Троян викрадає гроші користувачів Android з облікових записів PayPal

Дослідження ESET
Грудень 2018 р.

НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Дослідники ESET виявили Android троян, який використовує нову техніку зловживання спеціальними можливостями, націлений на офіційний додаток PayPal та здатний обійти двофакторну аутентифікацію

Шкідливе програмне забезпечення, вперше виявлене спеціалістами ESET в листопаді 2018 року, поєднує в собі можливості дистанційного управління банківським трояном та нові можливості шкідливого використання служб спеціальних можливостей Android для націлювання на користувачів офіційного додатка PayPal.

На момент написання дослідження шкідливе програмне забезпечення маскувалось під інструмент для оптимізації роботи акумулятора та поширювалось за допомогою сторонніх магазинів додатків.

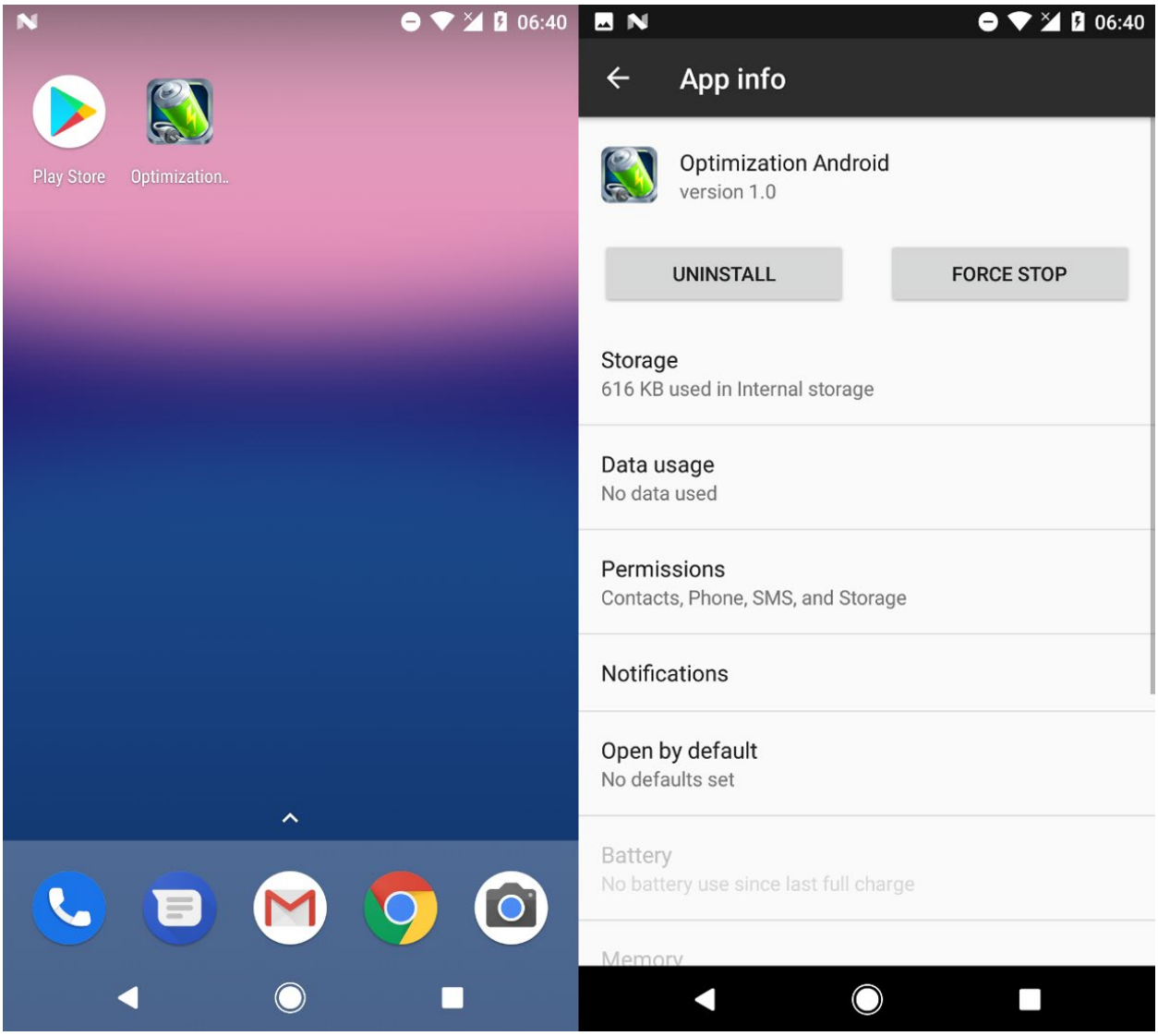

Рис. 1. Маскування, яке використовувало шкідливе програмне забезпеченням на момент написання дослідження

Як працює троян?

Після запуску додаток завершує роботу та приховує свій значок. Згодом функціонал трояна може бути розбитий на дві основні частини, як описано в наступних розділах.

Шкідливі спеціальні можливості, націлені на PayPal

Перша функція зловмисного програмного забезпечення полягає у викраденні грошей з облікових записів PayPal та вимагає активації шкідливих спеціальних можливостей. З рисунка 2 помітно, що цей запит представлений як звичайний запит функції «Увімкнути статистику**»**.

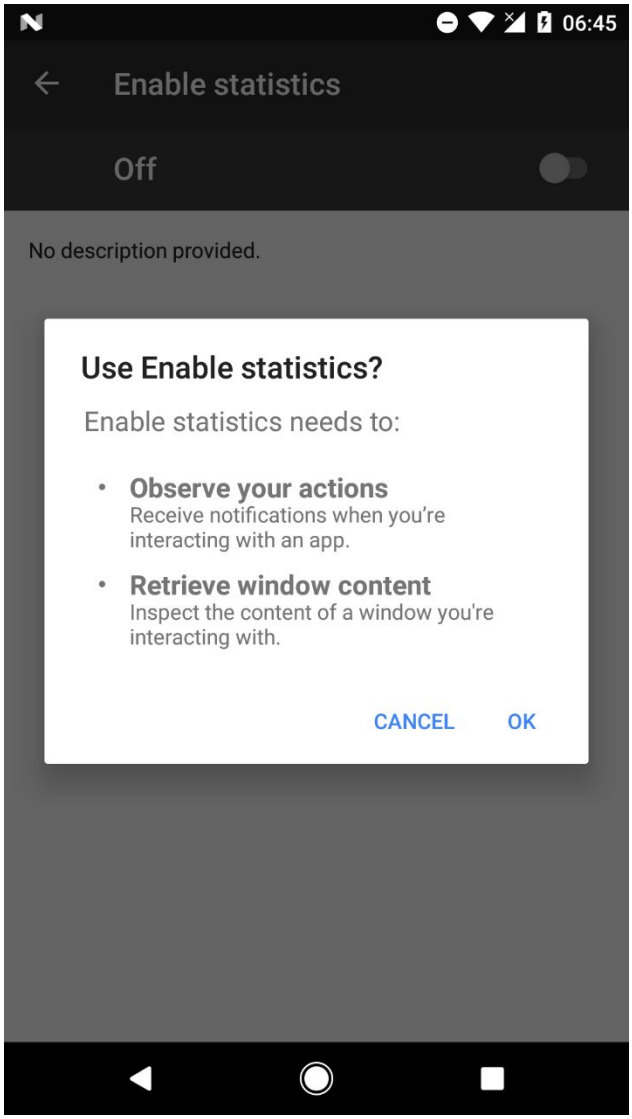

Рис. 2. Шкідливе програмне забезпечення, яке вимагає активації спеціальних можливостей маскуючись під запит функції «Увімкнути статистику»

Якщо на інфікованому пристрої було встановлено офіційний додаток PayPal, шкідливе програмне забезпечення відображало сповіщення, яке спонукало користувача відкрити цей додаток. Коли користувач відкривав додаток PayPal та здійснював вхід до системи, зловмисники, використовуючи шкідливі спеціальні можливості, (якщо перед цим вони були активовані користувачем) повторювали та імітували кліки користувача, щоб надіслати гроші жертви на PayPal адресу зловмисника.

Під час аналізу спеціалістів ESET програма намагалася переказати 1000 євро, але валюта, яка використовується, залежить від місця знаходження користувача. Весь процес триває близько 5 секунд. Для споживача немає реального способу, щоб втрутитися у цей процес.

Оскільки шкідливе програмне забезпечення орієнтується не на крадіжку облікових даних для входу в PayPal та щоб не чекати поки користувачі відкриють офіційний додаток PayPal, троян обходить систему двофакторної аутентифікації PayPal. Користувачі з двофакторною аутентифікацією просто виконують ще один крок у процесі входу в систему, але в кінцевому підсумку вони є такими ж уразливими до атаки трояна, як і ті, хто не використовує аутентифікацію. Відео з демонстрацією того як зловмисники викрадають гроші з рахунків користувачів доступне за посиланням.

Зловмисники не можуть викрасти гроші тільки у випадку, якщо користувач має недостатній баланс PayPal, а до облікового запису не підключено платіжну картку. Шкідливі спеціальні можливості активуються щоразу, коли запускається додаток PayPal, тому атака відбуватися декілька разів.

Спеціалісти ESET повідомили компанію PayPal про шкідливу техніку, яку використовує троянське програмне забезпечення та облікові записи PayPal, з яких зловмисники викрадали кошти.

Банківський троян використовує фішингові екрани

Друга функція зловмисного програмного забезпечення полягає у використанні фішингових екранів, які відображаються замість легітимних додатків.

За замовчуванням шкідливі програми завантажують створені в HTML екрани для п'яти програм — Google Play, WhatsApp, Skype, Viber та Gmail. Цей список є початковим та може змінитися в будь-який момент.

Чотири з п'яти накладених фішингових екранів націлені на визначення деталей кредитної картки (рис. 3); ще один екран націлений на Gmail та з’являється після входу в обліковий запис Gmail (рис. 4). Дослідники ESET вважають, що це пов'язано з особливостями функціонування PayPal, оскільки PayPal надсилає повідомлення на електронну пошту про кожну завершену транзакцію. Маючи доступ до облікового запису Gmail жертви, зловмисники могли видалити такі листи, щоб мати можливість довше залишалися непоміченими користувачами.

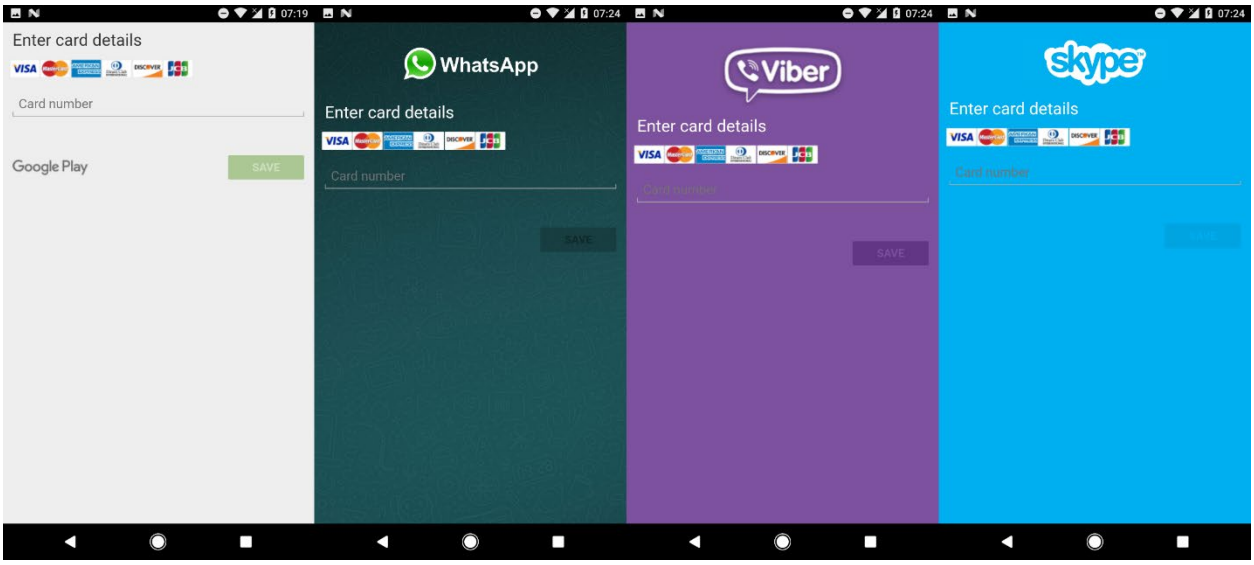

Рис. 3. Шкідливі накладені екрани для Google Play, WhatsApp, Viber та Skype, які вимагають дані про кредитну картку

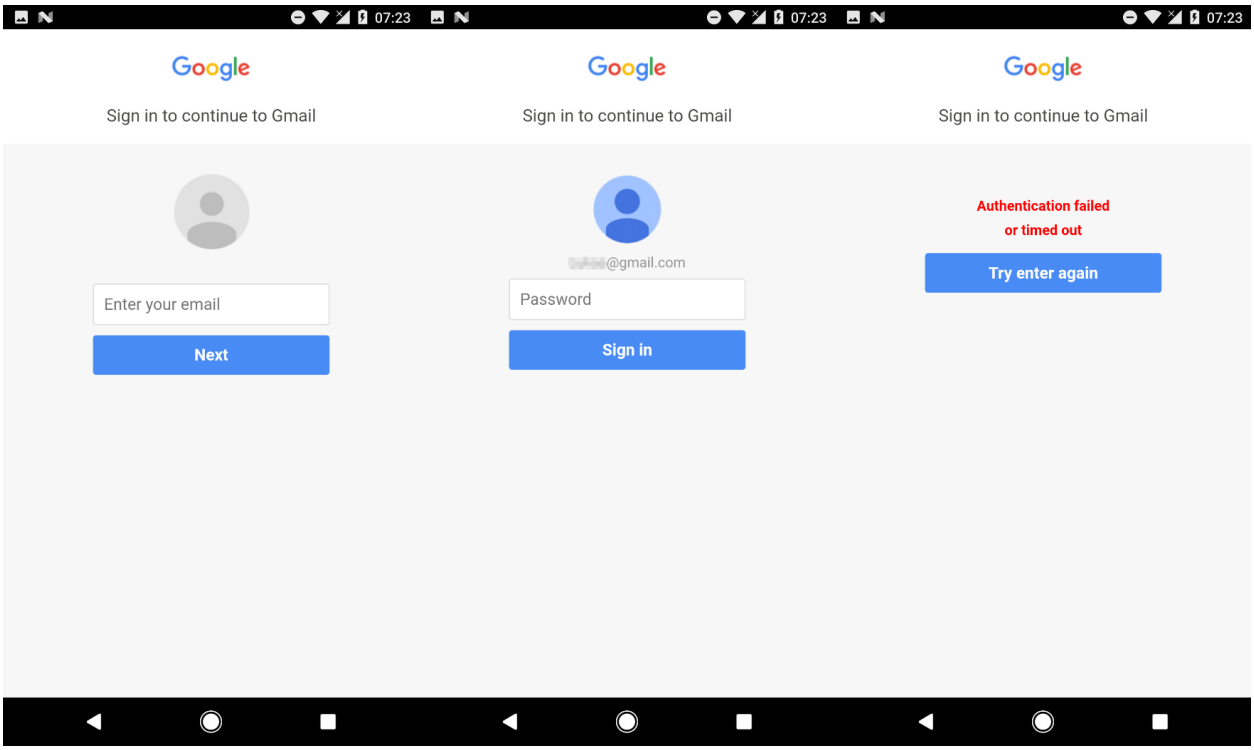

Рис. 4. Шкідливі накладені екрани для фішингу облікових даних Gmail

Спеціалісти ESET також бачили накладені екрани для легітимних банківських додатків, які вимагають введення облікових даних банківських рахунків Інтернет-банкінгу жертв (рис. 5).

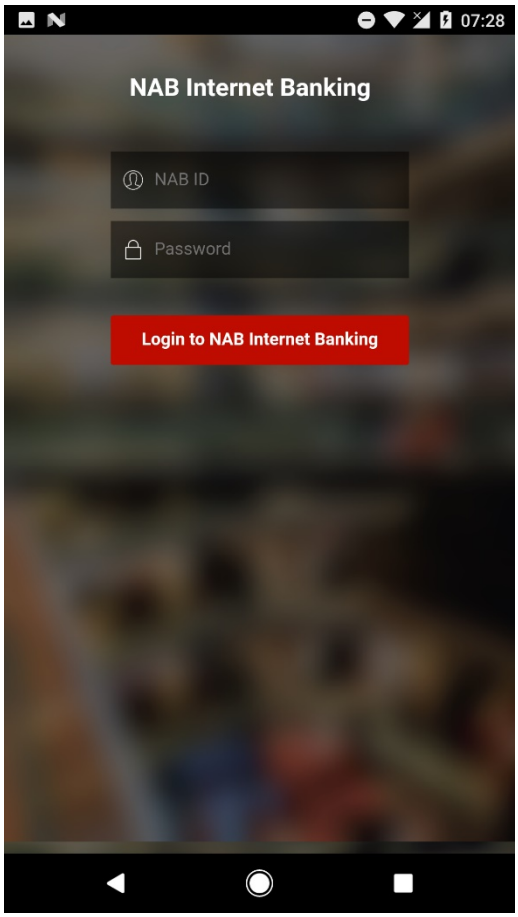

Рис.5. Шкідливий накладений екран для додатку мобільного банкінгу NAB (National Australia Bank)

На відміну від накладених екранів, які використовуються більшістю банківських троянських програм для Android, вони відображаються на екрані блокування. Таку техніку використовують також програми-вимагачі для Android. Даний спосіб дозволяє уникнути видалення накладеного екрану жертвами під час натискать кнопок «Назад» або «Головна». Уникнути накладеного екрана можна заповнивши фальшиву форму. Екран зникне навіть при введенні неправильних даних.

Відповідно до аналізу спеціалістів ESET, автори цього трояна шукали додаткові можливості для механізму накладання екрана. Код шкідливого програмного забезпечення містить рядки, в яких для телефону жертви заблоковано показ дитячої порнографії, але його можна розблокувати, надіславши електронний лист на вказану адресу. Такі рядки в коді нагадують ранні мобільні атаки, коли жертви боялися, вважаючи, що їх пристрої будуть заблоковані поліцією. Невідомо, чи розробники цього трояна планують вимагати у жертв гроші, чи ці функції будуть використовуватися для прикриття інших зловмисних дій.

Крім двох основних функцій, описаних вище, та в залежності від команд, отриманих від командного сервера, шкідливе програмне забезпечення також може:

- Перехоплювати та відправляти SMS-повідомлення; видаляти всі SMS-повідомлення; змінювати додаток для обміну SMS за замовчуванням (для обходу двофакторної аутентифікації на базі SMS)
- Отримувати список контактів
- Здійснювати та переадресовувати дзвінки
- Отримувати список встановлених додатків
- Встановлювати додатки та запускати їх
- Запускати взаємодію сокетів

Троянські програми ховаються і в Google Play

Спеціалісти ESET виявили п'ять шкідливих програм з аналогічними можливостями у магазині Google Play, спрямованих на бразильських користувачів.

Додатки, деякі з яких вже описувались спеціалістами інших антивірусних компаній, є інструментами для відстеження місцезнаходження інших користувачів Android, тепер видалені з Google Play. Насправді, додатки використовують спеціальні можливості для навігації всередині легітимних програм кількох бразильських банків. Крім того, троянські програми виманюють конфіденційну інформацію, накладаючи на додатки фішингові веб-сайти. Додатки, на які націлюється троян наведено в розділі «Ідентифікатори компроментації» цього дослідження.

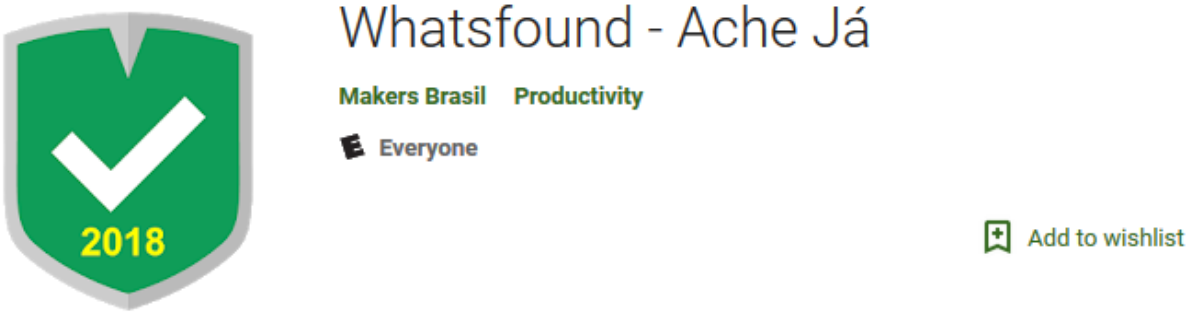

Рис. 6. Один зі шкідливих додатків у Google Play

Дані троянські програми також використовують спеціальні можливості, щоб запобігати спробам видалення під час повторного натискання кнопки «Назад», коли запускається антивірусна програма або додаток для управління пристроєм, на які націлений троян, або коли на екрані з’являються рядки про деінсталяцію.

Як запобігти інфікуванню

Користувачі, які встановили ці шкідливі програми, ймовірно, вже стали жертвою однієї з їх шкідливих функцій.

Якщо ви встановили троян, націлений на PayPal, спеціалісти ESET рекомендують змінити PIN код/пароль кредитної картки, паролі для входу в Інтернет-банкінг, перевірити свої банківські рахунки на наявність підозрілої активності, а також змінити пароль обліково запису Gmail. У випадку виявлення незвичайних операцій, ви можете повідомити про проблему в службу підтримки PayPal.

Для пристроїв, які непридатні для використання через накладення фальшивого екрана блокування, спеціалісти ESET рекомендують використовувати безпечний режим Android та видалити додаток під назвою «Оптимізація Android» у розділі «Налаштування»>«Загальні»>Управління програмами/Програми.

Видалення шкідливого додатку в безпечному режимі рекомендується також бразильським користувачам, які встановили один з троянів в Google Play.

Щоб уникнути інфікування шкідливим програмним забезпеченням, націленим на Android у майбутньому, дослідники ESET радять вам:

- Завантажувати додатки лише з офіційного магазину Google Play
- Під час завантаження додатків із Google Play звертати увагу на кількість завантажень, оцінку програм та відгуки
- Звертати увагу на те, які дозволи ви надаєте встановленим додаткам
- Регулярно оновлювати програмне забезпечення та використовувати надійні рішення для захисту пристроїв

Продукти ESET виявляють та блокують шкідливі програми, як Android/Spy.Banker.AJZ та Android/Spy.Banker.AKB

Ідентифікатори компроментації

Android троян, націлений на користувачів PayPal

SHA-1	ESET detection name
1C555B35914ECE5143960FD8935EA564	Android/Spy.Banker.AJZ

Банківський Android троян, спрямований на бразильських користувачів

Назва пакета	SHA-1	Назва виявлення ESET
service.webview.kiszweb	FFACD0A770AA4FAA261C903F3D2993A2	Android/Spy.Banker.AKB
service.webview.webkisz	D6EF4E16701B218F54A2A999AF47D1B4	Android/Spy.Banker.AKB
com.web.webbrickd	5E278AAC7DAA8C7061EE6A9BCA0518FE	Android/Spy.Banker.AKB
com.web.webbrickz	2A07A8B5286C07271F346DC4965EA640	Android/Spy.Banker.AKB
service.webview.strongwebview	75F1117CABC55999E783A9FD370302F3	Android/Spy.Banker.AKB

Додатки, на які націлена загроза (фішингові накладення)

- com.uber
- com.itaucard
- com.bradesco
- br.com.bb.android
- com.netflix

- gabba.Caixa
- com.itau
- Будь-який додаток, який має рядок «twitter»

Додатки, на які націлена загроза (навігація через додаток)

- com.bradesco
- gabba.Caixa
- com.itau
- br.com.bb
- Any app containing the string “santander”

Додатки для захисту від загроз та управління пристроєм, на які націлена загроза

- com.vtm.uninstall
- com.ddm.smartappunsintaller
- com.rhythm.hexise.uninst
- com.GoodTools.Uninstalle
- mobi.infolife.uninstaller
- om.utils.uninstalle
- com.jumobile.manager.systemapp
- com.vsrevogroup.revouninstallermobi
- oo.util.uninstall
- om.barto.uninstalle
- om.tohsoft.easyuninstalle
- vast.android.mobile
- avast.android.cleane
- om.antiviru
- om.avira.andro
- om.kms.free

Дослідження подано в перекладі. Оригінал доступний за посиланням.