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
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Impact</th>
<th>Possible fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper authorization of SMS commands (CWE-285)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bypass payment to access admin console (CWE-284)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command injection (CWE-926)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforcing weak registration password (CWE-521)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missing proper password encryption (CWE-326)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Victim data kept on the server after account removal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leak of sensitive information during IPC communication (CWE-927)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial access to admin console (CWE-285)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote livestream of video and audio from victim device (CWE-284)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Running as a system application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source code and superadmin credentials leak (CWE-200)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FORENSIC ANALYSIS**

**PREVENTION TIPS**

**CONCLUSION**

**IOCS**

**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.

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](image)

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](image)
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.
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**

*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 pdf
- 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](image)

**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.
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.

![False and misleading claims](https://via.placeholder.com/150)

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.

“I discovered the betrayal.”

With SpyLive 360 Spy I found out that my wife was cheating on me for over 5 years with a work person.

![Stalkerware review](https://via.placeholder.com/150)
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 10** // This photo is available on a stock image website (https://unsplash.com/photos/29pFbI_D1Sc)

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

**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.

![Stalkerware issues](image)

**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.
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.

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](image)
Figure 16 // Registering device to a server

![Figure 17](image)
Figure 17 // Data extraction from victim’s device

![Figure 18](image)
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.
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.

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

Figure 22 // Leaked and accessible victim data files
### Android stalkerware vulnerabilities

![Table of victim data](image1.png)

**Figure 23** // Victim data available based on email address

![Table of recorded phone calls](image2.png)

**Figure 24** // Recorded phone calls

![Table of video recordings](image3.png)

**Figure 25** // Video recordings of a victim device's 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.

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.
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: 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 -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 30](image)

Figure 31 // Requests to grant superuser rights

![Figure 31](image)
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.

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.

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

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

Figure 34 // Unprotected and exported broadcast receiver

```
if (COMMAND.equals(intent.getAction())) {
    D.e((Runnable) new D(context, intent.getStringExtra("command"), intent.getStringExtra("param"), 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.

![User registration with enforced PIN as a password](image1)

**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.

![Server returns the stalker’s email and MD5-hashed password](image2)

**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.
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.
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.
Figure 41 // Open API control panel

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.
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 43 // Server data leak](image)

![Figure 44 // Possibility to perform successful stalkerware data extraction](image)
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.
## Android stalkerware vulnerabilities

<table>
<thead>
<tr>
<th>App name</th>
<th>Website</th>
<th>SHA-1</th>
<th>Detection name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllTracker</td>
<td><a href="https://alltracker%5B.%5Dorg">https://alltracker[.]org</a></td>
<td>FCD903B94FEC81DPEACF8B091767F4958DC31F0</td>
<td>Android/Monitor.Alltracker.A</td>
</tr>
<tr>
<td>Appma</td>
<td><a href="https://appma%5B.%5Dcom">https://appma[.]com</a></td>
<td>301C9C847FEC03097A01C82A601B0016EF68215</td>
<td>Android/Monitor.MobileTracker.D</td>
</tr>
<tr>
<td>Appspy</td>
<td><a href="https://appspyfree%5B.%5Dcom">https://appspyfree[.]com</a></td>
<td>418268781FE1F4660D4CAB142285DC96C10C</td>
<td>Android/Monitor.Spyoo.U</td>
</tr>
<tr>
<td>A-Spy</td>
<td><a href="http://a-spy%5B.%5Dcom">http://a-spy[.]com</a></td>
<td>29D7C4055C32F362735772814B97C66F9939944</td>
<td>Android/Monitor.ScreenMon.B</td>
</tr>
<tr>
<td>CatWatchful</td>
<td><a href="https://catwatchful%5B.%5Dcom">https://catwatchful[.]com</a></td>
<td>AAA8616064C732785413F21C773E3C92C8C49</td>
<td>Android/Monitor.Catwatch.A</td>
</tr>
<tr>
<td>Cerberus</td>
<td><a href="https://cerberusapp%5B.%5Dcom">https://cerberusapp[.]com</a></td>
<td>4CA878D25A489BDE19DA37593BBEB14EA442C50</td>
<td>Android/Monitor.Cerberus.A</td>
</tr>
<tr>
<td>ClevGuard</td>
<td><a href="https://www.clevguard%5B.%5Dcom">https://www.clevguard[.]com</a></td>
<td>B29A92EE8995B310045F9E46BE4367DEA23DDB3</td>
<td>Android/Monitor.Guardian.BN</td>
</tr>
<tr>
<td>Copy9</td>
<td><a href="https://copy9%5B.%5Dcom">https://copy9[.]com</a></td>
<td>BB676A0137D65B33B58DE1E6D1B8D7A048</td>
<td>Android/Monitor.Spyoo.U</td>
</tr>
<tr>
<td>EaseMon</td>
<td><a href="https://www.easeemon%5B.%5Dcom">https://www.easeemon[.]com</a></td>
<td>1B4ABFB5BE8F787BCEDA0C7540E1C0402A081D</td>
<td>Android/Monitor.ikeyMonitor.C</td>
</tr>
<tr>
<td>Easy Phone Tracker</td>
<td><a href="https://easyphonetrack%5B.%5Dcom">https://easyphonetrack[.]com</a></td>
<td>B4C472FD8D16D74E736E8B55BAA2BD918912012</td>
<td>Android/Monitor.SpyPhone.Q</td>
</tr>
<tr>
<td>EvaSpy</td>
<td><a href="https://evaspy%5B.%5Dcom">https://evaspy[.]com</a></td>
<td>8CA3D60AD8FD3D384370ACFADDDC2997F225D5D7D</td>
<td>Android/Monitor.TIFamily.G</td>
</tr>
<tr>
<td>Flexispy</td>
<td><a href="https://www.flexispy%5B.%5Dcom">https://www.flexispy[.]com</a></td>
<td>582128A4E8B20EE1D9E8035597FE0D7482C1HD</td>
<td>Android/Riskware.Tracer.I</td>
</tr>
<tr>
<td>FoneMate</td>
<td><a href="https://www.myfonemate%5B.%5Dcom">https://www.myfonemate[.]com</a></td>
<td>DB023F56897CD56ED70A225A41B995B5D6E71</td>
<td>Android/Monitor.Mspy.O</td>
</tr>
<tr>
<td>Forever Spy</td>
<td><a href="https://foreverspy%5B.%5Dcom">https://foreverspy[.]com</a></td>
<td>D78BB4BAB62F6BF6A92BEC49025CA0DB686C4D</td>
<td>Android/TrojanDownloader.Agent.JN</td>
</tr>
<tr>
<td>Free Android Spy</td>
<td><a href="https://www.freeandroidspy%5B.%5Dcom">https://www.freeandroidspy[.]com</a></td>
<td>9AA443296555F38AAG532B97A29F9CBBDK6D1</td>
<td>Android/Monitor.FreeAndSpy.B</td>
</tr>
<tr>
<td>GPS tracker - Loki</td>
<td><a href="http://asgardtech%5B.%5Dru">http://asgardtech[.]ru</a></td>
<td>40CD1A8FDF5A2668B76433F3DF1EB8B9001A99</td>
<td>Android/Monitor.Lokimon.A</td>
</tr>
<tr>
<td>GuestSpy</td>
<td><a href="https://guestspy%5B.%5Dcom">https://guestspy[.]com</a></td>
<td>41826F81F1F4660D4C142285DC6C906C10C</td>
<td>Android/Monitor.Spyoo.U</td>
</tr>
<tr>
<td>Hightster</td>
<td><a href="https://hightermobile%5B.%5Dcom">https://hightermobile[.]com</a></td>
<td>1DA210433A8D48DCC8CF1DC404FB4998EE38C09CF</td>
<td>Android/Monitor.Highster.E</td>
</tr>
<tr>
<td>App name</td>
<td>Website</td>
<td>SHA-1</td>
<td>Detection name</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>iKeyMonitor</td>
<td><a href="https://ikeymonitor%5B.%5Dcom">https://ikeymonitor[.]com</a></td>
<td>8402731AD77DCTE805590100A4594BA633FD247D</td>
<td>Android/Monitor.ikeyMonitor.C</td>
</tr>
<tr>
<td>i-Monitor</td>
<td><a href="https://imonitorke%5B.%5Dcom">https://imonitorke[.]com</a></td>
<td>01B9C342F0F9F4F81853A0EB8454548E90A440A6C</td>
<td>Android/Monitor.iMonitor.A</td>
</tr>
<tr>
<td>iSpyoo</td>
<td><a href="https://ispyoo%5B.%5Dcom">https://ispyoo[.]com</a></td>
<td>1AD880677874084ED7760FABC80C232DBF7AF7B7</td>
<td>Android/Monitor.Spyoo.U</td>
</tr>
<tr>
<td>iSPYOO</td>
<td><a href="https://www.theispyoo%5B.%5Dcom">https://www.theispyoo[.]com</a></td>
<td>DB023F956897CD56ED7D0A225A41B9905B58E71</td>
<td>Android/Monitor.Mspy.O</td>
</tr>
<tr>
<td>JJSpy</td>
<td><a href="https://www.jjspy%5B.%5Dcom">https://www.jjspy[.]com</a></td>
<td>we couldn't obtain sample of jjspy, most likely very similar like mspy</td>
<td>Android/Monitor.SpydioTrack.C</td>
</tr>
<tr>
<td>Key Logger</td>
<td><a href="https://trackmyphones%5B.%5Dcom/keyboard">https://trackmyphones[.]com/keyboard</a></td>
<td>143AB1A7C1A97E4290982A760056A1C878C0A7D</td>
<td>Android/Monitor.SpydioTrack.C</td>
</tr>
<tr>
<td>letmespy</td>
<td><a href="http://www.letmespy%5B.%5Dcom">http://www.letmespy[.]com</a></td>
<td>DB023F956897CD56ED7D0A225A41B9905B58E71</td>
<td>Android/Monitor.Letmespy.B</td>
</tr>
<tr>
<td>Lost Android</td>
<td><a href="https://www.androidlost%5B.%5Dcom">https://www.androidlost[.]com</a></td>
<td>6D115A8188B7E8A6ACD5C1E9A5F516F32B1</td>
<td>Android/Monitor.Androidlost.F</td>
</tr>
<tr>
<td>Message and Call Tracker</td>
<td><a href="https://callsmstracker%5B.%5Dcom">https://callsmstracker[.]com</a></td>
<td>05BFBE16FDF7E96585CA533829A3BD229AA0B79</td>
<td>Android/Monitor.CallTrack.D</td>
</tr>
<tr>
<td>MeuSpy</td>
<td><a href="https://meuspy%5B.%5Dcom">https://meuspy[.]com</a></td>
<td>837157DB81A2667343D6F0922378F45055CD38F</td>
<td>Android/Monitor.Meuspy.F</td>
</tr>
<tr>
<td>Mobile Tracker Free</td>
<td><a href="https://mobile-tracker-free%5B.%5Dcom">https://mobile-tracker-free[.]com</a></td>
<td>AD63FF027D525B5875EF7A47CCD13A11C1BAD7A</td>
<td>Android/Monitor.MobileTracker.D</td>
</tr>
<tr>
<td>MobileSpy</td>
<td><a href="https://mobilespy%5B.%5Dat">https://mobilespy[.]at</a></td>
<td>40CAD1ABFD5485746B76433FB3DF1E889001A99</td>
<td>Android/Monitor.MobileTracker.D</td>
</tr>
<tr>
<td>mSpy</td>
<td><a href="https://www.mspy%5B.%5Dcom">https://www.mspy[.]com</a></td>
<td>DB023F956897CD56ED7D0A225A41B9905B58E71</td>
<td>Android/Monitor.Mspy.O</td>
</tr>
<tr>
<td>Neatspy</td>
<td><a href="https://neatspy%5B.%5Dcom">https://neatspy[.]com</a></td>
<td>2a756b58efe8f47a42d44dbf4d1da54120d2e72b</td>
<td>Android/Monitor.Drower.F</td>
</tr>
<tr>
<td>Netspy</td>
<td><a href="https://www.netspy%5B.%5Dnet">https://www.netspy[.]net</a></td>
<td>607F8EBD72DC468BF1D1AE333ED14F31F9765027</td>
<td>Android/Monitor.AppSpy.A</td>
</tr>
<tr>
<td>OwnSpy</td>
<td><a href="https://en.ownspy%5B.%5Dcom">https://en.ownspy[.]com</a></td>
<td>C64A811624F92E92E64A58966CA0B9E02CC81FF</td>
<td>Android/Monitor.OwnSpy.B</td>
</tr>
<tr>
<td>PhoneSheriff</td>
<td><a href="https://www.phonesheriff%5B.%5Dcom">https://www.phonesheriff[.]com</a></td>
<td>E80AFA67A241C0D7EFF7FBB1E166E7899D867E</td>
<td>Android/Monitor.MobileSpyQ</td>
</tr>
<tr>
<td>PhoneSpying</td>
<td><a href="https://www.phonespying%5B.%5Dcom">https://www.phonespying[.]com</a></td>
<td>AB3D045F5DEAA46F2A2633185080C5927B60277</td>
<td>Android/Monitor.AppSpy.A</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>available on 3rd party stores</td>
<td>19ABCCAD9A2F6DCE6179B4765B663F6692249206D4</td>
<td>Android/Monitor.Androspy.E</td>
</tr>
<tr>
<td>Secret Video Recorder</td>
<td>alternative app stores</td>
<td>AF98616E8EA0381615BF43DD7BFA797CD3F1288</td>
<td>Android/Monitor.SecretCam.A</td>
</tr>
<tr>
<td>App name</td>
<td>Website</td>
<td>SHA-1</td>
<td>Detection name</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Smart Aggregation</td>
<td><a href="https://sap4mobile%5B.com">https://sap4mobile[.com</a>]</td>
<td>C53A2F7F8EA2EF721A73F6CFP1EFSBC1FDDBB221</td>
<td>Android/monitor.TrackPlusAJ</td>
</tr>
<tr>
<td>Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spy to Mobile</td>
<td><a href="https://spytomobile%5B.com">https://spytomobile[.com</a>]</td>
<td>0BF26855240C3F51615E56C58ECD87370D90011</td>
<td>Android/monitor.TrackPlusAL</td>
</tr>
<tr>
<td>SpyToApp</td>
<td><a href="http://www.spytoapp%5B.com">http://www.spytoapp[.com</a>]</td>
<td>1FF5A3CD8FF7170424CCE3270315411538A6434</td>
<td>Android/monitor.Spyoo.L</td>
</tr>
<tr>
<td>SpYrac</td>
<td><a href="https://spytrac%5B.com">https://spytrac[.com</a>]</td>
<td>0EB40553722C625488CE0F0DC0D3A9790C2B6</td>
<td>Android/monitor.TiFamily.G</td>
</tr>
<tr>
<td>TalkLog</td>
<td><a href="https://talklog%5B.tools">https://talklog[.tools</a>]</td>
<td>C65711C6D1290F282CE96AD755B06E0CB0D5D80C</td>
<td>Android/monitor.TalkLog.A</td>
</tr>
<tr>
<td>TISPY</td>
<td><a href="https://tispy%5B.net">https://tispy[.net</a>]</td>
<td>3CA1A3275949B6660BDD6F6C4EDDDA8B8AF437C</td>
<td>Android/monitor.TiFamily.G</td>
</tr>
<tr>
<td>Track My Phone</td>
<td><a href="https://trackmyphones%5B.com">https://trackmyphones[.com</a>]</td>
<td>6DAD186D54C4DAD75F872696EE92313D792673X</td>
<td>Android/monitor.Trackme.B</td>
</tr>
<tr>
<td>Track My Phone Remotely</td>
<td><a href="https://trackmyphones%5B.com%5D/cgi-bin/GCM/TrackMyPhone.cgi">https://trackmyphones[.com]/cgi-bin/GCM/TrackMyPhone.cgi</a></td>
<td>8CC2088DA4CF525A8520D3F950997A6988D8C707B</td>
<td>Android/monitor.SpyioTrack.C</td>
</tr>
<tr>
<td>Ultra Monitor</td>
<td><a href="https://www.spyequipmenuk%5B.co.uk/android-ultra-spy-phone-software">https://www.spyequipmenuk[.co.uk/android-ultra-spy-phone-software</a>]</td>
<td>8B58767F71A26A2F5D25587F9554F5D638320DB</td>
<td>Android/SpyAgent.AZY</td>
</tr>
<tr>
<td>VIPTrack</td>
<td><a href="http://89.47.91%5B.com%5D/viptrack/">http://89.47.91[.com]/viptrack/</a></td>
<td>122279033215F07E86A57CBBEB4F7E1DA194082</td>
<td>Android/monitor.WtSpy.A</td>
</tr>
</tbody>
</table>
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.