VB2021
localhost

7 - 8 October, 2021 / vblocalhost.com

ANDROID STALKERWARE VULNERABILITIES

Lukas Štefanko
ESET, Slovakia

lukas.stefanko@eset.com

ABSTRACT

If nothing else, stalkerware apps encourage clearly ethically questionable behaviour, 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 analysed 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 the 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, at the time of writing this paper, 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 labelled 'stalkerware' [1]. 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? 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 else 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 mimics 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 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, legally be 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 carefully whether to use 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 both more user data 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.

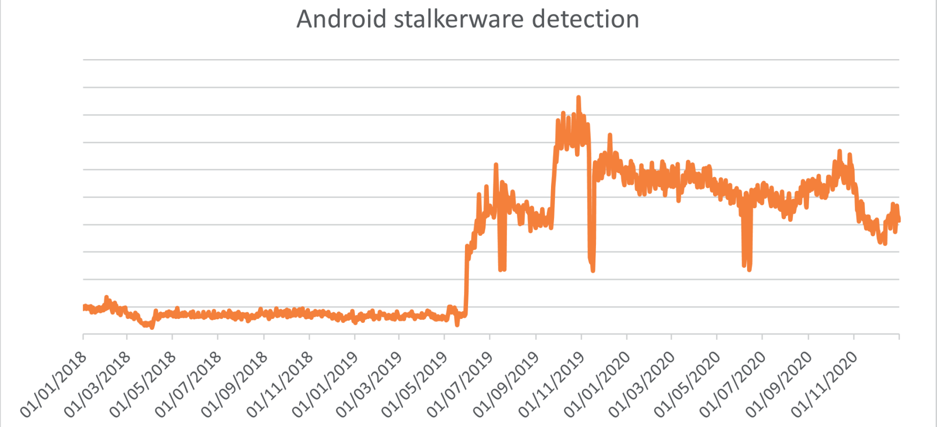


Figure 1: Based on our detection telemetry, usage of Android stalkerware is increasing.

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 seven of 58 vendors whose products were identified as having serious issues had actually fixed them at the time of writing this paper.

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 analysed apps from 86 vendors from these sources:

1. Indicators on Stalkerware [2]
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 [3]; 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.

Of all analysed vendors, 32 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 a greater level of 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 jail-broken or the stalker needs to have the victim's *iCloud* credentials (which are commonly further protected with multi-factor authentication).

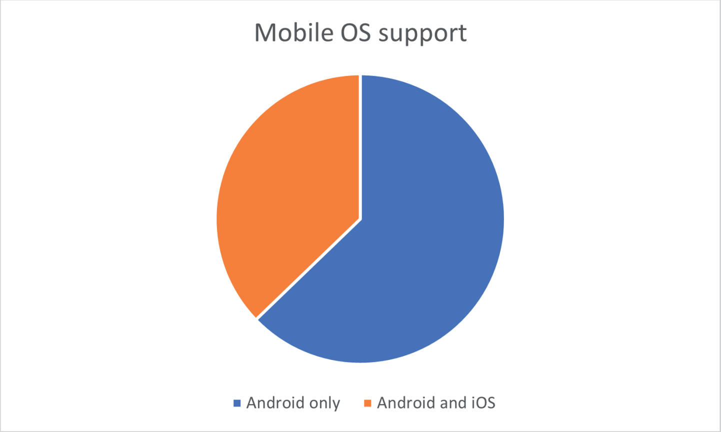
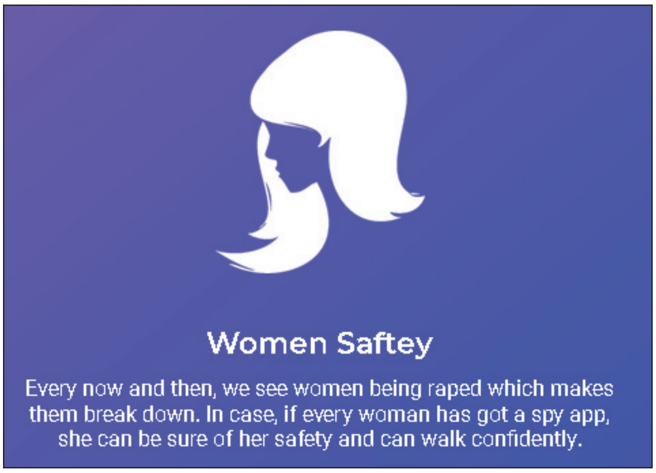


Figure 2: Stats for mobile stalkerware availability by platform.

Not stalkerware

In 2020, *Google* made a move towards limiting stalkerware app distribution by restricting these apps on *Google Play Store* [4] 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 unsavoury example of this that we found.



Women Saftey

Every now and then, we see women being raped which makes them break down. In case, if every woman has got a spy app, she can be sure of her safety and can walk confidently.

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

If we break down these apps' 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 employee privacy since many of the analysed apps work only if every permission is enabled. This 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. 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 analysed apps could hide themselves from the user's view. The apps that were not hidden disguised their presence using various legitimate-seeming names such as Sync Service, Wifi, Security Service, Data Controller, Cloud Backup, Internet Service, Kernel Launcher and Update.

Analysed apps

Altogether we analysed 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 analysed them using static and dynamic analysis techniques to observe their behaviours 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 or 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 [5] 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 analysing 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.

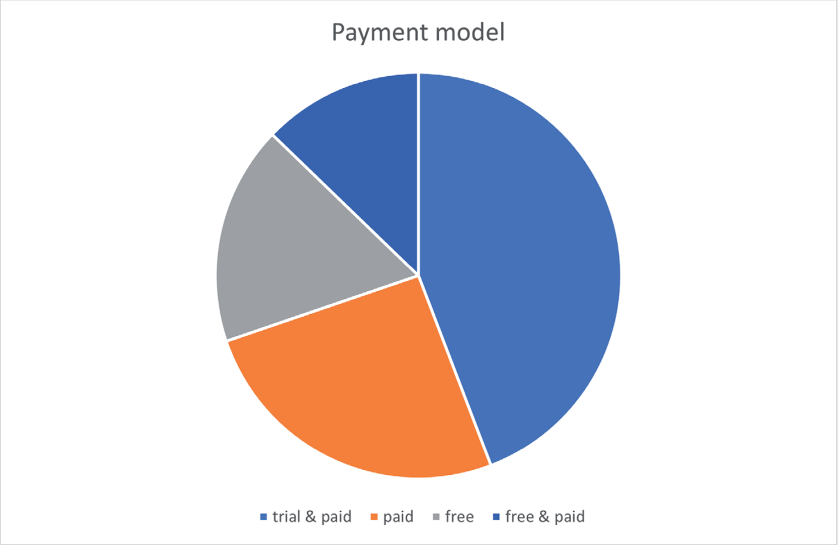


Figure 4: Analysed stalkerware apps based on payment model.

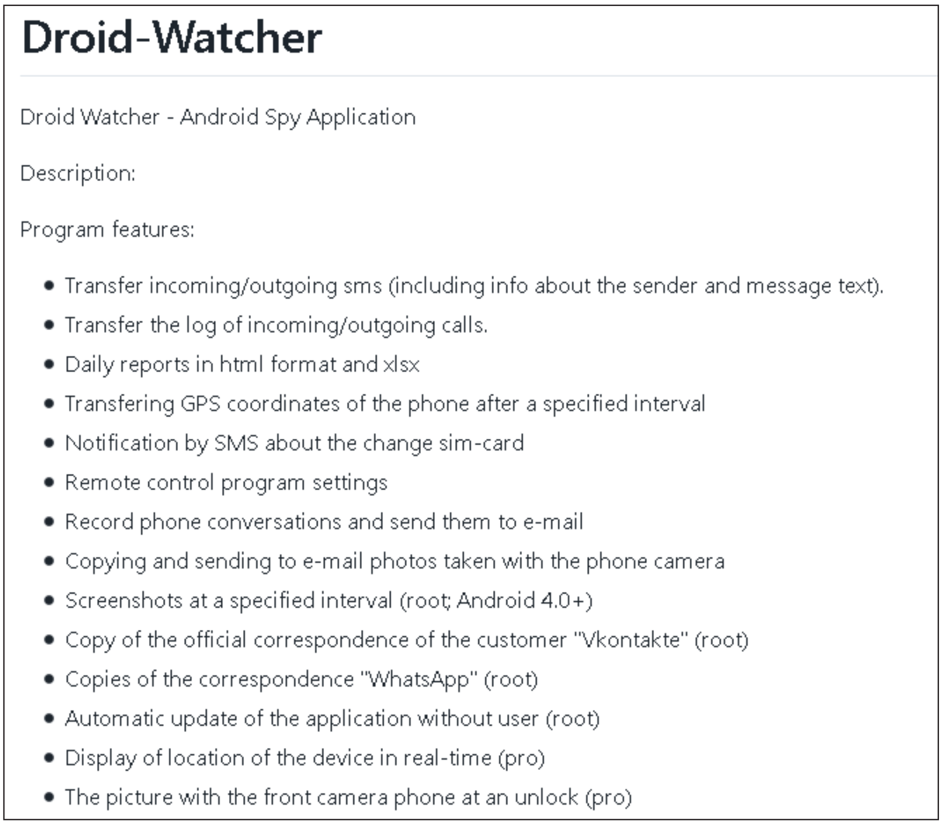
Because of these limitations, of the 86 available apps, we performed dynamic analysis on 72. We couldn't completely analyse 14 paid apps. Additionally, not all the paid features were tested in trial and paid apps.

UNEXPECTED BEHAVIOUR

During analysis we identified some odd characteristics of the apps 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 [6] 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
- Transfering 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 also be 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.

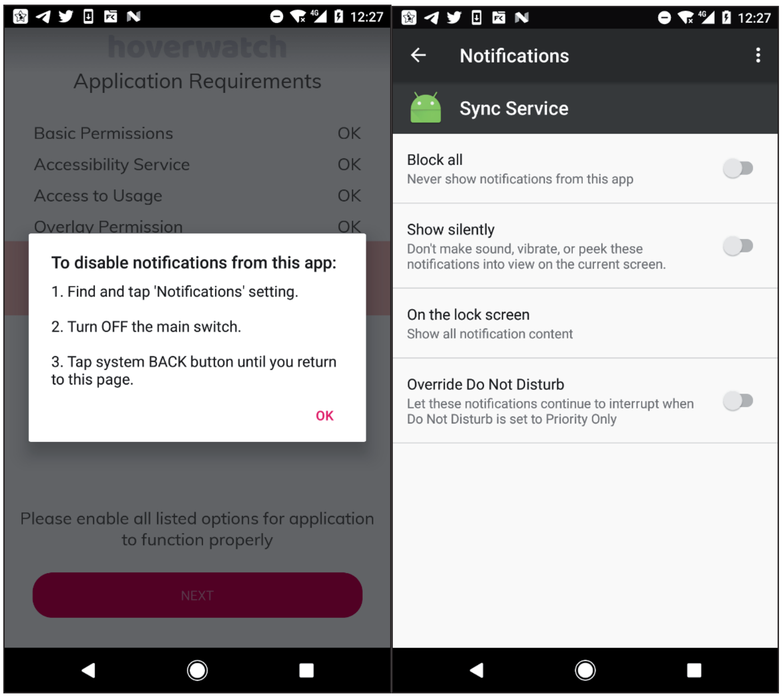
One stalkerware vendor decided to use a Metasploit payload and provided it on their site as a monitoring app. This appears to be a quick-and-dirty way to get into the stalkerware business.

Hard-coded licence keys

Some stalkerware doesn't even protect itself from piracy; in one app, we found hard-coded licence 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.



Application Requirements

Basic Permissions OK
Accessibility Service OK
Access to Usage OK
Overlay Permission OK

To disable notifications from this app:

1. Find and tap 'Notifications' setting.
2. Turn OFF the main switch.
3. Tap system BACK button until you return to this page.

OK

Please enable all listed options for application to function properly

NEXT

Notifications

Sync Service

Block all
Never show notifications from this app

Show silently
Don't make sound, vibrate, or peek these notifications into view on the current screen.

On the lock screen
Show all notification content

Override Do Not Disturb
Let these notifications continue to interrupt when Do Not Disturb is set to Priority Only

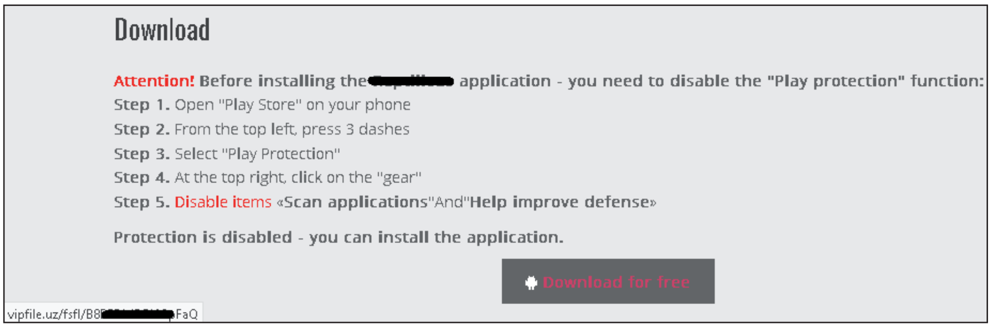
Figure 6: Block all notifications request.

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

App hosted on third-party servers

Some stalkerware, such as that 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*), which afterwards leaves devices unprotected from other threats and stalkerware itself.



Download

Attention! Before installing the [redacted] application - you need to disable the "Play protection" function:
Step 1. Open "Play Store" on your phone
Step 2. From the top left, press 3 dashes
Step 3. Select "Play Protection"
Step 4. At the top right, click on the "gear"
Step 5. Disable items «Scan applications"And"Help improve defense»

Protection is disabled - you can install the application.

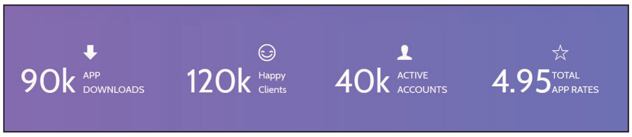
Download for free

vipfile.uz/fsfl/B8[redacted]FaQ

Figure 7: Downloading stalkerware from third-party 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.

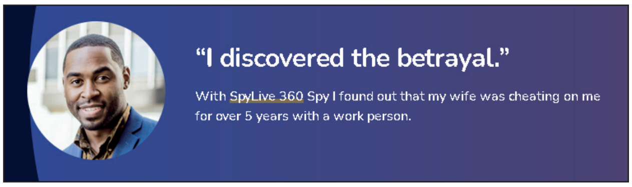


90k APP DOWNLOADS
120k Happy Clients
40k ACTIVE ACCOUNTS
4.95 TOTAL APP RATES

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 skincare 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.

Figure 9: Apparent stalkerware client review.

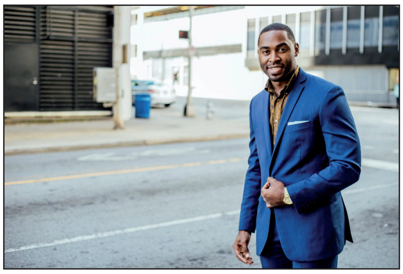


Figure 10: This photo is available on a stock image website (https://unsplash.com/photos/29pFbI_D1Sc).

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

Another app claimed 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.

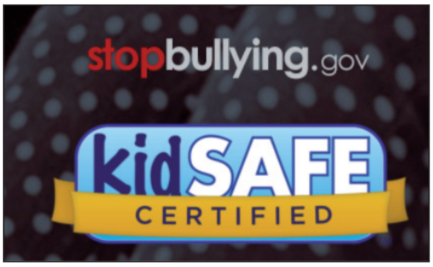
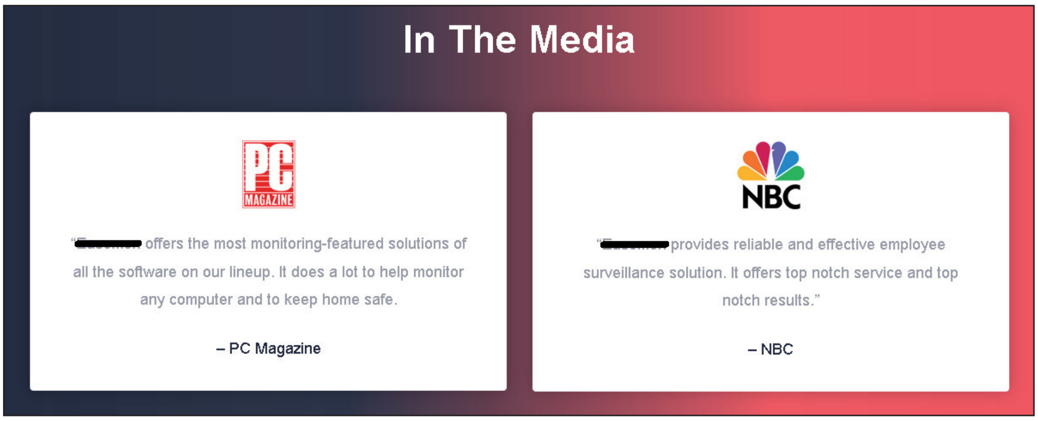


Figure 11: Claiming to be part of various official child protection programmes.



In The Media

“[redacted] 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.

– PC Magazine

“[redacted] provides reliable and effective employee surveillance solution. It offers top notch service and top notch results.”

– NBC

Figure 12: Claiming to be quoted in the media.

COORDINATED VULNERABILITY DISCLOSURE

ESET follows a 90-day coordinated disclosure policy [7] 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 or by creating a support ticket, and 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, in one case because our email wasn't delivered due to the recipient inbox apparently being full and, in the other case because creating a new support ticket always resulted in an error.

We started reporting these vulnerabilities to affected vendors on 19 December 2020. Among the 86 apps tested, we discovered serious issues in 58. 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.

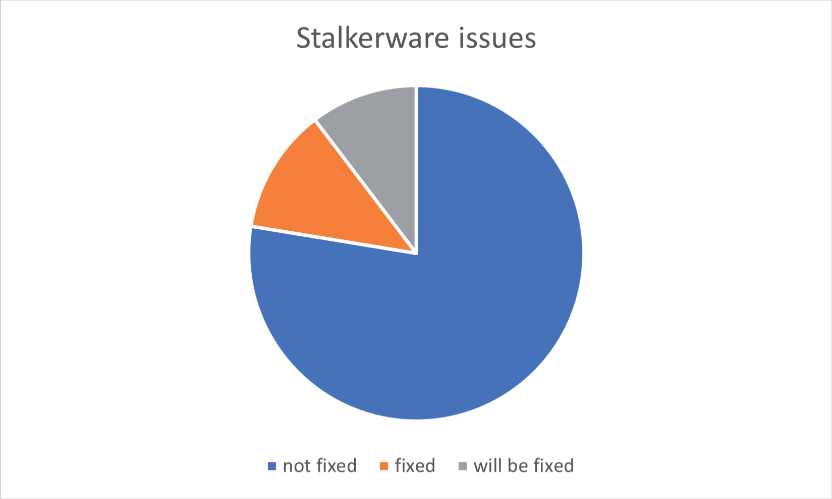


Figure 13: Statistics of security issues that are or will be fixed.

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.

ANALYSIS OF ISSUES

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

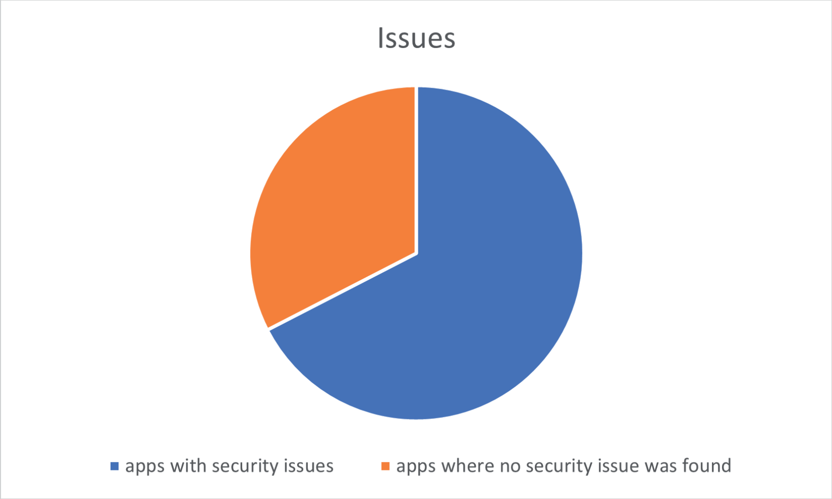


Figure 14: Balance of security issues found.

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 analysed stalkerware apps.

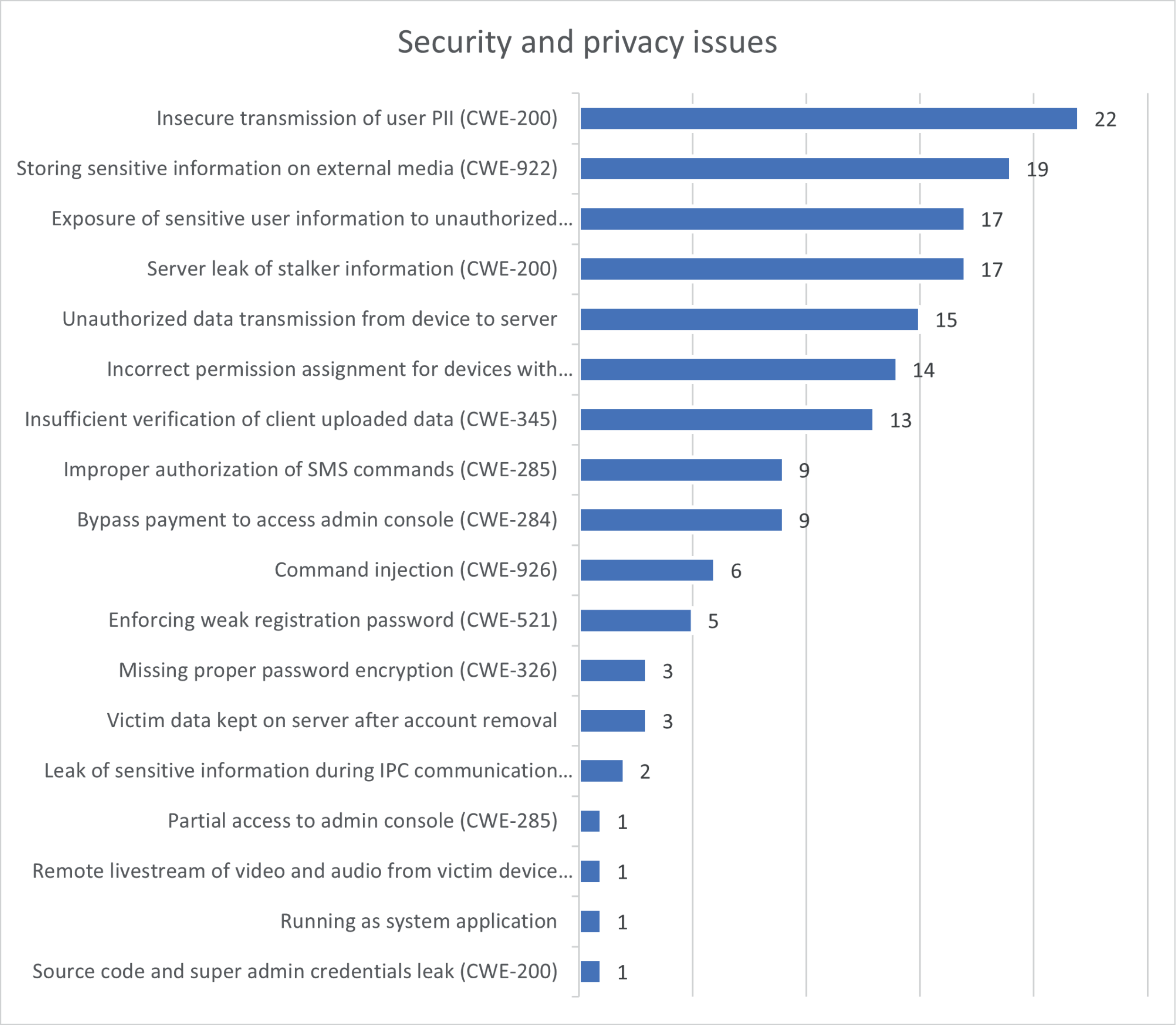


Figure 15: Breakdown of security and privacy issues uncovered in this research.

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

Insecure transmission of victim and stalker PII (CWE-200 [8])

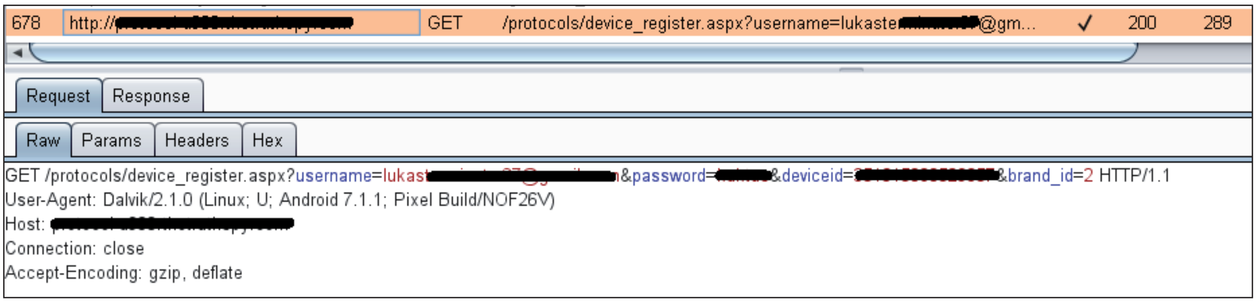
This was the issue identified most often, discovered in 22 stalkerware apps. Sensitive victim and/or stalker information was transmitted from victim devices to the stalkerware server over the unencrypted HTTP protocol and was not further protected – without integrity check or encryption. Figures 16,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

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

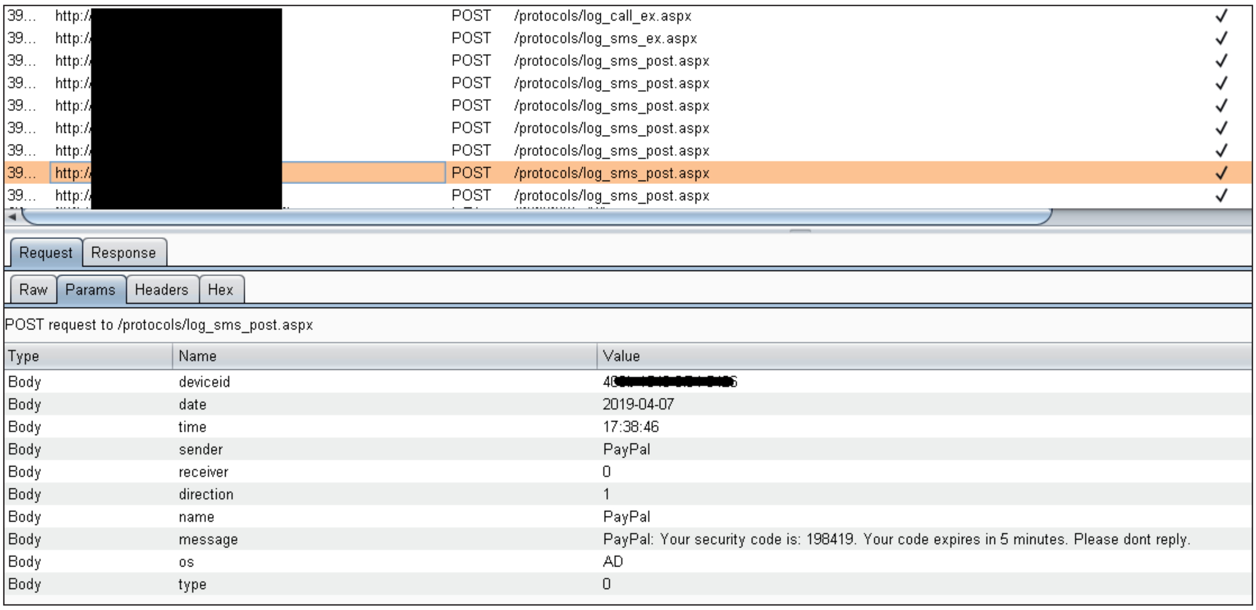
Use the HTTPS protocol to transmit user PII. Further, use an additional layer of end-to-end encryption.



```
678   http://[redacted]   GET   /protocols/device_register.aspx?username=lukaste[redacted]@gm...   ✓   200   289
```

```
GET /protocols/device_register.aspx?username=lukast[redacted]n&password=[redacted]&deviceid=[redacted]&brand_id=2 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; Pixel Build/NOF26V)
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate
```

Figure 16: Registering device to a server.

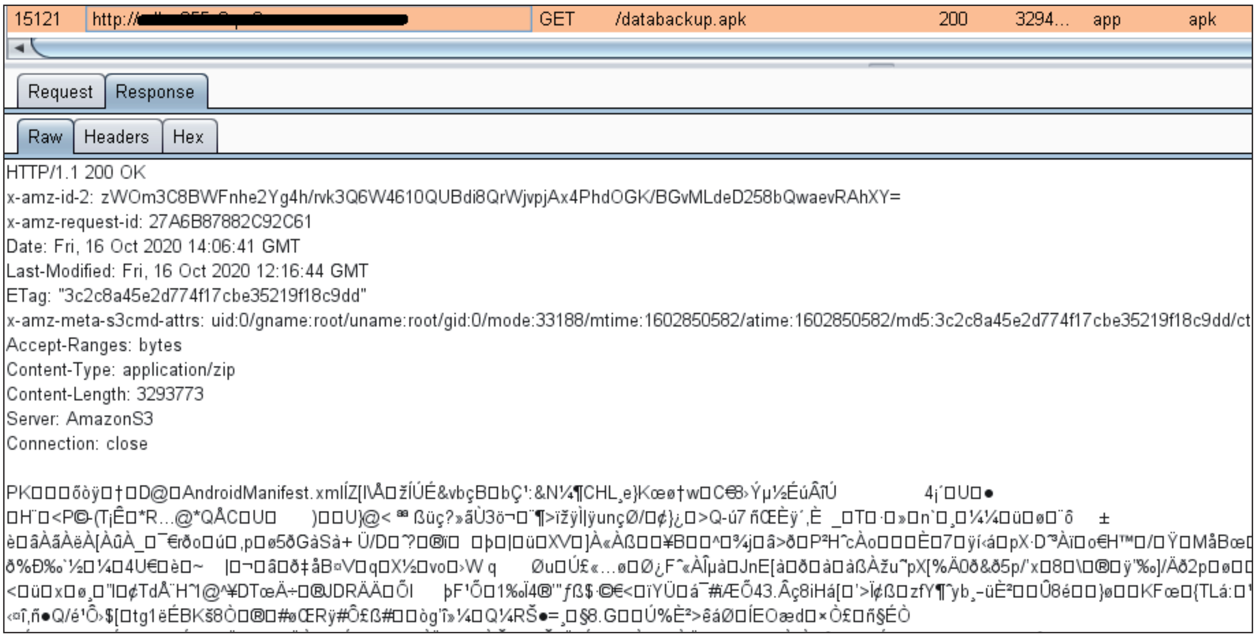


39...	http:/[redacted]	POST	/protocols/log_call_ex.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_ex.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓

POST request to /protocols/log_sms_post.aspx

Type	Name	Value
Body	deviceid	4[redacted]6
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 17: Data extraction from victim's device.



```
15121   http://[redacted]   GET   /databackup.apk   200   3294...   app   apk
```

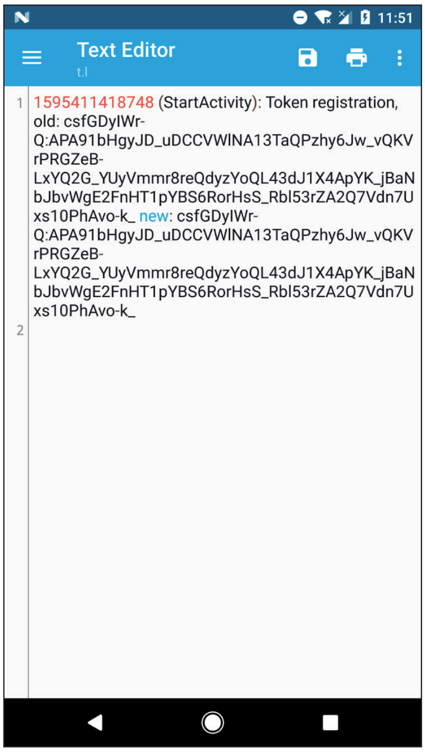
```
HTTP/1.1 200 OK
x-amz-id-2: zWOm3C8BWFnhe2Yg4h/rvk3Q6W4610QUBdi8QrWjvpjAx4PhdOGK/BGvMLdeD258bQwaevRAhXY=
x-amz-request-id: 27A6B87882C92C61
Date: Fri, 16 Oct 2020 14:06:41 GMT
Last-Modified: Fri, 16 Oct 2020 12:16:44 GMT
ETag: "3c2c8a45e2d774f17cbe35219f18c9dd"
x-amz-meta-s3cmd-attrs: uid:0/gname:root/uname:root/gid:0/mode:33188/mtime:1602850582/atime:1602850582/md5:3c2c8a45e2d774f17cbe35219f18c9dd/ct
Accept-Ranges: bytes
Content-Type: application/zip
Content-Length: 3293773
Server: AmazonS3
Connection: close

PK□□□õòÿ□†□D@□AndroidManifest.xmlÍZ[lÅ□žÍÚÉ&vbçB□bÇ¹:&N¼¶CHL¸e}Kœø†w□C€8›Ýµ½ÉúÂîÚ             4¡´□U□●
□H¨□<P©-(T¡Ê□*R…@*QÅC□U□      )□□U}@< ª ßüç?»ãÙ3ö¬□¨¶>ïžÿl|ÿunçØ/□¢}¿□>Q-ú7 ñŒÈÿ´,È  _□T□·□»□n`□¸□¼¼□ü□ø□¨ô    ±
è□âÀãÀëÀ[ÀûÀ_□¯€rðo□ú□,p□ø5ðGàSà+ Ü/D□˜?□®ï□  □þ□|□ü□XV□]À«Àß□□¥B□□^□¾j□â>ð□P²H˜cÀo□□□È□7□ÿí‹á□pX·D˜³Àï□o€H™□/□Ÿ□MåBœ□
ð%Ð%‰`½□¼□4U€□è□~    |□¬□â□ð‡åB¤V□q□X½□vo□›W q       Øu□Ú£«…ø□Ø¿F˜«ÀÎµà□JnE[à□ð□à□àßÀžu˜pX[%Ä0ð&ð5p/'x□8□\□®□ÿ'‰]/Äð2p□ø□□
<□ü□x□ø¸□"I□¢TdÅ¨H˜1@^¥DTœÄ÷□®JDRÄÄ□ÕI      þF¹Õ□1%ₒÎ4®'"ƒß$·©€<□ïYÜ□á¯#ÆÕ43.Âç8iHá[□'>Ì¢ß□zfY¶˜yb¸-üÈ²□□Û8é□□}ø□□KFœ□{TLá:□'
‹¤î,ñ●Q/é¹Ô›$[□tg1ëÉBKš8Ò□®□#øŒRÿ#Ô£ß#□□òg'î»¼□Q¼RŠ●=¸□§8.G□□Ú%È²>êáØ□ÍEOæd□×Ò£□ñ§ÉÒ
```

Figure 18: Downloading payload of stalkerware.

Storing sensitive information on external media (CWE-922 [9])

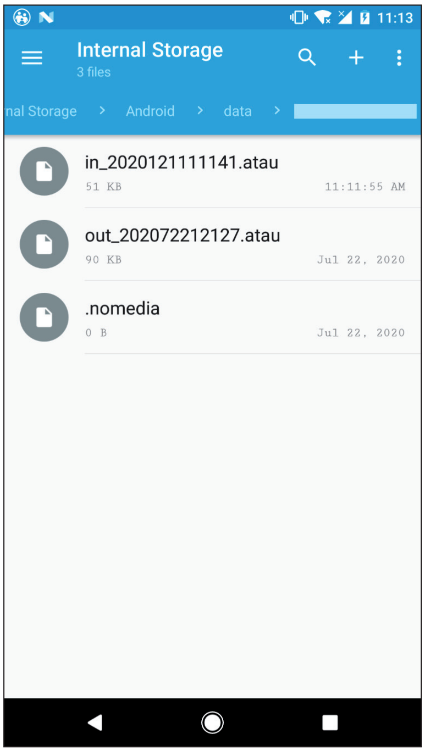
Stalkerware's main goal is to gather personal information and send it to the stalkerware server where it can be viewed by the stalker. These files first need to be stored on the victimized device and then transmitted. Unfortunately, 19 analysed apps store files such as keystroke logs, photos, recorded 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 Figures 19, 20 and 21.

This applies only to *Android* devices with OS below *Android 10*, because of scoped storage [10] 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 successfully be accessed by an adversary.



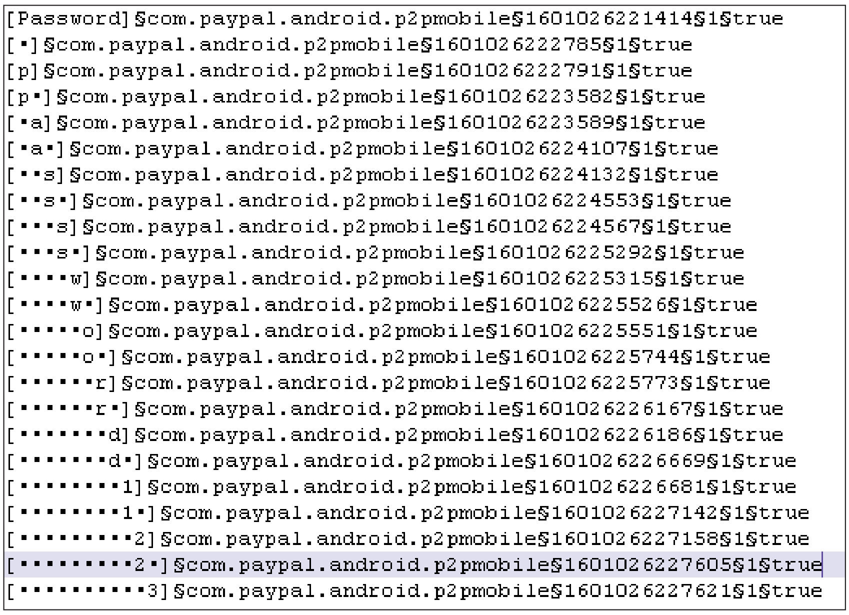
```
1595411418748 (StartActivity): Token registration, old: csfGDyIWr-Q:APA91bHgyJD_uDCCVWlNA13TaQPzhy6Jw_vQKVrPRGZeB-LxYQ2G_YUyVmmr8reQdyzYoQL43dJ1X4ApYK_jBaNbJbvWgE2FnHT1pYBS6RorHsS_Rbl53rZA2Q7Vdn7Uxs10PhAvo-k_ new: csfGDyIWr-Q:APA91bHgyJD_uDCCVWlNA13TaQPzhy6Jw_vQKVrPRGZeB-LxYQ2G_YUyVmmr8reQdyzYoQL43dJ1X4ApYK_jBaNbJbvWgE2FnHT1pYBS6RorHsS_Rbl53rZA2Q7Vdn7Uxs10PhAvo-k_
```

Figure 19: Admin account token permanently stored on external media.



in_2020121111141.atau	51 KB	11:11:55 AM
out_202072212127.atau	90 KB	Jul 22, 2020
.nomedia	0 B	Jul 22, 2020

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]§com.paypal.android.p2pmobile§1601026224567§1§true
[▪▪▪s▪]§com.paypal.android.p2pmobile§1601026225292§1§true
[▪▪▪▪w]§com.paypal.android.p2pmobile§1601026225315§1§true
[▪▪▪▪w▪]§com.paypal.android.p2pmobile§1601026225526§1§true
[▪▪▪▪▪o]§com.paypal.android.p2pmobile§1601026225551§1§true
[▪▪▪▪▪o▪]§com.paypal.android.p2pmobile§1601026225744§1§true
[▪▪▪▪▪▪r]§com.paypal.android.p2pmobile§1601026225773§1§true
[▪▪▪▪▪▪r▪]§com.paypal.android.p2pmobile§1601026226167§1§true
[▪▪▪▪▪▪▪d]§com.paypal.android.p2pmobile§1601026226186§1§true
[▪▪▪▪▪▪▪d▪]§com.paypal.android.p2pmobile§1601026226669§1§true
[▪▪▪▪▪▪▪▪1]§com.paypal.android.p2pmobile§1601026226681§1§true
[▪▪▪▪▪▪▪▪1▪]§com.paypal.android.p2pmobile§1601026227142§1§true
[▪▪▪▪▪▪▪▪▪2]§com.paypal.android.p2pmobile§1601026227158§1§true
[▪▪▪▪▪▪▪▪▪2▪]§com.paypal.android.p2pmobile§1601026227605§1§true
[▪▪▪▪▪▪▪▪▪▪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

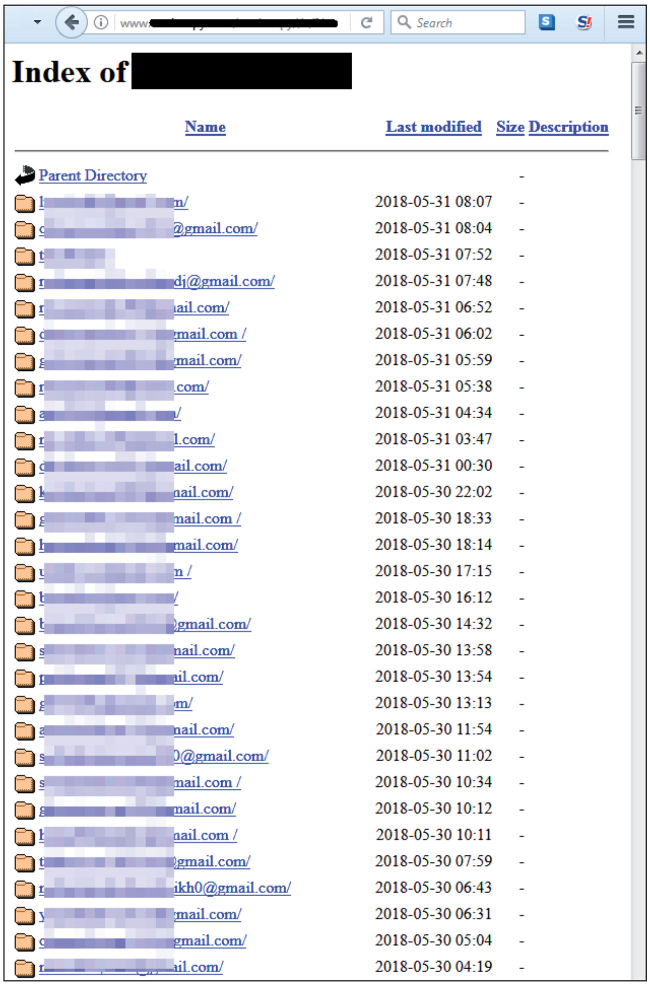
Store sensitive data in internal app's storage or encrypt them before storing on external storage.

Exposure of sensitive victim information to unauthorized user (CWE-200 [8])

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. A few examples are displayed in Figures 23, 24 and 25.

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

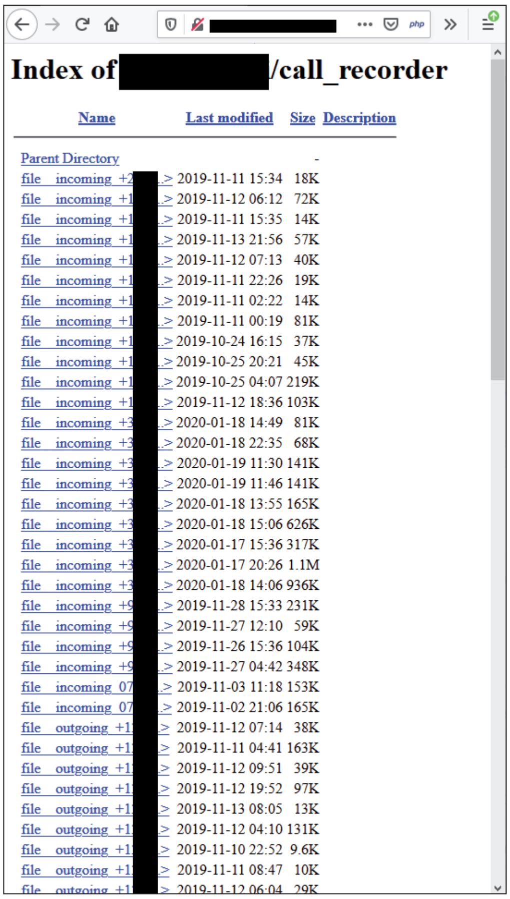
Figure 22: Leaked and accessible victim data files.



Index of [redacted]

Name	Last modified	Size	Description
Parent Directory		-	
[redacted]m/	2018-05-31 08:07	-	
[redacted]@gmail.com/	2018-05-31 08:04	-	
[redacted]	2018-05-31 07:52	-	
[redacted]dj@gmail.com/	2018-05-31 07:48	-	
[redacted]ail.com/	2018-05-31 06:52	-	
[redacted]mail.com /	2018-05-31 06:02	-	
[redacted]mail.com/	2018-05-31 05:59	-	
[redacted].com/	2018-05-31 05:38	-	
[redacted]/	2018-05-31 04:34	-	
[redacted]l.com/	2018-05-31 03:47	-	
[redacted]ail.com/	2018-05-31 00:30	-	
[redacted]nail.com/	2018-05-30 22:02	-	
[redacted]mail.com /	2018-05-30 18:33	-	
[redacted]mail.com/	2018-05-30 18:14	-	
[redacted]n /	2018-05-30 17:15	-	
[redacted]/	2018-05-30 16:12	-	
[redacted]gmail.com/	2018-05-30 14:32	-	
[redacted]nail.com/	2018-05-30 13:58	-	
[redacted]il.com/	2018-05-30 13:54	-	
[redacted]m/	2018-05-30 13:13	-	
[redacted]nail.com/	2018-05-30 11:54	-	
[redacted]0@gmail.com/	2018-05-30 11:02	-	
[redacted]mail.com /	2018-05-30 10:34	-	
[redacted]mail.com/	2018-05-30 10:12	-	
[redacted]nail.com /	2018-05-30 10:11	-	
[redacted]gmail.com/	2018-05-30 07:59	-	
[redacted]ikh0@gmail.com/	2018-05-30 06:43	-	
[redacted]mail.com/	2018-05-30 06:31	-	
[redacted]gmail.com/	2018-05-30 05:04	-	
[redacted]il.com/	2018-05-30 04:19	-	

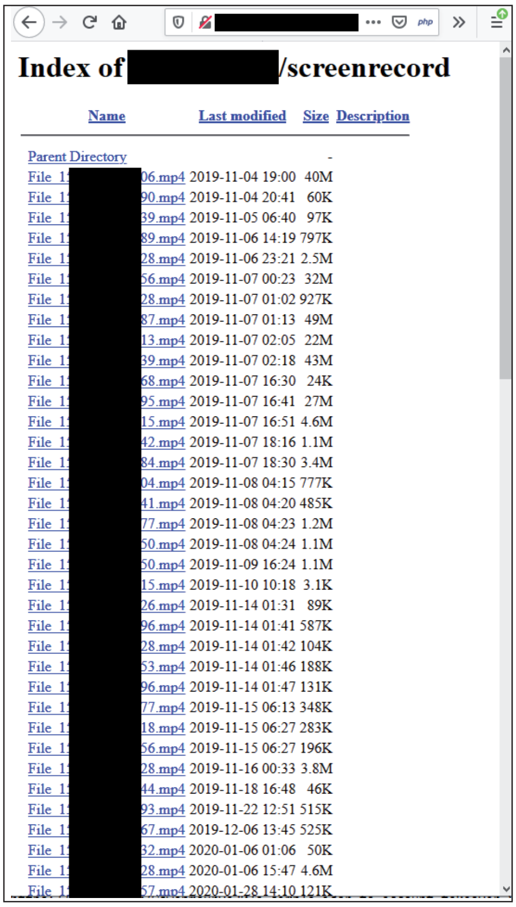
Figure 23: Victim data available based on email address.



Index of [redacted]/call_recorder

```
Name                  Last modified     Size  Description

Parent Directory                          -
file  incoming  +2[redacted]..> 2019-11-11 15:34   18K
file  incoming  +1[redacted]..> 2019-11-12 06:12   72K
file  incoming  +1[redacted]..> 2019-11-11 15:35   14K
file  incoming  +1[redacted]..> 2019-11-13 21:56   57K
file  incoming  +1[redacted]..> 2019-11-12 07:13   40K
file  incoming  +1[redacted]..> 2019-11-11 22:26   19K
file  incoming  +1[redacted]..> 2019-11-11 02:22   14K
file  incoming  +1[redacted]..> 2019-11-11 00:19   81K
file  incoming  +1[redacted]..> 2019-10-24 16:15   37K
file  incoming  +1[redacted]..> 2019-10-25 20:21   45K
file  incoming  +1[redacted]..> 2019-10-25 04:07  219K
file  incoming  +1[redacted]..> 2019-11-12 18:36  103K
file  incoming  +3[redacted]..> 2020-01-18 14:49   81K
file  incoming  +3[redacted]..> 2020-01-18 22:35   68K
file  incoming  +3[redacted]..> 2020-01-19 11:30  141K
file  incoming  +3[redacted]..> 2020-01-19 11:46  141K
file  incoming  +3[redacted]..> 2020-01-18 13:55  165K
file  incoming  +3[redacted]..> 2020-01-18 15:06  626K
file  incoming  +3[redacted]..> 2020-01-17 15:36  317K
file  incoming  +3[redacted]..> 2020-01-17 20:26  1.1M
file  incoming  +3[redacted]..> 2020-01-18 14:06  936K
file  incoming  +9[redacted]..> 2019-11-28 15:33  231K
file  incoming  +9[redacted]..> 2019-11-27 12:10   59K
file  incoming  +9[redacted]..> 2019-11-26 15:36  104K
file  incoming  +9[redacted]..> 2019-11-27 04:42  348K
file  incoming  07[redacted]..> 2019-11-03 11:18  153K
file  incoming  07[redacted]..> 2019-11-02 21:06  165K
file  outgoing  +1[redacted]>   2019-11-12 07:14   38K
file  outgoing  +1[redacted]>   2019-11-11 04:41  163K
file  outgoing  +1[redacted]>   2019-11-12 09:51   39K
file  outgoing  +1[redacted]>   2019-11-12 19:52   97K
file  outgoing  +1[redacted]>   2019-11-13 08:05   13K
file  outgoing  +1[redacted]>   2019-11-12 04:10  131K
file  outgoing  +1[redacted]>   2019-11-10 22:52  9.6K
file  outgoing  +1[redacted]>   2019-11-11 08:47   10K
file  outgoing  +1[redacted]>   2019-11-12 06:04   29K
```

Figure 24: Recorded phone calls.



Index of [redacted]/screenrecord

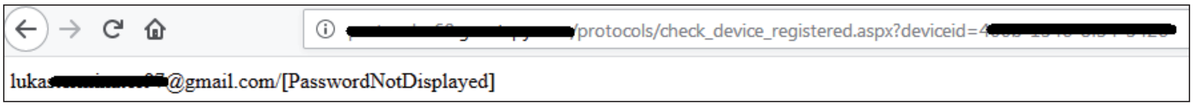
```
Name                  Last modified     Size  Description

Parent Directory                          -
File 1[redacted]06.mp4 2019-11-04 19:00   40M
File 1[redacted]90.mp4 2019-11-04 20:41   60K
File 1[redacted]39.mp4 2019-11-05 06:40   97K
File 1[redacted]89.mp4 2019-11-06 14:19  797K
File 1[redacted]28.mp4 2019-11-06 23:21  2.5M
File 1[redacted]56.mp4 2019-11-07 00:23   32M
File 1[redacted]28.mp4 2019-11-07 01:02  927K
File 1[redacted]87.mp4 2019-11-07 01:13   49M
File 1[redacted]13.mp4 2019-11-07 02:05   22M
File 1[redacted]39.mp4 2019-11-07 02:18   43M
File 1[redacted]68.mp4 2019-11-07 16:30   24K
File 1[redacted]95.mp4 2019-11-07 16:41   27M
File 1[redacted]15.mp4 2019-11-07 16:51  4.6M
File 1[redacted]42.mp4 2019-11-07 18:16  1.1M
File 1[redacted]84.mp4 2019-11-07 18:30  3.4M
File 1[redacted]04.mp4 2019-11-08 04:15  777K
File 1[redacted]41.mp4 2019-11-08 04:20  485K
File 1[redacted]77.mp4 2019-11-08 04:23  1.2M
File 1[redacted]50.mp4 2019-11-08 04:24  1.1M
File 1[redacted]50.mp4 2019-11-09 16:24  1.1M
File 1[redacted]15.mp4 2019-11-10 10:18  3.1K
File 1[redacted]26.mp4 2019-11-14 01:31   89K
File 1[redacted]96.mp4 2019-11-14 01:41  587K
File 1[redacted]28.mp4 2019-11-14 01:42  104K
File 1[redacted]53.mp4 2019-11-14 01:46  188K
File 1[redacted]96.mp4 2019-11-14 01:47  131K
File 1[redacted]77.mp4 2019-11-15 06:13  348K
File 1[redacted]18.mp4 2019-11-15 06:27  283K
File 1[redacted]56.mp4 2019-11-15 06:27  196K
File 1[redacted]28.mp4 2019-11-16 00:33  3.8M
File 1[redacted]44.mp4 2019-11-18 16:48   46K
File 1[redacted]93.mp4 2019-11-22 12:51  515K
File 1[redacted]67.mp4 2019-12-06 13:45  525K
File 1[redacted]32.mp4 2020-01-06 01:06   50K
File 1[redacted]28.mp4 2020-01-06 15:47  4.6M
File 1[redacted]57.mp4 2020-01-28 14:10  121K
```

Figure 25: Video recordings of a victim devices' screens.

Server leak of stalker information (CWE-200 [8])

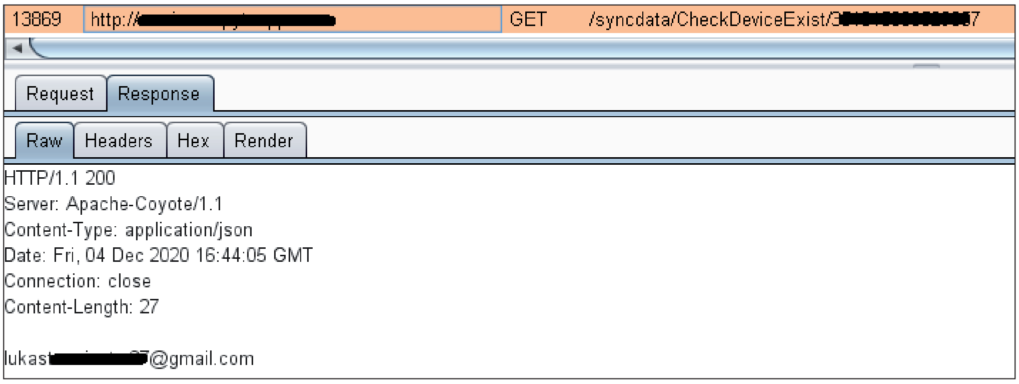
When a victim identifies stalkerware on a device, either using security software or forensic analysis, in some cases it is possible to retrieve information from the app vendor's server about the stalker (see Figure 26) and possibly what data were gathered. All the victim needs to know is the unique device 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 has been used against this smartphone in the past, as seen in Figure 27.



```
[redacted]/protocols/check_device_registered.aspx?deviceid=[redacted]

lukas[redacted]@gmail.com/[PasswordNotDisplayed]
```

Figure 26: Retrieving the stalker's email address.



```
13869   http://[redacted]   GET   /syncdata/CheckDeviceExist/3[redacted]7
```

```
HTTP/1.1 200
Server: Apache-Coyote/1.1
Content-Type: application/json
Date: Fri, 04 Dec 2020 16:44:05 GMT
Connection: close
Content-Length: 27

lukas[redacted]@gmail.com
```

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

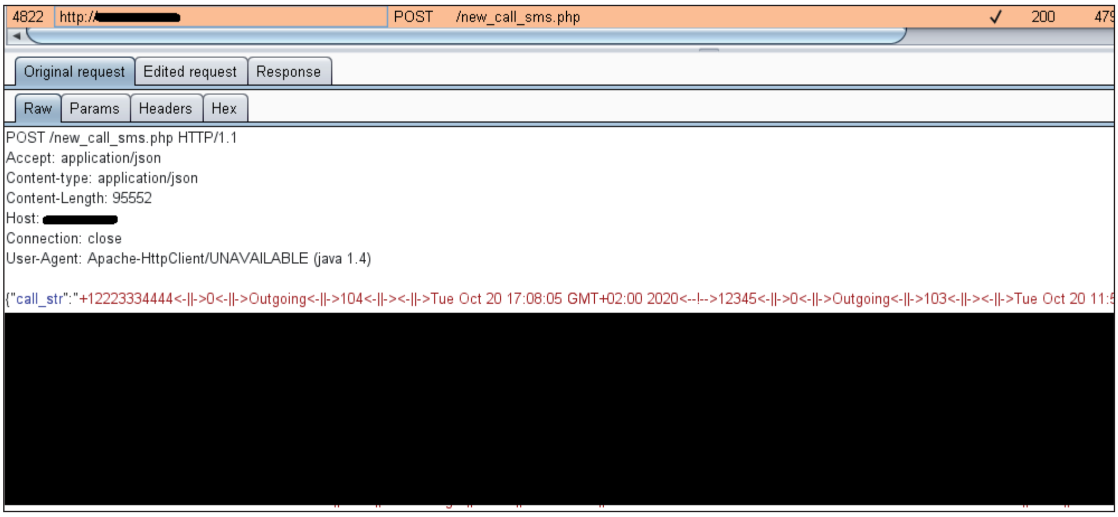
Impact

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 behaviour is more typical of malicious apps and was observed in 15 analysed 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 behaviour 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 licence 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.



```
POST /new_call_sms.php HTTP/1.1
Accept: application/json
Content-type: application/json
Content-Length: 95552
Host: [redacted]
Connection: close
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

{"call_str":"+12223334444<-||->0<-||->Outgoing<-||->104<-||-><-||->Tue Oct 20 17:08:05 GMT+02:00 2020<--!-->12345<-||->0<-||->Outgoing<-||->103<-||-><-||->Tue Oct 20 11:5
```

[redacted]

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

Impact

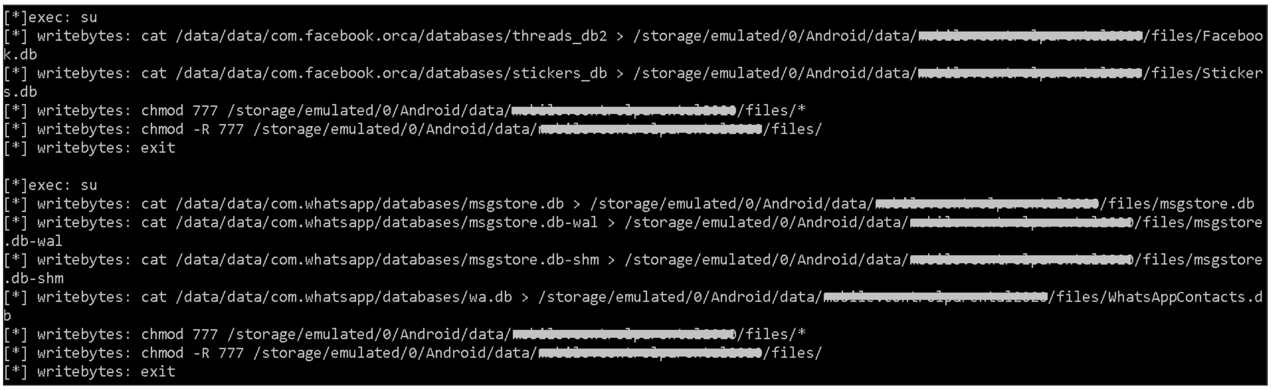
In case of a data breach, the stalkerware server might contain victims' data, even though the app was never actually used.

Incorrect permission assignment for devices with superuser privileges (CWE-732 [11])

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 analysed.

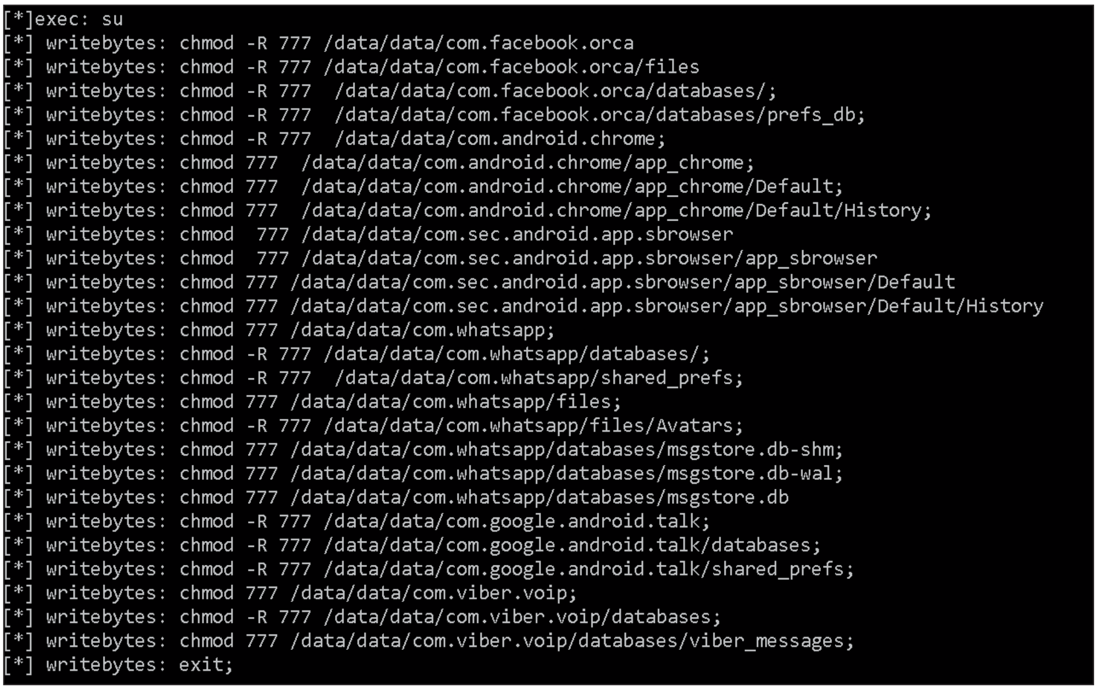
To obtain internal files of targeted apps that contain contacts, chat messages or browsing history, stalkerware first needs to change permissions for these files or directories and then send them to its server. Changing permissions was done in all cases with the `chmod 777` command (Figure 30), which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

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



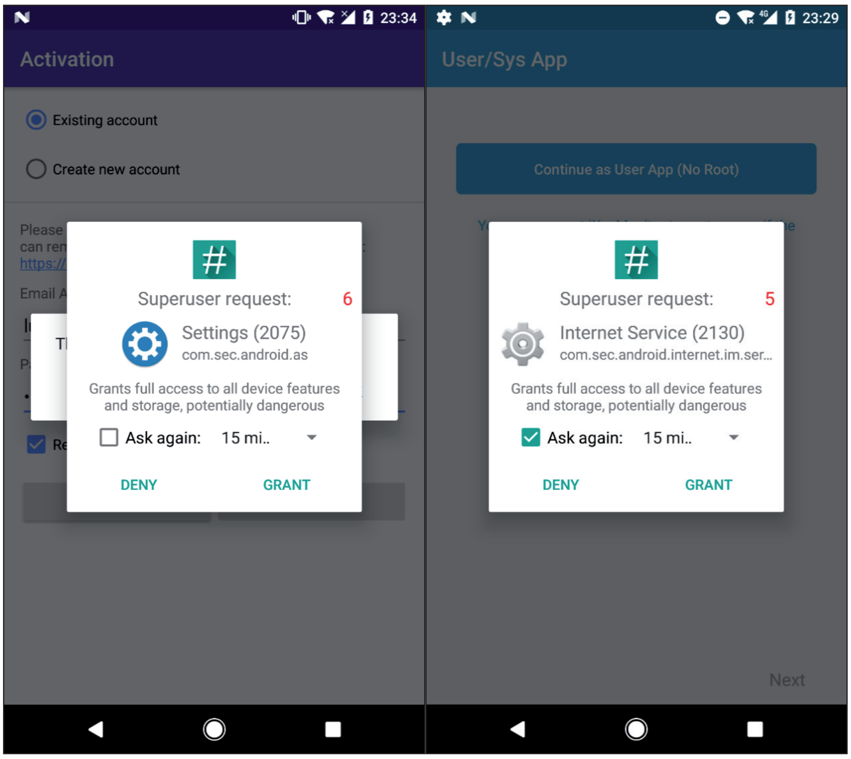
```
[*]exec: su
[*] writebytes: cat /data/data/com.facebook.orca/databases/threads_db2 > /storage/emulated/0/Android/data/[redacted]/files/Faceboo
k.db
[*] writebytes: cat /data/data/com.facebook.orca/databases/stickers_db > /storage/emulated/0/Android/data/[redacted]/files/Sticker
s.db
[*] writebytes: 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.d
b
[*] 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 target8ed apps.



Superuser request: 6
Settings (2075)
com.sec.android.as
Grants full access to all device features and storage, potentially dangerous
□ Ask again: 15 mi..

Superuser request: 5
Internet Service (2130)
com.sec.android.internet.im.ser...
Grants full access to all device features and storage, potentially dangerous
☑ Ask again: 15 mi..

Figure 31: Requests to grant superuser rights.

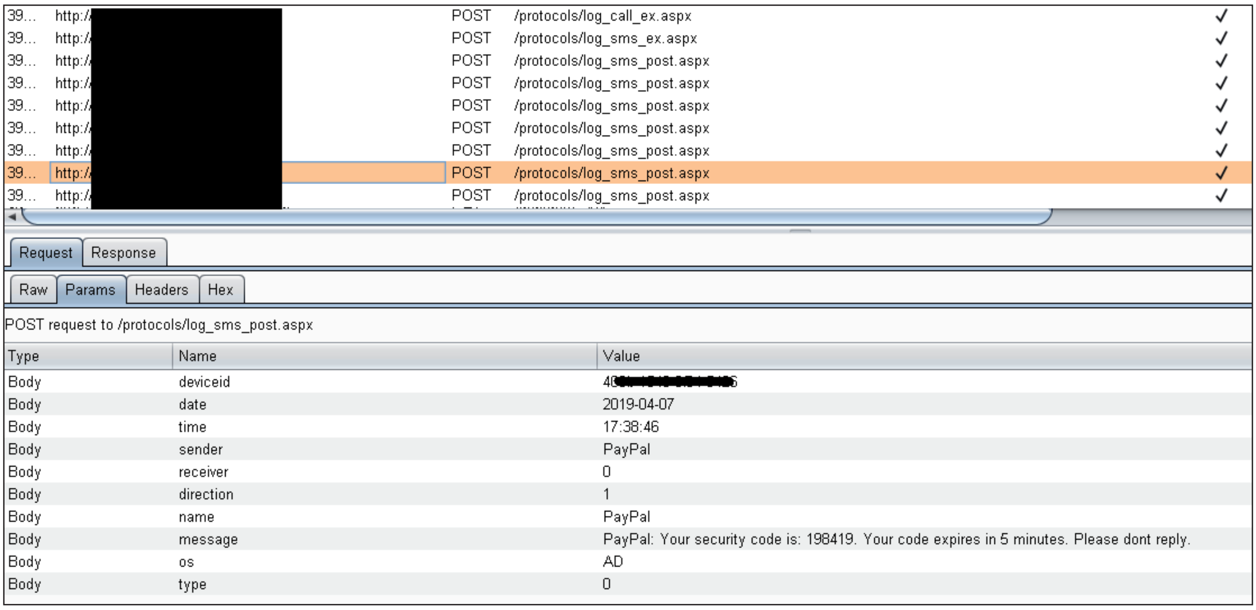
Impact

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 [12])

This issue was found in 13 of the analysed 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 easily be extracted by other apps installed on a device and could then be used to upload fabricated text messages, photos, phone calls and other fictitious data to the server, to frame victims or make their lives more difficult.



39...	http:/[redacted]	POST	/protocols/log_call_ex.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_ex.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓
39...	http:/[redacted]	POST	/protocols/log_sms_post.aspx	✓

POST request to /protocols/log_sms_post.aspx

Type	Name	Value
Body	deviceid	[redacted]
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 [13])

In the case of no Internet connection, nine analysed stalkerware apps allow receipt of commands via text messages. Unfortunately, in these cases the stalkerware doesn't verify if a command is from the stalker and executes it automatically. 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 licence expired.

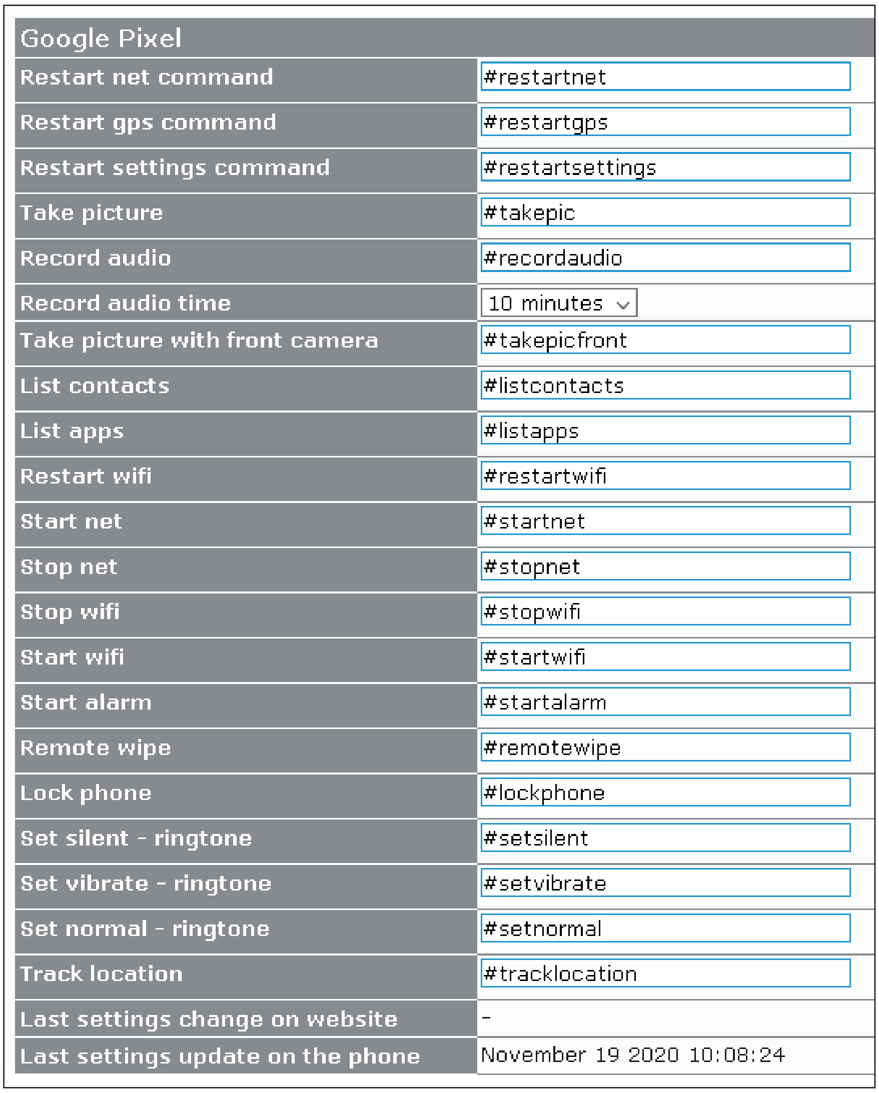
Even though the list of commands covers a wide spectrum of device control, not all the commands are valuable for a remote attacker. During our tests, we identified the most useful as: retrieving the GPS location in a return SMS, wiping external storage, and making the stalkerware call the SMS sender 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) 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 [14])

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 licence or not was done only on the main



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.

(dashboard) page. If a stalker directly accesses the URLs to view other website sections such as Calls, Contacts, Messages, then licence authentication is missing and the server provides the requested pages.

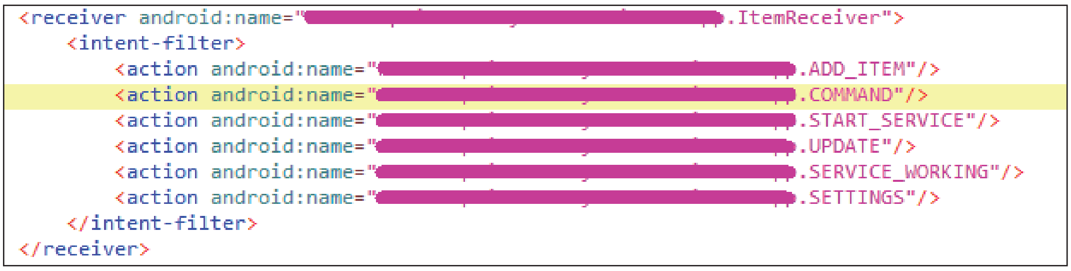
Impact

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

Command injection (CWE-926 [15])

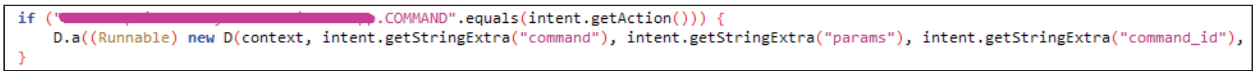
Six analysed apps exported an unprotected component (broadcast receiver) that can be triggered by any app installed on the device, such as in the example in Figure 34. We identified exported components that would allow an attacker to record surrounding audio, take device screenshots, and in one case 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. This 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

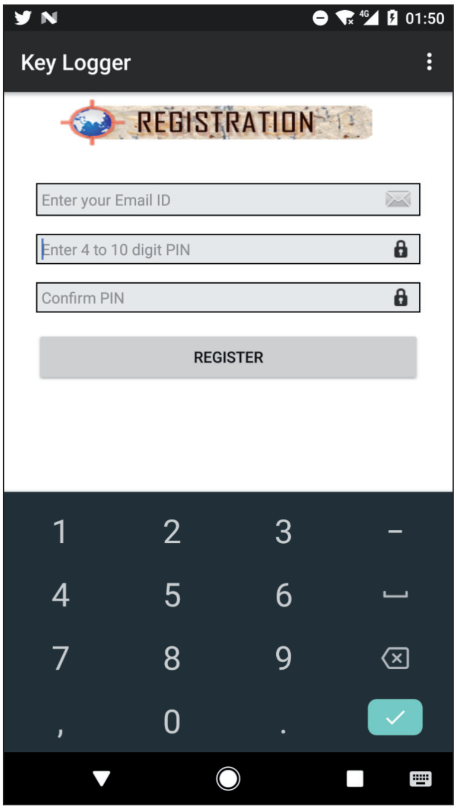
Third-party apps could trigger functionality from stalkerware without any permission, and then access the results – photos, recorded audio and screenshots – because they are stored on external media.

Possible fix

Set permission to restrict access of an exported component.

Enforcing weak registration password (CWE-521 [16])

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.



Enter your Email ID

Enter 4 to 10 digit PIN

Confirm PIN

Figure 36: User registration with enforced PIN as a password.

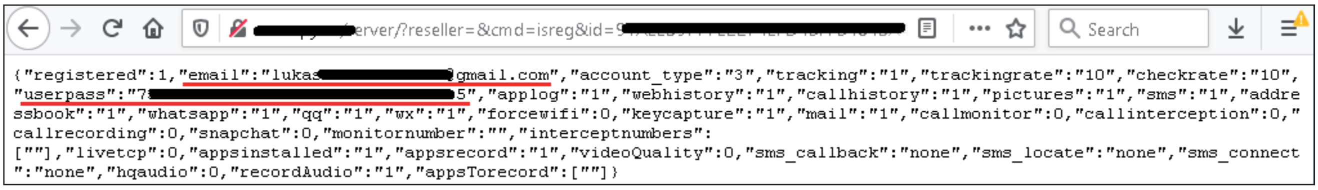
Impact

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 [17])

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.



[redacted]erver/?reseller=&cmd=isreg&id=9[redacted]

```
{"registered":1,"email":"lukas[redacted]gmail.com","account_type":"3","tracking":"1","trackingrate":"10","checkrate":"10",
"userpass":"7[redacted]5","applog":"1","webhistory":"1","callhistory":"1","pictures":"1","sms":"1","addre
ssbook":"1","whatsapp":"1","qq":"1","wx":"1","forcewifi":0,"keycapture":"1","mail":"1","callmonitor":0,"callinterception":0,"
callrecording":0,"snapchat":0,"monitornumber":"","interceptnumbers":
[""],"livetcp":0,"appsinstalled":"1","appsrecord":"1","videoQuality":0,"sms_callback":"none","sms_locate":"none","sms_connect
":"none","hqaudio":0,"recordAudio":"1","appsTorecord":[""]}
```

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.

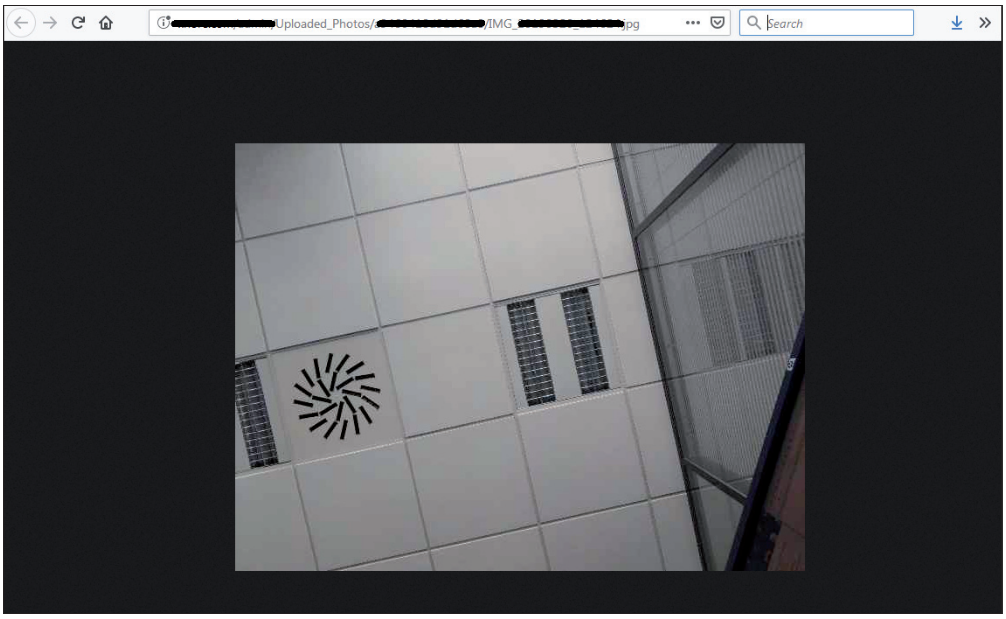
Possible fix

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

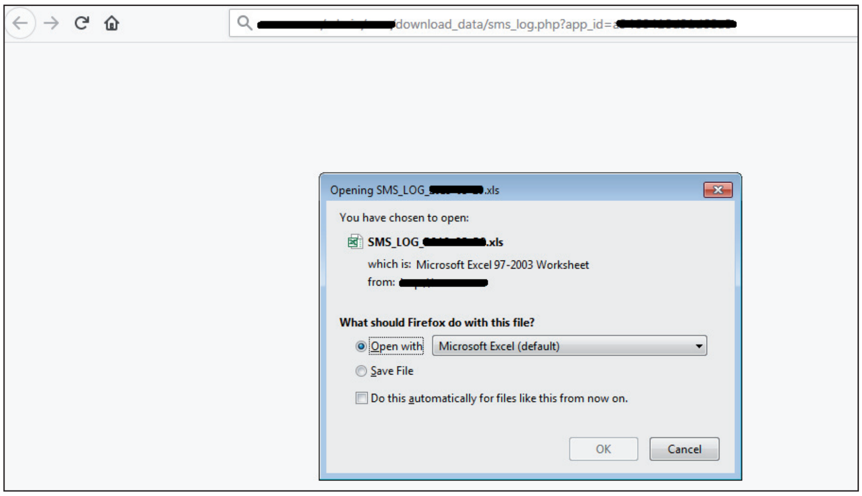
What happens when the stalking ends? In our tests, when the stalker removed data logs, unlinked the victim smartphone and removed their account from the monitoring service, the gathered victim information was, for some vendors, still available on the server.

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.



[redacted]Uploaded_Photos/[redacted]/IMG_[redacted]jpg

Figure 38: Accessing our photos after account removal.



[redacted]download_data/sms_log.php?app_id=[redacted]

Opening SMS_LOG_[redacted].xls

You have chosen to open:

SMS_LOG_[redacted].xls

which is: Microsoft Excel 97-2003 Worksheet

from: [redacted]

What should Firefox do with this file?

● Open with Microsoft Excel (default)

○ Save File

□ Do this automatically for files like this from now on.

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 already be removed from the server.

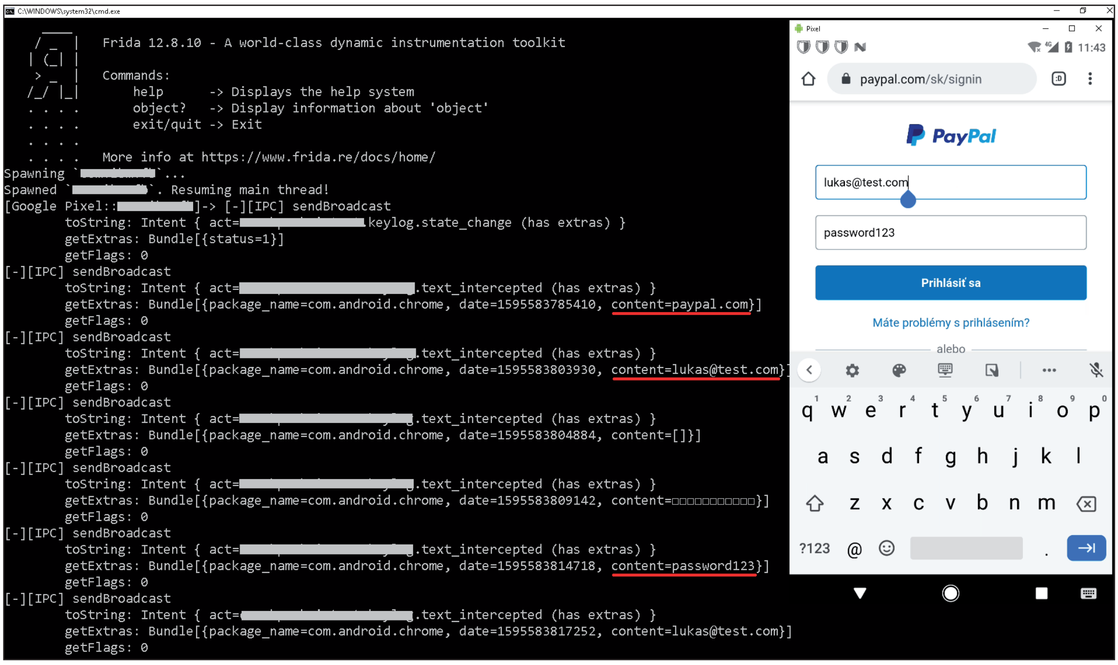
Possible fix

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 [18])

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 analysed. 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.



C:\WINDOWS\system32\cmd.exe

```
     ____
    / _  |   Frida 12.8.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://www.frida.re/docs/home/
Spawning `[redacted]`...
Spawned `[redacted]`. Resuming main thread!
[Google Pixel::[redacted]]-> [-][IPC] sendBroadcast
        toString: Intent { act=[redacted].keylog.state_change (has extras) }
        getExtras: Bundle[{status=1}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583785410, content=paypal.com}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583803930, content=lukas@test.com}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583804884, content=[]}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583809142, content=□□□□□□□□□□□}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583814718, content=password123}]
        getFlags: 0
[-][IPC] sendBroadcast
        toString: Intent { act=[redacted].text_intercepted (has extras) }
        getExtras: Bundle[{package_name=com.android.chrome, date=1595583817252, content=lukas@test.com}]
        getFlags: 0
```

paypal.com/sk/signin

PayPal

lukas@test.com

password123

Figure 40: Leak of all user text input.

Impact

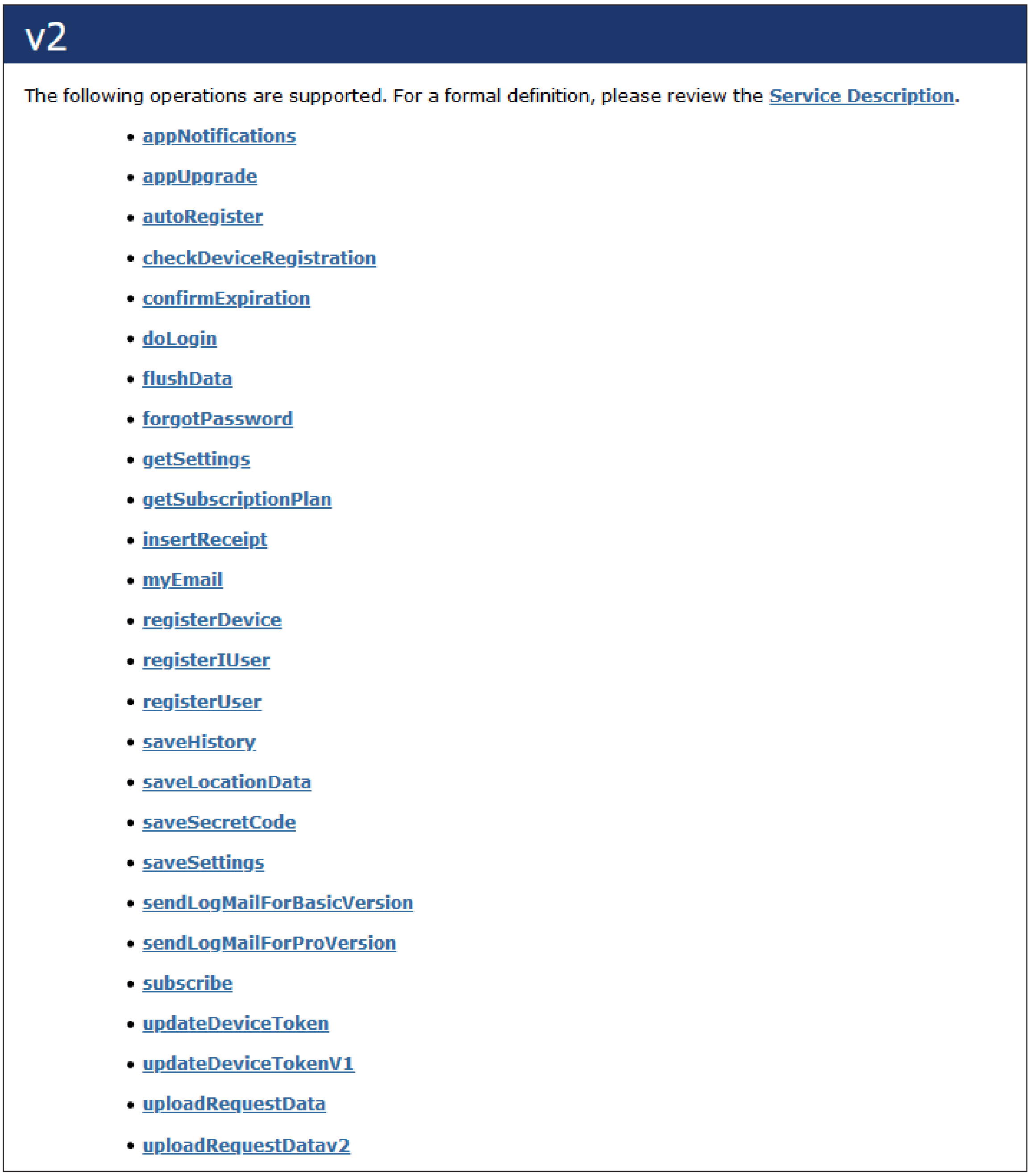
Any app installed on the device could snoop on all keystrokes without necessary permissions.

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 [13])

The stalkerware server of one analysed 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.

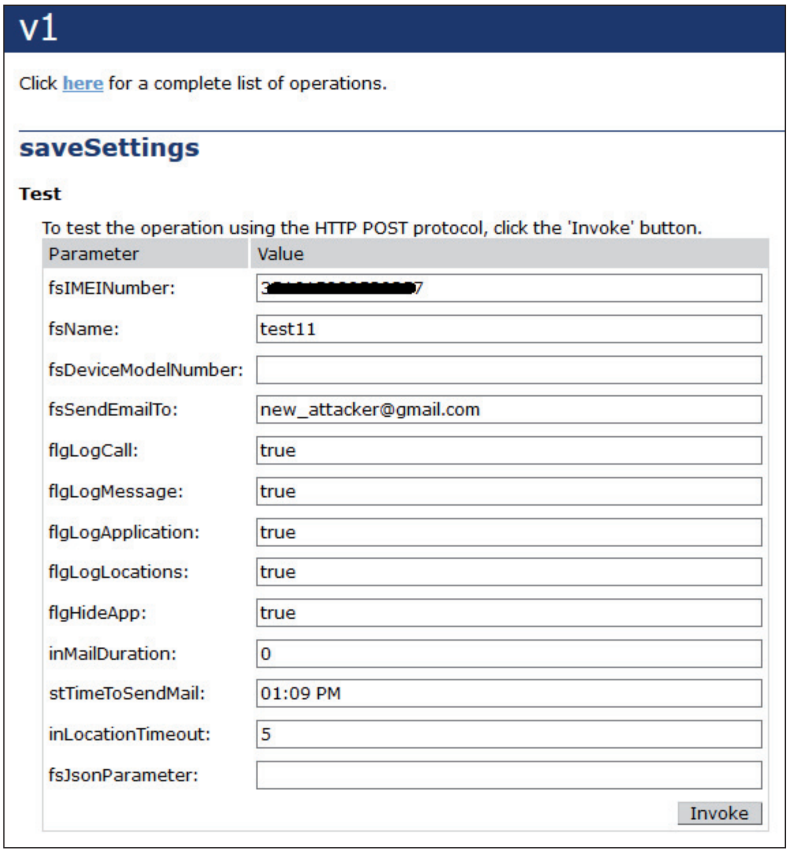


v2

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:	[redacted]
fsName:	test11
fsDeviceModelNumber:	
fsSendEmailTo:	new_attacker@gmail.com
flgLogCall:	true
flgLogMessage:	true
flgLogApplication:	true
flgLogLocations:	true
flgHideApp:	true
inMailDuration:	0
stTimeToSendMail:	01:09 PM
inLocationTimeout:	5
fsJsonParameter:	

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 the stalker.

Possible fix

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

Remote livestream of video and audio from victim device (CWE-284 [14])

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, one app we examined 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.

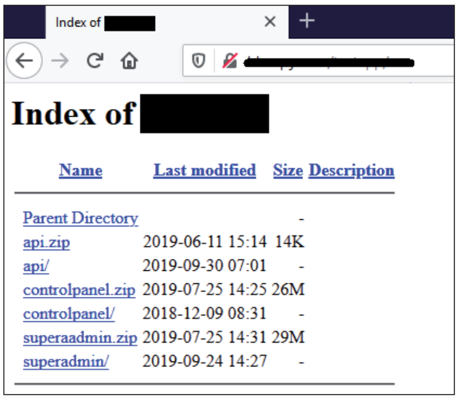
As a result, this action would make it a permanent system stalkerware that can only be removed either remotely by the stalker or with physical access to the device and using ADB tools as superuser.

Possible fix

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

Source code and superadmin credentials leak (CWE-200 [8])

One of the analysed 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.



Index of [redacted]

[redacted]

Index of [redacted]

Name	Last modified	Size	Description
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 the 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 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 the private data of the analysed app.

Of 86 stalkerware apps it was possible to extract such data from 55 of them.

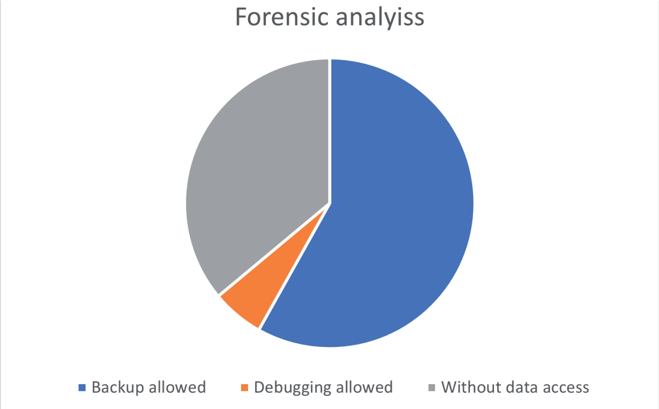


Figure 44: Possibility to perform successful stalkerware data extraction.

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 often related to harassment and other forms of violence. Victims might be psychologically coerced, intimidated or physically forced into disabling this type of protection or into revealing their passcode – especially if they live in the same household as their cyberstalker.

Victims should consider carefully before 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 [1], whoever installed it will know that it was removed or disabled, which could have negative 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 multi-factor authentication.

CONCLUSION

Based on our data, *Android* stalkerware has become more and more widely used over the last two years. 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 of the 86 apps we analysed.

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, of 58 vendors with security and/or privacy problems, 45 have not fixed the issues, six have promised to issue a patch but still have not done so, and just seven have fixed the problems. Among the 45 vendors whose apps are still not fixed, 44 haven’t even replied to our coordinated vulnerability disclosure email messages.

REFERENCES

[1] Coalition Against Stalkerware. https://stopstalkerware.org/.

[2] https://github.com/Te-k/stalkerware-indicators.

[3] Mobile Operating System Market Share Worldwide. Statcounter. https://gs.statcounter.com/os-market-share/mobile/worldwide.

[4] Enabling dishonest behavior. https://support.google.com/adspolicy/answer/6016086?hl=en&ref_topic=1626336.

[5] Man-in-the-Disk: A New Attack Surface for Android Apps. Check Point Blog. https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/.

[6] https://github.com/Odrin/Droid-Watcher.

[7] ESET coordinated vulnerability disclosure policy. https://www.eset.com/int/research/vulnerability-disclosure-policy/.

[8] CWE-200: Exposure of Sensitive Information to an Unauthorized Actor. https://cwe.mitre.org/data/definitions/200.html.

[9] CWE-922: Insecure Storage of Sensitive Information. https://cwe.mitre.org/data/definitions/922.html.

[10] Scoped storage. https://developer.android.com/training/data-storage#scoped-storage.

[11] CWE-732: Incorrect Permission Assignment for Critical Resource. https://cwe.mitre.org/data/definitions/732.html.

[12] CWE-345: Insufficient Verification of Data Authenticity. https://cwe.mitre.org/data/definitions/345.html.

[13] CWE-285: Improper Authorization. https://cwe.mitre.org/data/definitions/285.html.

[14] CWE-284: Improper Access Control. https://cwe.mitre.org/data/definitions/284.html.

[15] CWE-926: Improper Export of Android Application Components. https://cwe.mitre.org/data/definitions/926.html.

[16] CWE-521: Weak Password Requirements. https://cwe.mitre.org/data/definitions/521.html.

[17] CWE-326: Inadequate Encryption Strength. https://cwe.mitre.org/data/definitions/326.html.

[18] CWE-927: Use of Implicit Intent for Sensitive Communication. https://cwe.mitre.org/data/definitions/927.html.

IOCS

App name	Website	SHA-1	Detection name
Aispyer	https://www.aispyer[.]com	aacedb68f05402fa1f6c3450ecbd8a3b02a47a435c3d745670644f201720abaf	Android/Monitor.Aispyer.A
AllTracker	https://alltracker[.]org	731acb120c86e4896704546c861703e2086149b385583a67a727b900943f0b04	Android/Monitor.Alltracker.A
Android Monitor	https://www.androidmonitor[.]com	eaebcdfb2fdc44f3766399f1eafa6dbb3f4233e42805feca603bed97a14b5469	Android/Monitor.FreeAndSpy.B
AntiFurto Droid WEB	http://www.antifurtodroid[.]com	9dd4b366ad54960ec3e7ac473267d9818d37790bf8b5f05333997be230bd2aad	Android/Monitor.TheftSpy.G
Appmia	https://appmia[.]com	62c7cd419b22019dd16adbcfe60c6bcd1388375fc3c9af47c668a5f0190176eb	Android/Monitor.MobileTracker.D
Appspy	https://appspyfree[.]com	201625b0ab47027bd2dcb27f88c5c0cf96e4bc32505083cb7036639c6a4a8b24	Android/Monitor.Spyoo.U
A-Spy	http://www.a-spy[.]com	4de2d4cadf566abaefe945faa0a3a6e55d7a88c4b19d9249b04122702c3d5945	Android/Monitor.ScreenMon.B
BlurSpy	https://www.blurspy[.]com	36bd1f5093fbd6bceadb56e65455abdfd5ecf805682c17b9a233054bcaad0ee2	Android/Monitor.BlurSpy.A
CatWatchful	https://catwatchful[.]com	fdc7693d92dd4db644cc18f51b7cad7de86a10a589a3390c7cbb293621dd5343	Android/Monitor.Catwatch.A
Cerberus	https://cerberusapp[.]com	eb0997a778170623f60472699b4cffd5cca6525dcbc749412161df2d786a990e	Android/Monitor.Cerberus.A
ClevGuard	https://www.clevguard[.]com	0951e4a309801afc8c60e331f253eebf000cab2ae4bc004478c568539034da89	Android/Monitor.Guardian.BN
Cocospy	https://www.cocospy[.]com	c6a6539c8c0dbfdfe609ccc73029d134719c655b75bd0e6ade8a366897634067	Android/Monitor.Drower.D
Copy9	https://copy9[.]com	50e77ee23b9d3c9283291ba89278bb83b4965fc5d475f9015e1a1d7e2f3c61de	Android/Monitor.Spyoo.U
Couple Tracker	https://coupletracker[.]com	c4cb6a92fb4227949cf2820b75405304439ef04da9be336904c31e6129120450	Android/Monitor.LoveTrack.B
DDI Utilities	https://ddiutilities[.]com	a71b17d433953f3add4788c5a12e08af94a286c9464f219db4fcd7d13a115ade	Android/Monitor.Highster.B
EaseMon	https://www.easemon[.]com	356c993fcf81fc578e049c9a4d52c9cb13d88343ad95891c6b0afc4a8bcfbbd6	Android/Monitor.IkeyMonitor.C

Easy Logger	https://logger[.]mobi	67f5640e4c1f64c94d423254530ec09c59a10fc8821000403037b65cdc40a5bc	Android/Monitor.Easylogger.A
Easy Phone Tracker	https://easyphonetrack[.]com	c174af86a5cd60e1b6869c596eca0e7e41056736c6834b73799983ce5da3dd15	Android/Monitor.SpyPhone.Q
EvaSpy	https://evaspy[.]com	6902aa7ed19183b6039546b8a9b57d28da93eb321422a4dee6ce21b011e1a21f	Android/Monitor.TiFamily.G
Flexispy	https://www.flexispy[.]com	D55BB89706A7E2726350E7739980B3188588DA22D983CD413E73F0044A6518B1	Android/Riskware.Tracer.I
Fone tracker	https://fonetracker[.]com	a27a0a98cd50ea8384de7599dd808e37b61e7c635f578437a1b621bc1ec6e5c0	Android/Monitor.Spyoo.U
FoneMate	https://www.myfonemate[.]com	570e2036e58885b33ae57125db89f08a8645565a4ec9ca9306d8b99570062e47	Android/Monitor.Mspy.O
Fonemonitor	https://fonemonitor[.]co	15fc2ca31516f06ea1ec75cb83c3fec66318bd21f15f67839115e1a4bdcd3b25	Android/Packed.Jiagu.D
Forever Spy	https://foreverspy[.]com	d42576c60d7fcc19e91c328e8ecf2ff69c6aff1e5134750bba2dd516ac188667	Android/TrojanDownloader.Agent.JN
Free Android Spy	https://www.freeandroidspy[.]com	80cb53cc7e117a326685fb4f6c929bca8b69392fa915f115e522d35cd421a43e	Android/Monitor.FreeAndSpy.B
GPS tracker - Loki	http://asgardtech[.]ru	75c76fe253a9347427793638b8a73f36a880d320fd440dcb156c9d9308459a9f	Android/Monitor.Lokimon.A
GuestSpy	https://guestspy[.]com	201625b0ab47027bd2dcb27f88c5c0cf96e4bc32505083cb7036639c6a4a8b24	Android/Monitor.Spyoo.U
Highster	https://highstermobile[.]com	2ab873c0b420b224fc1df482eec9d59a1309bec4afd675f5010a162d17998b59	Android/Monitor.Highster.E
Hoverwatch	https://www.hoverwatch[.]com	5e5003532c527630d29aa0acd6ad39c891ba0c4c4d6e388ee0bb84ed9d1f0dca	Android/Monitor.Hoverwatch.G
iKeyMonitor	https://ikeymonitor[.]com	f16206acc17faa1f53f10493805ce5c6ece8b0ce35280656669552894d3dd9fa	Android/Monitor.IkeyMonitor.C
i-Monitor	https://imonitorke[.]com	78cb36cc9aba70bc902b3c8ba1b86c7a5d72b056fd624349bbd3fd972341aacf	Android/Monitor.Imonitor.A
IntTel Track GPS	http://109.235.66[.]53/login	c0272432e1332bca159c049b8b9acefa5b591e95fa41740117a6f50048425995	Android/Monitor.Traca.F
iSpyoo	https://ispyoo[.]com	0873ad17005b00e65b15bff67fd5c03f4b8a5af147aa1274ab203a4a747f1693	Android/Monitor.Spyoo.U

iSPYOO	https://www.theispyoo[.]com	570e2036e58885b33ae57125db89f08a8645565a4ec9ca9306d8b99570062e47	Android/Monitor.Mspy.O
JJSpy	https://www.jjspy[.]com	We couldn’t obtain a sample of JJSpy, but it’s most likely very similar to mSpy	
Key Logger	https://trackmyphones[.]com/keyboard	1757972048f24774d979963104c04d36cae519367500e1972bd528f9b936b8c4	Android/Monitor.SpydioTrack.C
letmespy	http://www.letmespy[.]com	570e2036e58885b33ae57125db89f08a8645565a4ec9ca9306d8b99570062e47	Android/Monitor.Letmespy.B
Lost Android	https://www.androidlost[.]com	249a1ca204c51d741ef23b614bdc54c223c154dc7f7738b8b44821f85ef88675	Android/Monitor.Androidlost.F
Message and Call Tracker	https://callsmstracker[.]com	f10fbacc7e679a433cfafc4c5506df6292e0cfd5ac0630d5a018fb549dd50188	Android/Monitor.CallTrack.D
MeuSpy	https://meuspy[.]com	4499cb9f5f366dd6cd5b37a098e6204fd7f225cab29e8cade0b95cec0f39a929	Android/Monitor.Meuspy.F
Minspy	https://minspy[.]com	ce271fe1f0987bb6e646593fb08f36edf915ed0f11960473f6cb95aba9e8d1f0	Android/Monitor.Drower.F
Mobile Tool	https://mtoolapp[.]net/ https://mobiletool[.]ru/ https://mtoolapp[.]biz/	3a929c05e45fb20e0e469cf410cae85e01732058e414a4c0ccd25295a4dd3b95	Android/Monitor.Mobtool.B
Mobile Tracker Free	https://mobile-tracker-free[.]com	ffbf021788db3cb9a1e7ff12d49f31ca54c323fe695721750eed806e7d75977f	Android/Monitor.MobileTracker.D
MobileSpy	https://mobilespy[.]at	75c76fe253a9347427793638b8a73f36a880d320fd440dcb156c9d9308459a9f	Android/Monitor.MobileTracker.D
Mobistealth	https://www.mobistealth[.]com/	d89acb7a643630cdcf3678db62a7d8d8a80c8cf71a68e10847deb4a4c31bd00c	Android/Monitor.Androspy.E
mSpy	https://www.mspy[.]com	570e2036e58885b33ae57125db89f08a8645565a4ec9ca9306d8b99570062e47	Android/Monitor.Mspy.O
Mxspy	https://mxspy[.]com	bd269b9cc54edc2c1424a800e4fa55f34f7ea4b00322f6b6177a8cc95468d998	Android/Monitor.Spyoo.U
Neatspy	https://neatspy[.]com	cb0292635fe1b34a41777cab425828cf52a2a6efe83171e9a1b75c32b0b10142	Android/Monitor.Drower.F
NeoSpy	https://neospy[.]net/ http://neospy[.]pro/ https://neospy[.]tech/	d8b3b7cbb6a34ab2e01b07cd01a0c7ea8062f8ed448a987429f30fb363d389ab	Android/Monitor.Neospy.G
Netspy	https://www.netspy[.]net	5dc4f281c4def955616c97402dae29d3d4fc7ac6b63d4e54c21f6baf2d36c35c	Android/Monitor.AppSpy.A

OwnSpy	https://en.ownspy[.]com	4b074a8d33900e0e0b54e4fc0a79a9657d54f2618bc5f4f16c5e3059ae5b4506	Android/Monitor.OwnSpy.B
PhoneSheriff	https://www.phonesheriff[.]com	4f79d0554488f871590188ecdd374fe7767e42f370e4b15fe4e2ee38b4398709	Android/Monitor.MobileSpy.Q
PhoneSpying	https://www.phonespying[.]com	8c5d95ffe5860dce230e821645ff1fd5aa79723802fd2f8e2221801aa07d29a2	Android/Monitor.AppSpy.A
Remote Audio Recorder	https://trackmyphones[.]com/SpyAudio	d7897d07995a90a03ad224f696f2bb703719e8937b996bb41e0702c7938b09af	Android/Monitor.SpydioTrack.C
Remote Desktop	available on 3rd party stores	a2145c0971163c94dc9de6ad6f104f558612306d70d800711077f2f5c3f60c48	Android/Monitor.Androspy.E
Reptilicus	https://reptilicus[.]net/	c78e6dd91a475d60b5b89fd0cfb5475da2bab83acaf8a338d0f24c934d2f3a28	Android/Monitor.Reptilicus.G
Secret Video Recorder	alternative app stores	84365b342e590a25eff42ee351cd26f546ebac7e18e47456290abfe1dcc4ec0d	Android/Monitor.SecretCam.A
Shadow SPY	https://www.shadow-spy[.]com	ebdd719b01b484e75ea477feec129390204c3e7b02d9b11b7290ee3233728bd0	Android/Monitor.Shadspy.B
Smart Aggregation Platform	https://sap4mobile[.]com	2da2d4ae0f41c4dbd27d8a54409c40237dbb722d0485c5469b5c2f3f39559405	Android/Monitor.TrackPlus.AJ
Snoopza	https://snoopza[.]com	8ceccb0637ecb2ebe90a96ea63e99603be67e4e4e20b2195c69feef633136558	Android/Monitor.Hoverwatch.G
Spapp Monitoring	https://www.spappmonitoring[.]com	f767a4b271abbc21ca0e1194fb8b8425f9df2df78e55fb0f851b4281b7326895	Android/Monitor.SpyPhone.Q
Spy to Mobile	https://spytomobile[.]com/en	6fc7ed162f6bbadd7bf345f62270b91c256125befb4f9199474a49bfac26453b	Android/Monitor.TrackPlus.AL
Spycell	https://spycell[.]net	201625b0ab47027bd2dcb27f88c5c0cf96e4bc32505083cb7036639c6a4a8b24	Android/Monitor.Spyoo.U
SpyHuman	https://spyhuman[.]com	f1408db265a20e78eb1df9675ff2cfdf60a959c8445a9241a45218e72c0826b6	Android/Monitor.Humanspy.G
Spyic	https://spyic[.]com	a6b1ec9a59c2e9dcbe550a737dc028d8f174f11b9a69c397f81438c0e93ecc3a	Android/Monitor.Drower.F
Spyier	https://spyier[.]com	7b9464102c37803c6e8d117419ad07a75ebb85dc54cc1a95dba05f433fc89990	Android/Monitor.Drower.F
Spyine	https://spyine[.]com	c35c864a7f3e9ee97418249b4460b20aa6919bb2976ff8489a3e13172911c19a	Android/Monitor.Drower.F

Spylive 360	https://spylive360[.]com	ffa1751b7677a762d006f4c8fed57253cbf592db98e1914c252965a8de621cb7	Android/Monitor.SpyLive.A
Spyphone Mobile Tracker	https://www.spyfone[.]com/ https://www.spyphone[.]com/ https://www.phonetracker[.]com/	b60e3d8e5f31b19251cd8c47d6430cfbcb7fcf3a9e9397bbddd92a27150a665e	Android/Monitor.TrackPlus.AP
SpyToApp	http://www.spytoapp[.]com	77cee7c7c27f19137da5fbf949e6d9bc3acaa1fb462e6a69125da8934744e45d	Android/Monitor.Spyoo.L
SpyTrac	https://spytrac[.]com	0fb032fb0e3162ba5d5b43bebeccb1385a883c9b53e3d21b4443bdf5700255b0	Android/Monitor.TiFamily.G
Spyzee	https://spyzee[.]com	201625b0ab47027bd2dcb27f88c5c0cf96e4bc32505083cb7036639c6a4a8b24	Android/Monitor.Spyoo.U
Spyzie	https://spyzie[.]io	efd1ced7031ead2ee8ec6dbf8e7fdcb5bb36e3edf8294552fe954157c4dd2bf7	Android/Monitor.Spyzie.B
TalkLog	https://talklog[.]tools	0d578a21430e6ef89019974813b797809375fa2297b35df08175167a2bad96aa	Android/Monitor.TalkLog.A
Teensafe	https://teensafe[.]net	be2a85c5e79a352a9ad717c04fa9ab0e30d5afea2ce4c529a4ba13a5478cf872	Android/Packed.Jiagu.D
TheTruthSpy	https://thetruthspy[.]com	4d1a074aa3f4d66935437647949047fd19b0316ad5a357b86771dcb5e18ad587	Android/Monitor.Spyoo.U
TISPY	https://tispy[.]net	8df3248d4c1635ac75629bbc3b2abae46466b5eb5d7a8277f37ef3e0789dd0b2	Android/Monitor.TiFamily.G
Track My Phone	https://trackmyphones[.]com	a7d65ad2e1a5afb761c226caf684cfd09e86451b75e849c3a5b32aefc53ee511	Android/Monitor.Trackme.B
Track My Phone Remotely	https://trackmyphones[.]com/cgi-bin/GCM/trackMyPhone.cgi	0649ac7dc4c9a3675c56018242d2a7195b4f94d9eb6f30dcb40a44ea79928aab	Android/Monitor.SpydioTrack.C
TrackView	http://trackview[.]net	075f3885b78189ea8e898dc1b77f297d02468d288f52a9da022d451a3d2e52dc	Android/Monitor.Androspy.E
Ultra Monitor	https://www.spyequipmentuk[.]co.uk/android-ultra-spy-phone-software/	20e6ab7ba28dad9343b51f847d2da71d04ac7e7b08dcbd45e3aa9f7db07c4185	Android/Spy.Agent.AZY
UniSafe	https://usafe[.]ru/	56713bfe280bc3feb27b3b9ca25921f7e8886bbf7e645cfc39f0d80e64d67c68	Android/Monitor.SafeTracker.B
Video Rec	https://trackmyphones[.]com/cgi-bin/SpyVideo/spyvideo.cgi	b6fa6c5a413a7bc8b469f42966225ff888abdc35c5171d18e010ac2ada9603db	Android/Monitor.SpydioTrack.C
VIPTrack	http://89.47.91[.]131/viptrack/	c253a652ab4262072431e9729710a25e5554e09ac8dff4452f1c20a7271b1a57	Android/Monitor.Viptrack.A

WtSpy	http://wt-spy[.]com	4600ceebdd8da0f82798167e1484e4c8e787cfe271050078c4811b770149b7c4	Android/Monitor.Wtspy.A
Xnore	http://xnore[.]com	35fa07d5a39c670c2143718b6cedf713f32f61d93bc264939439748f6a835cc0	Android/Spy.Agent.QI