Android ransomware is back

welivesecurity.com/2019/07/29/android-ransomware-back/

July 29, 2019

ESET researchers discover a new Android ransomware family that attempts to spread to victims' contacts and deploys some unusual tricks

Lukas Stefanko

29 Jul 2019 - 04:35PM

ESET researchers discover a new Android ransomware family that attempts to spread to victims' contacts and deploys some unusual tricks

UPDATE (July 30th, 2019): Due to rushing with the publication of this research – in order to warn about this threat as soon as possible – we erroneously stated that "because of the hardcoded key value that is used to encrypt the private key, it would be possible to decrypt files without paying the ransom by changing the encryption algorithm to a decryption algorithm". However, this "hardcoded key" is an RSA-1024 public key, which can't be easily broken, hence creating a decryptor for this particular ransomware is close to impossible. Hat tip goes to Alexey Vishnyakov from Positive Technologies who drew our attention to this inaccuracy.

After two years of decline in Android ransomware, a new family has emerged. We have seen the ransomware, detected by ESET Mobile Security as Android/Filecoder.C, distributed via various online forums. Using victims' contact lists, it spreads further via SMS with malicious links. Due to narrow targeting and flaws in execution of the campaign, the impact of this new ransomware is limited. However, if the operators start targeting broader groups of users, the Android/Filecoder.C ransomware could become a serious threat.

Android/Filecoder.C has been active since at least July 12th, 2019. Within the campaign we discovered, Android/Filecoder.C has been distributed via malicious posts on Reddit and the "XDA Developers" forum, a forum for Android developers. We reported the malicious activity to XDA Developers and Reddit. The posts on the XDA Developers forum were removed swiftly; the malicious Reddit profile was still up at the time of publication.

Android/Filecoder.C spreads further via SMS with malicious links, which are sent to all contacts in the victim's contact list.

After the ransomware sends out this batch of malicious SMSes, it encrypts most user files on the device and requests a ransom.

Users with ESET Mobile Security receive a warning about the malicious link; should they ignore the warning and download the app, the security solution will block it.

Distribution

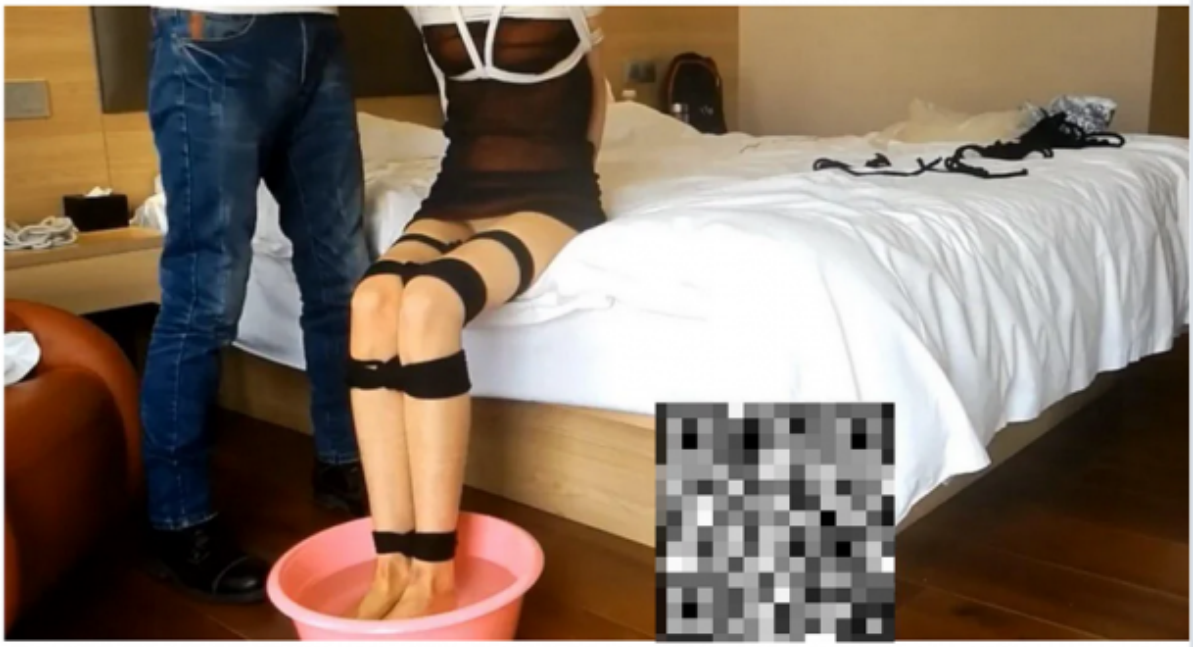
The campaign we discovered is based on two domains (see the IoCs section below), controlled by the attackers, that contain malicious Android files for download. The attackers lure potential victims to these domains via posting or commenting on Reddit (Figure 1) or XDA Developers (Figure 2).

Mostly, the topics of the posts were porn-related; alternatively, we've seen also technical topics used as a lure. In all comments or posts, the attackers included links or QR codes pointing to the malicious apps.

r/CCJ2 · Posted by u/ronn1e_r 8 days ago

1

fxxking my [redacted] gf in hotel



1 Comment Give Award Share Save Hide Report 100% Upvoted

[redacted] · Posted by u/ronn1e_r 8 days ago + JOIN

1

fxxking my [redacted] gf in hotel

1 Comment Share Save ···

[redacted]1e_r 1 point · 8 days ago

you guys can watch all videos from this app , scan QR first.

have fun .

Reply Share ···

[redacted] Posted by u/ronn1e_r 8 days ago + JOIN

1

Fxxking my [redacted] gf in Jinan China.

[removed]

Comment Share Save ···

[redacted]1e_r commented on I think I've realized why I've stopped having casual sex. · **r/sex** · Posted by u/size_progression

[redacted]1e_r 1 point · 13 days ago

Real-life remote sex simulation, new users experience three times of climax for free, http://ric[redacted].xyz/sex[redacted].apk

you will come back to thank me !

Reply Share ···

[redacted]1e_r commented on Shy girlfriend swallowing my load. pornhub.com/view_v... nsfw · **r/couplesgonewild** · Posted by u/Masticates

ronn1e_r 1 point · 13 days ago

Have you ever played this sex simulation app?

http://ric[redacted].xyz/sex[redacted].apk

Reply Share ···

[redacted]1e_r commented on VERIFIED COUPLE ✅ Watch us! (: pornhub.com/view_v... nsfw · **r/couplesgonewild** · Posted by u/Masticates

ronn1e_r 1 point · 13 days ago

[redacted]

Karma 1

Cake day July 8, 2019

FOLLOW

MORE OPTIONS

TROPHY CASE (1)

Verified Email

About Careers Press

Advertise Blog Help

The Reddit App Reddit Coins Reddit Premium Reddit Gifts

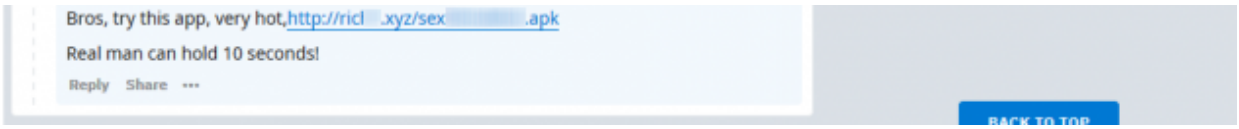
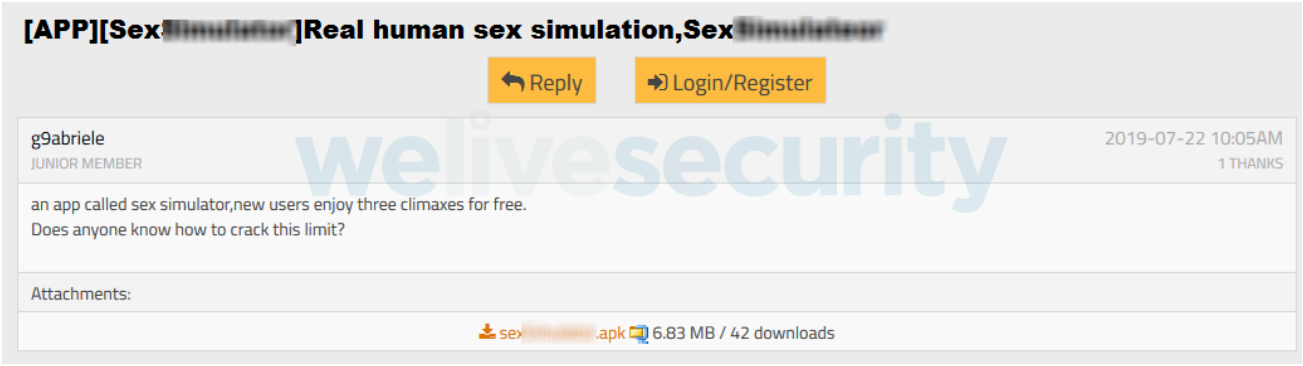


Figure 1. The attacker's Reddit profile with malicious posts and comments



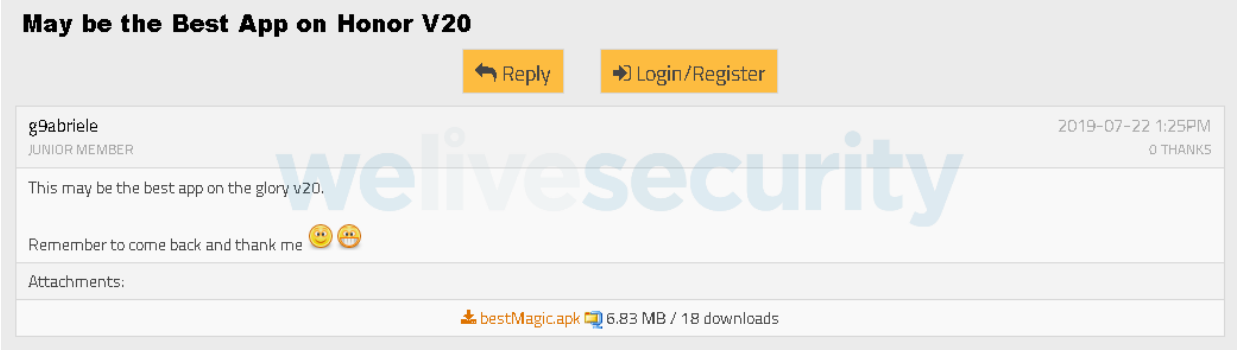


Figure 2. Some of the attackers' malicious posts on the XDA Developers forum

In one link that was shared on Reddit, the attackers used the URL shortener bit.ly. This bit.ly URL was created on Jun 11, 2019 and as seen in Figure 3 its statistics show that, at the time of writing, it had reached 59 clicks from different sources and countries.

Figure 3. Statistics for the bit.ly link shared on Reddit during the ransomware campaign

Spreading

As previously mentioned, the Android/Filecoder.C ransomware spreads links to itself via SMS messages to all the entries in the victim's contact list.

These messages include links to the ransomware; to increase the potential victims' interest, the link is presented as a link to an app that supposedly uses the potential victim's photos, as seen in Figure 4.

To maximize its reach, the ransomware has the 42 language versions of the message template seen in Figure 5. Before sending the messages, it chooses the version that fits the victim device's language setting. To personalize these messages, the malware prepends the contact's name to them.

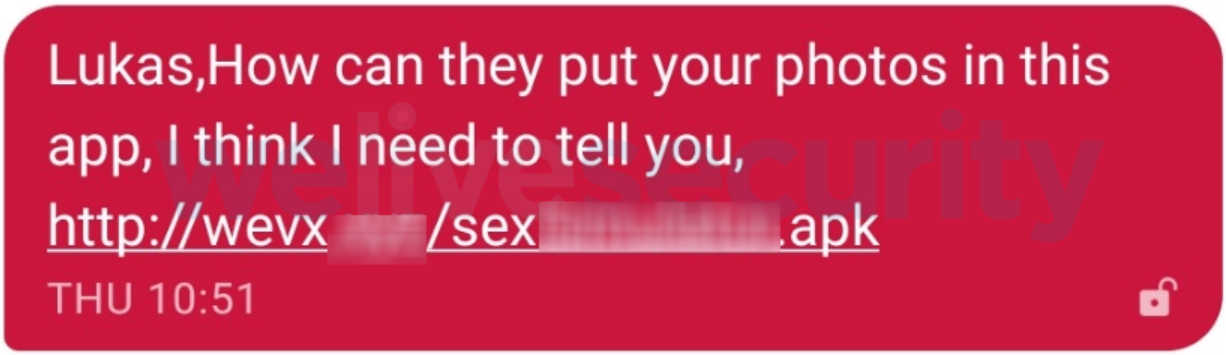


Figure 4. An SMS with a link to the ransomware; this language variant is sent if the sending device has the language set to English

af: Hoe kan hulle jou foto's in hierdie inligting plaas, ek dink ek moet jou vertel,
am: እንዴት ፎቶዎችዎን በዚህ መተግበሪያ ውስጥ ማስቀመጥ ይችላሉ, እኔ ሊነግሩኝ እንደሚፈልጉ ያስባታል,
ar: كيف يمكنهم وضع صورك في هذا التطبيق ، أعتقد أنني بحاجة لإخبارك ،
az: Bu tətbiqdə şəkillərinizi necə yerləşdirə bilərlər, mən sizə deməliyəm ki,
be: Як яны могуць змясціць вашыя фатаграфіі ў гэтым дадатку, я думаю, што мне трэба сказаць вам,
bg: Как могат да поставят снимките ви в това приложение, мисля, че трябва да ви кажа,
bn: তারা এই অ্যাপ্লিকেশনে আপনার ফটোগুলি কিভাবে রাখবে, আমার মনে হয় আপনাকে বলতে হবে,
bs: Kako mogu staviti svoje fotografije u ovu aplikaciju, mislim da vam moram reći,
ca: Com poden posar les teves fotos en aquesta aplicació, crec que us he de dir,
cs: Jak mohou dát své fotografie do této aplikace, myslím, že vám musím říct,
cy: Sut y gallant roi eich lluniau yn yr ap hwn, rwy'n credu bod angen i mi ddweud wrthych
da: Hvordan kan de sætte dine billeder i denne app, jeg tror jeg skal fortælle dig,
de: Wie können sie Ihre Fotos in diese App setzen, ich denke, ich muss Ihnen sagen,
el: Πώς μπορούν να βάλουν τις φωτογραφίες σας σε αυτή την εφαρμογή, νομίζω ότι πρέπει να σας πω,
en: How can they put your photos in this app, I think I need to tell you,
eo: Kiel ili povas meti viajn fotojn en ĉi tiun programon, mi pensas, ke mi devas diri al vi,
es: ¿Cómo pueden poner sus fotos en esta aplicación? Creo que necesito decirles,
et: Kuidas nad saavad oma fotodesse selle rakenduse panna, ma arvan, et pean teile ütlema,
eu: Nola jarri zure argazkiak aplikazio honetan? Nik uste dut esan behar zaitut,
fa: چگونه می توان عکس های خود را در این برنامه قرار داد، فکر می کنم باید به شما بگویم، fi: Miten he voivat laittaa valokuvia tähän sovellukseen, mielestäni minun täytyy kertoa teille,
fil: Paano nila mailalagay ang iyong mga larawan sa app na ito, sa palagay ko kailangan kong sabihin sa iyo,
fr: Comment peuvent-ils mettre vos photos dans cette application, je pense que je dois vous dire,
fy: Hoe kinne se jo foto's yn dizze app sette, ik tink dat ik jo sizze
ga: Conas is féidir leo do chuid grianghraf a chur san aip seo, sílim go gcaithfidh mé a rá leat,
gd: Ciamar as urrainn dhaibh na dealbhan agad a chur san aplacaid seo, tha mi a 'smaoineachadh gum feum mi innse dhut,
gl: Como poden poñer as túas fotos nesta aplicación, creo que teño que dicirlle,
gu: તેઓ આ ફોટામાં તમારા ફોટા કેવી રીતે મૂકી શકે છે, મને લાગે છે કે મારે તમને કહેવાની જરૂર છે,
ha: Ta yaya za su sa hotunanka a cikin wannan app, ina ganin ina bukatar in gaya maka,
haw: Pehea e hiki ai iā lākou ke kau i kāu mau ki'i ma kēia polokalamu, mana'o wau e ha'i aku iā'oe,
hi: वे आपकी तस्वीरें इस ऐप में कैसे डाल सकते हैं, मुझे लगता है कि मुझे आपको बताने की जरूरत है,
hr: Kako mogu staviti svoje fotografije u ovu aplikaciju, mislim da vam moram reći,
hu: Hogyan helyezhetik el a fotókat ebben az alkalmazásban, azt hiszem, meg kell mondanom,
hy: Ինչպես կարող են դրանք տեղադրել այս հավելվածում, կարծում եմ, ես պետք է ասեմ ձեզ,
ig: Kedu ka ha ga esi tinye foto gị na ngwa a, echere m na m ga-agwa gị,
in: Bagaimana mereka bisa meletakkan foto Anda di aplikasi ini, saya pikir saya perlu memberi tahu Anda,
is: Hvernig geta þeir sett myndirnar þínar í þessari app, ég held að ég þarf að segja þér,
it: Come possono mettere le tue foto in questa app, penso di doverti dire,
iw: איך הם יכולים לשים את התמונות שלך באפליקציה הזו, אני חושב שאני צריך לספר לך,
ja: どのように彼らはこのアプリにあなたの写真を入れることができます、私はあなたに言う必要があると思[...]kulolu hlelo lokusebenza, ngicabanga ukuthi ngidinga ukukutshela,
zh: 有人把你的照片传到网上了,

Figure 5. A total of 42 language versions that are hardcoded in the ransomware

Functionality

Once potential victims receive an SMS message with the link to the malicious application, they need to install it manually. After the app is launched, it displays whatever is promised in the posts distributing it – most often, it's a sex simulator online game. However, its main

purposes are C&C communication, spreading malicious messages and implementing the encryption/decryption mechanism.

As for C&C communication, the malware contains hardcoded C&C and Bitcoin addresses in its source code. However, it can also dynamically retrieve them: they can be changed any time by the attacker, using the free Pastebin service.

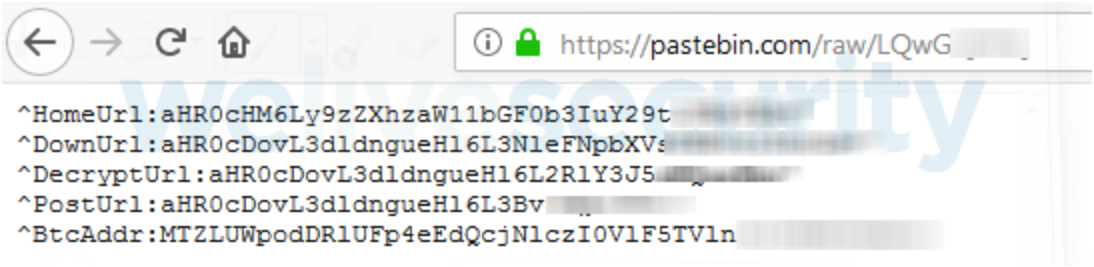


Figure 6. An example of a set of addresses for the ransomware to retrieve C&C addresses

The ransomware has the ability to send text messages, due to having access to the user's contact list. Before it encrypts files, it sends a message to each of the victim's contacts using the technique described in the "Spreading" section above.

Next, the ransomware goes through files on accessible storage – meaning all the device's storage except where system files reside – and encrypts most of them (see the "File encryption mechanism" section below). After the files are encrypted, the ransomware displays its ransom note (in English) as seen in Figure 7.

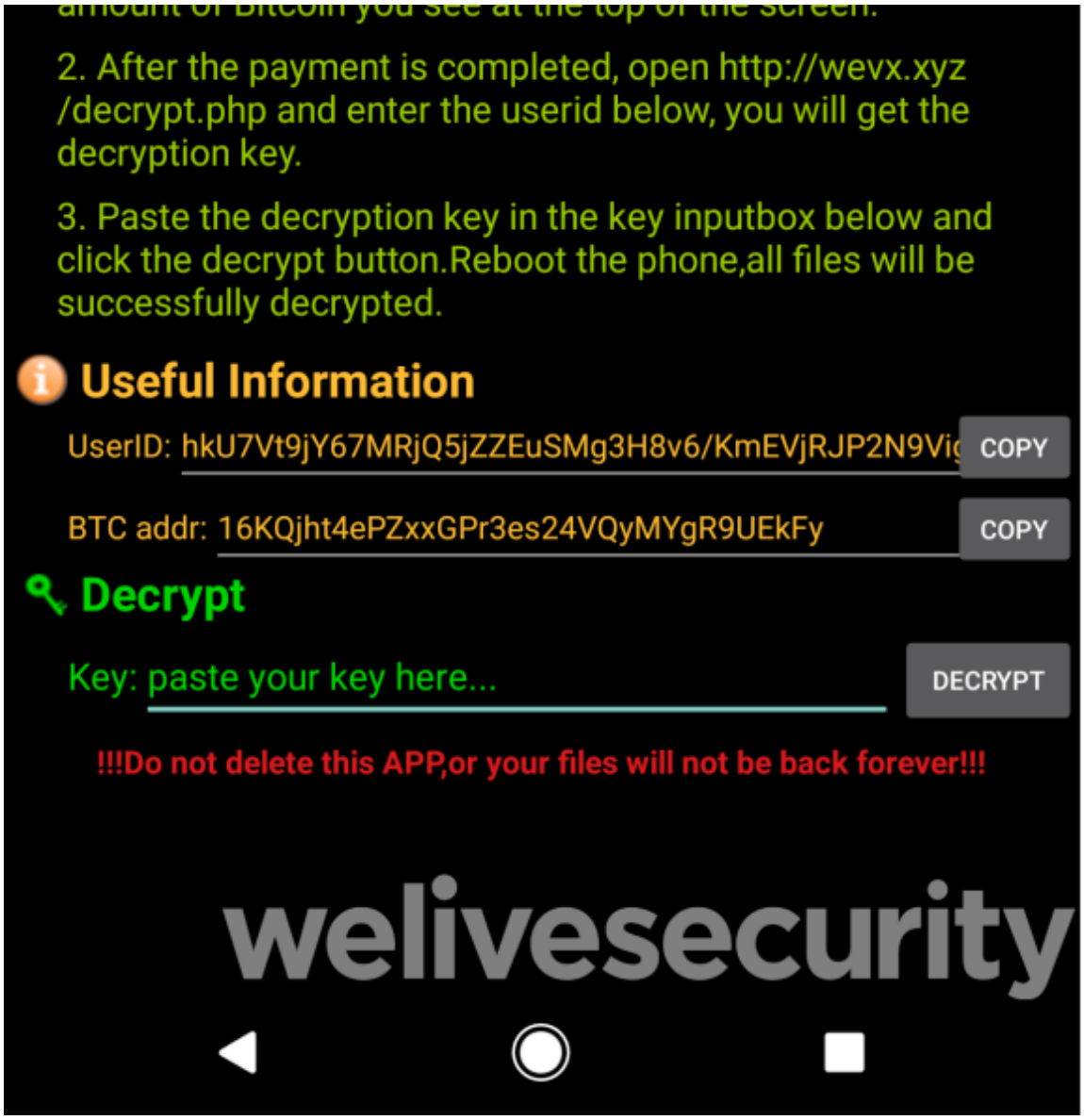


Figure 7. A ransom note displayed by Android/Filecoder.C

It is true that if the victim removes the app, the ransomware will not be able to decrypt the files, as stated in the ransom note. Also, according to our analysis, there is nothing in the ransomware's code to support the claim that the affected data will be lost after 72 hours.

As seen in Figure 8, the requested ransom is partially dynamic. The first part of what will be the amount of bitcoins to be requested is hardcoded – the value is 0.01 – while the remaining six digits are the user ID generated by the malware.

This unique practice may serve the purpose of identifying the incoming payments. (In Android ransomware, this is typically achieved by generating a separate Bitcoin wallet for each encrypted device.) Based on the recent exchange rate of approximately US$9,400 per bitcoin, the derived ransoms will fall in the range US$94-188 (assuming that the unique ID is generated randomly).

```
TextView btcPrice = (TextView)this.findViewById(0x7F07009E);  // id:textView12
String tail = Utils.getNumberFromUid(uid);
btcPrice.setText("0.01" + tail + " BTC");
```

Figure 8. How the malware calculates the ransom

Unlike typical Android ransomware, Android/Filecoder.C doesn't prevent use of the device by locking the screen.

As seen in Figure 9, at the time of writing, the mentioned Bitcoin address, which can be dynamically changed but was the same in all cases we've seen, has recorded no transactions.

Summary	
Address	16KQjht4ePZxxGPr3es24VQyMYgR9UEkFy
Hash 160	3a53ee2760d732423b8c8b109285540d7b404a31
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Figure 9. The Bitcoin address used by the attackers

File encryption mechanism

The ransomware uses asymmetric and symmetric encryption. First, it generates a public and private key pair. This private key is encrypted using the RSA algorithm with a hardcoded public key stored in the code and sent to the attacker's server. The attacker can decrypt that private key and, after the victim pays the ransom, send that private key to the victim to decrypt their files.

When encrypting files, the ransomware generates a new AES key for each file that will be encrypted. This AES key is then encrypted using the public key and prepended to each encrypted file, resulting in the following pattern: ((AES)public_key + (File)AES).seven

The file structure is seen in Figure 10.

Figure 10. Overview of encrypted file structure

The ransomware encrypts the following filetypes, by going through accessible storage directories:

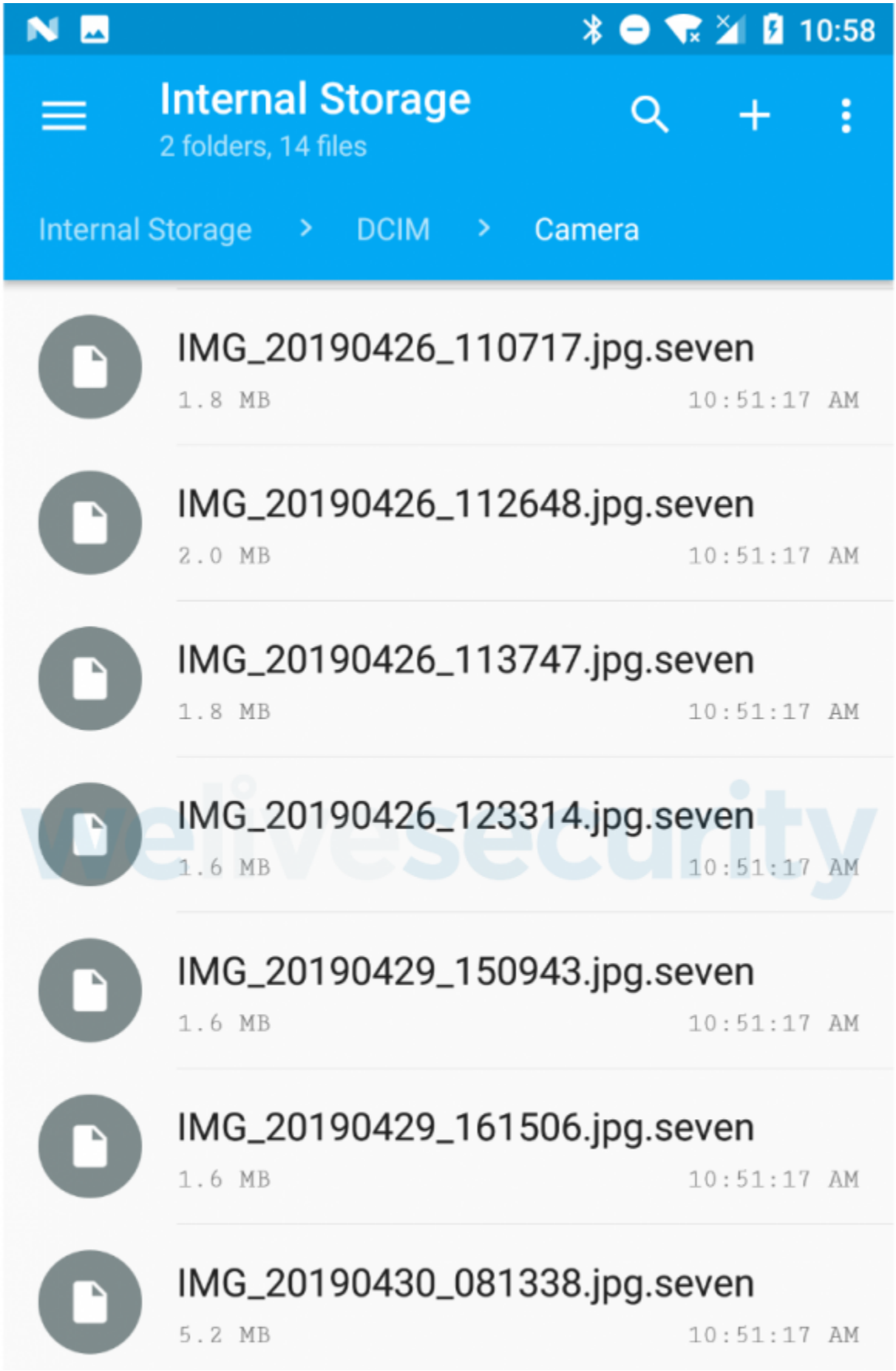
“.doc”, “.docx”, “.xls”, “.xlsx”, “.ppt”, “.pptx”, “.pst”, “.ost”, “.msg”, “.eml”, “.vsd”, “.vsdx”, “.txt”, “.csv”, “.rtf”, “.123”, “.wks”, “.wk1”, “.pdf”, “.dwg”, “.onetoc2”, “.snt”, “.jpeg”, “.jpg”, “.docb”, “.docm”, “.dot”, “.dotm”, “.dotx”, “.xlsm”, “.xlsb”, “.xlw”, “.xlt”, “.xlm”, “.xlc”, “.xltx”, “.xltm”, “.pptm”, “.pot”, “.pps”, “.ppsm”, “.ppsx”, “.ppam”, “.potx”, “.potm”, “.edb”, “.hwp”, “.602”, “.sxi”, “.sti”, “.sldx”, “.sldm”, “.sldm”, “.vdi”, “.vmdk”, “.vmx”, “.gpg”, “.aes”, “.ARC”, “.PAQ”, “.bz2”, “.tbk”, “.bak”, “.tar”, “.tgz”, “.gz”, “.7z”, “.rar”, “.zip”, “.backup”, “.iso”, “.vcd”, “.bmp”, “.png”, “.gif”, “.raw”, “.cgm”, “.tif”, “.tiff”, “.nef”, “.psd”, “.ai”, “.svg”, “.djvu”, “.m4u”, “.m3u”, “.mid”, “.wma”, “.flv”, “.3g2”, “.mkv”, “.3gp”, “.mp4”, “.mov”, “.avi”, “.asf”, “.mpeg”, “.vob”, “.mpg”, “.wmv”, “.fla”, “.swf”, “.wav”, “.mp3”, “.sh”, “.class”, “.jar”, “.java”, “.rb”, “.asp”, “.php”, “.jsp”, “.brd”, “.sch”, “.dch”, “.dip”, “.pl”, “.vb”, “.vbs”, “.ps1”, “.bat”, “.cmd”, “.js”, “.asm”, “.h”, “.pas”, “.cpp”, “.c”, “.cs”, “.suo”, “.sln”, “.ldf”, “.mdf”, “.ibd”, “.myi”, “.myd”, “.frm”, “.odb”, “.dbf”, “.db”, “.mdb”, “.accdb”, “.sql”, “.sqlitedb”, “.sqlite3”, “.asc”, “.lay6”, “.lay”, “.mml”, “.sxm”, “.otg”, “.odg”, “.uop”, “.std”, “.sxd”, “.otp”, “.odp”, “.wb2”, “.slk”, “.dif”, “.stc”, “.sxc”, “.ots”, “.ods”, “.3dm”, “.max”, “.3ds”, “.uot”, “.stw”, “.sxw”, “.ott”, “.odt”, “.pem”, “.p12”, “.csr”, “.crt”, “.key”, “.pfx”, “.der”

However, it doesn’t encrypt files in directories that contain the strings “.cache”, “tmp”, or “temp”.

The ransomware also leaves files unencrypted if the file extension is “.zip” or “.rar” and the file size is over 51,200 KB/50 MB, and “.jpeg”, “.jpg” and “.png” files with a file size less than 150 KB.

The list of filetypes contains some entries unrelated to Android and at the same time lacks some typical Android extensions such as .apk, .dex, .so. Apparently, the list has been copied from the notorious WannaCryptor aka WannaCry ransomware.

Once the files are encrypted, the file extension ".seven" is appended to the original filename, as seen in Figure 11.



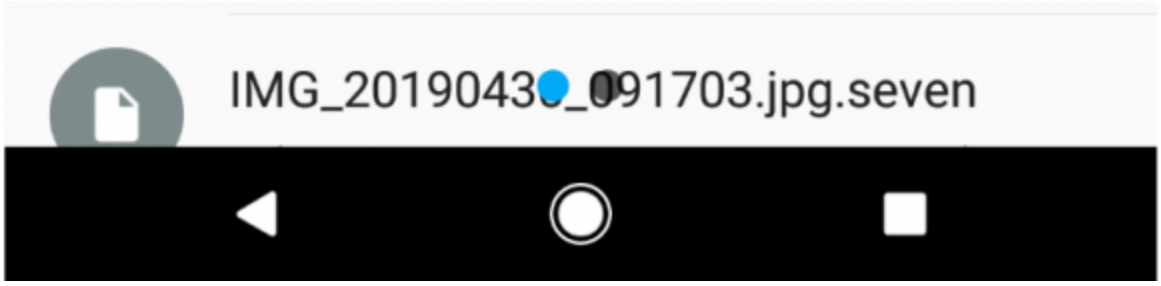


Figure 11. Encrypted files with the extension ".seven"

Decryption mechanism

Code to decrypt encrypted files is present in the ransomware. If the victim pays the ransom, the ransomware operator can verify that via the website seen in Figure 12 and send the private key to decrypt the files.

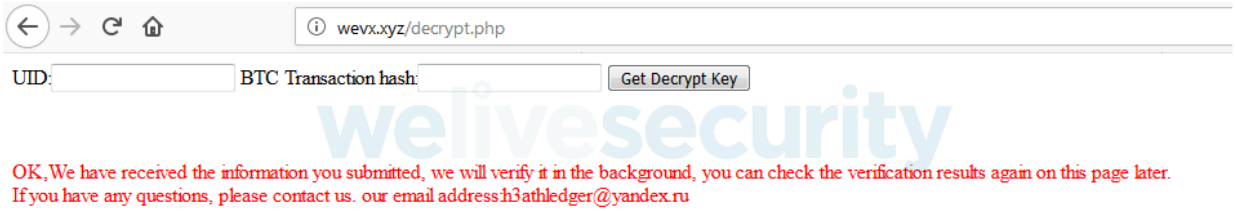


Figure 12. Ransom payment verification web page

How to stay safe

- First of all, keep your devices up to date, ideally set them to patch and update automatically, so that you stay protected even if you're not among the most security savvy users.
- If possible, stick with Google Play or other reputable app stores. These markets might not be completely free from malicious apps, but you have a fair chance of avoiding them.
- Prior to installing any app, check its ratings and reviews. Focus on the negative ones, as they often come from legitimate users, while positive feedback is often crafted by the attackers.
- Focus on the permissions requested by the app. If they seem inadequate for the app's functions, avoid downloading the app.
- Use a reputable mobile security solution to protect your device.

Indicators of Compromise (IoCs)

Hash	ESET detection name
B502874681A709E48F3D1DDFA6AE398499F4BD23	Android/Filecoder.C

Hash	ESET detection name
D5EF600AA1C01FA200ED46140C8308637F09DFCD	Android/Filecoder.C
B502874681A709E48F3D1DDFA6AE398499F4BD23	Android/Filecoder.C
F31C67CCC0D1867DB1FBC43762FCF83746A408C2	Android/Filecoder.C

Bitcoin address

16KQjht4ePZxxGPr3es24VQyMYgR9UEkFy

Servers

http://rich7[.]xyz
http://wevx[.]xyz
https://pastebin[.]com/raw/LQwGQ0RQ

Contact e-mail address

h3athledger@yandex[.]ru

Affected Android versions

Android 5.1 and above

29 Jul 2019 - 04:35PM

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

Newsletter

Discussion