they're paying for a legitimate product. However, some fake AV authors decided to make their software more aggressive by adding lock-screen ransomware behavior.

Most lock-screen ransomware on Windows belongs to the so-called police ransomware category, and the same trend can be observed on Android. Police ransomware increases its chance of success (of a

payment by the victim) by using another scareware tactic – they try to scare the afflicted users by displaying a message purportedly from a law enforcement agency, such as the FBI, claiming that illegal activities has been detected on their device.

File-encrypting crypto-ransomware was the only missing kid on the "Android malware block" until the May 2014 appearance of a family that *ESET dubbed Simplocker*.

Ransomware on Android has continued to evolve and new families have been discovered over the past three years. The most noteworthy are described in the following sections.

Android defender

Android Defender, which was first spotted in mid-2013, is a typical example of a fake antivirus and probably the first actual ransomware targeting Android.

As is evident from Figure 4, the graphical user interface of the application tries to make it appear to the victims that they're dealing with a legitimate security application. Interestingly, during the fake scan, the trojan displays names of files that actually exist on the phone's memory card, which makes it even more believable. The malware names shown are real too, except the phone isn't actually infected with them.

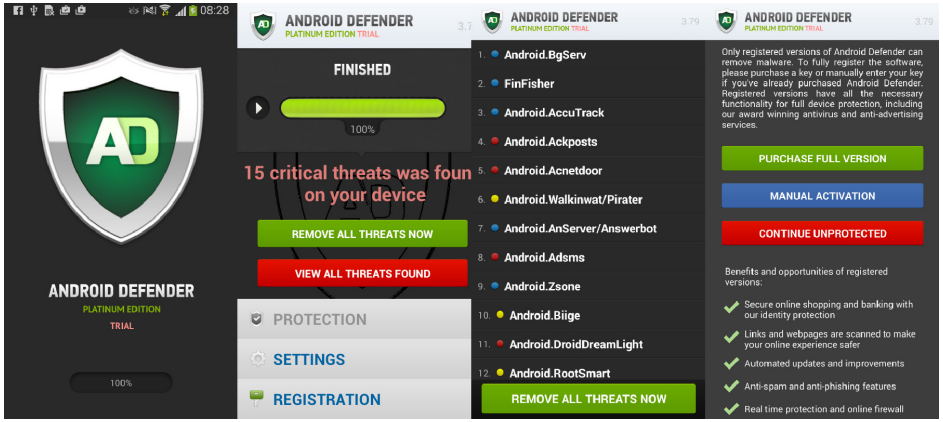
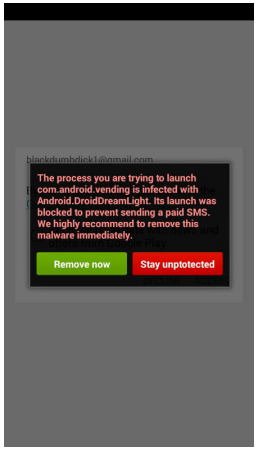
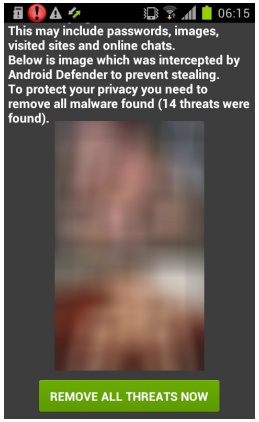


Fig. 4: Fake AV called Android Defender with a convincing GUI



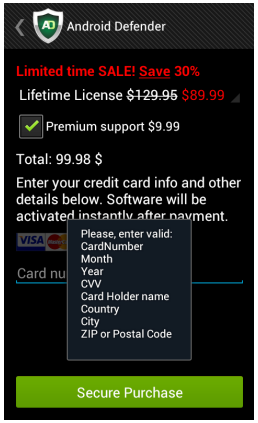
At this stage, the user still has the option of "continuing unprotected" and closing the app. However, a background service belonging to the fake AV makes the phone practically unusable by displaying never-ending malware warning popups each time the user tries to launch an application. Clicking "Stay unprotected" dismisses the currently displayed popup, only to see another one pop up, and so on...

Fig. 5: Incessant Android Defender popups make the infected device practically unusable



In the event that this behavior has not persuaded the victims to believe that they are truly infected and to pay for the "full version" of the scam software, it will switch to an even more aggressive mode six hours after its initial launch. Android Defender displays a full-screen window with hardcore pornographic images that can't be closed.

Fig. 7: Android Defender purchase options



In the event that the infected user gives up and decides to pay, the fraud will set him or her back by at least 89.99 USD. What's even worse is that the user's credit card details are now in the hands of the malware operators (or anyone sniffing on the network, as the data are sent unencrypted) and available for further misuse.

ESET Mobile Security detects Android Defender as *Android/FakeAV.B*.

Fig. 6: Android Defender locks the screen displaying pornographic images

Ransomware meets fake av, meets...porn

The second fake AV ransomware example doesn't go under a made-up name like Android Defender, but instead parasitizes the name of a legitimate Android security application from Avast[1]. Fake copies of

legitimate antivirus programs used to be the domain of rogue AVs on Windows. Curiously, the malware, detected by ESET as *Android/FakeAV.E* also abuses another well-known brand: it spreads by pretending to be a mobile app for the adult video website PornHub.

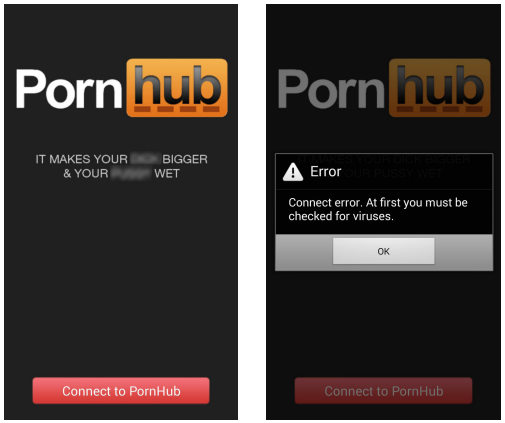


Fig. 8 – 1st disguise of Android/FakeAV.E: fake PornHub app

When the app is launched, instead of showing pornographic videos, it shows the user a message that says the device must first be "checked for viruses". After clicking OK, the fake AV, which is made to look like Avast, runs its scam scan.

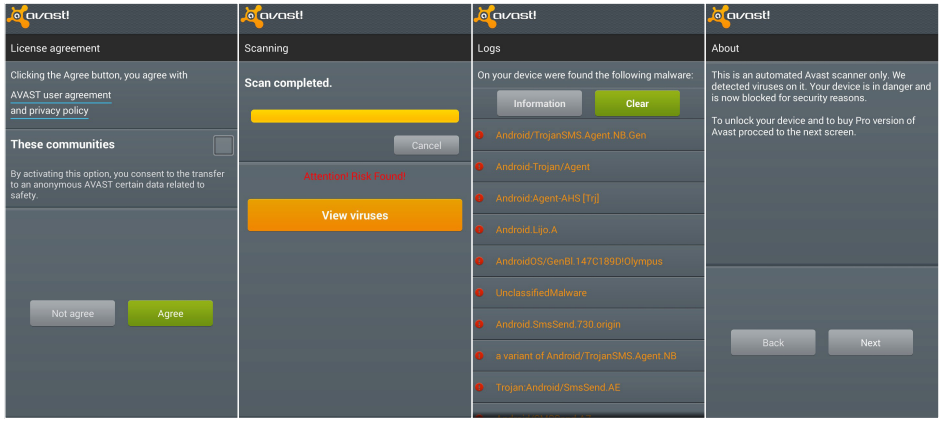


Fig. 9 – 2nd disguise of Android/FakeAV.E: fake Avast app

The narrative in this fraud is rather odd. First, the message shown by the fake Avast GUI states that the "device is in danger and is now blocked for security reasons" and that a Pro version must be bought.

While a legitimate antivirus would obviously not render a device unusable, that text is more-or-less corresponds to rogue AV behavior. However, the ransom nag screen that's displayed as the devices is locked talks about an obligation to pay a 100 USD fine to avoid legal consequences.

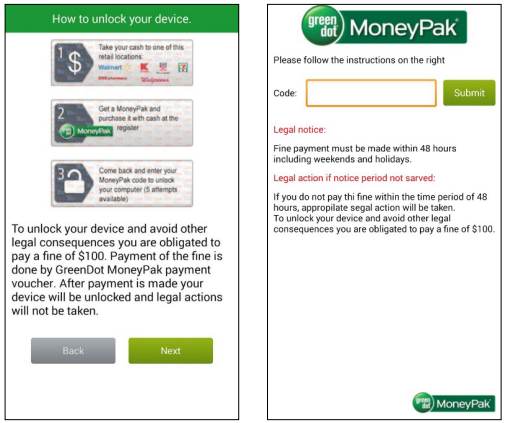


Fig. 10 – Android/FakeAV.E ransom screens

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

It appears as if the authors of this malware took the ransom message screens from a different ransomware program, even incorporating the same typographic errors.

Police ransomware

Lock-screen ransomware on Windows has used various themes in the past. Some earlier examples included lock-screens that appeared as a blue-screen-of-death (BSOD), or a Windows activation message. While we still occasionally spot various new lock-screen themes, the one that recurs most commonly in recent years is police ransomware. Reveton is one of the best-known families of this type.

Police ransomware claims that the device has been locked by a local law enforcement agency because illegal content or activity has been detected. The ransom messages sometime quote some Criminal Code article but say that the user can get away with just a fee. Police ransomware often uses 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*.

Fig. 11 First police ransomware variants were targeting Russian-speaking Android users.

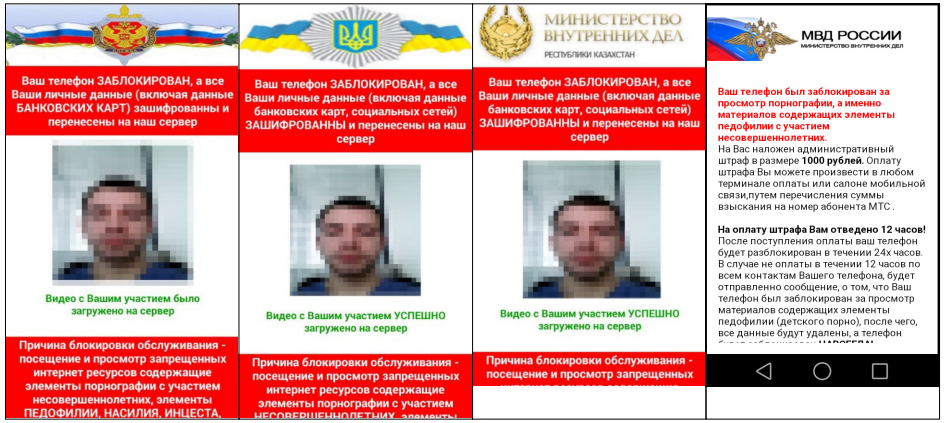


Fig. 12 – Android/Locker variants capable of displaying a camera shot and adjusting the ransom screen based on the user's location – example shows Russian, Ukrainian, and Kazakh banners

Fig. 13 Android/Koler variants shift to targeting English-speaking users

Simplocker

In May 2014, ESET detected the first file-encrypting ransomware for Android – an expected evolution, as this kind of malware has been extremely widespread on the Windows platform in the recent years, Cryptolocker, Cryptowall, Locky, and TorrentLocker being just a few of many infamous examples.

After launch, the trojan displayed a ransom message as shown in Figure 14 and encrypted files in a separate program thread in the background. *Android/Simplocker.A* scanned the SD card2[2] for files with any of the following image, document or video extensions – JPEG, JPG, PNG, BMP, GIF, PDF, DOC, DOCX, TXT, AVI, MKV, 3GP, MP4 – and encrypted them using the AES cipher. The encryption key used was hardcoded inside the binary as plain text, so it was trivial to decode them, unlike the more established Windows crypto-ransomware families. For this reason, we dubbed the malware Android/Simplocker and believed that these first variants were either just a proof-of-concept or an early development version of a more serious threat.

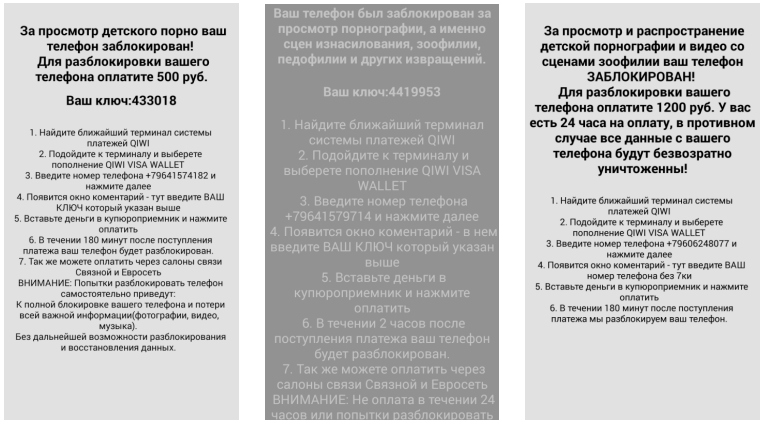


Fig. 14 – Ransom requests from initial Russian versions of Android/Simplocker

The ransom message 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. The

malware instructs the victim to make the payment using prepaid money vouchers, such as MoneXy or QIWI, because these are not as easily traceable as if the payments were made with regular credit cards.

Some Simplocker variants also display a photo of the victim taken with the phone's camera to increase the scareware factor.

Fig. 15 – Simplocker using the front camera feed to intimidate the victim

Simplocker distribution vectors

Android/Simplocker usually tries to trick the user into installing it by camouflaging itself as a legitimate and popular application – a common technique for Android malware. Typically, the camouflage revolves around internet porn (some malicious apps pretend to be an adult video, an app for viewing adult videos, etc.), popular games like Grand Theft Auto: San Andreas, or common applications like Flash Player.

However, Android/Simplocker has also been using a less common spreading mechanism – through trojan-downloaders. Trojan- downloaders are common in the world of Windows malware but not that common on Android. They're small programs whose sole purpose (and also the only reason why they're malicious) is to download other malware.

The reason why the trojan-downloader strategy has a greater chance of slipping under the radar of Android market application scanning (such as Bouncer on the official Google Play, for example) or even escaping the notice of a more careful Android user is that:

2 The threat also affected devices without a physical SD card. On such devices, the internal memory appears as an emulated SD card.

- All the application does is open a URL outside the app – this does not, in itself, qualify as malicious behavior
- The downloader has practically no "potentially harmful" application permissions – so even a user who scrutinizes app permissions during installation may allow this one

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 Android/Simplocker spreading through the official Google Play store.

Simplocker in English

Only one month after discovering the first Simplocker variants, we began detecting new versions of this ransomware that featured a few significant improvements.

The most noticeable change was the language: *Android/Simplocker.I* now displayed ransom screens in English instead of Russian. The victim was led to believe that the device was blocked by the FBI after detecting illegal activity – software piracy, child pornography, and so on – typical behavior of police ransomware. The ransom demanded was now in

the range of 200 USD to 500 USD and the victim was instructed to pay it using a MoneyPak voucher. Like some of the previous Android/ Simplocker variants, this one also used the scareware tactic of displaying the camera feed from the device.

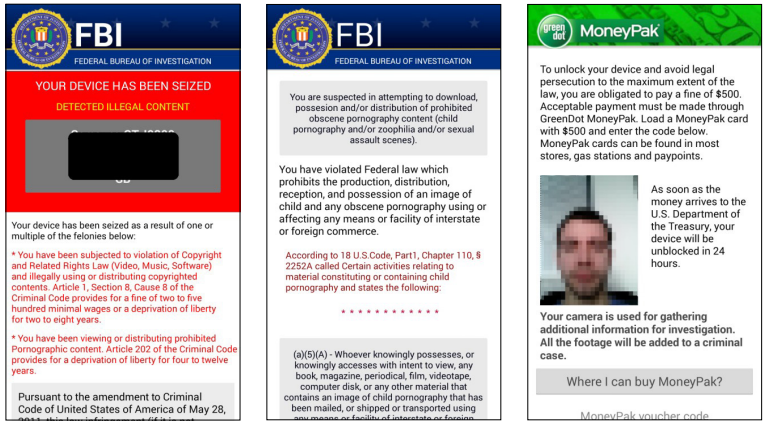


Fig. 16 – Android/Simplocker ransom messages in English

The latest variants have slightly changed the ransom request visuals. Instead of the FBI, it is the NSA that's accusing the victim of "attending forbidden pornographic sites" (sic) and asking for a 500 USD payment.

Fig. 17 – Latest Android/Simplocker NSA ransom messages

In addition to encrypting documents, images and videos on the device's SD card, the trojan now also encrypts archive files: ZIP, 7z and RAR. This

"upgrade" can have very unpleasant consequences. Many Android file backup solutions store the backups as archive files. If the user gets infected with Android/Simplocker.I, these backups will be encrypted as well.

More advanced Simplocker variants also ask to be installed as Device Administrator, which makes them a lot more difficult to remove, since the user must first 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. Using XMPP makes it more difficult to trace the C&C servers than if HTTP were used. Android/ Simplocker uses this instant messaging communication protocol to send information about the infected device to the server and to execute commands received. A third type of C&C server addressing used by some Android/Simplocker variants is the use of 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 it was no longer possible to decrypt the hijacked files easily.

Lockerpin

In previous Android lockscreen 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 device user locked out, it wasn't too difficult to get rid of the malware, and thus to unlock the device, by using Android Debug Bridge (ADB) or deactivating Device Administrator rights and uninstalling the malicious application in Safe Mode.

Unfortunately, with *Android/Lockerpin*, which we discovered in August 2015, malware writers have stepped up their game. If a user becomes infected with this Android ransom-locker, the only way to remove the PIN lock screen is if the device was previously rooted or has an MDM solution installed that is capable of resetting the PIN. Otherwise, the last option is a factory reset, which deletes all data on the device.

The technique that Lockerpin uses for locking the device is extremely simple – it leverages the built-in Android PIN screen locking mechanism. It is able to set a PIN on the device, or even change it if it was already set. It is able to do so, provided that the victim has granted the malicious app Device Administrator privileges.

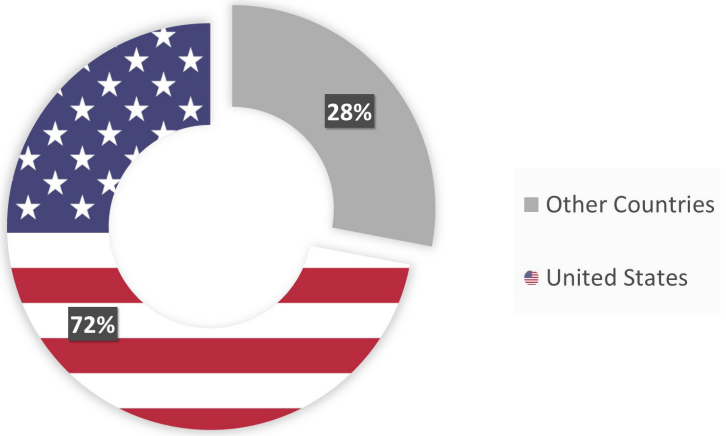


Fig. 18 – Android/Lockerpin geographic distribution

According to ESET's LiveGrid® statistics, most of the infected Android devices are in the USA, with a percentage share of 72%. This is part of a trend whereby Android malware writers are shifting from targeting mostly Russian and Ukrainian users to targeting victims in the United States, where arguably they can make bigger profits.

The malware has been spreading disguised as an app for viewing adult videos.

Earlier versions of the Android/Locker family obtain Device Administrator status in just the same way as all other Android trojans, which use them mostly as protection against uninstallation – they rely on the user willingly activating the elevated privileges.

In the latest versions, however, the trojan obtains Device Administrator rights using a much more covert tap-jacking technique. The system Device Admin activation window is overlaid with the trojan's malicious window which pretends to be an "Update patch installation". The gist of the technique is that the fake Continue button is placed perfectly over the underlying Activate button. So when the victims click through this innocuous-looking installation they have inadvertently granted the malware Device Administrator privileges.

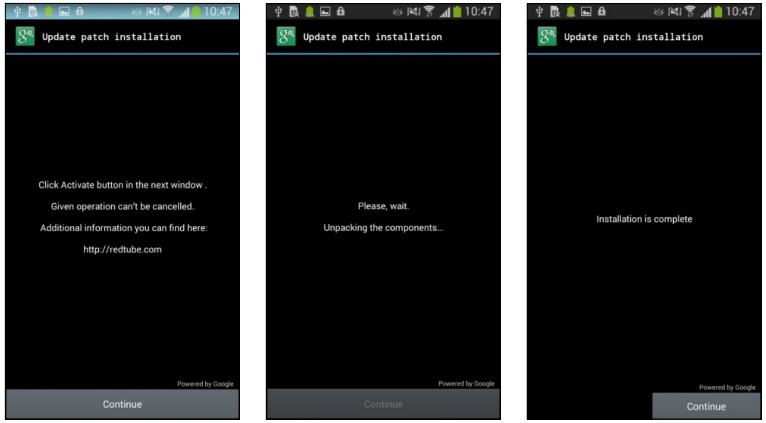
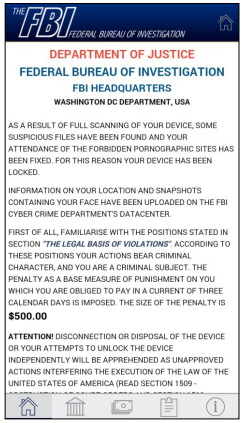
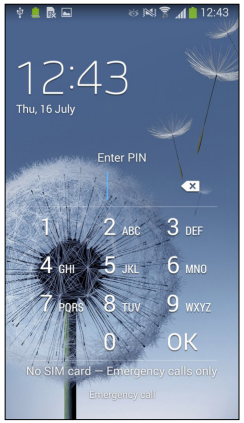


Fig. 19 – Android/Lockerpin covertly obtaining Device Administrator rights by tap-jacking



After installation, the typical police ransomware scenario ensues. The user is shown a bogus message from the FBI requesting a 500 USD ransom for allegedly viewing and harboring forbidden pornographic material.

Fig. 20 – Android/Lockerpin ransom message



After a specified time delay following the display of the ransom message, the PIN will be 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.

Fig. 21 – Device locked by Android/Lockerpin

Lockerpin's aggressive self–defense

Not only does Android/Lockerpin acquire Device Admin privileges in a novel and covert manner; it also uses an aggressive self-defense mechanism to make sure it keeps them. When users attempt to deactivate Device Admin for the malware, they will fail because the trojan has already registered a call-back function to reactivate the privileges immediately after removal is attempted.

Similar to when Device Administrator is first activated by the trojan, if a removal attempt is made, the Device Administrator window is again overlaid with a bogus window as shown in Figure 22. Pressing Continue effectively reactivates the elevated privileges.

Fig. 22 – Android/Lockerpin blocking attempts to revoke Device Administrator rights

As an extra layer of self-protection, the ransomware also attempts to kill running AV processes when the user tries to deactivate its Device Admin rights. The trojan tries 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

Fig. 23 – Android/Lockerpin attempting to kill running AV processes

The malware will 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.

Jisut

This strange ransomware family detected by ESET security solutions as *Android/LockScreen.Jisut* saw a significant spike in activity in 2016 – the number of detections doubling compared to 2015.

Most of the seen variants try to lock user out of the device, but oddly demand no ransom. Their only visible activity is a change of wallpaper or a sound playing in the background, strengthening our presumption it has been created mainly as a prank and not just for financial gain.

However, ESET has also documented variants that ask the victim to pay ransom. To make the process simpler and more straightforward, the attackers add QR code allowing the infected user to either write message to the attacker or directly make the payment. Some samples were even trying to sell the app or its source code.

One of the Jisut ransomware variants seen in the beginning of 2017 also had a special ability, which hasn't been reported before. It demanded ransom by using voice message, making it the first "speaking Android ransomware" detected in the wild. After infecting the device, a female voice speaking Chinese "congratulated" the victim and asked for 40 Yuans (approx. 6 dollars) to unlock it.

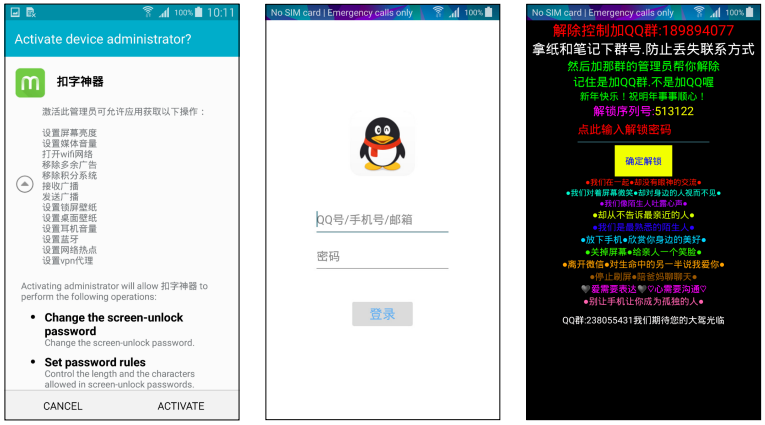


Fig. 24 – Android/Jisut requests admin rights, harvests QQ credentials and on top of locking the screen demands the ransom by voice message.

This variant is most widespread in China and is likely the work of newbie Chinese teenage cybercriminals.

Most ransomware – lock-screens as well as crypto-ransomware – demands payment via pre-paid cash vouchers or by Bitcoin, precisely for the reason that these payment methods are virtually untraceable. However, the gang behind Jisut took a whole different approach and doesn't seem to care about its anonymity. The ransomware nag screens include contact information on the Chinese social network QQ and urge the victims to contact the authors in order to get their files back. If the information in the QQ profiles is valid, the malware operators are Chinese youths between 17 and 22 years old.

The first variants of Android/LockScreen.Jisut started appearing in the first half of 2014. Since then, we have detected hundreds of variants that all behave somewhat differently or display different ransom messages, but all of them are based on the same code template.

The whole Jisut malware family is unlike any other known LockScreen ransomware. One type of Jisut behavior is to create a full screen Activity (Android developer term for "window") overlaying all other Activities. The full screen overlay is just a black background so the device appears as if it was locked or switched off. If the user brings up the menu to shut down or restart the device, a joke message will be displayed. Some samples feature a variation to the previous activity: they play music from the famous shower scene from Alfred Hitchcock's Psycho, while vibrating the device in an infinite loop.

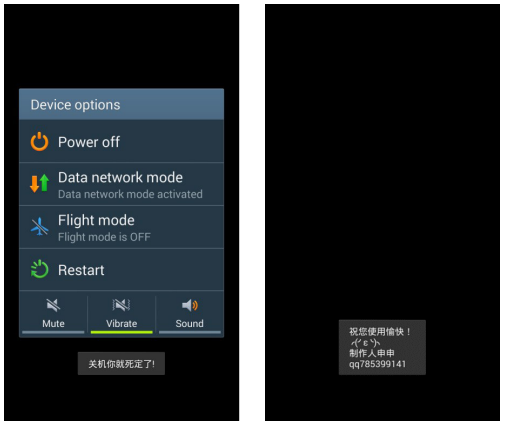


Fig. 25 – Jisut prank messages: Left: "Off, you are dead!" Right: "I hope you have fun! Producer Shen Shen"

Another Jisut variant asks the user to click a button that says "I am an idiot" 1000 times. Nothing happens after the counter reaches 1000; it's reset to zero and the frustrated user can continue clicking indefinitely.

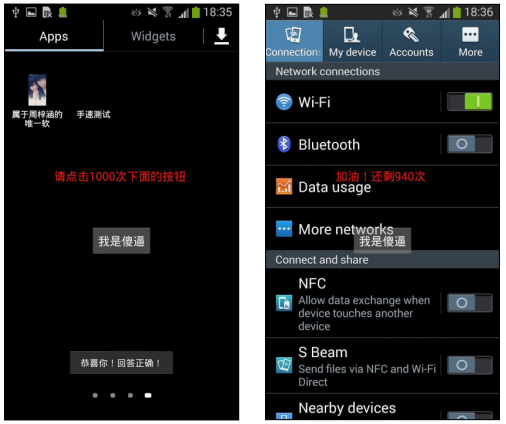


Fig. 26 – Android/LockScreen.Jisut: "Please click the button below 1000 times"

In addition to the described silly behavior, most Android/LockScreen. Jisut variants also contain harmful functionality. Like Android/Lockerpin, they're able to set or change the device lock screen PIN or password.

Some variants don't rely on the legitimate built-in Android lock screen functionality but display their own full-screen window mimicking the lock screen, as the police ransomware Android/Locker and Android/ Koler families do.

Fig. 27 – Device locked with PIN or password by Android/LockScreen.Jisut

Fig. 28 – More vivid custom lock screens with the malware author's QQ number

In addition to the ransomware aspect, some variants can spread by sending an SMS message with a URL link to the malware to all user contacts.

Charger

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

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

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

Based on the commands it received, it could also extract and send 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.

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 avoiding unofficial app stores and having a mobile security app installed and kept up to date. Additionally, it is

important to have a functional backup of all of 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 – 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.

For most simple lock-screen ransomware families, booting the device into Safe Mode – so third-party applications (including the malware) will not load – will do the trick and the user can easily uninstall the malicious application. The steps for booting into Safe Mode can vary on different device models. (Consult your manual, or ask Google – the search engine.) 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.

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.

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.

We also 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.

File-encrypting crypto-ransomware is extremely popular among malware writers and there are many different families of Windows Filecoders (the ESET detection name for the category). Many of them have jumped on to the ransomware bandwagon, hoping to copy the success of Cryptolocker and the like, but our technical analyses of all those families has shown that many of them are implemented poorly. For users, this means two things: Firstly, that even if they do pay up, their files may not get decrypted. Secondly, that it may be possible to decrypt their files without paying.

As far as ransomware on Android is concerned, we have seen several variants where the code for decrypting files or uninstalling the lock- screen was missing altogether, so paying would not have solved anything.

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 of the entire ransomware economy – *FBI estimates go as high as $1 billion for 2016* – suggests that giving in to attackers' demands only fuels the problem.

As mentioned above, prevention by adhering to basic security principles, using updated security software on Android, and backing up your data (not only on the device itself) is a much more sensible option. And with all of those precautions being readily available and easy to use, there really is no reason not to do so.


ENJOY SAFER TECHNOLOGY™