



ANDROID STALKERWARE VULNERABILITIES

Author:
Lukáš Štefanko

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
INTRODUCTION	3
COMPROMISE SCENARIO	3
Who is the attacker?	4
VULNERABILITY CLASSES	4
Takeaways	4
WHY WE DID THIS RESEARCH?	5
SOURCE OF ANDROID STALKERWARE	5
Platform.	6
Not stalkerware	6
Analyzed apps.	7
Payment model limitations	7
UNEXPECTED BEHAVIOR	8
Taking open source premium	8
Metasploit stalkerware.	9
Hardcoded license keys	9
Disabling app notifications	9
App hosted on third-party servers	9
False and misleading claims	10
COORDINATED VULNERABILITY DISCLOSURE	12
ANALYSIS OF ISSUES	12
Insecure transmission of victim and stalker PII (CWE-200)	14
Impact	15
Possible fix	15
Storing sensitive information on external media (CWE-922)	15
Impact	16
Possible fix	16
Exposure of sensitive victim information to unauthorized user (CWE-200)	16
Server leak of stalker information (CWE-200)	18
Impact	18
Unauthorized data transmission from device to server	18
Impact	19
Incorrect permission assignment for devices with superuser privileges (CWE-732)	19
Impact	21
Insufficient verification of client uploaded data (CWE-345)	21
Impact	21
Possible fix	21

Improper authorization of SMS commands (CWE-285)	22
Impact22
Bypass payment to access admin console (CWE-284)	23
Impact23
Command injection (CWE-926)	23
Impact23
Possible fix23
Enforcing weak registration password (CWE-521)	24
Impact24
Missing proper password encryption (CWE-326)	24
Impact25
Possible fix25
Victim data kept on the server after account removal	25
Impact26
Possible fix26
Leak of sensitive information during IPC communication (CWE-927)	26
Impact27
Possible fix27
Partial access to admin console (CWE-285)27
Impact29
Possible fix29
Remote livestream of video and audio from victim device (CWE-284)	29
Impact29
Possible fix29
Running as a system application	29
Possible fix29
Source code and superadmin credentials leak (CWE-200)	29
Impact30
FORENSIC ANALYSIS	30
PREVENTION TIPS31
CONCLUSION31
IOCS	32

Author:

Lukáš Štefanko

May 2021

EXECUTIVE SUMMARY

If nothing else, stalkerware apps encourage clearly ethically questionable behavior, leading most mobile security solutions to flag them as undesirable or harmful. However, given that these apps access, gather, store, and transmit more information than any other app their victims have installed, we were interested in how well these apps protected that amount of especially sensitive data. Hence, we manually analyzed 86 stalkerware apps for the Android platform, provided by 86 different vendors. This analysis identified many serious security and privacy issues that could result in an attacker taking control of a victim's device, taking over a stalker's account, intercepting victim's data, framing the victim by uploading fabricated evidence, or achieving remote code execution on the victim's smartphone. Across 58 of these Android applications we discovered a total of 158 security and privacy issues that can have a serious impact on a victim; indeed, even the stalker or the app's vendor may be at some risk. Following our 90-day coordinated disclosure policy, we repeatedly reported these issues to affected vendors. Unfortunately, to this day, only six vendors have fixed the issues we reported in their apps. Forty-four vendors haven't replied and seven promised to fix their problems in an upcoming update, but still have not released patched updates as of this writing. One vendor decided not to fix the reported issues.

INTRODUCTION

Mobile spying is often the goal of remote threat actors who commonly use social engineering to trick potential victims into installing a malicious application that allows them to remotely access and control the victim's device. This gives an attacker power over individuals to reveal their secrets, follow their steps, snoop on their communications, listen in on their phone calls, observe their habits, access their private files, steal their passwords and possibly blackmail them. In such cases, the attacker is not concerned with the location of the victim and the software used is malicious and can be purchased from underground forums or black markets.

However, similar software – but with a different marketing strategy – can be obtained, even for free in some cases, from dozens of websites. Within the security industry, such software is usually labeled [stalkerware](#). It is also sometimes known as spouseware, although in most cases it is promoted as a tool for monitoring children, employees, girlfriends and/or wives. Successfully locating this kind of tool online isn't difficult at all; you certainly don't have to browse underground websites.

COMPROMISE SCENARIO

So, how does a potential adversary (the role we refer to herein as the "stalker") install a stalkerware app on an Android device? The answer is that it typically takes about two minutes. In this scenario a stalker must have physical access to the intended victim's device, which means the stalker is most likely someone from the victim's family, social or work circles. Lock screen protection must be disabled on the device or the stalker needs to know the unlock PIN, etc. The stalker then visits the stalkerware vendor's website to download and install the app. If the device has security software and/or default Play Protect active, these first need to be deactivated by the stalker, or threat discovery warnings from the security software overridden, to successfully complete the installation.

After launch, the stalkerware app needs to be configured and synchronized with the stalker's account at the associated monitoring service and the app must be allowed all of the Android permissions it requires. The app may also be hidden from the victim's view. In case the victim finds the app in a list of installed apps, it typically will mimic a legitimate system app name such as Settings, Data Controller, Cloud Backup, etc., to create the impression that its extensive list of required permissions is necessary, and that the app shouldn't be removed.

From this moment, the adversary can gather any sensitive information from the targeted device.

As a result of these actions, the stalker may leave behind some traces indicating that the device has been compromised, such as the stalkerware vendor's website not being removed from the browser history or the downloaded installer APK file being left in the Download directory.

Who is the attacker?

In this white paper we define a person who installs and remotely monitors or controls stalkerware as a stalker. We use the term stalker regardless of both the relative status of stalkers and their victims, and of any stated intention. Hence, employers who may, within their jurisdiction, be legally installing such software on company-supplied devices to be used by their employees, or parents installing such software on their children's phones, are considered "stalkers" herein.

Likewise, a victim is a targeted person that a stalker spies on via the stalkerware installed on the device the victim uses and via its associated monitoring service. Victims are usually within the close family, social or employment circles of their stalkers.

Finally, an attacker is a third party whom the stalker and victim are not usually aware of. An attacker can carry out actions such as exploiting security issues or privacy flaws in stalkerware and/or in its associated monitoring services, resulting in the attacker accessing sensitive information about the victim and/or the stalker, taking control of the victim's device, possibly gaining control of a stalker's account on a stalkerware monitoring service, or even gaining control over the whole monitoring service.

VULNERABILITY CLASSES

Vulnerabilities discovered in this research can be divided into three main categories, based on the possibility of misusing them by an attacker:

1. Stalkerware monitoring server issues
2. Application issues
3. Network leaks

Takeaways

These categories require different approaches to exploitation. For server issues, the attacker doesn't need to be authorized to access the victim's, or perhaps stalker's, sensitive data. Exploiting application security problems needs to be done by a third-party app installed on the same device. Network leaks could be misused by an attacker on the same network as the victim.

This research should also serve as a warning to potential future users of stalkerware, to consider using software against their spouses and loved ones (they are from their close circle; they should care about them) since not only is it unethical, but it also might result in revealing private and intimate information of their spouses, children and employees, and expose their victims to risks that might be used against them. Since there could be a close relationship between stalker and victim, it might lead to exposing private information about the stalker as well. During our research, we identified that some stalkerware keeps information about the stalkers using the app and gathers their victims' data on a server, even after the stalkers requested the data's deletion.

WHY WE DID THIS RESEARCH?

Stalkerware gathers, stores, and uploads more, and more sensitive, user data than any other app that its victims have installed, including social media apps.

Based on our detection data, stalkerware apps have become more and more common in the last couple of years (see [Figure 1](#)), which is another reason to find out how they treat their victims' data. In 2019 we saw almost five times more stalkerware detections than in 2018, and in 2020 there were 48% more than in 2019.

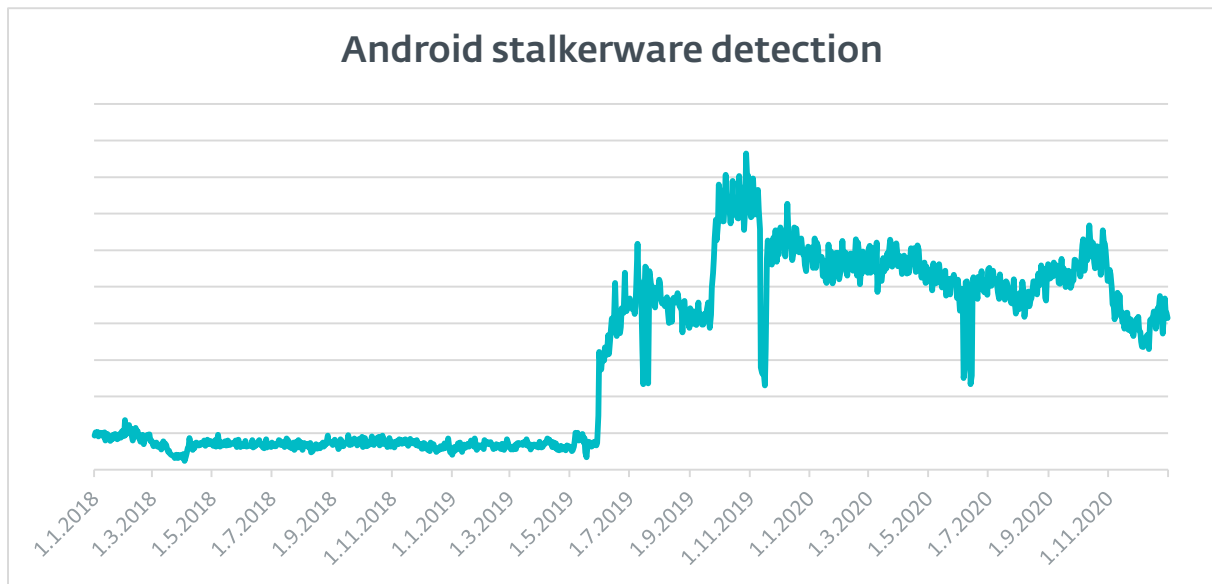


Figure 1 // Based on our detection telemetry, usage of Android stalkerware is increasing

Because of this, we were interested in the security and privacy aspects of these apps, so decided to search for issues that impact the victims, stalkers or vendors.

We were also interested in the ability to perform forensic analysis of a device that has stalkerware installed, with the possibility of recovering valuable data about the date of installation and what data had been extracted, and even whether identifying the stalker might be possible.

Following our reports to vendors, only 7 of 58 vendors whose products were identified as having serious issues had actually fixed them at the time of writing.

SOURCE OF ANDROID STALKERWARE

Our goal was to cover a wide range of Android stalkerware products, based on their popularity using Google search, paid advertisements, and the most prevalent in actual use based on ESET telemetry data.

We analyzed apps from 86 vendors from these sources:

1. Indicators on Stalkerware - <https://github.com/Te-k/stalkerware-indicators>
2. ESET's top detection stats for Android stalkerware
3. Top Google search results
4. Promoted Google Ads

Platform

During our research we focused on the Android platform as it accounts for around 72% of the mobile [market share in the last year](#); all the vendors mainly provide an Android app solution since it doesn't require the stalker to root a device when side-loading a stalkerware app.

From all analyzed vendors, 32 of them also provided an iOS solution. Fortunately for potential victims, installing these apps on iOS devices is much more difficult and requires the stalker to have more technical skill. Based on the instructions available on vendors' websites on how to spy on iOS, we found two ways – the device needs to be jailbroken or the stalker needs to have the victim's iCloud credentials (which are commonly further protected with multifactor authentication).

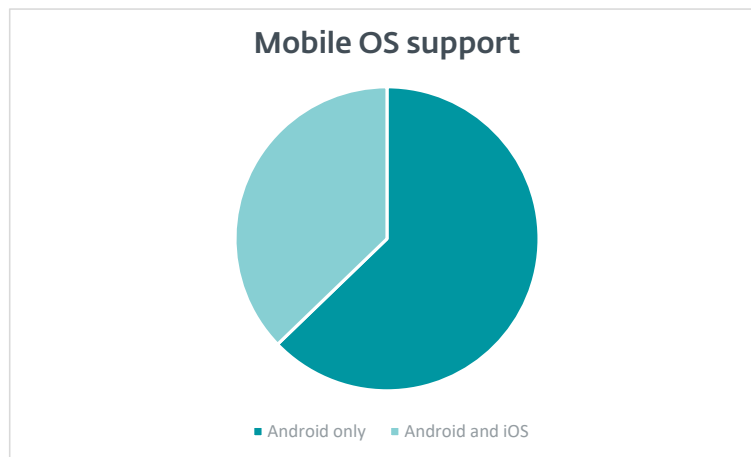


Figure 2 // Stats for mobile stalkerware availability by platform

Not stalkerware

In 2020, Google made a move towards limiting stalkerware app distribution by [restricting these apps on Google Play Store](#) and [not allowing advertisements for them in Google's advertising services](#). Further, as many of these products cannot be purchased using PayPal due to PayPal's restrictions on computer and phone surveillance products, their vendors make other payment methods available.

However, to stay under the radar, the majority of stalkerware providers are presented as child, employee, or women "protectors", yet the word "spy" is used many times on their websites. [Figure 3](#) depicts perhaps the most unsavory example of this that we found.

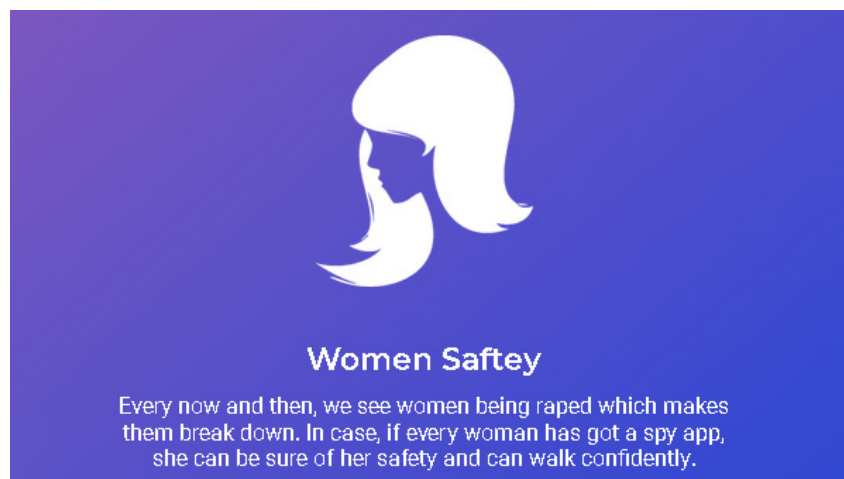


Figure 3 // A stalkerware app's claim to monitor women allegedly for their safety

If we break down these app's claims, their suggestion that they are **child monitors** installed on kids' smartphones doesn't stand up to inspection, as these apps don't offer features to truly protect children; they only spy on them. In a real-world scenario, parents would install parental control apps that prevent their kids from visiting restricted websites, that control the time spent playing games and online, and that review newly installed apps or the device's location. These are the real functions of legitimate "parental control" apps.

Claiming they are **employee monitors** also doesn't stand up to inspection, considering the features these apps provide. At least in BOYD scenarios, it would be an invasion of their privacy since many of the analyzed apps work only if every permission is enabled. It means, that these apps could read and send to the employer all incoming messages from social media apps or SMS, record phone calls and surrounding audio, collect all keystrokes, etc. And, in real employee monitoring situations, that may purportedly protect the employer from liability, legitimate apps would provide functions to prevent accessing various kinds of websites and prevent use of certain apps, rather than just providing functionalities to spy on everything the device's user is doing.

In both cases (child and employee monitor) these apps should be clearly visible so that the user is aware of them. However, most of the analyzed apps could hide themselves from the user's view. The apps that were not hidden disguised their presence as various legitimate-seeming names such as Sync Service, Wifi, Security Service, Data Controller, Cloud Backup, Internet Service, Kernel Launcher, Update, etc.

Analyzed apps

Altogether we analyzed 86 stalkerware apps provided by 86 different vendors. In one case, the same app was offered by two vendors. We counted this as just one app in our statistics. We started to gather apps and manually analyzed them using static and dynamic analysis techniques to observe their behaviors and capabilities.

We focused on privacy and security issues with actual impacts on the victims, stalkers, or vendors. To the extent that we could test flaws in authentication or access control systems on remote devices, we did so only to access data originally sourced from our own test devices. We have not performed any unauthorized remote code execution nor deliberately tried to access data that was not exfiltrated from our own test devices.

This might mean that some further, serious, suspected security or privacy shortcomings were not fully investigated.

This report does not include security issues with minor impact such as logcat leaks, no app restrictions against login brute-force, [Man-in-the-Disk](#) attacks, unused app permissions, disabled SSL CA validation, missing code obfuscation, etc.

Payment model limitations

The goal of stalkerware vendors is to sell their products and services. We tried to gather samples of as many of these apps as possible, but not all the latest versions were available for free (see [Figure 4](#)). We do not want to support these vendors, so we did not purchase any of their products; we worked with apps available either from our samples database or from public sources.

This presented some limitations to our analysis. When analyzing some paid apps, we couldn't perform complete dynamic analysis to observe data exchange with full access to the admin panel, and trial or free versions of some apps do not have all features available, which also limits dynamic analysis.

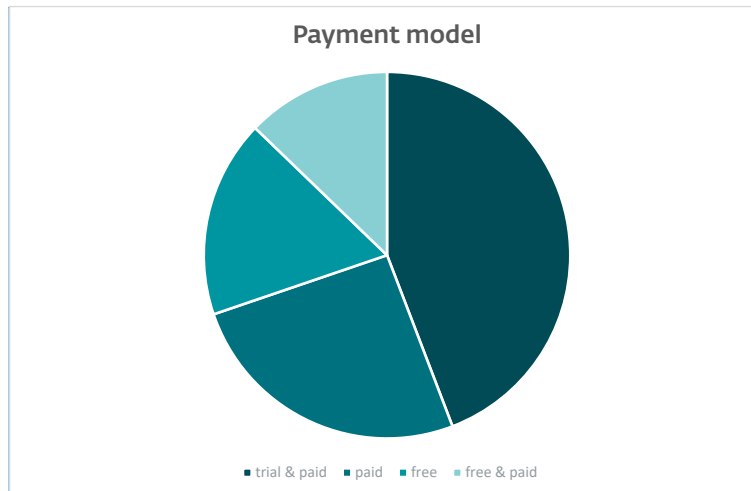


Figure 4 // Analyzed stalkerware apps based on payment model

Because of these limitations, from the 86 available apps, we performed dynamic analysis on 72 of them. We couldn't completely analyze fourteen paid apps. Additionally, not all the paid features were tested in trial and paid apps.

UNEXPECTED BEHAVIOR

During analysis we identified odd app discoveries we believe are important to mention.

Taking open source premium

We identified nine different vendors that have similar product websites and admin consoles, and provide only a paid version of their stalkerware. Following analysis of these apps, we recognized that their source code was the same, including the discovered security issues. Their code is based on the open-source Android spyware called [Droid-Watcher](#) that is available on GitHub (that version's features are presented in [Figure 5](#)), but with expanded and updated functionality, since Droid-Watcher was published seven years ago and has been unmaintained since.

Droid-Watcher

Droid-Watcher - Android Spy Application

Description:

Program features:

- Transfer incoming/outgoing sms (including info about the sender and message text).
- Transfer the log of incoming/outgoing calls.
- Daily reports in html format and .xlsx
- Transferring GPS coordinates of the phone after a specified interval
- Notification by SMS about the change sim-card
- Remote control program settings
- Record phone conversations and send them to e-mail
- Copying and sending to e-mail photos taken with the phone camera
- Screenshots at a specified interval (root; Android 4.0+)
- Copy of the official correspondence of the customer "Vkontakte" (root)
- Copies of the correspondence "WhatsApp" (root)
- Automatic update of the application without user (root)
- Display of location of the device in real-time (pro)
- The picture with the front camera phone at an unlock (pro)

Figure 5 // Droid-Watcher features

Metasploit stalkerware

Metasploit is a free penetration testing framework that can be also used in offensive security. Hence, using Metasploit it is possible to generate Android spying applications that are remotely controlled. It is important to state that Metasploit payloads are widely detected as trojans and often used by threat actors of many stripes.

One stalkerware vendor decided to use a Metasploit payload and provided it on their site as a monitoring app. This appears to be a quick-and-dirty way to get into the stalkerware business.

Hardcoded license keys

Some stalkerware doesn't even protect itself from piracy; in one app, we found hardcoded license keys in cleartext, not protected from reverse engineering in any way. Because of that, it would be simple to steal the software.

Disabling app notifications

App notifications can display app warnings, upcoming updates or errors. As seen in [Figure 6](#), a couple of stalkerware apps would request, during initial set up, that the stalker block all the app's notifications, which would hide any stalkerware presence through such notifications.

This clearly states that this stalkerware app must be hidden, in all cases, from the victim's view.

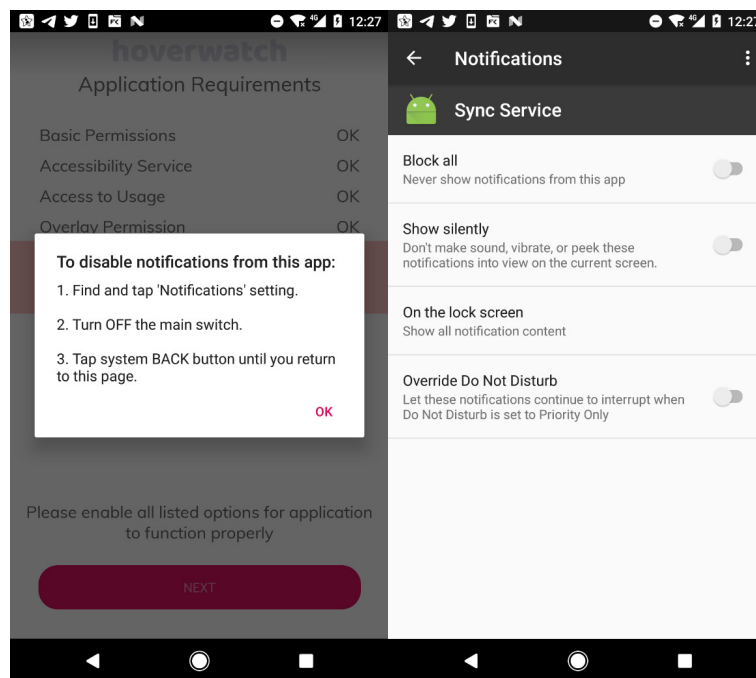


Figure 6 // Block all notifications request

App hosted on third-party servers

Some stalkerware, such as seen in [Figure 7](#), provided its app to download not from its own server, but rather from third-party file hosting services. This is slightly surprising and might raise a question about legitimacy, since the app could have been modified or the link redirected.

It is also worth noting that one of the install instructions for many stalkerware apps (again, as seen in [Figure 7](#)) is to disable default Android security – Google Play Protect – that afterwards leaves devices unprotected from other threats and stalkerware itself.

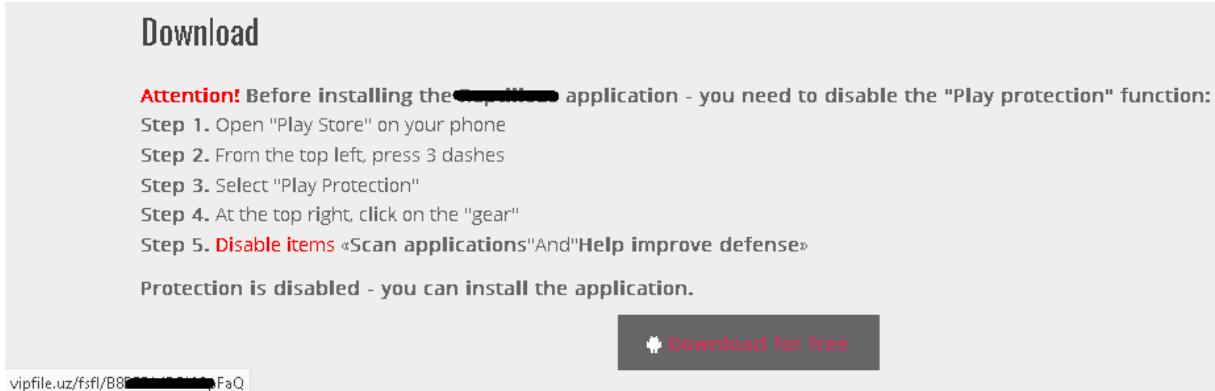


Figure 7 // Downloading stalkerware from file upload service

False and misleading claims

Some of the vendors present a lot of claims on their websites to attract more potential clients. Most of these claims simply can't be verified by a third party, such as the number of clients or positive reviews from clients; however, in some cases this was possible. The Tracker Spy app (now offline) claimed, as can be seen in Figure 8, to have 120,000 "happy clients" and 90,000 app downloads.

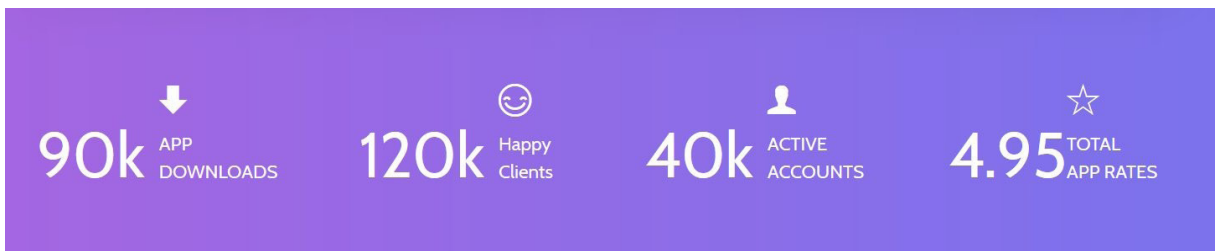


Figure 8 // Reputed popularity of the Tracker Spy app

It seems unlikely that 30,000 of their customers would be "happy" to have paid for this app and then not downloaded, installed and used it for its intended purposes. Further, in 2018 this app was available for a month on Google Play Store, but achieved only 100+ installs (meaning 101–999). It seems highly improbable that it would have been downloaded from the vendor's website more than 89,000 times.

Most vendor websites include reputed client reviews, where we believe most to be fake or default reviews included as part of the website design's template, including fictitious names and companies for which they supposedly work, as well as stock or "stolen" images being used. For example, the stalkerware review image seen in Figure 9 is apparently cropped from the stock image in Figure 10, or maybe from an online advertisement for a reputable skin care product range (not shown) that also used the same stock image.

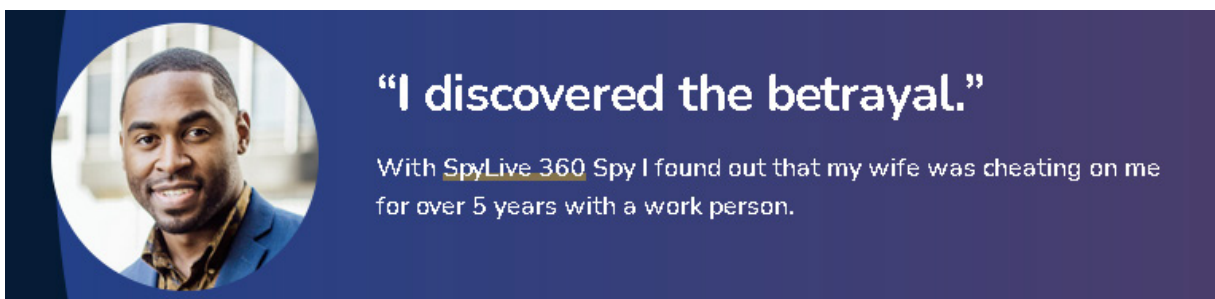


Figure 9 // Apparent stalkerware client review



Figure 10 // This photo is available on a stock image website (https://unsplash.com/photos/29pFbI_D1Sc)

One of the ways to attract potential clients is by falsely increasing product credibility with such fake customer reviews.

Another app was claiming to be participating in child support programs (see Figure 11) and to have been positively reviewed by major media outlets (see Figure 12). However, we couldn't find the source on those brands official websites; the only mention was on the stalkerware site.



Figure 11 // Claiming to be part of various official child protection programs

In The Media



<div style="text-align: center; margin-bottom: 10px;">  </div> <p style="text-align: center;">"████████ offers the most monitoring-featured solutions of all the software on our lineup. It does a lot to help monitor any computer and to keep home safe.</p> <p style="text-align: center;">– PC Magazine</p>	<div style="text-align: center; margin-bottom: 10px;">  </div> <p style="text-align: center;">"████████ provides reliable and effective employee surveillance solution. It offers top notch service and top notch results."</p> <p style="text-align: center;">– NBC</p>
--	---

Figure 12 // Claiming to be quoted in the media

COORDINATED VULNERABILITY DISCLOSURE

ESET follows a 90-day *coordinated disclosure period* when reporting security and privacy issues to other vendors. Our goal is to make sure the vendor receives reports and has sufficient time to respond and fix the issue. To this end, we made as many as three notification attempts, based on contacts available on the affected vendors' websites.

We attempted to contact affected vendors via email address, by creating a support ticket or, in some cases, we used both when we did not receive a timely first response. Our email messages briefly informed the affected vendors of the issues we had found and their impact. In two cases, we were not successful in delivering these notifications to a vendor because our email wasn't delivered due, in one case, to the recipient inbox apparently being full and, in the other case, creating a new support ticket always resulted in an error.

We started reporting these vulnerabilities to affected vendors on December 19, 2020. Among the 86 apps tested, we discovered serious issues in 58 of them. Fourteen vendors communicated with us. Seven of them have already patched the issues. Six vendors responded that they would issue a patch but these apps are still not fixed at the time of writing. One of these vendors decided not to fix the reported issues. From the remaining 44 vendors we have had no response, even after following notifications through email or their support.

As most of the reported security issues have not been fixed, we decided not to link any security issues to specific apps or vendors so as to not negatively affect victims of these stalkerware apps.

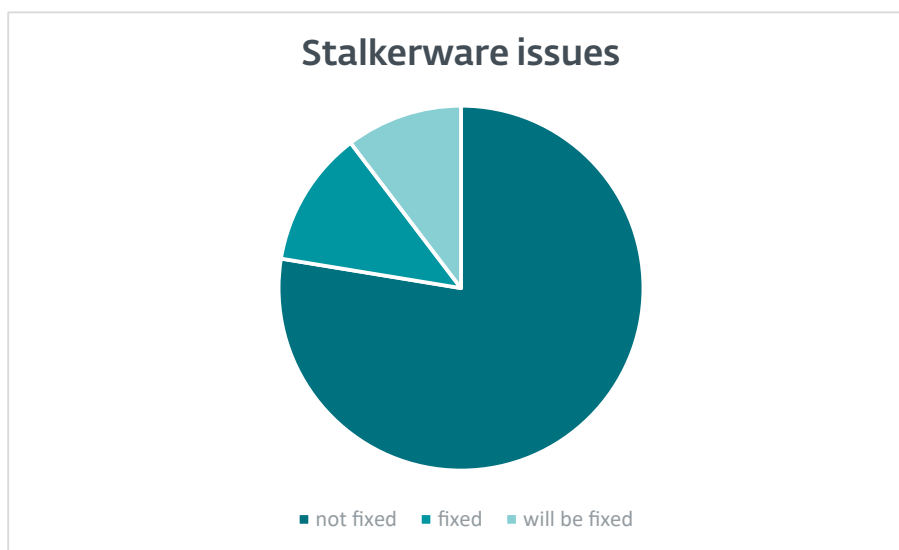


Figure 13 // Statistics of security issues that are or will be fixed

ANALYSIS OF ISSUES

As we mentioned above, 58 of the analyzed apps had security or privacy issues; only 28 had no such issues that we were able to find.

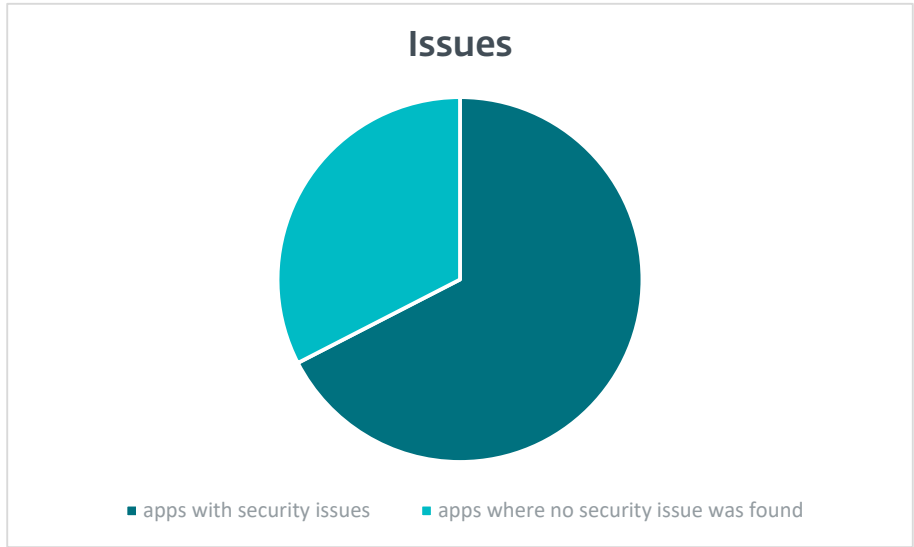


Figure 14 // Balance of security issues found

Altogether, in those 58 stalkerware apps, we found 158 security and privacy issues. In Figure 15, these issues are ordered based on prevalence of occurrence across the analyzed stalkerware apps.

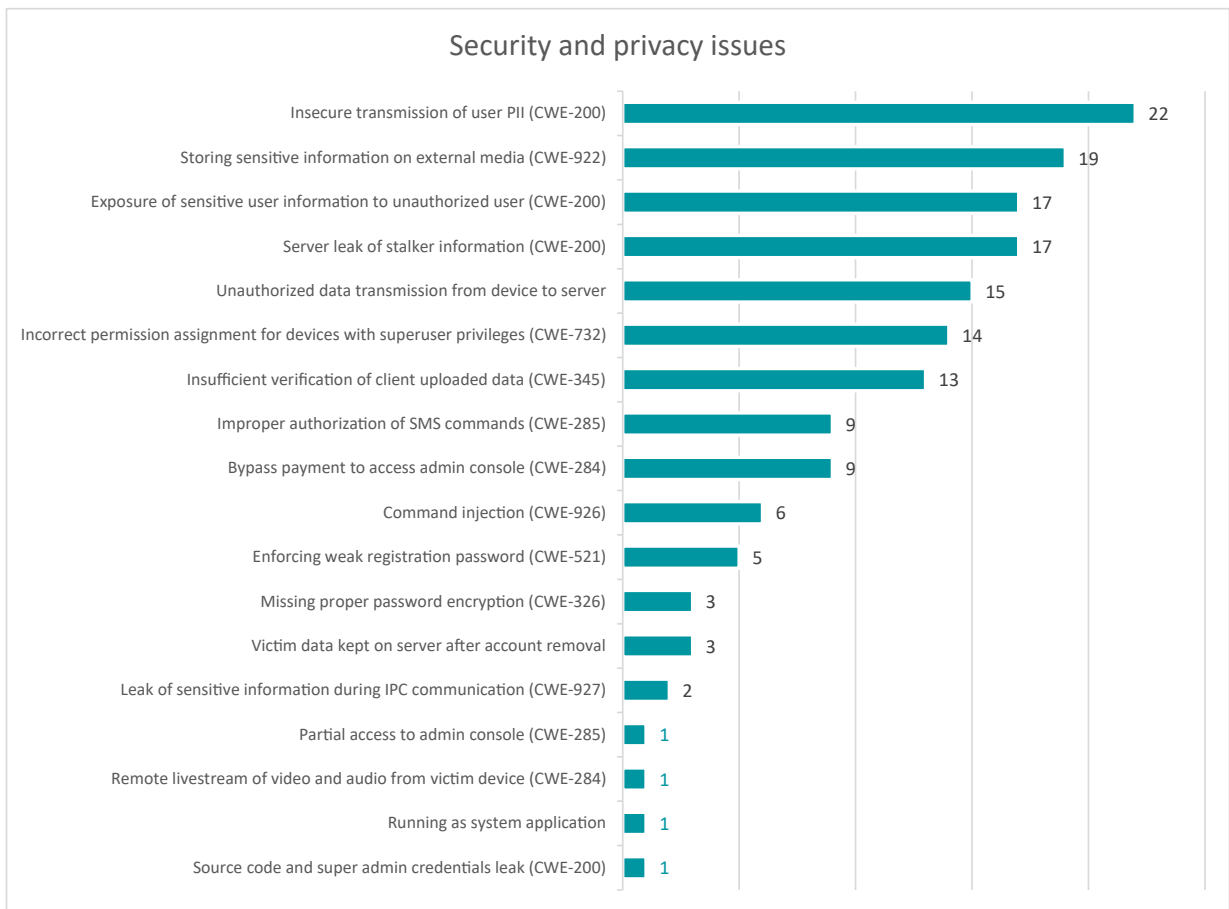


Figure 15 // Breakdown of security and privacy issues uncovered in this research

Below, we briefly discuss each of these 18 categories of vulnerabilities and privacy shortcomings.

Insecure transmission of victim and stalker PII (CWE-200)

This was the issue identified most often, discovered in 22 stalkerware apps. Sensitive victim and/or stalker information was transmitted from victim devices to the stalkerware server over the unencrypted HTTP protocol and was not further protected – without integrity check or encryption. [Figure 16](#), [Figure 17](#) and [Figure 18](#) provide just three of very many sad episodes of such bad practice that we observed in this research.

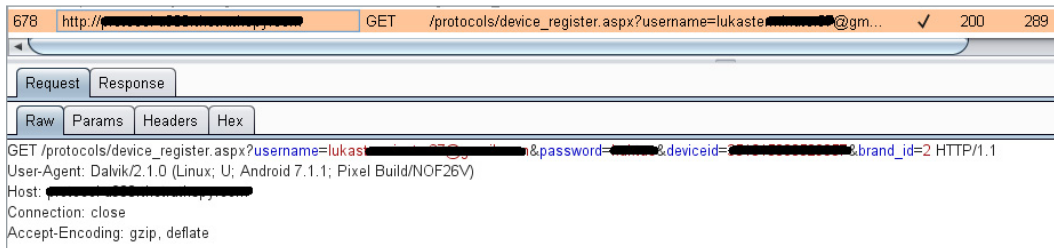


Figure 16 // Registering device to a server

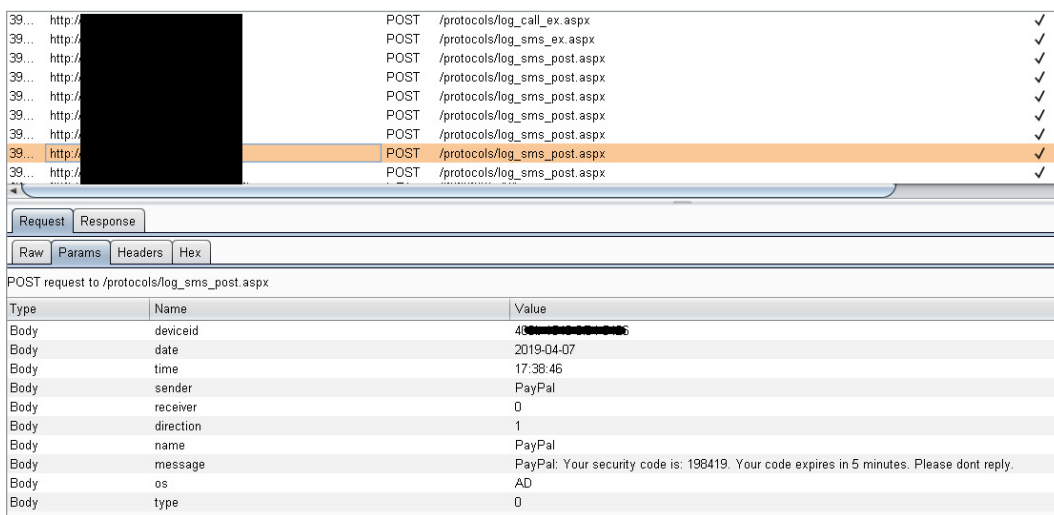


Figure 17 // Data extraction from victim's device

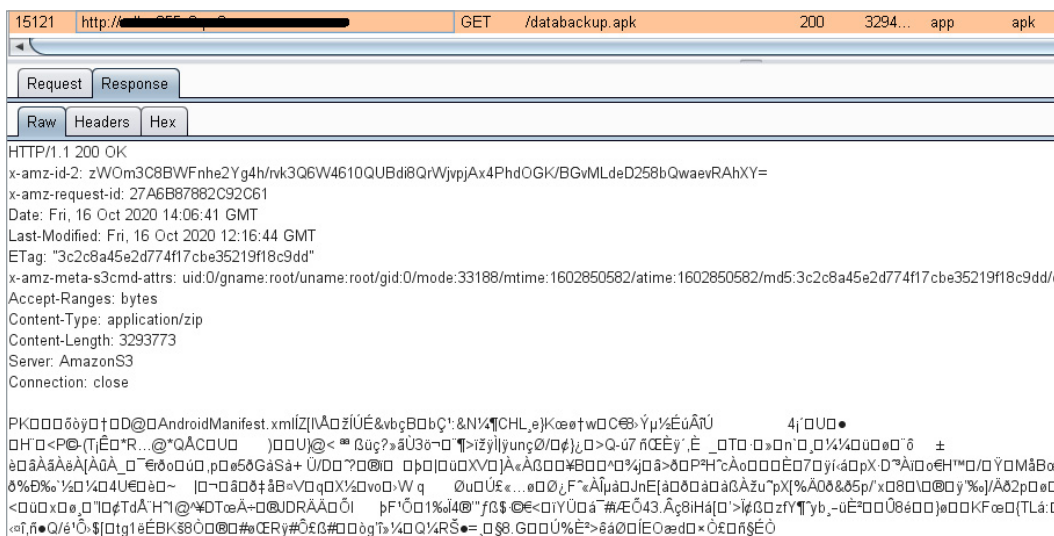


Figure 18 // Downloading payload of stalkerware

Impact

An attacker on the same network could intercept network traffic and steal or change transmitted data. Because of that, it would be possible to obtain admin credentials, all uploaded data such as text messages, call log, contact list, keystroke logs, browsing history, recorded phone calls, pictures, screenshots or even replace downloaded binary files that will be executed without integrity check. As a result, the attacker could take over the stalker's account, access the victim's private information and trigger remote code execution.

Possible fix

Use the HTTPS protocol to transmit user PII. Further, use an additional layer of end-to-end encryption.

Storing sensitive information on external media (CWE-922)

Stalkerware's main goal is to gather personal information and send it to the stalkerware server where it can be viewed by the stalker. These files first need to be stored on the victimized device and then transmitted. Unfortunately, 19 analyzed apps store files such as keystroke logs, photos, recorded phone calls, recorded surrounding audio, calendar events, browser history, contact lists, received number, account tokens, etc. on external media that is shared with other apps installed on the device and accessible with the `android.permission.WRITE_EXTERNAL_STORAGE` permission. Some examples are provided in [Figure 19](#), [Figure 20](#) and [Figure 21](#).

This applies only to Android devices with OS below Android 10, because of [scoped storage](#) implemented in apps targeting Android 10 and higher, which restricts access to application data directories on external storage. In some cases these files are stored temporarily; however, they could still be successfully accessed by an adversary.

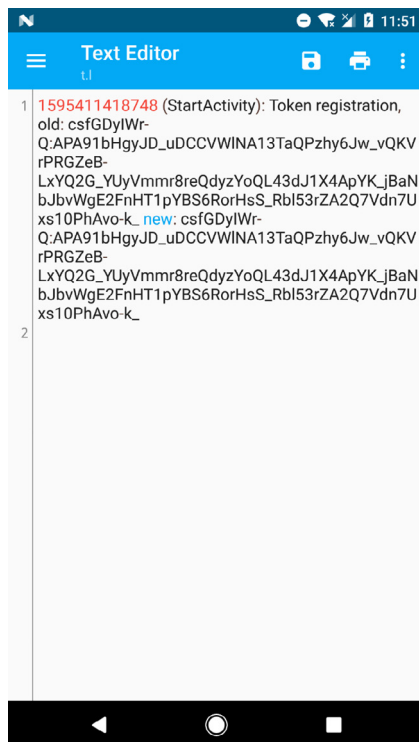


Figure 19 // Admin account token permanently stored on external media

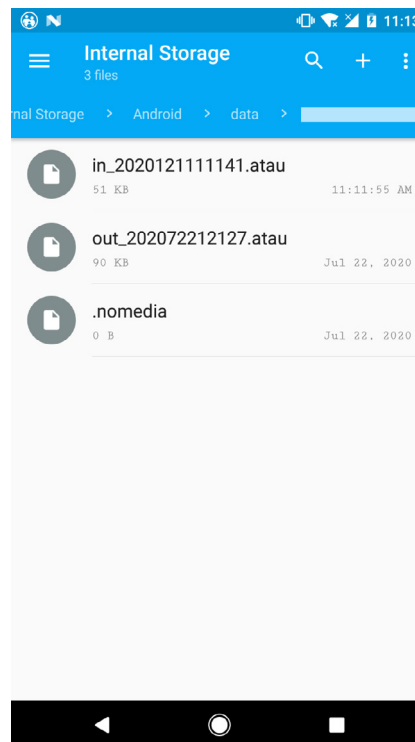


Figure 20 // Insecurely stored incoming and outgoing recorded phone calls


```

[Password] $com.paypal.android.p2pmobile$1601026221414$1$true
[.] $com.paypal.android.p2pmobile$1601026222785$1$true
[p] $com.paypal.android.p2pmobile$1601026222791$1$true
[p.] $com.paypal.android.p2pmobile$1601026223582$1$true
[.a] $com.paypal.android.p2pmobile$1601026223589$1$true
[.a.] $com.paypal.android.p2pmobile$1601026224107$1$true
[.s] $com.paypal.android.p2pmobile$1601026224132$1$true
[.s.] $com.paypal.android.p2pmobile$1601026224553$1$true
[.s.s] $com.paypal.android.p2pmobile$1601026224567$1$true
[.s.s.] $com.paypal.android.p2pmobile$1601026225292$1$true
[.s.w] $com.paypal.android.p2pmobile$1601026225315$1$true
[.s.w.] $com.paypal.android.p2pmobile$1601026225526$1$true
[.s.o] $com.paypal.android.p2pmobile$1601026225551$1$true
[.s.o.] $com.paypal.android.p2pmobile$1601026225744$1$true
[.s.r] $com.paypal.android.p2pmobile$1601026225773$1$true
[.s.r.] $com.paypal.android.p2pmobile$1601026226167$1$true
[.s.d] $com.paypal.android.p2pmobile$1601026226186$1$true
[.s.d.] $com.paypal.android.p2pmobile$1601026226669$1$true
[.s.1] $com.paypal.android.p2pmobile$1601026226681$1$true
[.s.1.] $com.paypal.android.p2pmobile$1601026227142$1$true
[.s.2] $com.paypal.android.p2pmobile$1601026227158$1$true
[.s.2.] $com.paypal.android.p2pmobile$1601026227605$1$true
[.s.3] $com.paypal.android.p2pmobile$1601026227621$1$true

```

Figure 21 // Stored keystroke logs including typed passwords

Impact

Any third-party app installed on a device could access these files without proper permission. Such an app would only need `android.permission.WRITE_EXTERNAL_STORAGE` permission.

Possible fix

Store sensitive data in internal app's storage or encrypt them before storing on external storage.

Exposure of sensitive victim information to unauthorized user (CWE-200)

Stalkerware servers exposed user data stored on them, either through open directory listings (see [Figure 22](#)) or predictable names. It would be possible for an attacker to access what seem to be recorded calls, photos, email addresses, IP logs, IMEI numbers, phone numbers, usernames, addresses, call logs, text messages, Facebook and WhatsApp messages, GPS locations or even source code and backups and other data without any authentication. We identified 17 apps with such leaks, and a few examples are displayed in [Figure 23](#), [Figure 24](#) and [Figure 25](#).

Data leak	File count
IP logs	1,353,000+
User pictures	182,000+
Client info (IMEIs, usernames, addresses, SMSes, etc.)	167,000+
Recorded phone calls	130,000+
IMEI numbers	11,200+
Client emails	3,750+

Figure 22 // Leaked and accessible victim data files

Name	Last modified	Size	Description
Parent Directory	-	-	-
l...m/	2018-05-31 08:07	-	-
s...@gmail.com/	2018-05-31 08:04	-	-
t.../	2018-05-31 07:52	-	-
f...dj@gmail.com/	2018-05-31 07:48	-	-
f...ail.com/	2018-05-31 06:52	-	-
c...mail.com/	2018-05-31 06:02	-	-
f...mail.com/	2018-05-31 05:59	-	-
f...com/	2018-05-31 05:38	-	-
s.../	2018-05-31 04:34	-	-
f...l.com/	2018-05-31 03:47	-	-
c...ail.com/	2018-05-31 00:30	-	-
l...nail.com/	2018-05-30 22:02	-	-
f...nail.com/	2018-05-30 18:33	-	-
h...mail.com/	2018-05-30 18:14	-	-
u...n/	2018-05-30 17:15	-	-
t.../	2018-05-30 16:12	-	-
l...gmail.com/	2018-05-30 14:32	-	-
s...nail.com/	2018-05-30 13:58	-	-
f...ail.com/	2018-05-30 13:54	-	-
f...m/	2018-05-30 13:13	-	-
s...nail.com/	2018-05-30 11:54	-	-
s...@gmail.com/	2018-05-30 11:02	-	-
s...nail.com/	2018-05-30 10:34	-	-
s...nail.com/	2018-05-30 10:12	-	-
l...nail.com/	2018-05-30 10:11	-	-
f...gmail.com/	2018-05-30 07:59	-	-
f...ikh0@gmail.com/	2018-05-30 06:43	-	-
y...mail.com/	2018-05-30 06:31	-	-
s...gmail.com/	2018-05-30 05:04	-	-
f...ail.com/	2018-05-30 04:19	-	-

Figure 23 // Victim data available based on email address

Name	Last modified	Size	Description
Parent Directory	-	-	-
file_incoming +...	2019-11-11 15:34	18K	-
file_incoming +...	2019-11-12 06:12	72K	-
file_incoming +...	2019-11-11 15:35	14K	-
file_incoming +...	2019-11-13 21:56	57K	-
file_incoming +...	2019-11-12 07:13	40K	-
file_incoming +...	2019-11-11 22:26	19K	-
file_incoming +...	2019-11-11 02:22	14K	-
file_incoming +...	2019-11-11 00:19	81K	-
file_incoming +...	2019-10-24 16:15	37K	-
file_incoming +...	2019-10-25 20:21	45K	-
file_incoming +...	2019-10-25 04:07	219K	-
file_incoming +...	2019-11-12 18:36	103K	-
file_incoming +...	2020-01-18 14:49	81K	-
file_incoming +...	2020-01-18 22:35	68K	-
file_incoming +...	2020-01-19 11:30	141K	-
file_incoming +...	2020-01-19 11:46	141K	-
file_incoming +...	2020-01-18 13:55	165K	-
file_incoming +...	2020-01-18 15:06	626K	-
file_incoming +...	2020-01-17 15:36	317K	-
file_incoming +...	2020-01-17 20:26	1.1M	-
file_incoming +...	2020-01-18 14:06	936K	-
file_incoming +...	2019-11-28 15:33	231K	-
file_incoming +...	2019-11-27 12:10	59K	-
file_incoming +...	2019-11-26 15:36	104K	-
file_incoming +...	2019-11-27 04:42	348K	-
file_incoming 07...	2019-11-03 11:18	153K	-
file_incoming 07...	2019-11-02 21:06	165K	-
file_outgoing +1...	2019-11-12 07:14	38K	-
file_outgoing +1...	2019-11-11 04:41	163K	-
file_outgoing +1...	2019-11-12 09:51	39K	-
file_outgoing +1...	2019-11-12 19:52	97K	-
file_outgoing +1...	2019-11-13 08:05	13K	-
file_outgoing +1...	2019-11-12 04:10	131K	-
file_outgoing +1...	2019-11-10 22:52	9.6K	-
file_outgoing +1...	2019-11-11 08:47	10K	-
file_outgoing +1...	2019-11-12 06:04	29K	-

Figure 24 // Recorded phone calls

Name	Last modified	Size	Description
Parent Directory	-	-	-
File 1...06.mp4	2019-11-04 19:00	40M	-
File 1...90.mp4	2019-11-04 20:41	60K	-
File 1...89.mp4	2019-11-05 06:40	97K	-
File 1...89.mp4	2019-11-06 14:19	797K	-
File 1...28.mp4	2019-11-06 23:21	2.5M	-
File 1...56.mp4	2019-11-07 00:23	32M	-
File 1...28.mp4	2019-11-07 01:02	927K	-
File 1...87.mp4	2019-11-07 01:13	49M	-
File 1...13.mp4	2019-11-07 02:05	22M	-
File 1...89.mp4	2019-11-07 02:18	43M	-
File 1...68.mp4	2019-11-07 16:30	24K	-
File 1...95.mp4	2019-11-07 16:41	27M	-
File 1...15.mp4	2019-11-07 16:51	4.6M	-
File 1...42.mp4	2019-11-07 18:16	1.1M	-
File 1...84.mp4	2019-11-07 18:30	3.4M	-
File 1...04.mp4	2019-11-08 04:15	777K	-
File 1...41.mp4	2019-11-08 04:20	485K	-
File 1...77.mp4	2019-11-08 04:23	1.2M	-
File 1...50.mp4	2019-11-08 04:24	1.1M	-
File 1...50.mp4	2019-11-09 16:24	1.1M	-
File 1...15.mp4	2019-11-10 10:18	3.1K	-
File 1...26.mp4	2019-11-14 01:31	89K	-
File 1...96.mp4	2019-11-14 01:41	587K	-
File 1...28.mp4	2019-11-14 01:42	104K	-
File 1...53.mp4	2019-11-14 01:46	188K	-
File 1...96.mp4	2019-11-14 01:47	131K	-
File 1...77.mp4	2019-11-15 06:13	348K	-
File 1...18.mp4	2019-11-15 06:27	283K	-
File 1...56.mp4	2019-11-15 06:27	196K	-
File 1...28.mp4	2019-11-16 00:33	3.8M	-
File 1...44.mp4	2019-11-18 16:48	46K	-
File 1...93.mp4	2019-11-22 12:51	515K	-
File 1...57.mp4	2019-12-06 13:45	525K	-
File 1...82.mp4	2020-01-06 01:06	50K	-
File 1...28.mp4	2020-01-06 15:47	4.6M	-
File 1...57.mp4	2020-01-28 14:10	121K	-

Figure 25 // Video recordings of a victim devices' screens

Server leak of stalker information (CWE-200)

When a victim identifies stalkerware on a device, either using security software or forensic analysis, in some cases it is possible to retrieve information from the app vendor's server about the stalker (see [Figure 26](#)) and possibly what data were gathered. All the victim needs to know is the unique device ID. Most of the stalkerware that had this issue used IMEI, `android_id` or serial number as the device ID.

This happens because the server API returns client (i.e. the stalker's) data in response to unauthenticated requests. Using this technique, it is possible to verify whether stalkerware was used against this smartphone in the past, as seen in [Figure 27](#).

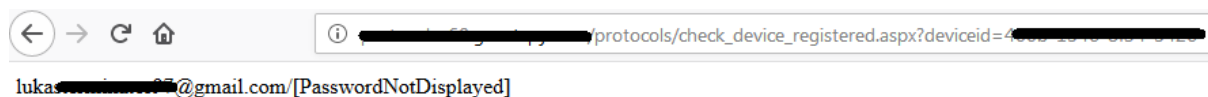


Figure 26 // Retrieving the stalker's email address

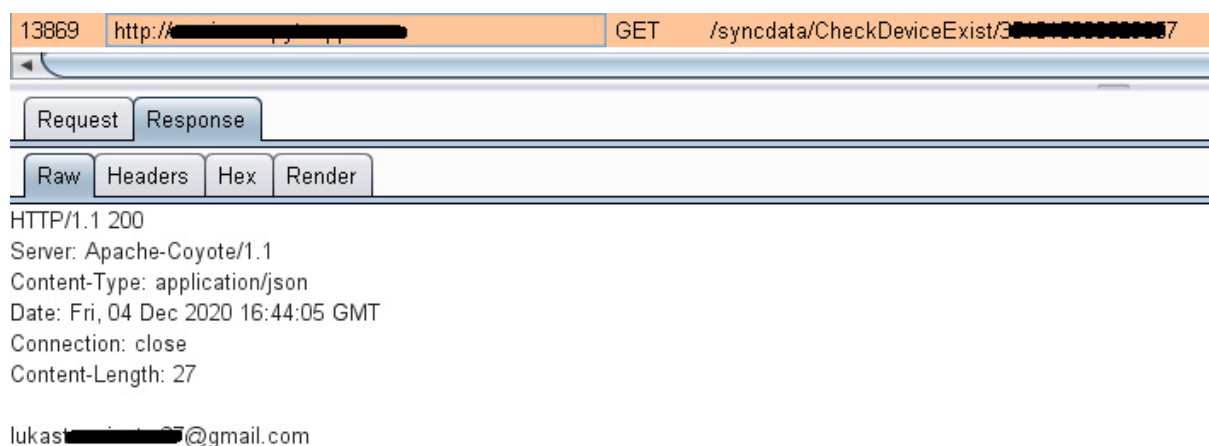


Figure 27 // Retrieving the stalker's email address from a different stalkerware server

Impact

Leak of victim's and stalker's data based on the unique device ID. This possibly creates an opportunity to brute-force device IDs and dump all the stalkerware clients.

Unauthorized data transmission from device to server

This behavior is more typical of malicious apps and was observed in 15 analyzed apps. The problem is that an app sends sensitive victim data such as call logs, email addresses, text messages, etc. to the stalkerware server before the stalker registers and sets up an account ([Figure 28](#)). This behavior might be a problem in two cases. If the stalker installs the app and after launch realizes that it doesn't provide all its features for free, the app might be removed without being used, yet the victim's PII might still remain on the stalkerware server. In the other case, once the license has expired, the stalkerware still sends victim PII to the server, even though it is no longer accessible by the stalker.

This happens because the stalkerware app first requests that all permissions be allowed and only then continues by creating or pairing to an account.

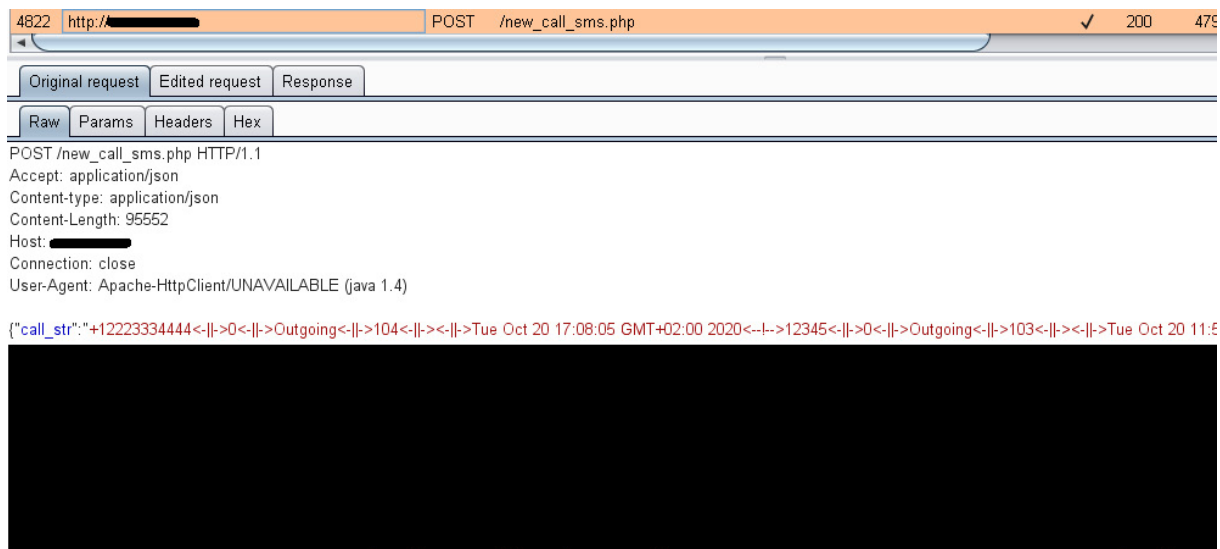


Figure 28 // User call log uploaded to server right after start of app

Impact

In case of a data breach, the stalkerware server might contain victims' data, even though the app was never actually used.

Incorrect permission assignment for devices with superuser privileges (CWE-732)

This applies only to rooted smartphones. If the stalker grants full access to the stalkerware, the app can then access private files of other apps installed on the device, such as social media, IM or browser applications (Figure 29). This capability was found in 14 of the apps we analyzed.

To obtain internal files of targeted apps that contain contacts, chat messages or browsing history, stalkerware first needs to change permissions for these files or directories and then send them to its server. Changing permissions was done in all cases with the `chmod 777` command (Figure 30), which makes the files readable, writable and executable by all applications.

For clarification, none of the analyzed stalkerware tried to root a device, only requested superuser rights.

```
[*]exec: su
[*] writebytes: cat /data/data/com.facebook.orca/databases/threads_db2 > /storage/emulated/0/Android/data/[redacted]/files/Facebook.k.db
[*] writebytes: cat /data/data/com.facebook.orca/databases/stickers_db > /storage/emulated/0/Android/data/[redacted]/files/Stickers.db
[*] writebytes: chmod 777 /storage/emulated/0/Android/data/[redacted]/files/*
[*] writebytes: chmod -R 777 /storage/emulated/0/Android/data/[redacted]/files/
[*] writebytes: exit

[*]exec: su
[*] writebytes: cat /data/data/com.whatsapp/databases/msgstore.db > /storage/emulated/0/Android/data/[redacted]/files/msgstore.db
[*] writebytes: cat /data/data/com.whatsapp/databases/msgstore.db-wal > /storage/emulated/0/Android/data/[redacted]/files/msgstore.db-wal
[*] writebytes: cat /data/data/com.whatsapp/databases/msgstore.db-shm > /storage/emulated/0/Android/data/[redacted]/files/msgstore.db-shm
[*] writebytes: cat /data/data/com.whatsapp/databases/wa.db > /storage/emulated/0/Android/data/[redacted]/files/WhatsAppContacts.db
[*] writebytes: chmod 777 /storage/emulated/0/Android/data/[redacted]/files/*
[*] writebytes: chmod -R 777 /storage/emulated/0/Android/data/[redacted]/files/
[*] writebytes: exit
```

Figure 29 // Sensitive files copied to external media

```

[*]exec: su
[*] writebytes: chmod -R 777 /data/data/com.facebook.orca
[*] writebytes: chmod -R 777 /data/data/com.facebook.orca/files
[*] writebytes: chmod -R 777 /data/data/com.facebook.orca/databases/;
[*] writebytes: chmod -R 777 /data/data/com.facebook.orca/databases/prefs_db;
[*] writebytes: chmod -R 777 /data/data/com.android.chrome;
[*] writebytes: chmod 777 /data/data/com.android.chrome/app_chrome;
[*] writebytes: chmod 777 /data/data/com.android.chrome/app_chrome/Default;
[*] writebytes: chmod 777 /data/data/com.android.chrome/app_chrome/Default/History;
[*] writebytes: chmod 777 /data/data/com.sec.android.app.sbrowser
[*] writebytes: chmod 777 /data/data/com.sec.android.app.sbrowser/app_sbrowser
[*] writebytes: chmod 777 /data/data/com.sec.android.app.sbrowser/app_sbrowser/Default
[*] writebytes: chmod 777 /data/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History
[*] writebytes: chmod 777 /data/data/com.whatsapp;
[*] writebytes: chmod -R 777 /data/data/com.whatsapp/databases/;
[*] writebytes: chmod -R 777 /data/data/com.whatsapp/shared_prefs;
[*] writebytes: chmod 777 /data/data/com.whatsapp/files;
[*] writebytes: chmod -R 777 /data/data/com.whatsapp/files/Avatars;
[*] writebytes: chmod 777 /data/data/com.whatsapp/databases/msgstore.db-shm;
[*] writebytes: chmod 777 /data/data/com.whatsapp/databases/msgstore.db-wal;
[*] writebytes: chmod 777 /data/data/com.whatsapp/databases/msgstore.db
[*] writebytes: chmod -R 777 /data/data/com.google.android.talk;
[*] writebytes: chmod -R 777 /data/data/com.google.android.talk/databases;
[*] writebytes: chmod -R 777 /data/data/com.google.android.talk/shared_prefs;
[*] writebytes: chmod 777 /data/data/com.viber.voip;
[*] writebytes: chmod -R 777 /data/data/com.viber.voip/databases;
[*] writebytes: chmod 777 /data/data/com.viber.voip/databases/viber_messages;
[*] writebytes: exit;

```

Figure 30 // Changing file access permissions of targeted apps

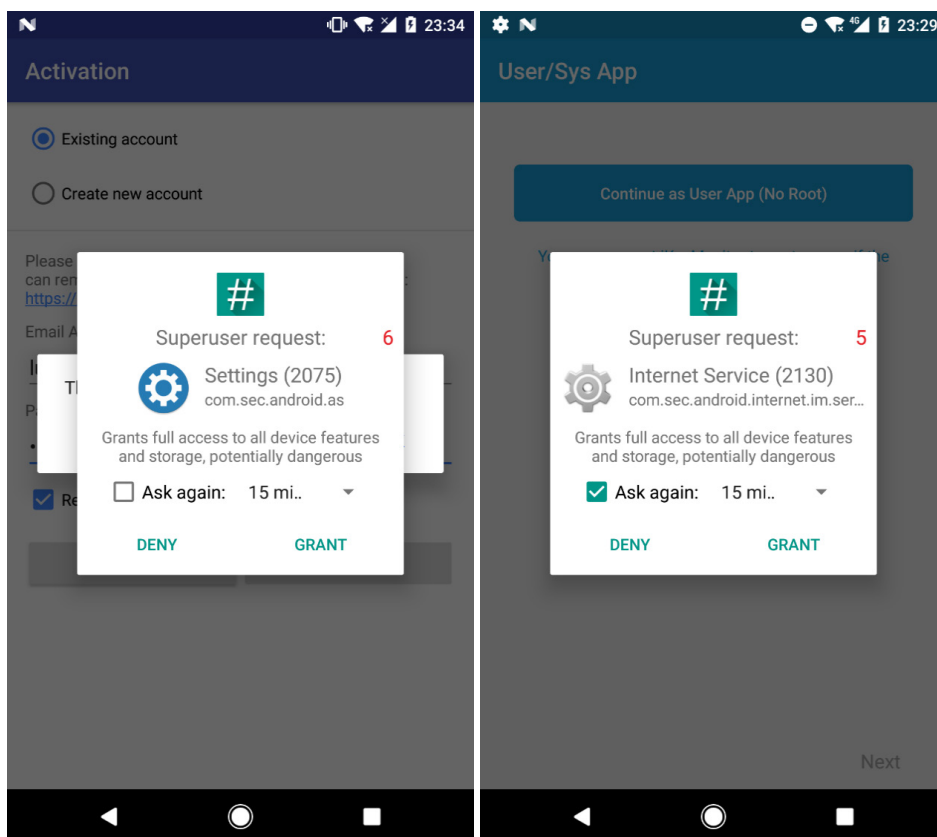


Figure 31 // Requests to grant superuser rights

Impact

Any app installed on a device can read and write to these files without being granted superuser rights. To access files it would only need `android.permission.WRITE_EXTERNAL_STORAGE` permission.

Insufficient verification of victim uploaded data (CWE-345)

This issue was found in 13 of the analyzed apps, that were responsible for uploading victim data to the stalkerware server, with no associated tokens or cookies to identify the victimized device (see [Figure 32](#)). Instead, these apps depended on only a unique device ID such as IMEI or `android_id` during the client/server communication.

With appropriate permission, those identifiers can be easily extracted by other apps installed on a device and could then be used to upload fabricated text messages, photos and phone calls, and other fictitious data to the server, to frame victims or make their lives more difficult.

The screenshot shows a list of HTTP requests in a network analysis tool. The requests are POST requests to `/protocols/log_sms_post.aspx`. The device ID is visible in the request body of the selected request.

Type	Name	Value
Body	deviceid	48[REDACTED]06
Body	date	2019-04-07
Body	time	17:38:46
Body	sender	PayPal
Body	receiver	0
Body	direction	1
Body	name	PayPal
Body	message	PayPal: Your security code is: 198419. Your code expires in 5 minutes. Please dont reply.
Body	os	AD
Body	type	0

Figure 32 // Text messages uploaded to server based on device ID

Impact

There are two possible ways to misuse this. First, since some of these apps also only used HTTP to communicate with the server, rather than HTTPS, an attacker on the same network could intercept and replace data being uploaded to the server to control what the stalker will see. Second, any app that has the `android.permission.READ_PHONE_STATE` permission enabled (for requesting IMEI) could obtain the unique device ID to upload any data to the server as if it were the stalkerware.

Possible fix

Upload data to the server based on a token received from the server that is not accessible to third-party apps. Make sure to use HTTPS, instead of HTTP, since just adding a token to the unencrypted traffic would not prevent an attacker on the same network from intercepting transmitted data and impersonating the stalkerware.

Improper authorization of SMS commands (CWE-285)

In the case of no internet connection, nine analyzed stalkerware apps allow receiving commands from text messages. Unfortunately, in these cases the stalkerware doesn't verify if a command is from the stalker and automatically executes it. SMS commands for these apps are available on the vendors' websites – an example listing is provided in [Figure 33](#). Moreover, these stalkerware apps would still process commands received via SMS, even after the app license expired.

Google Pixel	
Restart net command	#restartnet
Restart gps command	#restartgps
Restart settings command	#restartsettings
Take picture	#takepic
Record audio	#recordaudio
Record audio time	10 minutes ▾
Take picture with front camera	#takepicfront
List contacts	#listcontacts
List apps	#listapps
Restart wifi	#restartwifi
Start net	#startnet
Stop net	#stopnet
Stop wifi	#stopwifi
Start wifi	#startwifi
Start alarm	#startalarm
Remote wipe	#remotewipe
Lock phone	#lockphone
Set silent - ringtone	#setsilent
Set vibrate - ringtone	#setvibrate
Set normal - ringtone	#setnormal
Track location	#tracklocation
Last settings change on website	-
Last settings update on the phone	November 19 2020 10:08:24

Figure 33 // Indicative list of SMS commands

Even though the list of commands covers a wide spectrum of device control, not all the commands are valuable for a remote attacker. During our tests, we identified the most useful to be retrieving the GPS location in a return SMS, wiping external storage, and making the stalkerware call the SMS sender back so the attacker could listen in on surrounding audio.

Impact

Any app installed on a device with `android.permission.READ_PHONE_STATE` (for apps targeting SDK API level 29 and below; that is, Android OS versions before 9.0) or `android.permission.READ_PHONE_NUMBERS` (for API level 30 and above; that is Android OS versions 9.0 and higher) permission could obtain the device's phone number and the package name of stalkerware installed, to get a list of supported SMS commands from the server. Thus, anyone with the phone number and knowledge of the available commands could remotely control such a device if the appropriate stalkerware is installed.

Bypass payment to access admin console (CWE-284)

For nine vendors with paid products it was possible for non-paid access to the paid features admin console due to improper access control. This happened because verifying whether a logged in user has a license or not was done only on the main (dashboard) page. If a stalker directly accesses the URLs to view other website sections such as Calls, Contacts, Messages, then license authentication is missing and the server provides the requested pages.

Impact

Although this security issue negatively affects only the software vendor, it shows their overall lack of attention to security details.

Command injection (CWE-926)

Six analyzed apps exported an unprotected component (broadcast receiver) that can be triggered by any app installed on the device, such as in the example in [Figure 34](#). We identified exported components that would allow an attacker to record surrounding audio, take device screenshots and in one case the ability to inject any command to the stalkerware app that should otherwise be received from the admin console ([Figure 35](#)). It was possible to trigger commands responsible for erasing external media, enabling GPS, and wiping the device. Gathered files (recorded audio, screenshots) are stored on shared external storage.

In one app, the stalker can schedule, within the stalkerware app, various commands based on events such as unlocking the device, Wi-Fi status change, charging of the device, etc. It means, for example, that every time the victim unlocks their smartphone, a photo from the front camera could be taken. All these commands and paired actions are stored on external media in an unprotected database. Because of this, it would be possible for an unauthorized third-party app to inject commands on custom events.

```
<receiver android:name="[REDACTED].ItemReceiver">
  <intent-filter>
    <action android:name="[REDACTED].ADD_ITEM"/>
    <action android:name="[REDACTED].COMMAND"/>
    <action android:name="[REDACTED].START_SERVICE"/>
    <action android:name="[REDACTED].UPDATE"/>
    <action android:name="[REDACTED].SERVICE_WORKING"/>
    <action android:name="[REDACTED].SETTINGS"/>
  </intent-filter>
</receiver>
```

Figure 34 // Unprotected and exported broadcast receiver

```
if ([REDACTED].COMMAND.equals(intent.getAction())) {
    D.a((Runnable) new D(context, intent.getStringExtra("command"), intent.getStringExtra("params"), intent.getStringExtra("command_id"),
}
```

Figure 35 // Unprotected receiver parses commands

Impact

Third-party apps could trigger functionality from stalkerware without any permission, and then access the results – photos, recorded audio and screenshots – because they are stored on external media.

Possible fix

Set permission to restrict access of an exported component.

Enforcing weak registration password (CWE-521)

While setting up the admin account on a victim's device, five of these apps required the admin password to be a four-to-ten-digit PIN – see [Figure 36](#). All of these apps were developed by the same vendor.

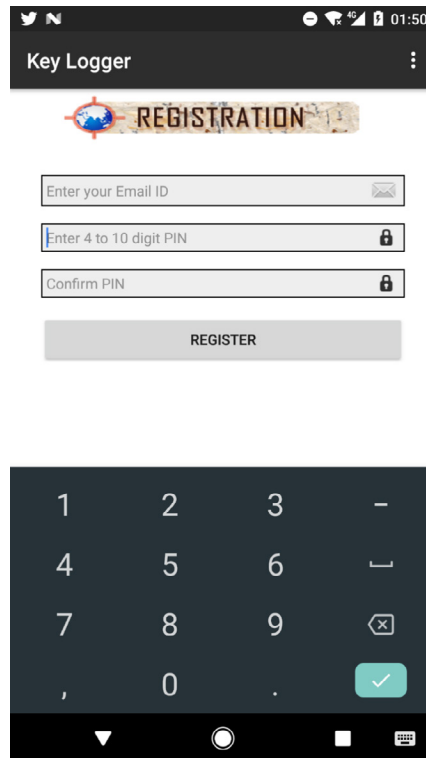


Figure 36 // User registration with enforced PIN as a password

Impact

Enforcing only digits in a password with limited length makes it easier to guess the admin password or possibly brute force it in case there is no server protection.

Missing proper password encryption (CWE-326)

Because of the possibility of retrieving client data from the stalkerware server (as described in the Server leak of stalker information (CWE-200) section), it is possible to get the password of an admin account in an unsalted, MD5-hashed form, as seen in [Figure 37](#). Based on that, we can assume that the server stores client data in a weak, non-encrypted format that can be returned to anyone who knows the device ID.

Account information from the server is requested by the stalkerware to automatically pair and synchronize the device with the assigned stalker account. The config file contains the hashed password as part of its data.

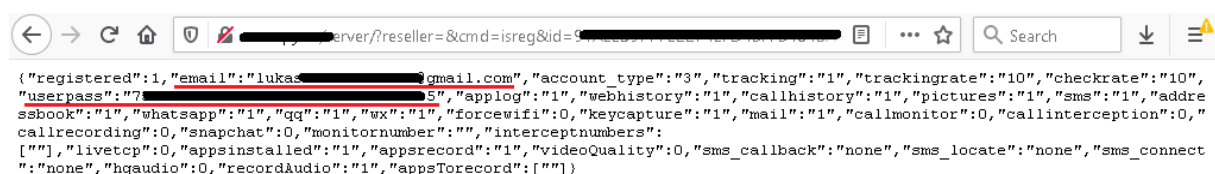


Figure 37 // Server returns the stalker's email and MD5-hashed password

Impact

Any third-party app on a device running Android 9 and below could access the serial number of a device and obtain the client login name in cleartext and the password in MD5-hashed format. This a weak protection of a password and can be brute forced easily, which would result in account takeover.

It might be the same impact in case of a server data breach.

Possible fix

Use standard and verified encryption mechanisms to protect victim and client data on the server. Do not allow unauthorized users access to client data.

Victim data kept on the server after account removal

What happens when the stalking ends? In our tests, when the stalker removed data logs, unlinked the victim smartphone and removed their account from the monitoring service, the gathered victim information was, for some vendors, still available on the server.

We identified two scenarios. In the first one, data is left on the server and accessible to an attacker who knows the correct URL even though the stalker can no longer log into the admin console (two separate examples are seen in [Figure 38](#) and [Figure 39](#)). In the second, after an explicit request to remove all collected data, it was kept on the server for the next 90 days.

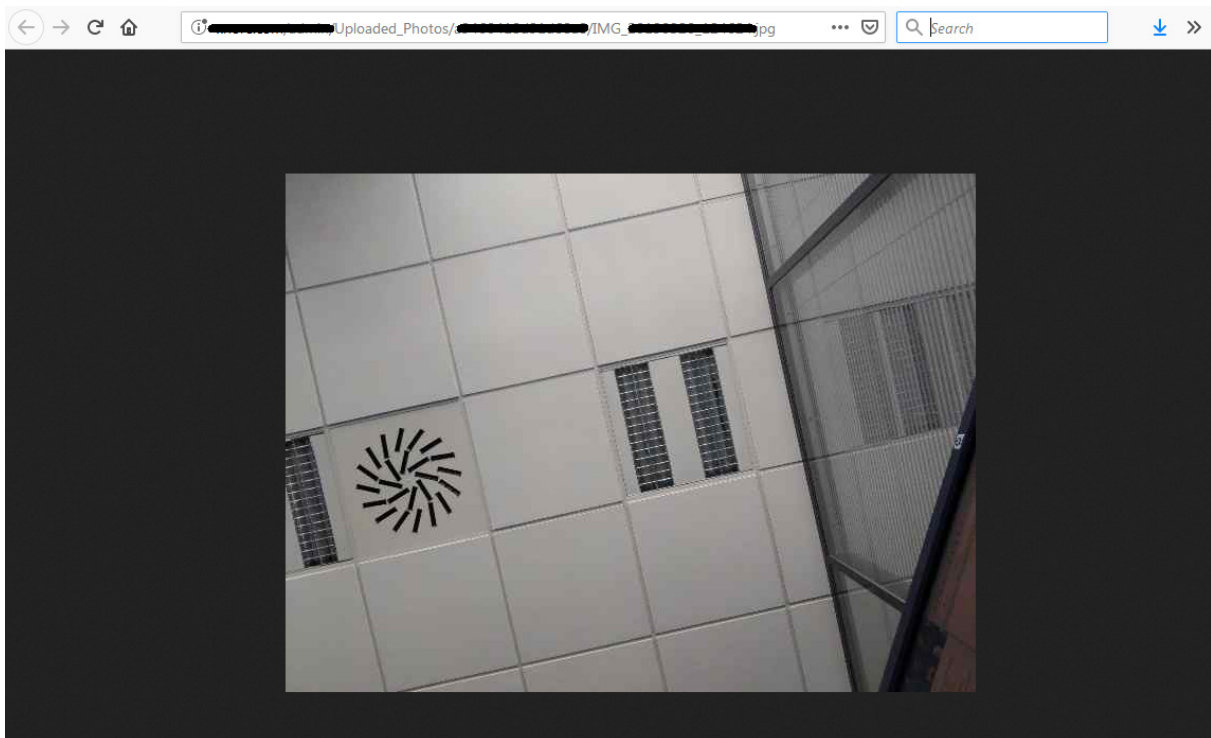


Figure 38 // Accessing our photos after account removal

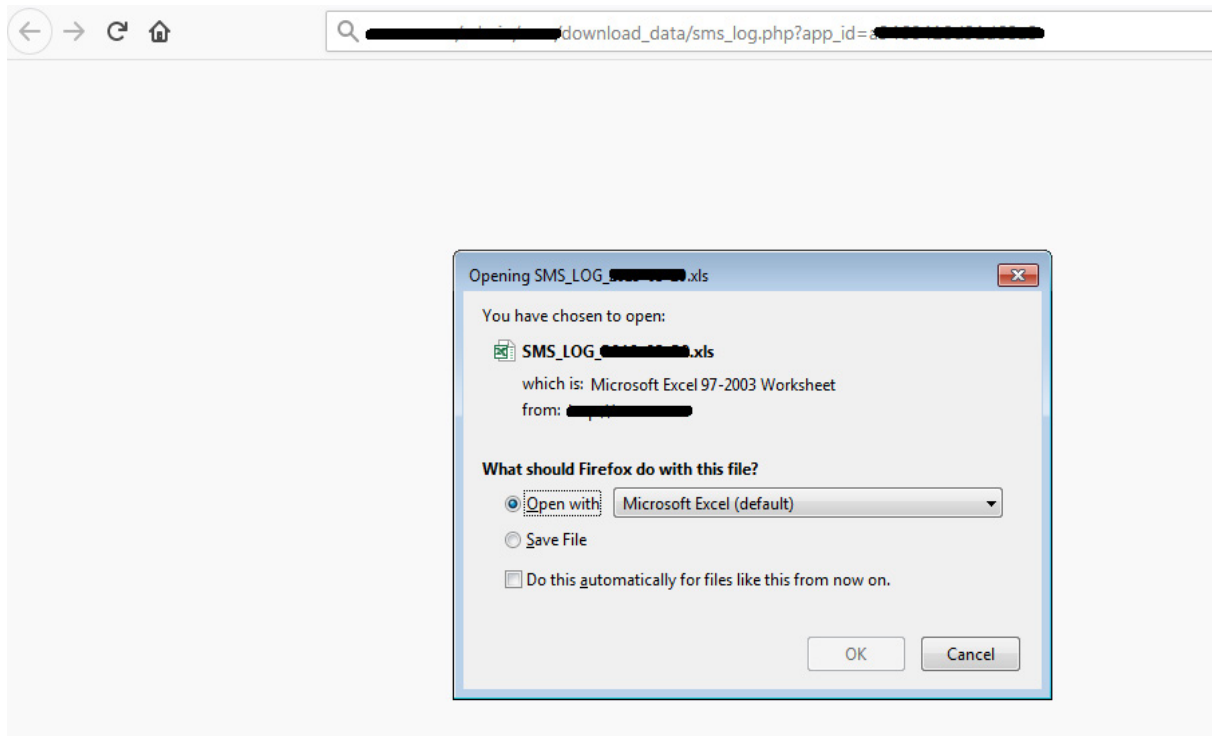


Figure 39 // Accessing our SMS logs after requesting data removal from the server

Impact

In the case of bypassing access control to access client resources or a server data breach, it would be possible to access victims' gathered information, even though such data should be already removed from the server.

Possible fix

Restrict data access without authorization. Make sure all victim files are immediately removed from stalkerware servers.

Leak of sensitive information during IPC communication (CWE-927)

Android apps, including stalkerware, have defined various app components that can communicate with each other - within or outside the application. This is typically done using broadcasts that will pass data to another component that will process them. These broadcasts can be divided in two categories - implicit and explicit. When an implicit broadcast is sent, it doesn't specify the targeted component, only the action. Because of that, any application that has registered this action can receive and process this implicit broadcast and the data bundled with it. An explicit broadcast explicitly specifies which component will receive it, to make sure an unauthorized app will not access bundled data.

We were able to identify implicit broadcasts containing sensitive data being sent by two apps we analyzed. This data was the result of keylogger activity, meaning it would leak everything typed by a victim, including visible passwords - see [Figure 40](#) - to other apps installed on the device.

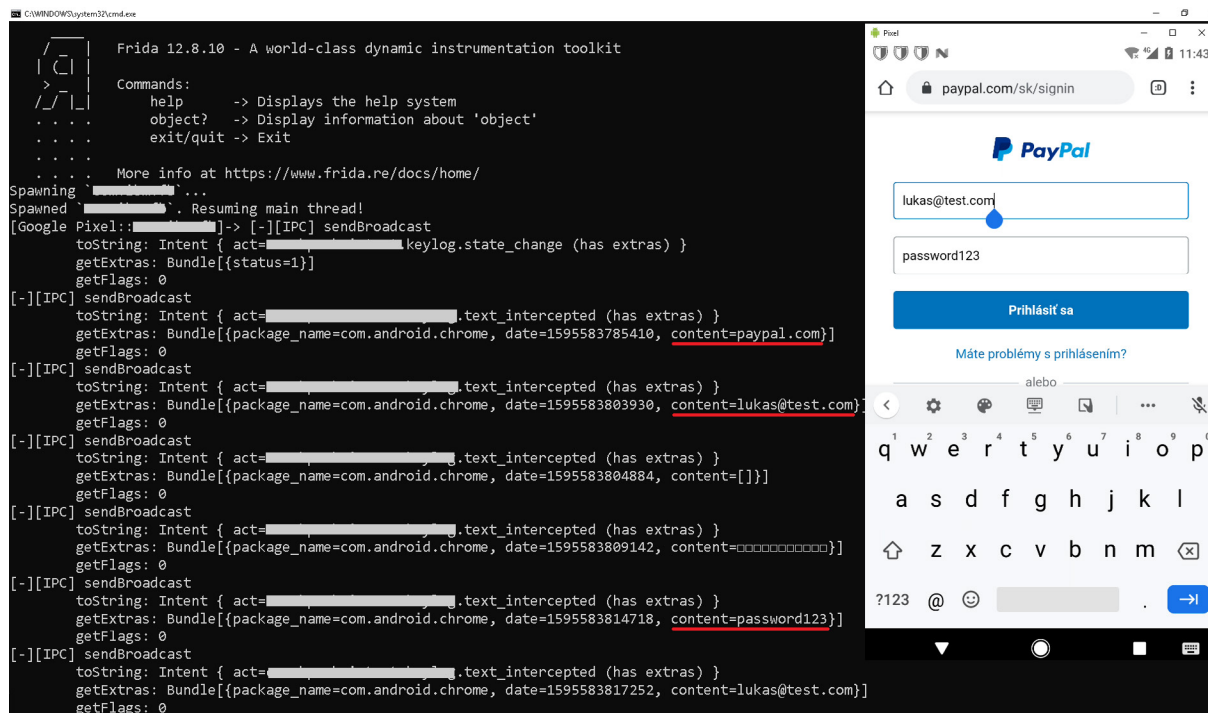


Figure 40 // Leak of all user text input

Impact

Any app installed on the device could snoop on all keystrokes without necessary permissions.

Possible fix

Instead of implicit intents, use explicit intents for broadcast of data within the same application. Use a signature permission protection level.

Partial access to admin console (CWE-285)

The stalkerware server of one analyzed app allows access to the admin console, and partial control of any device (see Figure 41) with the same stalkerware installed, based solely on knowing the device IMEI number. The app can send scheduled reports containing recent call logs, and send and receive text messages, to the email address configured by the stalker. For an attacker, besides obtaining details about a victim, this vulnerability makes it possible to replace the email address where scheduled reports will be sent, as seen in Figure 42, without any authentication by, or notification to, the original email address.

v2

The following operations are supported. For a formal definition, please review the [Service Description](#).

- [appNotifications](#)
- [appUpgrade](#)
- [autoRegister](#)
- [checkDeviceRegistration](#)
- [confirmExpiration](#)
- [doLogin](#)
- [flushData](#)
- [forgotPassword](#)
- [getSettings](#)
- [getSubscriptionPlan](#)
- [insertReceipt](#)
- [myEmail](#)
- [registerDevice](#)
- [registerIUser](#)
- [registerUser](#)
- [saveHistory](#)
- [saveLocationData](#)
- [saveSecretCode](#)
- [saveSettings](#)
- [sendLogMailForBasicVersion](#)
- [sendLogMailForProVersion](#)
- [subscribe](#)
- [updateDeviceToken](#)
- [updateDeviceTokenV1](#)
- [uploadRequestData](#)
- [uploadRequestDatav2](#)

Figure 41 // Open API control panel

v1

Click [here](#) for a complete list of operations.

saveSettings

Test

To test the operation using the HTTP POST protocol, click the 'Invoke' button.

Parameter	Value
fsIMEINumber:	<input type="text" value="3[REDACTED]7"/>
fsName:	<input type="text" value="test11"/>
fsDeviceModelNumber:	<input type="text"/>
fsSendEmailTo:	<input type="text" value="new_attacker@gmail.com"/>
figLogCall:	<input type="text" value="true"/>
figLogMessage:	<input type="text" value="true"/>
figLogApplication:	<input type="text" value="true"/>
figLogLocations:	<input type="text" value="true"/>
figHideApp:	<input type="text" value="true"/>
inMailDuration:	<input type="text" value="0"/>
stTimeToSendMail:	<input type="text" value="01:09 PM"/>
inLocationTimeout:	<input type="text" value="5"/>
fsJsonParameter:	<input type="text"/>

Figure 42 // Exchanging email address for received reports

Impact

Any attacker with the device ID of the stalkerware victim could receive the victim's personal data without authentication or the knowledge of the victim or stalker.

Possible fix

Don't allow unauthorized users to access the control console.

Remote livestream of video and audio from victim device (CWE-284)

Many stalkerware apps allow a stalker to watch a livestream from a victim's device from the front or back camera. In one of the apps, when the stalker makes this request, the app first creates a server request using a unique ID to inform the server it's ready, then the server will send a command to the stalkerware app with the same unique ID to initiate the livestream. The stalker can use the same unique ID to watch and listen to what is happening in the device's surroundings over the RTMP protocol.

This can be misused by an attacker. For an unauthorized attacker to trigger and watch a livestream, two things are necessary: links to the server that triggers stream on the device and the device ID. Server links can be extracted from the stalkerware app, since they are available in cleartext. The device ID is a value generated randomly on the device, then encrypted using a custom algorithm and stored on external shared storage. Without this value it is impossible to launch a stream from any device.

Since the encrypted ID is available on shared storage and the decryption algorithm can be extracted from the stalkerware, it is possible for any app on the device to get the ID and trigger a broadcast from the device without permission. This is possible even from a locked smartphone.

Impact

Any third-party app could obtain and decrypt the device ID and share it outside of the app. Hence, anyone with the server link and device ID could trigger the server to send a command to the device to launch a livestream from it without any user notice.

Possible fix

Don't allow an unauthorized user to trigger the livestream functionality.

Running as a system application

Stalkerware apps in many cases request superuser permission, mimicking legitimate system applications. However, in one app we examined, it escalates its privileges and makes itself a system application. System apps are pre-installed applications on the system partition. These apps can't be removed in the way regular non-system apps installed from Play Store can. Because of that, it is impossible for victims to uninstall this app from their smartphones, since it would survive even a factory reset.

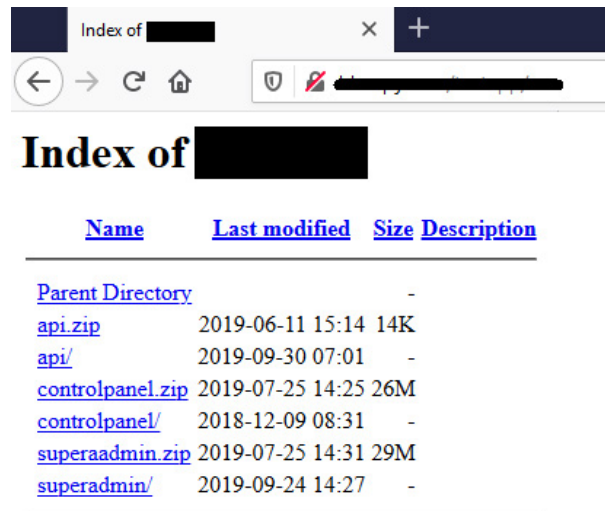
As a result, this action would make it a permanent system stalkerware that can only be removed either remotely by the stalker or with physical access to the device and using ADB tools as superuser.

Possible fix

Identify package name of stalkerware application and uninstall it using superuser rights.

Source code and superadmin credentials leak (CWE-200)

One of the analyzed stalkerware servers was keeping a backup of its control panel source code accessible, without authorization, in an open directory. This source code includes the superadmin credentials, providing access to all accounts on this stalkerware server.



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
api.zip	2019-06-11 15:14	14K	
api/	2019-09-30 07:01	-	
controlpanel.zip	2019-07-25 14:25	26M	
controlpanel/	2018-12-09 08:31	-	
superaadmin.zip	2019-07-25 14:31	29M	
superadmin/	2019-09-24 14:27	-	

Figure 43 // Server data leak

Impact

This issue could lead to account takeover of stalkers' accounts because they were manageable by the superadmin account, and the possibility for an attacker to access data and take control of a stalker's victim's device.

FORENSIC ANALYSIS

With successful forensic analysis it is possible to access internal files of a stalkerware app and read data such as the email address of the stalker, what data had been gathered from a device, or when it was gathered. Because of that, before victims decide to remove this software, they can first try to identify who has been spying on them.

For a forensic analysis it is important to have physical access to a compromised device. To successfully extract an app's data, it needs to have either a data backup or the debuggable flag enabled in the Android manifest. If either of these conditions hold – see Figure 44 – it is possible to access private data of the analyzed app.

From 86 stalkerware apps it was possible to extract app's data from 55 of them.

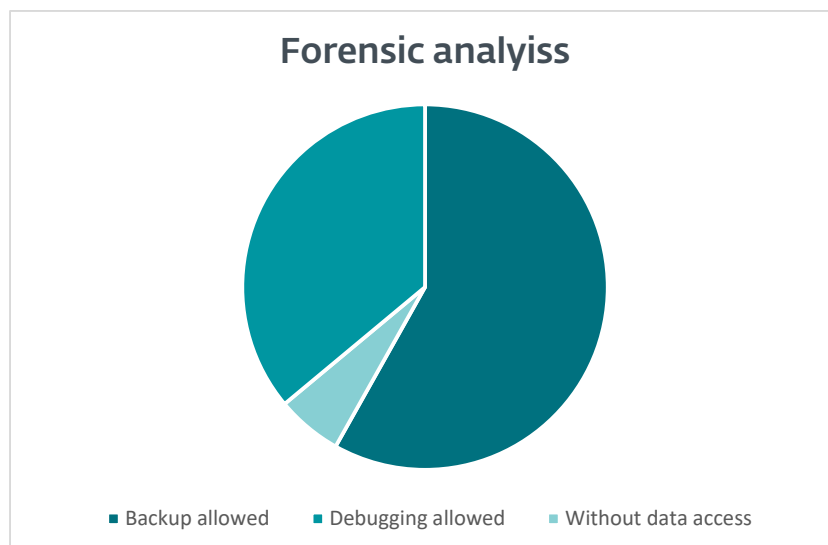


Figure 44 // Possibility to perform successful stalkerware data extraction

PREVENTION TIPS

If potential victims want to prevent anyone from manipulating their mobile device, they must protect it with a strong passcode that is not easily guessed and not shared with anyone. However, we fully understand that stalking is oftentimes interrelated to harassment and other forms of violence. Victims might be psychologically coerced, intimidated or physically forced into disabling this type of protection or to reveal their passcode. Especially if they live in the same household as their cyberstalker.

Victims should carefully consider deleting any stalkerware or software with this type of functionality that they might find. A potential stalkerware threat should be identified if they scan their device with a trustworthy security solution. As is pointed out by stopstalkerware.org, whoever installed it will know that it was removed or disabled, and it could result in consequences.

In extreme cases where cyberstalking is only one part of a very unhealthy and abusive relationship dynamic, victims can decide to reach out to law enforcement. That however requires careful preparation. On a safe device or through a trustworthy person, they can contact organizations that offer help. If they do that on a mobile or any other device that has stalkerware or spouseware installed, the perpetrator will know about it. Another option for seeking help might be using a spare mobile phone with a new phone number, new email address, new passwords and enabled multifactor authentication.

CONCLUSION

For the last two years, based on our data, Android stalkerware has become more and more widely used. There are many vendors providing such software, mostly hiding behind the guise of employee or child monitoring applications. Once we realize that these monitoring apps gather, store and transmit more personal information about their victims than any other app they have installed in their smartphone, it naturally raises questions about the security level of these apps, and how well the very sensitive data they extract is stored and protected.

This research should help answer this question, since we were able to identify, using static and dynamic analysis, 158 serious security and privacy issues in 58 apps out of the 86 apps we analyzed.

What appears to be a bigger problem is unwillingness to fix these issues after we repeatedly reported them to the affected vendors. At the time of writing, from 58 vendors with security and/or privacy problems, 45 vendors are not fixed, 7 are fixed and 6 promised to issue a patch but still have not. Among the 45 vendors' apps that are still not fixed, 44 haven't even replied to our coordinated vulnerability disclosure email messages.

IOCS

App name	Website	SHA-1	Detection name
Aispyer	https://www.aispyer[.]com	41E63825D6457E62704016850ED3DA169B4F8D74	Android/Monitor.Aispyer.A
AllTracker	https://alltracker[.]org	FCD903B94FECA81DFEACFB091767F4958DC31FF0	Android/Monitor.Alltracker.A
Android Monitor	https://www.androidmonitor[.]com	D775A31B9B8C6DEF265D9C9B61C308C773CA04B3	Android/Monitor. FreeAndSpy.B
AntiFurto Droid WEB	http://www.antifurtodroid[.]com	271F63D2E44D4F8A01976EFC2C568238D9866C26	Android/Monitor.TheftSpy.G
Appmia	https://appmia[.]com	301C9C847FBC083097A01C82A601B0016EF68215	Android/Monitor. MobileTracker.D
Appspy	https://appspyfree[.]com	41826F781FB1F4660D4CABC142285DC6C906C10C	Android/Monitor.Spyoo.U
A-Spy	http://www.a-spy[.]com	29D7C40F59C32F362735772814B97C46F9939944	Android/Monitor.ScreenMon.B
BlurSpy	https://www.blurspy[.]com	9550AB258E5BDD9E807B0B630F24001FD0991F9	Android/Monitor.BlurSpy.A
CatWatchful	https://catwatchful[.]com	AA8A6116064CC732785413F21C773E3C392C8C49	Android/Monitor.Catwatch.A
Cerberus	https://cerberusapp[.]com	4CA878D25A4899DE1D9CA37593BBBE14AE442C50	Android/Monitor.Cerberus.A
ClevGuard	https://www.clevguard[.]com	B29A92EB8995B310045F9E46BE4367ADEA23DD83	Android/Monitor.Guardian.BN
Cocospy	https://www.cocospy[.]com	6460711077311A860D07CF478ADE28342F98AE86	Android/Monitor.Drower.D
Copy9	https://copy9[.]com	BBE67A01376D65B334B58D1E5E1E6D01B8DA0748	Android/Monitor.Spyoo.U
Couple Tracker	https://coupletracker[.]com	60916D6E205DC6C8C3B79198211775F6D33B2AE2	Android/Monitor.LoveTrack.B
DDI Utilities	https://ddiutilities[.]com	3CDD9F398D7D8C6DAB5E1B20D418E4E7C858D06E	Android/Monitor.Highster.B
EaseMon	https://www.easemon[.]com	1E4ABFB04E87F87BCEDA0CC7540B1C00402A081D	Android/Monitor. IkeyMonitor.C
Easy Logger	https://logger[.]mobi	D3FD085959E7241903B9A6371DF7A1D7DCC291F3	Android/Monitor.Easylogger.A
Easy Phone Tracker	https://easyphonetrack[.]com	B4C472FD8D16BD74EE73E6B55BAA2BD918912012	Android/Monitor.SpyPhone.Q
EvaSpy	https://evaspy[.]com	8CA3D60AD8FD3584370ACFADDFC29979F25D57D3	Android/Monitor.TiFamily.G
Flexispy	https://www.flexispy[.]com	58E128A4AEB20EE1D9E80355977FEDB74482C1ED	Android/Riskware.Tracer.I
Fone tracker	https://fonetracker[.]com	26A6D36D332EBF1665442A4FE4F1D6F5234F3C10	Android/Monitor.Spyoo.U
FoneMate	https://www.myfonemate[.]com	DB023F956897CD56ED7D0A225A4A1B9905BD5E71	Android/Monitor.Mspy.O
Fonemonitor	https://fonemonitor[.]co	FFECA9BDB0A88E4AE0878B4664CE6B99744C7DF9	Android/Packed.Jiagu.D
Forever Spy	https://foreverspy[.]com	D7BB84B4AE62BFBFA9A92ECB49025CA0D8B6BC4D	Android/TrojanDownloader. Agent.JN
Free Android Spy	https://www.freeandroidspy[.]com	9A4432965755F38AAAA532B97A29F9C9BBEDE6D1	Android/Monitor. FreeAndSpy.B
GPS tracker - Loki	http://asgardtech[.]ru	40CAD1ABFDA54B5746B76433FB3DF1E8B9001A99	Android/Monitor.Lokimon.A
GuestSpy	https://guestspy[.]com	41826F781FB1F4660D4CABC142285DC6C906C10C	Android/Monitor.Spyoo.U
Highster	https://highstermobile[.]com	1D1A210433A8D4BDC8CFDC404F84998EE38C09CF	Android/Monitor.Highster.E

App name	Website	SHA-1	Detection name
Hoverwatch	https://www.hoverwatch[.]com	9B9B670EAB150A26217D1BA59F707C9242525912	Android/Monitor. Hoverwatch.G
iKeyMonitor	https://ikeymonitor[.]com	8402731AD77DC7E805590100A4594BA063FD247D	Android/Monitor. IkeyMonitor.C
i-Monitor	https://imonitorke[.]com	01B9C342F09F4F81853A0EB4545D84E09A440A6C	Android/Monitor.Imonitor.A
IntTel Track GPS	http://109.235.66[.]53/login	0974885435D59C02D3CF7EE7385B922D8B08500F	Android/Monitor.Traca.F
iSpyoo	https://ispyoo[.]com	1AD88067787408E4DB7760FABC80C23DBF7AF7B7	Android/Monitor.Spyoo.U
iSPYOO	https://www.theispyoo[.]com	DB023F956897CD56ED7D0A225A4A1B9905BD5E71	Android/Monitor.Mspy.O
JJSpy	https://www.jjspy[.]com	we couldn't obtain sample of jjspy, most likely very similar like mspy	
Key Logger	https://trackmyphones[.]com/keyboard	143AB1A7C1A97E42909B2A76005B3A1C87BCA07D	Android/Monitor. SpydioTrack.C
letmespy	http://www.letmespy[.]com	DB023F956897CD56ED7D0A225A4A1B9905BD5E71	Android/Monitor.Letmespy.B
Lost Android	https://www.androidlost[.]com	6DE115A8188B7EEAADACD141E3A95FA51D6F3B21	Android/Monitor.Androidlost.F
Message and Call Tracker	https://callsmstracker[.]com	05BFE61FDF7E9605BCA5643289A3BD229AAA0B79	Android/Monitor.CallTrack.D
MeuSpy	https://meuspy[.]com	837157DB81A2667343D6F0922378F4505DDCD38F	Android/Monitor.Meuspy.F
Minspy	https://minspy[.]com	9CE99F72066E7AB82AB2B0E12BCC7E526581D7B2	Android/Monitor.Drower.F
Mobile Tool	https://mtoolapp[.]net/ https://mobiletool[.]ru/ https://mtoolapp[.]biz/	2BBE1868836F38C6D40F5B108556A1F1AA530B45	Android/Monitor.Mobtool.B
Mobile Tracker Free	https://mobile-tracker-free[.]com	AD63FF027D525B5B75EF7A47CCDD13A11C1EAD7A	Android/Monitor. MobileTracker.D
MobileSpy	https://mobilespy[.]at	40CAD1ABFDA54B5746B76433FB3DF1E8B9001A99	Android/Monitor. MobileTracker.D
Mobistealth	https://www.mobistealth[.]com/	03A9082896DBBFE692A019B35993B1019A6CAC89	Android/Monitor.Androsy.E
mSpy	https://www.mspy[.]com	DB023F956897CD56ED7D0A225A4A1B9905BD5E71	Android/Monitor.Mspy.O
Mxspy	https://mxspy[.]com	EBE21947284E144ADD737491B12037764714F254	Android/Monitor.Spyoo.U
Neatspy	https://neatspy[.]com	2a756b58efe8fd7a42d44dbf4d1da54120d2e72b	Android/Monitor.Drower.F
NeoSpy	https://neospy[.]net/ http://neospy[.]pro/ https://neospy[.]tech/	2F3A9E8CC0F49A55603A87CBACAB4B261A85259B	Android/Monitor.Neospy.G
Netspy	https://www.netspy[.]net	607FBED72C0468BFD18AE333EDC14F31F9765D27	Android/Monitor.AppSpy.A
OwnSpy	https://en.ownspy[.]com	C64A811624F92E92064A58966CA00B9E02CC81FF	Android/Monitor.OwnSpy.B
PhoneSheriff	https://www.phonesheriff[.]com	E80AFA67A241C0F7EFF7FBFB1E166E27B99D867E	Android/Monitor.MobileSpy.Q
PhoneSpying	https://www.phonespying[.]com	AB3D045FDBDAF4DF2A2633185080CD5927B60277	Android/Monitor.AppSpy.A
Remote Audio Recorder	https://trackmyphones[.]com/SpyAudio	99D549C4C720B2647CEA480401FA3EC22B51595E	Android/Monitor. SpydioTrack.C
Remote Desktop	available on 3rd party stores	19AECAD9A2FDC6179B4765B663F6692249206D4	Android/Monitor.Androsy.E
Reptilicus	https://reptilicus[.]net/	970165C823BD1EF3864E04C438F6C3C085DF6B39	Android/Monitor.Reptilicus.G
Secret Video Recorder	alternative app stores	AF98616E8EA0831615BF4DD7BAF4797CD3F1288	Android/Monitor.SecretCam.A

App name	Website	SHA-1	Detection name
Shadow SPY	https://www.shadow-spy[.]com	03ED620FDDEDC21CBBD15F49E0018F9279005FD3	Android/Monitor.Shadspy.B
Smart Aggregation Platform	https://sap4mobile[.]com	C53AF7F8EA2EF721A73F6CFF1EF5CB1FDDFBE221	Android/Monitor.TrackPlus.AJ
Snoopza	https://snoopza[.]com	0646351A5CC54696EEA67B012CD103C2F1F85296	Android/Monitor.Hoverwatch.G
Spapp Monitoring	https://www.spappmonitoring[.]com	F3D27AA5DB723FB9C3BE6BB4D3A2236B124F6510	Android/Monitor.SpyPhone.Q
Spy to Mobile	https://sptomobile[.]com/en	0BF2685524C03F45161E546C5BCD87370DD9D011	Android/Monitor.TrackPlus.AL
Spycell	https://spycell[.]net	41826F781FB1F4660D4CABC142285DC6C906C10C	Android/Monitor.Spyoo.U
SpyHuman	https://spyhuman[.]com	F567EFF3134B04C0EFBC14FA6BC4916BB851AE0C	Android/Monitor.Humanspy.G
Spyic	https://spyic[.]com	E71ACDF3C55FDB20794275641B6E97C5C1772404	Android/Monitor.Drower.F
Spyier	https://spyier[.]com	7C10E5B7DEF0F16CA012162544FBBB4D8CA93AEB	Android/Monitor.Drower.F
Spyine	https://spyine[.]com	77d249af13b2827ef8fe47b8f46be90e079818ea	Android/Monitor.Drower.F
Spylive 360	https://spylive360[.]com	A5181D223D9D1215E9A8D536A6F0D608AB17768B	Android/Monitor.SpyLive.A
Spyphone Mobile Tracker	https://www.spyfone[.]com/ https://www.spyphone[.]com/ https://www.phonetracker[.]com/	43114DE5A2584AC511EC5B16DFBE983B68812E95	Android/Monitor.TrackPlus.AP
SpyToApp	http://www.spytoapp[.]com	1FF5A3CD8FF7170424CCE37048D15411358A6434	Android/Monitor.Spyoo.L
SpyTrac	https://spytrac[.]com	0EB40553722C62B5E48BCE0F0CD03AA979DC2BE6	Android/Monitor.TiFamily.G
Spyzee	https://spyzee[.]com	41826F781FB1F4660D4CABC142285DC6C906C10C	Android/Monitor.Spyoo.U
Spyzie	https://spyzie[.]jio	7cfa88ebe8350ba24aa3acf329b2ad639d416c5e	Android/Monitor.Spyzie.B
TalkLog	https://talklog[.]tools	C67111CED1290FB28C96AD775806EC8DB0BD580C	Android/Monitor.TalkLog.A
Teensafe	https://teensafe[.]net	749ECD4CB53CF07BCB6CF6C2EF8D9C864E237949	Android/Packed.Jiagu.D
TheTruthSpy	https://thetruthspy[.]com	C5597748A7236D85897C3488869B617C8B4AAD54	Android/Monitor.Spyoo.U
TISPY	https://tispy[.]net	3CA1A32759498B06660BDDF6FC4EDD0A8BAF437C	Android/Monitor.TiFamily.G
Track My Phone	https://trackmyphones[.]com	6DADE1ED5C4DAD78F786BE96EE923133D792673E	Android/Monitor.Trackme.B
Track My Phone Remotely	https://trackmyphones[.]com/cgi-bin/GCM/trackMyPhone.cgi	8CC208DA4CF52FA5B2043F950997A698ED8C707B	Android/Monitor.SpydioTrack.C
TrackView	http://trackview[.]net	ECDF07F1DA7E29727870C0D6665709A02BAF3D53	Android/Monitor.Androspy.E
Ultra Monitor	https://www.spyequipmentuk[.]co.uk/android-ultra-spy-phone-software/	8B5876F71A26A2F5D25E87F9554F5DD638B320DB	Android/Spy.Agent.AZY
UniSafe	https://usafe[.]ru/	DA86289CB85181C29081B9B79E76324E1E69B892	Android/Monitor.SafeTracker.B
Video Rec	https://trackmyphones[.]com/cgi-bin/SpyVideo/spyvideo.cgi	6BE8F4818BA14EEA62ADCAAB9D6C59F6F9AC599D	Android/Monitor.SpydioTrack.C
VIPTrack	http://89.47.91[.]j131/viptrack/	122279033215FE07BE86A57CBEB4F7E1DA194082	Android/Monitor.Viptrack.A
WtSpy	http://wt-spy[.]com	898BD5CC79645FAD1AB448CE2227C211878BB24D	Android/Monitor.Wtspy.A
Xnore	http://xnore[.]com	134DC61F737A29FD630608E2D063128E98F01526	Android/Spy.Agent.QI

ABOUT ESET

For 30 years, [ESET®](#) has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn [100 Virus Bulletin VB100](#) awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on [LinkedIn](#), [Facebook](#) and [Twitter](#).



ENJOY SAFER TECHNOLOGY™