Final Report for OPC Contributions Program 2022-2023

"**Privacy Analysis of Technologies Used in Intimate Partner Abuse**"

Mohammad Mannan and Amr Youssef

Student team members:
Philippe Mangeard, Xiufen Yu, Bhaskar Tejaswi, Rohan Pagey

Concordia Institute for Information Systems Engineering (CIISE)
Concordia University, Montreal

Abstract

Intimate partner violence (IPV) is a form of abuse occurring in romantic relationships, more frequently, against the female partner. IPV can vary in severity and frequency, ranging from emotional abuse or stalking, to recurring and severe violent episodes over a long period of time. In all cases, it can have lasting impact on the victim's physical and mental health. IPV is a prevalent problem all around the world that can take various forms, affecting many, and easy access to IPV tools (also known as stalkerware applications) is also helping foster such behaviors; e.g., mobile apps allowing non-tech-savvy individuals to spy on their targets. These apps provide features for monitoring and remotely controlling a compromised mobile device as discreetly as possible, infringing on the privacy of the phone's user and security of their data.

In this report, we detail our experimental privacy and security study which investigates stalkerware apps currently available for use by abusers. Vectors through which vulnerabilities found in stalkerware apps could be exploited by malicious actors, targeting the IPV services, IPV abusers, and IPV victims, are also studied. Measurements of web tracking on websites that provide help for IPV victims are also performed.

In particular, we design and implement (web/app stores) measurement pipeline to find and analyze IPV tools that can potentially be used by abusers as well as tools that are advertised to mitigate IPV attacks. We also perform measurements of web tracking on websites that provide help for IPV victims and explore features provided by online services that are used by IPV abusers. we also study vectors through which vulnerabilities found in stalkerware apps could be exploited by malicious actors, targeting the IPV services, IPV abusers, and IPV victims.

We identified 83 stalkerware apps and websites with websites still reachable as of March 2023, one of them was available on the Google Play Store. Among these applications, we found 25 to be duplicates of other already known stalkerware apps. We enumerated and experimentally verified many invasive capabilities offered by these apps to clearly identify the severe privacy risks posed by them; we also identified well-known third-party web services that also help run the IPV ecosystem. We also found that 29 apps/services are vulnerable to various exploitable attacks. Our findings include broken authentication mechanisms, insecure storage of sensitive data and other attack vectors exploitable by external attackers.

Additionally, we employed the web privacy measurement framework OpenWPM to do the privacy measurement on 323 anti-stalking websites. We found 210/323 (65.02%) anti-stalking websites included third-party trackers; a total of unique 40 third-party hosts tracked the web pages users browsed and the searched keywords. We detected 3 session replay services on 19 anti-stalking websites, which apparently collect usage information, and user PII and other sensitive data (when a data submission form is available).

1 Introduction

In 2018, 44% of women and 36% of men in Canada report having been victim of intimate partner violence (IPV) at some point during a relationship and felt fearful for a relative's life or for their own [1]. In addition, a 2020 report[1] from the Canadian feminicide observatory for justice and accountability revealed that 50% of the Canadian women killed in 2020 were in or had an intimate relationship with the accused. Intimate partner violence is a pervasive and insidious problem that can affect people of all genders, ages, and backgrounds. Women however account for the majority of IPV victims. In 2021, the World Health Organization (WHO) recognized IPV as a major global public health concern impacting millions around the world that could cause long-term health, social and economic consequences.

While physical violence is often the most visible form of abuse, it is not the only way that abusers can control and harm their partners. New technologies have greatly facilitated intimate partner violence over the past years (e.g., see [2–6]). One significant form of IPV involves invasion of privacy and remote monitoring, which can be performed through programs called stalkerware or spouseware apps. Fascendini and Fialová [7] identifies five characteristics that distinguish technology-related violence: Anonymity – the abuser's identity remains unknown to the victim; Action-at-a-Distance – abusers do not require any physical access to the victim; Automation – abusive actions can be automated using technologies, hence require less time and effort; Accessibility – the availability of various affordable technologies make them easily accessible to perpetrators; and Propagation and Perpetuity – compromising texts, images and videos multiply and persist for a long time.

Stalkerware apps, even though most of them are advertised as tools for monitoring children, employees, girlfriends, are mobile applications whose goal is to provide undetected remote control of the compromised phone to the abuser, along with activity monitoring. Their malicious nature and the way they facilitate non-consensual surveillance and cyberstalking of an intimate partner represent a severe threat to the privacy and security of IPV victims.

Previous studies have demonstrated the large size of the stalkerware landscape on mobile platforms, with hundreds of dual-use apps available on the Google Play Store [8], and dozens of companies designing stalking apps outside the scope of the official Android marketplace [9]. Even though extensive measures have been taken by Google Play Protect to detect and repress such apps, it is still very easy for abusers to bypass and disable these protections as, most of the time, they have physical access to the phone. This increasing number of stalkerware apps has been followed by an expanding amount of compromised phones and monitored data.

While stalkerware apps regularly process private pieces of information, the security mechanisms put in place to ensure their confidentiality are, in lots of cases, lacking. Multiple vulnerabilities have been found on stalkerware apps [10], threatening data privacy but also leaving open doors for third-party attackers to perform malicious actions, either against the victim's phone or the stalkerware's backend servers.

As the use of monitoring apps increased by 93% during the Covid-19 lockdown according to Avast [11], services to help victims and to raise awareness also gained more visibility, especially towards younger victims [12]. Websites like `stopstalkerware.org` are usually on first line when it comes to providing help for IPV victims. They offer documentation, links to help materials and mitigation tools. However, it is now common practice that, even non-commercial sites use web-trackers (some of which can be attributed to the

[1] `https://femicideincanada.ca/callitfemicide2020.pdf`

underlying development tools/libraries/platforms), which could pose a privacy threat to vulnerable/potential IPV victims, and may discourage them to use such sites.

We investigate, through a comprehensive and systematic experimental study, common Android applications that are currently being used by abusers as well as computer security tools/apps that can provide help to victims (referred to as "anti-stalkerware apps"). In particular:

- Design and implementation of a measurement pipeline to find and analyze technological tools (web/app stores) that can potentially be used by IPV abusers.
- Assessing the state of the stalkerware ecosystem, their capabilities and limitations.
- Identifying attack vectors on stalkerware apps that could lead to additional threats toward the victim from third party attackers, as well as the consequences such flaws could have on the victim.
- Identifying and evaluating the efficiency of counter-measure tools that the victim could use to gain leverage against the abuser and/or the installed stalkerware.
- Performing measurements of web tracking on websites that provide help for IPV victims.

Contributions and notable findings.

1) We assessed the state of the stalkerware ecosystem as of 2023, and collected information about 83 stalkerware apps. We sorted them to filter out 25 duplicate websites leading to identical APKs and then manually analyzed 58 apps to identify their capabilities. We also used keywords related to anti-stalking to collect 323 anti-stalking websites for privacy analysis.

2) We designed and implemented a pipeline to perform a security analysis of the listed stalkerware apps against five common vulnerability types. For anti-stalking websites, we used the OpenWMP [13] privacy analysis framework to measure 323 anti-stalking websites, identified various third-parties, detected session replay services, and analysed for possible privacy exposures.

3) We identified over 46 vulnerabilities that could allow external attacks to be performed, and cause additional harm to stalkerware victims.

4) We listed 24 different payment method services as well as 101 commercial trackers used by stalkerware websites. These trackers include well-known advertising services, user integration and analytic.

5) We tested the effectiveness and the requirements of 9 mitigation tools specialized in stalkerware detection against 8 chosen stalkerware apps to assess their ability to detect stalkerware apps.

6) We found that over 210/323 (65.02%) anti-stalking websites included third-party trackers. We listed 40 unique third-party hosts that gathered the web pages users browsed and the keywords in the Search functionality.

7) We detected 3 session replay services (Yandex, Hotjar and Clarity) on 19 anti-stalking websites, which apparently collect usage information, and user PII and other sensitive data (when a data submission form is available).

2 Related Work

Over the past years, a large number of studies has been conducted on the stalkerware industry [14, 15], revealing the expanding landscape of spyware apps and keeping track of emerging actors in the field [16–20]. Especially, the recent Covid-19 pandemic has significantly increased intimate partner violence [21]. In parallel, organizations helping IPV victims widened their reach with multiple emergency lines, websites and resources being provided online.

Chatterjee et al. [22] provided one of the first significant studies of the intimate partner stalking (IPS) spyware ecosystem where they identified several hundred of such IPS-relevant apps. While they found dozens of overt spyware tools, the majority are "dual-use" apps, i.e., apps that have a legitimate purpose (e.g., child safety or anti-theft), but are easily and effectively repurposed for spying on a partner. They also show how some dual-use app developers are encouraging their use in IPS via advertisements, blogs, and customer support services. The authors analyze existing anti-virus and anti-spyware tools, which mostly fail to identify dual-use apps as a threat. However, the authors did not focus on in-depth analysis of major IPS tools to understand their invasive features, how such features are implemented, and how they can remain hidden from the victim. The solutions specifically targeting IPS/IPV were also not analyzed.

With the growing exposure given to intimate partner violence exacerbated by the online presence of more and more actors in the field (stalkerware apps being distributed online, more help services being available on the internet, etc.) [2–6, 21–24], further analysis of the mechanisms used by these new tools became necessary.

Freed et al. [25] provide a qualitative study that focuses on how IPV abusers exploit technology to intimidate, monitor, impersonate, and harass their victims. The authors argue that many forms of IPV are technologically unsophisticated from the perspective of IT/security experts. For example, these attacks are often carried out by a user interface bounded adversary, i.e., an authenticated adversarial user who can interact with the victim's device or account via standard user interfaces, or by installing a readily available applications that enable remote spying on the victim. Still, such attacks are both very damaging to victims and difficult to counteract because they undermine the dominant threat models considered during the design stage of most systems (e.g., attackers not having physical device access). Thomas et al. [26] argue that security, privacy, and anti-abuse protections are failing to address the wide-spread threat of online harassment.

Our work relates to other studies of monitoring apps' technical capabilities [18, 27–29], focusing on thoroughly documenting stalkerware features, but only a handful of them highlighted their implementation/execution. They also considered 1 or 2 specific apps, and provided insight regarding the poor security state of these applications, highlighting flaws such as inconsistent encryption usage or hard-coded secrets.

More recently, Liu et al. [30] tested and investigated the features of stalkerware apps that enable non-consensual tracking of victims. They comprehensively listed the available features of 14 leading Android spyware apps and gave insightful details about their mechanisms.

Security vulnerabilities in stalkerware systems are abundant, with apps like mspy [31], TheTruthSpy [32], Cerberus [33], spyHuman [34] or Pegasus [35] leaking data of hundreds of thousands of users through data breaches. Unprotected databases are just one of many other flaws that can be found on monitoring apps and potentially exploited. ESET [10] manually analyzed 86 stalkerware applications, and reported over 18 critical vulnerabilities

that let an attacker perform actions such as remotely control the victim's device, hijack a stalker's account, capture victim's data, and upload forged data on behalf of the victim. They reported a substantial growth in the stalkerware usage in 2019 and 2020, correlated with the increase of IPV reports during the Covid-19 pandemic [21, 36].

Regarding monitoring apps detection and mitigation, notable works include comprehensive records of known stalkerware apps [10,37], often used as a baseline for spyware detection tools. Similar to traditional anti-viruses, Android spyware detectors mostly work via package name analysis, therefore requiring thorough and up-to-date spyware package databases. Fassl et al. [38] compared the users' reviews of 2 anti-stalkerware apps:Mobile Security, Antivirus & Cleaner by Lookout Mobile Security, and Anti Spy Mobile PRO (these two apps are not available on the Google Play Store anymore. New detection techniques using Android permissions [39], activity analysis with machine learning [40], or traffic examination through external hardware [41] are also emerging but are not suitable for user consumption yet because of their experimental state.

An analysis of the stalkerware monetization ecosystem has been conducted by Gibson et al. [42] on over 6000 android apps, sampled by the Stalkerware Threat List in 2021. They looked for keywords in the apps' code and evaluated the presence of payment/advertisement libraries used by the stalkerware apps. While this analysis is very comprehensive, it mainly focuses on "in-app monetization", and does not give lots of insights on the website part of the stalkerware environment.

Our research prioritized security and privacy analysis of monitoring apps and websites, while also trying to understand the extent of their capabilities. We mainly focused on vectors that could pose additional threats to the victim, especially from third party attackers. We also analyzed a larger set of mitigation tools to evaluate their efficiency. Our work features the first tracker analysis of stalkerware and anti-stalkerware websites, as well as a list of payment services available on monitoring apps' websites.

3 Methodology: Security and Privacy Analysis of Stalkerware and Anti-Stalkerware Apps

In this section, we introduce the pipeline put in place to analyse stalkerware and anti-stalkerware apps. We first describe the analysis setup and components used for its implementation, we then explain our app collection process, as well as the enumeration of their capabilities. We also provide a description of the main components of our stalkerware apps security analysis, separated into 5 distinct attack patterns, as well as our stalkerware website analysis on third-party services and web trackers. Finally, we give the methodology used to assess the performances of anti-stalkerware apps in regard to monitoring app detection.

3.1 Setup

To conduct our analysis on the target applications, we organize the testing platform as follows: a Google Pixel 3 phone running Android 12, with 2021 security update and 2022 Google play system update, and a Genymotion virtual device running Android 10, with Google API installed. The Google Pixel 3 phone is rooted to allow superuser rights in the Android Debug Bridge (ADB) shell and certificate pinning for our testing. Genymotion virtual devices are rooted by default and therefore do not need further configuration.

Our setup consists of an analysis device (workstation/laptop), on which our tools run. The victim's device is connected to the analysis device via ADB. To facilitate this connection, we enable developer options on the victim phone. Whenever possible, we downloaded the stalkerware APK directly on the device. On the computer, we used tools such as Jadx [43] to de-compile the Dalvik bytecode into Java and de-obfuscate it whenever possible, allowing for static analysis of the application's source code afterwards. In some cases, the website's download link pointed to an installer that would need to be run first. In this situation, we use ADB to get access to the application's package once fully installed and pull it from the phone through a superuser shell. Figure 1 illustrate our analysis setup and shows the different steps composing our approach.

We perform our analysis with the following objectives in mind:

1. Highlighting the most prominent and invasive features of IPV tools.
2. Identifying vulnerabilities in the stalkerware's environment that can expose the victim to a wider set of threats, beyond the abuser's.
3. Understanding how third party services allow stalkerware operations by providing tools supporting their economic model or infrastructure.

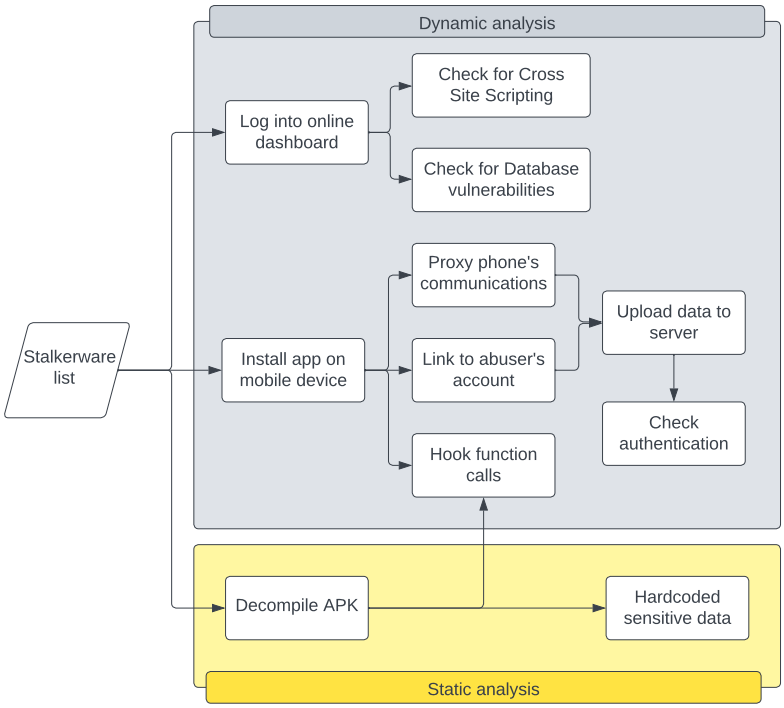

Figure 1: Overview of App analysis methodology

3.2 Stalkerware App Collection

Recently updated lists of stalkerware applications are not readily available; previous works on the topic provide multiple (non-exhaustive) lists of target apps, some of which became outdated over the years. Some stalkerware websites have been closed and are no longer distribute their apps, others have been re-opened under modified names with download links leading to the same APK. We manually tested the online availability of stalkerware apps listed in the ESET 2021 report [10] as well as AssoEchap's Stalkerware IOC list [37]. We also tried getting access to the Stalkerware Threat List (STL) established by the Coalition Against Stalkerware, which has been used in multiple other works on the topic. Unfortunately, we could not get any account for this service as their registration website seemed to be out of order. We tried contacting them about our study and our inability to register an account from their website, but received no response. We manually gathered information about 83 stalkerware apps, the availability of their online websites (14 were unreachable), their economic model (free, paid subscription, free trial) and whether the terms "spouse", "husband" or "wife", along with "spy" or "cheating" were present on the application's download source page (website or Google Play Store page). Checking the latter allowed us to separate stalkerware apps from legitimate applications that could be used in a legitimate way (we refer to such applications as "dual-use apps"). In cases when the application was only available behind a paywall, we also took note of the price required to have access to the application's features for a maximum of one month.

We found 83 applications with reachable online websites. 25 of these would redirect to the same APK download and turned out to be duplicates of other stalkerware apps. Notable examples include TheTruthSpy with 6 different websites, Cocospy with 7, and Mspy with 4. This correlates with information found on threat lists such as the Stalkerware Indicators of Compromise repository [37], with stalkerware apps like Mspy or Cocospy having more than 30 different websites on record. Out of the 86 applications found online, 49 of them were explicitly referencing spouse-ware features like the ability to "monitor cheating spouses", or "verify spouse loyalty". Three stalkerware websites showcased articles promoting such features; links to such articles are however only accessible from a browser search and are unreachable through normal website navigation. Duplicate app websites use similar ways of hiding their malicious nature, with only one of them not using the term "spouse", "wife" or "husband" anywhere on the website. Instead of spouse related messages, most websites promote features like children monitoring or employee surveillance, but showcase functionalities or reviews referring to intimate partners.

We chose to prioritize testing of free apps, and the ones offering free trials on account creation, as it is much more likely that an abuser chooses a free option rather than a paid version right from the start. We also note that very few of these apps were available on the Google Play Store, mainly because of their terms of service change in October 2020 [44], prohibiting the publication of any app that "present themselves as a spying/secret surveillance solution" fast moderation leading to quick detection and deletion of any applications offering features considered illegal.

Only one application in our list is available on the Play Store,[2] offering features such as GPS tracking and contact information gathering. It has been available since 2014 and has been downloaded over a million times. Even though it does not flag itself as a surveillance tool in the app description, the term "Spy" is used in its name. Many reviews for this app on the Google Play Store also feature the terms "spouse" and "spying", praise the efficiency

[2] `https://play.google.com/store/apps/details?id=com.phonetrackerofficial1`

of the app to secretly spy on someone, and seem to promote the app developer.

Mitigation tools dedicated to stalkerware apps are sparse, with only 2 Android apps listed on the Canadian Google Play Store explicitly referring to the term "stalker", "anti stalker" or "anti stalkerware" in their names. Searches with such keywords returns apps with more common tags like "spyware", "anti spyware" or "spyware detector". We chose 9 apps that were most likely to be chosen by a user looking for "spyware" or "stalkerware" detectors on the Google Play Store, and tested their effectiveness on 8 stalkerware apps selected based on their prevalence in web searches (6 appearing frequently, 2 less common).

3.3 Stalkerware App Capabilities

To identify potential vulnerabilities in the stalkerware environment, it is crucial to understand what kind of data these apps gather [30] and through which mechanisms. For each tested stalkerware, we gather information about the features they provide. We search on the app's website and its online dashboard for a comprehensive list of capabilities that the stalkerware can offer. We also look at the data packets sent by the phone to upload information to the backend servers through regular use. This step is the base for the rest of our analysis, as testing specific features also enable us the opportunity to understand their mechanisms and their flaws (if any).

3.4 Security Analysis

During our study, we identified and tested five common vulnerability types in the stalkerware apps ecosystem. This ecosystem includes the mobile application itself, the backend servers as well as the online dashboard used by the abuser to monitor the victim and browse the collected data. These vulnerabilities can lead to multiple other issues like victim's data leak or remote access to multiple phone functionalities by third party actors. Most of these weaknesses can be exploited by an attacker, without the need to be on the same network as the victim's device or the abuser's machine, as they can generally be conducted by sending a text message to the compromised device. Pre-requisites for such attacks include either knowing the victim's phone number or having physical access to the phone.

We perform dynamic analysis with the help of Frida [45], a dynamic code instrumentation toolkit, allowing us, among other features, to inject JavaScript code into apps during runtime. With Frida, we could hook function calls and inspect parameters dynamically. Frida's built-in tools also allow for simple native Java function hooking, as well as process listing and information gathering. Along with Frida, we use Burpsuite, an integrated platform offering multiple tools for performing security testing of web applications. The tools provided by Burpsuite include a proxy, a repeater and a decoder among others. We mostly use the first two during our work. With Burpsuite we could intercept HTTPS communications between the compromised mobile device and the stalkerware's backend servers.

In this section, we address each vulnerability separately, explaining how we verify their presence on tested stalkerware apps and discussing the potential impact it could have if exploited in real life scenarios.

3.4.1 Cross-site Scripting

After identifying what data the stalkerware gathers from the victim's phone, we check if web dashboards of the stalkerware apps lack user-input sanitization, which possibly could

lead to cross-site scripting (XSS) vulnerabilities. These vulnerabilities would allow a third party attacker to inject malicious JavaScript code into the web application through the victim's device. The payload would then be executed on the stalker's machine when browsing the dashboard, allowing the attacker to steal sensitive information such as session cookies, collected data or login credentials.

Cross-site scripting is possible when uploaded information like contact names, text messages, calendar data or any other user-input field is verified by neither the Android app nor the backend system. This allows unrestricted usage of special characters in strings, which when displayed to the abuser on the dashboard without proper validation, trick the browser into interpreting it as code. To assess the presence of XSS, we first compile a list of easy-to-edit inputs in the victim's device that are being reflected on the stalker's dashboard (most common ones are contacts and text messages). We then use XSS fuzzing payloads from a cloud based web service[3] and manually inject it into our identified inputs. We add a new contact in the device phone-book, and provide the XSS payload in the contact's name. We also send text messages containing the payload to and from the victim's phone.

Note that we just need to inject the payloads into the victim's device once. As soon as the monitoring app uploads it to the backend server, the payload will be displayed on the dashboard (when the stalker visits the dashboard), even if the compromised data is deleted from the phone afterwards. In this case, each time the abuser opens a web page containing the malicious string, the payload script will be executed.

3.4.2 Unrestricted File Upload

One of the key operations performed by stalkerware applications is to regularly upload the data from the phone, including photos, videos, and other files from the victim's phone storage to a remote server. In 38% (22) of the tested apps, a feature allows the abuser to access the device's internal storage (e.g., downloaded files, SD card storage, even system files if app is given admin rights). While this functionality does not make editing possible, the stalker can still navigate through the phone's storage and download any file they want. However, this process can present a significant security risk, as the lack of file verification during data synchronization can allow potentially dangerous files to be transferred from the phone to the backend server. This means that if a malicious file is present on the victim's phone, that file would be synced to the server and could be later downloaded by the abuser. An attacker could take advantage of this behaviour to collect information about the abuser or the victim. Using a similar method as the one used for XSS, they could send malicious files to a victim's phone and wait for it to be uploaded to the dashboard.

3.4.3 Broken Authentication and Access Control

Since the majority of monitoring apps use a centralized database platform to store victim's data, we verify whether authentication and access control are properly handled by the online platforms.

In order to test for broken authentication and access control flaws, we first create two accounts (abuser and an external attacker) on the stalkerware dashboard. We install the stalker app in the victim's phone using the abuser's credentials and browse the stalker dashboard with the same credentials. We run Auth analyzer[4] in the background while we

[3] `https://xss.report`

[4] `https://github.com/PortSwigger/auth-analyzer`

browse, by configuring it to replay requests using the external attacker's session tokens. An access control vulnerability is detected in case a replayed request (from external attacker's session) generates the same response as the browsed request (from the abuser's session). Similarly, to test for broken authentication flaws, we configure Auth analyzer to replay requests using null or blank sessions; a successful (`200 OK`) response code indicates the presence of broken authentication vulnerability.

Furthermore, we notice that JSON Web Tokens (JWTs) are being commonly used for authentication, managing user sessions, and controlling access to resources in stalkerware applications. Particularly, the signature field within JWTs ensures the server that the token has not been tampered with, and the server can then use this token to authorize the request. However, if the signature field is not properly verified, this may lead to authentication and authorization bypass. Any vulnerabilities in these areas can potentially put the victim or the abuser at risk of being compromised. In order to test for JWT related vulnerabilities, we first collect all corresponding tokens by logging into the stalker dashboard. Then we test for all signature related flaws by supplying the collected tokens to an open source tool.[5]

Another situation where authentication mechanisms could be misused is during data uploads from the phone to the backend server, as the online platform needs to identify the device and store the transferred information accordingly. To test this, we use Burpsuite's built in proxy to intercept data sent by the mobile device and check the packets sent during data upload. Without proper device authentication, an attacker could upload potentially malicious data to the backend server under the victim's identity. In addition to the lack of server-side file verification, this could lead to serious consequences for the victim as malicious, fake, or incriminating data could be forged and transmitted in their name.

3.4.4 Insecure Multi-media Storage

Online Storage. The victim's multi-media data (e.g., screenshots, images, videos, call recording audios) can be stored differently compared to text-based data (e.g., social media chats or text messages). It can be stored either on cloud (e.g., AWS), or on the stalkerware's server itself, albeit in a different directory. In both cases, we check if access to sensitive multi-media content is protected.

First, we collect and store the list of all relevant multi-media URLs in a log file. This is done by first syncing the victim's mobile data to the stalkerware's server, and then manually browsing the stalker's dashboard to identify all such URLs. We then make a cURL[6] request to each of the collected URL without providing any authentication token. A successful response (with `200 OK` status code and content body) indicates the presence of insecure storage of multi-media data. Second, we check if it is possible to guess the URLs to access the multi-media data of other victims. For example, the use of high entropy tokens (e.g., UUID) in the URL make the guessing infeasible, whereas the use of short numeric identifiers makes it possible for an adversary to quickly form and test potential URLs which may contain other victims' sensitive information. In case of high entropy tokens, we make use of the Wayback Machine[7] to find any leak of such tokens. Lastly, we repeat the process of triggering cURL requests on top of the log file, after deleting the stalker's account from the platform and uninstalling the Android app from the victim's device. This helps us to verify the retention status of the victim's multi-media data.

[5] `https://github.com/ticarpi/jwt_tool`
[6] `https://curl.se/`
[7] `https://archive.org/web/`

Local Storage. In addition to online information storage, stalkerware apps also use the phone's internal storage to cache data such as collected contact names, text messages, installed apps, keylogger history and app activity. Through static analysis of the device's internal files, it is possible to find credentials used for data uploads to the backend servers, as well as information used to link the phone to the abuser's account. This would be the easiest way for a victim to gather information about their stalker, as it can easily be performed with physical access to the phone.

Typically, accessing the content of the internal storage of applications requires root privileges on Android. However, by leveraging Android application backup functionality, the same can be done without rooting the phone. In both cases, we use ABD to pull the stalkerware's internal files. If the app had the "debug protection" parameter enabled, preventing the user from tampering with its local directory, we used the android backup functionality to fetch the application's data from the phone to our workstation. In other cases, we were able to directly pull the app directory with ADB pull, and browsed the SQLite databases with an online tool.[8]

3.4.5 Cross-Site Request Forgery

In Stalkerware applications, an external attacker can induce abusers to perform actions that they do not intend to perform (e.g., sending remote commands to victim's device, or deleting their own account). We call such an attack as a cross-site request forgery (CSRF), and an external attacker can exploit this by sending a malicious link to the abuser, and luring them to click on it.

We detect CSRF vulnerabilities in all of the state changing HTTP/S requests that are triggered upon browsing the stalkerware dashboard, as an abuser. First, we check for the presence of any random tokens (anti-csrf tokens) in the request body. Second, we check if those tokens are tied to the abuser session. Specifically, we test if the request can successfully be processed by supplying any valid anti-csrf token. To do this, we login into the external attacker's account and provide their anti-csrf token in the abuser's state changing requests. A successful execution of this request determines the presence of a CSRF vulnerability.

3.5 Third-party Services used by Stalkerware Websites

We analyze the corresponding websites of monitoring apps to identify and list all the external parties that provide support to stalkerware by offering their services. These services may include payment processing, cloud hosting, advertising, analytics, and web application firewall protection. By identifying these third-party providers, we can gain a better understanding of the infrastructure and resources that stalkerware relies on, and provide potential avenues for service providers to disrupt or shut down these services. Additionally, understanding the specific providers and services used by stalkerware can also provide valuable information for law enforcement and security professionals working against the use of these malicious apps. We manually check the payment options on stalkerware websites (with premium subscriptions available), and use the browser extension "Ghostery" to see what trackers are used.

[8] `https://inloop.github.io/sqlite-viewer/`

3.6 Anti-stalkerware Tools: Collection and Test Methodology

We conducted our analysis of solutions against stalkerware apps with two goals in mind: assessing the efficiency of stalkerware detection tools available on the Google Play Store, and evaluating their requirements. The latter includes necessary permissions, potential detection conditions and limitations.

The stalkerware set used for testing the apps is chosen in a way that would allow better understanding of the detection tools' limitations. We test free apps because of their higher likeliness of being used first by a stalker. Among the 9 chosen apps, TheTruthSpy is considered "well known" because of many technical articles citing its name during summer 2022. CatWatchful and Snoopza are considered "likely known" as their names can be found in some online articles listing "top monitoring apps". MobileSpy, OwnSpy and MeuSpy are considered as "less likely to be known". iKeyMonitor is a special case since it provides weekly builds of the app's package. The APK available on their website is recompiled every week with a different package name (com.android.internet.aXXXX, with "XXXX" denoting the built date). We used com.android.internet.a20230215, in other words, the Feb 15th 2023 build, and consider the app to be "very unlikely to be known" by package names databases. We also test one app downloaded from the Google Play Store (Spy Phone Labs Phone Tracker).

4 Results

4.1 Stalkerware App Capabilities

Most stalkerware apps use two separate systems in parallel: a monitoring app installed on the phone and a web based dashboard accessible by the abuser. This platform is linked to backend databases where the collected data can be found and also serves as a control panel through which the stalker can manage their subscriptions, enable/disable features or send remote commands to the phone.

Table 1 compiles a comprehensive list of the data collected by 58 monitoring apps for Android devices (duplicates excluded). 85% of them gather text messages and phone call logs, which, along with GPS tracking and geo-fencing (available on 87% of the apps) are the most common features. Other noteworthy functionalities include secret live recording with the device's camera (58%) or microphone (46%), a keylogger collecting keystrokes therefore potentially disclosing victim's passwords to the abuser (50%), access to file storage like photos, videos or documents (38%), and social media chat services compatibility (e.g., Facebook Messenger, Instagram, Whatsapp, Viber) found in 67% of them.

Stalkerware \ Feature	text messages	phone calls	geolocation	contacts	camera	microphone	notifications	file storage	keylogger	screen	apps	social media	web browers	wifi history	remote commands
Aispyer	★	★	★	★			★	★		★	★	★			
AllTracker	★	★	★	★	★	★	★	★	★	★		★			
Android Monitor	★	★	★			★		★		★	★	★			
AppSpy	★	★				★		★			★	★			
A-Spy	★	★	★	★	★			★	★	★		★			
CallSmsTracker	★	★	★								★				
CatWatchful	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Cerberus					★			★	★	★				★	★
ClevGuard	★	★	★	★	★	★			★	★	★	★	★	★	
Cocospy	★	★	★									★	★		
Couple Tracker	★	★	★												
Easy logger	★	★	★								★				
EvaSpy	★	★	★	★	★				★	★		★	★		★
Flexispy	★	★	★	★	★	★	★	★	★	★	★	★	★		
Fone tracker	★	★	★		★	★			★			★	★		
Free Android Spy			★	★	★										★
Highstermobile	★	★	★	★	★	★			★	★	★	★	★		★
HoverWatch	★	★	★	★	★							★			
iKeyMonitor	★	★	★	★	★		★		★	★	★		★		★
i-Monitor	★	★	★	★	★						★		★		
ispyoo	★	★	★	★	★	★						★			★
IzKid	★	★	★	★	★	★		★	★		★	★	★		★
jjSpy	★	★	★	★	★				★	★	★	★	★		
letmespy	★	★	★												★
Lost Android	★	★	★		★	★					★		★	★	★
Meuspy	★	★	★	★	★	★	★	★		★	★	★	★		★
MobileSpy	★	★	★	★				★	★		★	★	★	★	
Mobile-tracker-free	★	★	★	★	★					★	★	★	★		★
Mobistealth	★	★	★	★	★	★					★	★	★		
mSPY	★	★	★	★					★	★	★	★	★	★	★
mycellspy	★	★	★	★	★	★		★	★			★	★		
OwnSpy	★	★	★	★	★	★	★	★	★	★	★	★	★		★
Panspy	★	★	★					★	★		★	★	★	★	
Remote Audio Recorder						★									
Reptilicus	★	★	★			★		★				★			★
Shadow SPY	★	★	★	★			★	★	★		★				★
Snoopza	★	★		★	★					★		★	★		
spappmonitoring	★	★	★			★		★			★	★	★		
Spy to Mobile	★	★	★												
Spy24	★	★	★	★	★	★		★	★	★	★	★	★	★	★
SpyApp	★	★	★		★		★		★	★	★	★			
Spyera	★	★	★	★	★	★		★	★		★	★			★
Spyhuman	★	★	★	★		★		★			★	★	★		
Spyic	★	★	★					★	★		★	★	★		
Spyine	★	★	★					★	★		★	★	★		
Spylive 360	★	★	★		★	★		★			★	★	★		★
Spyphone Mobile Tracker	★	★	★										★		
TheTruthSpy	★	★	★	★	★	★	★		★		★	★	★	★	
TISPY	★	★	★	★	★			★	★	★	★	★	★		
Track My Phone	★	★	★		★										★
Track My Phone Remotely			★		★										
TrackView			★		★	★									
ttspy	★	★	★	★	★	★				★	★	★	★	★	
Umobix	★	★	★	★	★	★			★		★	★	★		★
USafe			★												
WtSpy												★			
Xnore	★	★	★	★	★	★							★		★
Xnspy	★	★	★	★		★		★		★	★	★	★	★	

Table 1: Features available on tested stalkerware apps. A star means that data is collected by the app.

After being collected by the Android app, the victim's data is sent to the abuser in two possible ways:

1) In 95% (55 out of 58) of the cases, the data is uploaded to an online database which can be browsed by the stalker through the web dashboard. The stalkerware database therefore stores all pictures, text messages, contact names and other collected information from the devices monitored by the platform.

2) When not using a centralized database system, data can be directly sent to the abuser's email address via regular reports. The apps using this approach however tend to offer less features than the ones providing a web-based control panel.

4.2 Security Vulnerabilities

4.2.1 Cross Site Scripting (XSS)

We identified 23 different apps whose online dashboard did not conduct any input validation before displaying it on the web page. Depending on where the XSS payload was planted (e.g., contact list, text message, file names), it is possible for the attacker to see related data on the displayed web page. A malicious actor would therefore be able to send an XSS payload as a text message to the victim's phone in order to have access to other messages sent or received by the device.

We found 18 apps were XSS could be performed through text message injection, by either sending or receiving a message containing a payload, among these 18 applications, 15 of them features social media compatibility and were therefore also vulnerable to XSS payload injections through these inputs. 16 apps (15 of them being in the first 18) were vulnerable through the contact list, and 11 through filenames.

XSS payloads can also be used to verify the presence of a stalkerware application on a phone. An attacker could send text messages containing a payload to random phone numbers, until a monitored phone uploads it to the app's backend servers. It should however be noted that this approach relies on the abuser logging into the online dashboard and loading the page displaying the payload. It is also possible that such an attack raises suspicion, either from the victim or the abuser. Receiving a text message containing an XSS payload could indicate to the victim that an unwanted app is targeted. Similarly, the abuser could become cautious if they notice strangely formatted messages on the dashboard. As XSS payloads are highly adjustable, if an attacker was to program the payload to send an notification when it is activated, it would allow them to hijack a session with no delay, by increasing the odds of the session cookies being still valid to the server.

4.2.2 Broken Authentication

Our analysis revealed that 8 stalkerware apps are using broken authentication mechanisms that could lead to account hijacking or unauthenticated command transmission. We found 2 applications (CatWatchful and Shadow Spy) using Google Identity Toolkit for credential verification and account management. It uses a token to identify the stalker on the victim's device and is exposed inside the shared_prefs directory, on the phone. This token can be used to issue commands to the monitored device, but also request API calls through Google Identity Toolkit (e.g. deleting abuser's account). One other app (Lost Android) uses Google Cloud Messaging to upload collected data (using Google's servers as intermediates for data upload and commands). The GCM key can be found unprotected on the victim's phone.

A button in the CatWatchful app also redirects to the abuser's online dashboard, while leaking their credentials in the redirection URL. Similarly, Reptilicus and Tispy send user credentials in the URL of the GET request on dashboard login and use the same PHP session ID cookie before and after user login.

One online dashboard (LetMeSpy) was only accessible through HTTP, therefore exposing the credentials of the abuser logging in to any interception attack. Another dashboard was providing JSON Web Tokens (JWT) vulnerable to null signature attack, allowing easy account takeover.

To authenticate the device to the backend platform during data uploads, stalkerware apps can use multiple identifiers, including a license number entered by the abuser, the phone's IMEI number, a fixed session ID or the stalker's credentials. Data uploads from the mobile device are also poorly secured in 4 separate apps, allowing replay attacks on packets sending information about the phone, installed apps, contacts, messages or GPS location. Authentication of the device is made with the license entered by the abuser and a session ID that seems to stay unchanged even after multiple data uploads.

We also found no stalkerware using certificate pinning, allowing for easy interception of the packets during data upload with only a few configuration steps on the phone. This means that anyone having access to the compromised mobile device could potentially collect the credentials used to authenticate the device to the online dashboard with a proxy.

4.2.3 Insecure Data storage

We identified issues regarding unauthorized data acquisition in 6 tested stalkerware apps. 3 of them displayed unrestricted file access control after access to data such as a picture was requested by the abuser on the online dashboard. Upon asking the backend server for a file, a static URL would be generated, allowing access to the file to anyone, regardless of authentication. However, the generated links had limited period of validity.

This vulnerability was mostly tested with pictures uploaded from the phone to the stalkerware's backend server and then requested from the dashboard. However, as it is a flaw inherent to the backend database configuration, all other data that can be given an URL on request from the dashboard could potentially be accessed by an unauthorized person. For pictures, generated URLs are made up from a mobile device's identifier along either the timestamp at which the picture was taken or uploaded, or seemingly random tokens.

Even though these flaws are of little use to the victim, stalkerware apps can also keep sensitive data about the abuser on the mobile device itself. 4 different phone apps store information in easily accessible locations on the mobile device, such as shared preferences. Data such as the abuser's email address, the stalkerware registration license, the application unlocking PIN code, even the abuser's password can be found in the internal files. Even though some cases require the phone to be rooted, these pieces of information can be used to identify the abuser or execute commands that would be reserved for the stalker.

Two apps provide functionalities to uninstall the stalkerware application from the phone, either remotely of from the phone itself. These ways of deleting the app differ from manually removing it from the phone's settings, as mechanisms are used to prevent access to such features (automatically redirecting the user to another legitimate app's settings when trying to access the stalkerware settings. These functionalities require authentication to be used (made insecure by storing the corresponding password/verification token on the phone).

In three stalkerware apps, we also found SQL databases containing a summary of all gathered data, as well as credentials like the abuser's email address and password or the

device's identifier to the backend server. We also identified 7 websites which use Google Firebase as their online database service, 3 of which have unsafe configurations leading to partial or complete leakage of the database information.

4.2.4 Unrestricted File Upload

During our analysis, we have not found a stalkerware conducting any kind of file verification when requesting files from the dashboard. This means that sending malicious files to the backend servers for them to be downloaded by the abuser is easily doable. Any one knowing the victim's phone number could send a malicious file (e.g., via a text message). The stalkerware will then automatically upload it to the online dashboard for it to be downloadable by the abuser.

The protection provided by the abuser's system is the only variable that could influence the gravity of such a vulnerability. Combined with data transfer presenting broken authentication mechanisms, an attacker could send files containing malicious code to the dashboard without having to download it on the phone. Someone could also send the payload directly to a victim unaware that they are being monitored, as the file only needs to stay on the phone for a relatively short amount of time (depending on the settings) in order for it to be uploaded to the stalkerware's backend server.

4.2.5 Cross-site Request Forgery

Five applications were found vulnerable to cross-site request forgery (CSRF) attacks. The change password functionalities in LetMeSpy and WTSpy are vulnerable to CRSF, making it possible for an attacker to take over the stalker's account. In Spapp Monitoring and Panspy, an attacker could change the email address of the notifications to receive all information in place of the stalker. In Spapp Monitoring, CSRF can also be abused to delete the stalker's account. In the case of Flexispy, CSRF can be exploited to add arbitrary alerts to the stalker's account, potentially flooding the dashboard.

4.3 Third-party Services

4.3.1 Payment Platforms

There are two main economic models that we identified for stalkerware applications : offering premium subscriptions allowing access to high-end features or display advertisement on the website and online dashboard. Alternatively, it is also possible for some website to allow third-party trackers for data collection. It is also not rare to find both on some websites.

We identified 46 stalkerware apps that are either completely free to use, or that feature a free version with limited functionalities, but no time restriction. 36 stalkerware apps were only offering a premium subscription, with 14 of them giving a variable free trial period of 1 to 7 days. Paid subscriptions could be done through monthly, seasonal or annual payments. All payments can be made with VISA or Mastercard but other means are available depending on the website (Discover, GiroPay, JCB, American Express, Diners Club International). Our analysis revealed that 34 apps are accepting payment through Paypal and 16 were compatible with crypto-currencies payments. See Figure 2 or Table 2 for a list of all services we found in the stalkerware ecosystem.

Even though companies like Paypal provide responsive answers to websites reports and can quickly disable their services for these hosts, it is also very easy to ask for Paypal

integration under a different company name, which is very common among stalkerware apps. Similarly, Google ads can be hard to restrict on websites as automatic verification is difficult, and illegality can be hard to prove as it differs from country to country.

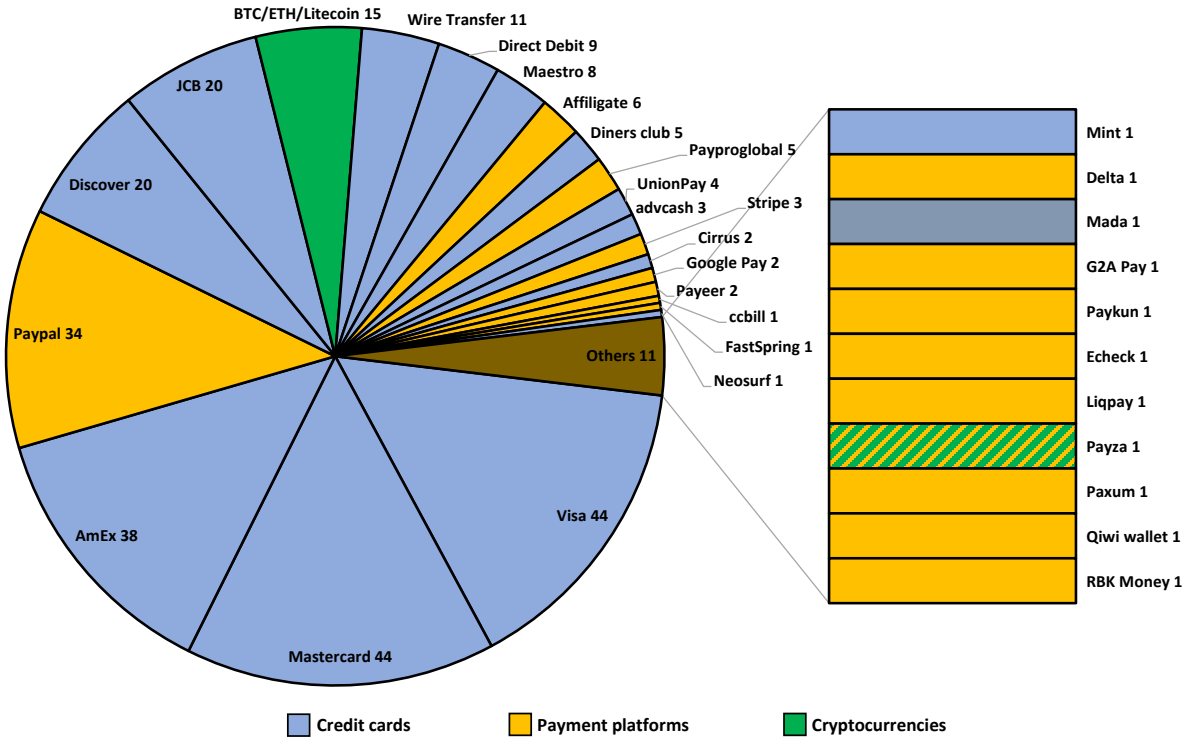

Figure 2: Payment methods used on stalkerware websites

4.3.2 Web trackers and hosting platforms

Figure 3 and Table 3 lists trackers found across 59 monitoring apps websites. The majority of these concern advertising, with over 20 websites using Google Adsense. Other trackers are related to user interaction with services like Tawk and Crisp, usually being used to collect information about users buying products or browsing through the webpage. Analytics are handled in great majority by Google Analytics trackers, that are found in 13% (8) of the websites. Cloudflare trackers were used on 2 websites using their hosting service in parallel, and Youtube trackers were present when video integration was used on the website.

Among the 58 analysed apps and related websites, we identified five stalkerware websites using Google Firebase as their backend database. One particular app (CatWatchful) was found to be hosted on FastlyCDN. Five other websites were found using Cloudflare's services, and one using HuaweiCloud.

Payment Method	**#Sites**
Visa	44
Mastercard	44
AmEx	38
Paypal	34
Discover	20
JCB	20
BTC/ETH/Litecoin	15
Wire Transfer	11
Direct Debit	9
Maestro	8
Affiligate	6
Diners club	5
Payproglobal	5
UnionPay	4
advcash	3
Stripe	3
Cirrus	2
Google Pay	2
Payeer	2
ccbill	1
FastSpring	1
Neosurf	1
Mint	1
Delta	1
Mada	1
G2A Pay	1
Paykun	1
Echeck	1
Liqpay	1
Payza	1
Paxum	1
Qiwi wallet	1
RBK Money	1

Table 2: Payment methods used on stalkerware websites

Category	**Tracker**	**#Sites**
Essential	Google Tag Manager	28
Advertising	Google Adsense	21
	DoubleClick	9
	Facebook	6
	Post Affiliate Pro	2
	Digital Window	1
	Yandex	1
	Bitrix24	1
User interaction	Tawk	4
	Crisp	4
	Zopim	3
	Livechat	1
	Zendesk	1
	Jivosite	1
	Push Engage	1
Analytics	Google Analytics	8
	Segment	1
	Mixpanel	1
	Sentry	1
	Jetpack	1
Others	Youtube	3
	Cloudflare	2

Table 3: Trackers found on stalkerware websites

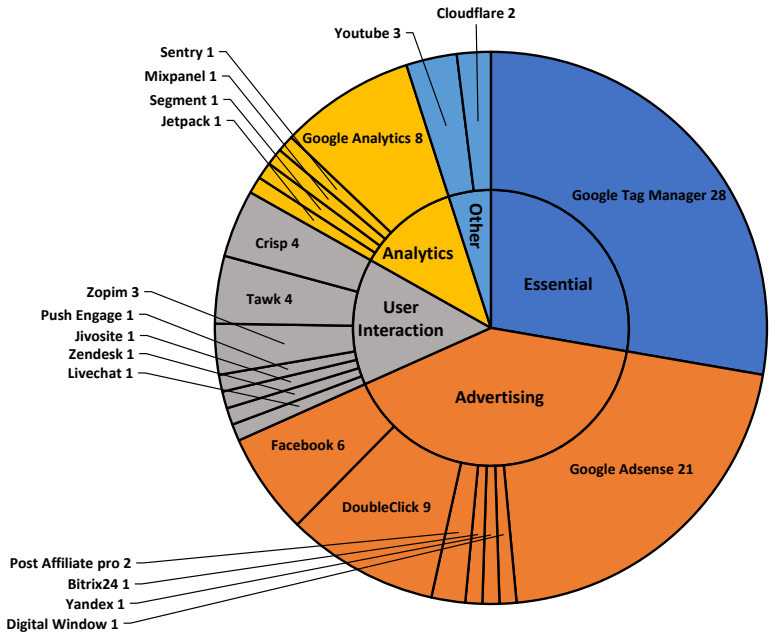

Figure 3: Trackers found on stalkerware websites

4.4 Mitigation Tools

Table 4 displays the specific results of each anti-stalkerware when tested against 8 different monitoring apps. Overall, "well known" and "Likely known" stalkerware apps were detected, with TheTruthSpy being found by 7 out of the 9 mitigation tools and CatWatchful by 6 out of 9. The weekly build of iKeyMonitor was never flagged as a malware, but apps from Malloc Privacy flagged all apps not downloaded from the Play Store. 2 tools (Malloc Privacy and Incognito Security Solutions) reported apps with risky permissions enabled, but needed the stalkerware to be entirely configured to flag it if it package name was unknown.

Two apps (Malloc Privacy and Foxbyte Code Inc.) gave different results before and after stalkerware configuration was done (giving permissions, etc). One app (World Globle Apps) claimed to use an "active" detection method, recording camera, microphone (and requested access to all three of these features) and location usage and alerting the user if any of them was used by another app. However none of these features flagged any stalkerware, even after multiple hours of phone usage. Regarding permissions asked by other anti-stalkerware apps, 4 asked for a total filesystem access (internal+external), 2 of them asked for internal storage access. Notifications, Usage access and package permissions were all requested once respectively. All permissions requested by tested mitigation tools are listed in Table 5.

The ease of use of each apps should also be noted. For example, Malloc Privacy flagged most apps as "not in Play Store" or having "critical permissions" but not as "spyware", it also only allows for one scan before requesting a premium subscription.

Package name	Version	Spy phone Labs Phone Tracker	Mobilespy	TheTruthSpy	Snoopza	own-Spy	CatWatchful	iKeyMonitor (weekly build)	MeuSpy
com.mallocprivacy.antistalkerfree	2.49	⊘	⊙	●	⊙	⊙	●		⊙
com.foxbytecode.spywarescanner	1.0.3	○		○	○	○	○		○
com.arcane.incognito	3.0.0.15		●	●	⊘	⊘	●		
com.protectstar.antispy.android	5.0.3	●		●	○	●	●		
com.cbinnovations.antispy	2.0.1	●		○	○	●	○		
com.protectstar.antivirus	1.2.5	●		●	○	●	●		
com.certo.android	2.1.2			○					
com.owneffect.spyware.detector	1.0.4								
com.world.globle.mobileantistalker.rs	1.4								

Table 4: Anti-stalkerware apps detection results. ●: flagged as stalkerware. ○: flagged as malware. ⊘: flagged because of critical permissions detected. ⊙: flagged because the app was not from the Play Store, and because of critical permissions. Empty: not flagged

Package name	Required permissions
com.mallocprivacy.antistalkerfree	Usage access
com.foxbytecode.spywarescanner	None
com.arcane.incognito	Storage access, notifications
com.protectstar.antispy.Android	All files access
com.cbinnovations.antispy	All files access
com.protectstar.antivirus	Storage access
com.certo.Android	All files access
com.owneffect.spyware.detector	Package query permissions
com.world.globle.mobileantistalker.rs	Camera, microphone, location

Table 5: List of analyzed anti-stalkerware apps' required permissions.

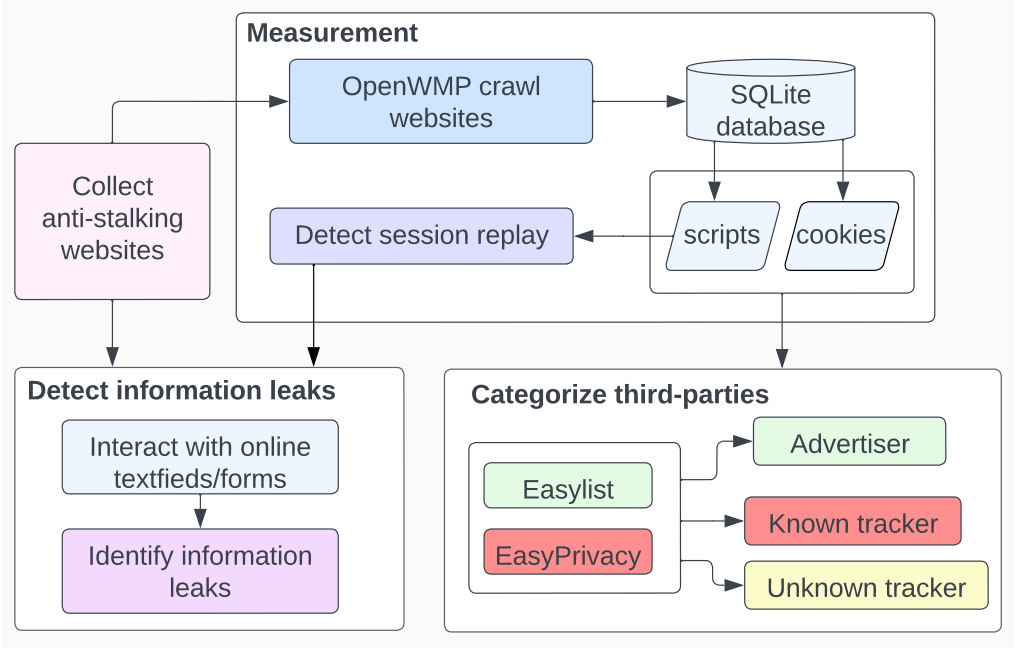

Figure 4: Privacy analysis methodology of anti-stalking websites

5 Privacy Analysis of Anti-stalking Websites

In this section, we detail our methodology for anti-stalking website collection, privacy analysis and measurement techniques for the collected websites. The privacy analysis methodology of anti-stalking websites comprises three key components. We collected the URLs of anti-stalking websites; then employed OpenWPM [13] to crawl the websites which save crawled information in a SQLite database; thereafter, we applied Easylist [46] to category third-party scripts/cookies and check whether there are session replay services on the websites or not; we engaged with online forms on those websites to identify leaks of users' sensitive information; see Figure 4.

5.1 Collecting Anti-stalking Websites

We start with the anti-stalking websites mentioned in the stopstalkerware [47] website which included 25 anti-stalking websites in the United States, United Kingdom, Germany, Australia, Italy, France, etc. Then we extended our anti-stalking website collection by searching for keywords, like, "anti-stalking", "stalking victims", "stalking support" and "stalking help". In total, we collected 77 anti-stalking websites in Canada and 246 websites outside of Canada; see Table 6. Note that the collected websites can be either dedicated to anti-stalking or related to anti-stalking, so they can be any websites that provide support or advice to victims, e.g., anti-stalking websites, government websites, university websites, websites for legal help, websites offering shelters to victims, non-profit organizations, etc. For websites in China, if we search keywords related to anti-stalking, domestic violence in Google or Baidu browser, most of the search results tend to be news reports rather than websites or

resources directly related to the topic. Generally, the Women Association websites provide the guide on violence against women and children, their primary role is to protect women and children. Therefore, we chose Women Association websites (e.g., www.bjwomen.gov.cn, hnflw.gov.cn, www.sxwomen.org.cn, www.womenvoice.cn) as our dataset in China. In total, we collected 108 Women Association websites along with 12 online legal support websites.

Country	**#Sites**
China	120
Canada	77
USA	34
EU	22
HK	14
UK	13
South America	12
Australia	7
Others	24

Table 6: Distribution of anti-stalking websites across countries

5.2 Privacy Measurements

Setup. We configured OpenWMP [13] web privacy measurement framework with 10 parallel browser instances in headless mode. We explicitly enabled OpenWPM instrumentations for HTTP requests, Javascript, cookies, DNS requests, callbacks and page navigations. We used a physical machine running Ubuntu 22.04 LTS, 48GB RAM, 500TB SSD, Intel Core i7-10700 CPU for our measurements in Feb. 2023. A total of 323 anti-stalking websites were crawled using OpenWPM from a city in North America. We saved the crawling result in a SQLite database for further analysis. The saved information in the database contains both stateful (i.e., scripts/cookies), and stateless forms of tracking metrics. We then examined the saved tracking scripts/cookies for third-party domains, i.e., domains of scripts/cookies that do not match the domain of the websites that they are on.

Categorize third-party scripts and cookies. We define a third-party entity as a domain from which scripts/cookies are included on a first-party website (i.e., anti-stalking website); i.e., all domains except the anti-stalking website domain. We use filtering rules [46] that block third-parties to identify three categories of third-party domains: EasyList rules block ad-related third-parties; EasyPrivacy block known trackers; third-parties that are not blocked by EasyList/EasyPrivacy are treated as unknown trackers.

Information leakage. To understand private information leakage, we manually browsed those websites, and tried functionalities such as registration/login, filing out forms, contact-us, and search. We tested 105unique URLs for Canadian websites and 220unique URLs for websites outside out Canada.

5.3 Results of Anti-stalking Websites in Canada

5.3.1 Third-party Tracking Javascript/Cookies

We found that 57/77 (74.03%) of anti-stalking websites in Canada included at least one known third-party tracking script; 20/77 (25.97%) anti-stalking websites had third-party

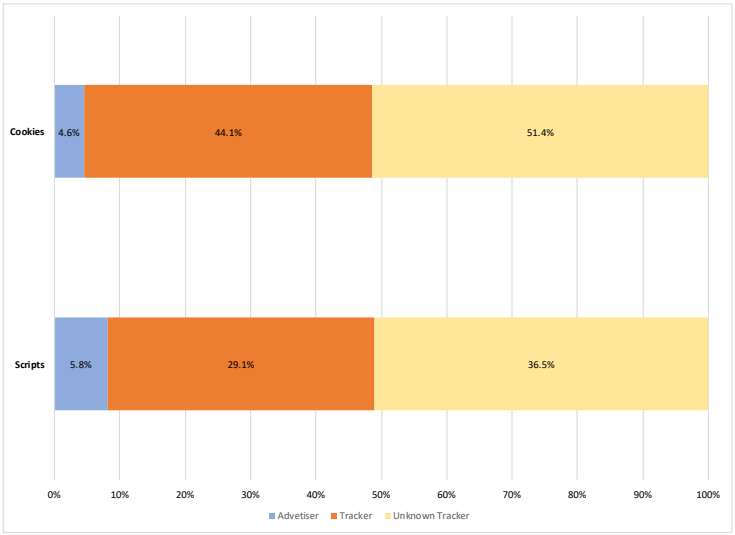

Figure 5: Proportions of third-party scripts/cookies in different categories (tracking, advertising, and unknown) included on anti-stalking websites in Canada.

tracking cookies. To better understand third-party scripts/cookies, we grouped them into the following three categories. We found that 288/499 (57.72%) third-party scripts were identified as known trackers; 29/499 (5.81%) third-party scripts were flagged as advertising; 182/499 (36.47%) were not recognized by Easylist [46], we labelled them as unknown trackers. Similarly, we found that 145/329 (44.07%) third-party cookies were categorized as known trackers; 15/329 (4.56%) third-party cookies identified as advertising; 169/329 (51.37%) were unknown trackers; see Figure 5.

The top-10 third-party tracking scripts included on the anti-stalking websites were: googlemanager.com (46/77, 59.74%), google-analytics.com (51/77, 66.23%); facebook.net (18/77, 23.38%); addthis.com(6/77, 7.79%); hotjar (4/77, 5.19%); sharethis.com (7/77, 9.09%); see Figure 6. Top known tracking cookies on anti-stalking websites were addthis.com included in 6 out of 77 websites; clarity.ms is Microsoft's session replay service [48] contained in 4 out of 77 websites; see Figure 7.

Third-party hosts tracking users' operations. We also listed some third-party hosts that tracked web pages victims browsed and the keywords users searched if the websites have the Search functionality; see Table 7. There were 6 hosts belonging to Google, www.google-analytics.com, www.google.ca, analytics.google.com, www.googleadservices.com, adservice.google.com, and ssl.google-analytics.com; 2 hosts are owned by Twitter; and 1 Chinese host (analytics.tiktok.com).

Online chat tracking. Diamondlaw.ca is a law firm with physical offices in BC, Ontario and Alberta, which offers legal services related to stalking. The website employed chat-api.intaker.com for customer online chat service. However, we noticed that the customer online chat service tracked all the web pages that victims visited when they browsed the

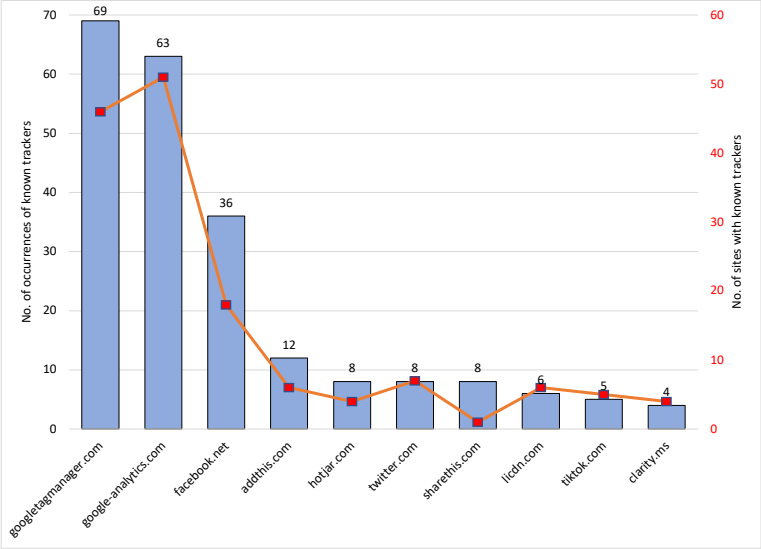

Figure 6: Top-10 known tracking scripts on Canadian anti-stalking sites - the bars show the number of occurrences of known tracking scripts (vertical axis to the left), while the line chart shows the number of anti-stalking websites with known tracking scripts.

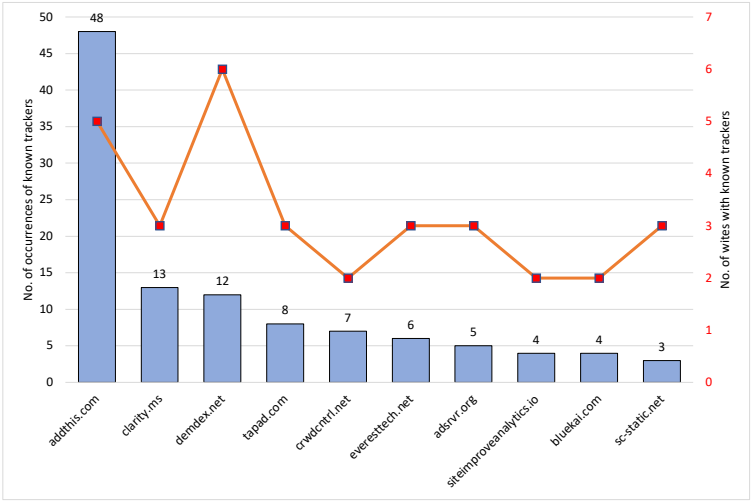

Figure 7: Top-10 known tracking cookies on Canadian anti-stalking sites - the bars show the number of occurrences of known tracking cookies (vertical axis to the left), while the line chart shows the number of anti-stalking websites with known tracking cookies.

Third-party Host	#Tracked Sites
www.google-analytics.com	53
www.google.ca	25
www.facebook.com	19
googleads.g.doubleclick.net	16
analytics.google.com	13
www.googleadservices.com	12
www.youtube.com	10
px.ads.linkedin.com	7
syndication.twitter.com	6
m.addthis.com	6
analytics.twitter.com	5
analytics.tiktok.com	5
adservice.google.com	4
bam.nr-data.net	4
ssl.google-analytics.com	3
global.siteimproveanalytics.io	2
dc.services.visualstudio.com	2
bat.bing.com	2
ct.pinterest.com	2
track.hubspot.com	2
t.sharethis.com	1
l.sharethis.com	1
live.clive.cloud	1
fndrsp.net	1
ec.editmysite.com	1
insight.adsrvr.org	1
pixel.wp.com	1

Table 7: Third-party hosts tracking users' operations in Canadian anti-stalking websites

website.

Expiration of tracking cookies. We examined the cookie validity duration, and found that 6/329 (1.82%) known tracking cookies set on anti-stalking websites, were valid for more than 1000 years, e.g., clarity.ms (3) and everesttech.net (3). Known tracking cookies that expire between 1 year and 5 years were addthis.com (45) and clarity.ms (3); see Table 8.

5.3.2 Session Replay

Session replay services are used to replay a visitor's session on the browser, to get a deeper understanding of a user's browsing experience; information replayed include user interactions on a website such as typed inputs, mouse movements, clicks, page visits, tapping and scrolling events. During this process, users' sensitive information can be exposed to third-party servers that host session replay scripts. We identified 2 session replay services in the analyzed 77 anti-stalking websites in Canada: Clarity on 4 websites (diamondlaw.ca, calgarydefence.com, ualberta.ca, torontomu.ca), Hotjar on 4 websites (lawrato.com, i-sight.com, canadianwomen.org, domesticshelters.org, etc). However, we did not observe users' private information was sent to these session replay servers; see Table 9.

		Cookie Expiry Duration			
Tracker	**#Sites**	**<1m**	**1m-1y**	**1y-5y**	**>1000y**
addthis.com	48	-	3	45	-
clarity.ms	13	4	3	3	3
demdex.net	12	-	12	-	-
tapad.com	8	-	8	-	-
crwdcntrl.net	7	-	7	-	-
everesttech.net	6	-	3	-	3
adsrvr.org	5	-	5	-	-
siteimproveanalytics.io	4	4	-	-	-
bluekai.com	4	-	4	-	-
sc-static.net	3	3	-	-	-

Table 8: The top-10 known tracking cookies and their expiry periods (m=month, y=year).

SRS	**Websites with SRS**
Clarity	diamondlaw.ca, calgarydefence.com, ualberta.ca,lawcentralalberta.ca
Hotjar	lawrato.com, canadianwomen.org, domesticshelters.org, i-sight.com

Table 9: Session replay services on anti-stalking websites in Canada. SRS: Session replay service

5.3.3 HTTP Plaintext Traffic

We observed that three websites used the plaintext HTTP protocol for the whole websites or core functions. For example, www.alberta.ca is the Alberta government website which provides family violence support (www.alberta.ca/family-violence-find-supports.aspx). Users are required to fill in their email, first name, last name, country, region, postcode, gender, age group to register an account for an online chat server. However, we observed the chat registration provided by a third-party domain (m2.icarol.com), utilized HTTP, exposing all information provided by the victims seeking help. The websites connectnetwork.ca and www.tandemlaw.ca used HTTP protocol as well.

5.3.4 Use Third-party Service for Core Functionality

We noticed that three websites in Canada, canadianlabour.ca, iheartmob.org and www.kruselaw.ca were using a third-party service for the sign-up functionality, which led to victims' sensitive information sent to the third-party domain, instead of the website's domain. Consequently, victims' private information, such as first name, last name, email, phone, message, city, country and the flag of subscription filled at canadianlabour.ca, was sent to actionnetwork.org; first name, last name, email and country of victims were sent to actionnetwork.org when victims asked for support in iheartmob.org.

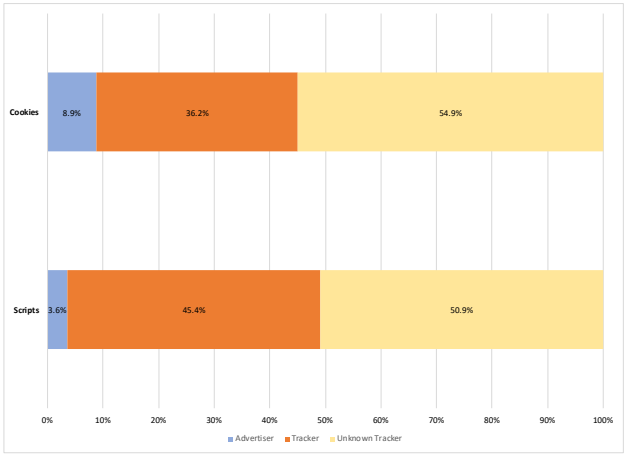

Figure 8: Proportions of third-party scripts/cookies in different categories (tracking, advertising, and unknown) included on anti-stalking websites.

5.4 Results of Anti-stalking Websites in Other Countries

5.4.1 Third-party Tracking Javascript/Cookies

We found that 115/246 (46.75%) websites included third-party known tracking scripts; in contrast, merely 13/246 (5.28%) websites were identified with third-party known tracking cookies. The proportion of websites with third-party tracking cookies is much lower than websites with third-party tracking scripts. One possible reason is that EasyPrivacy list does not include rules for Chinese websites.

We found that 337/742 (45.42%) third-party scripts were used for tracking, merely 27/742 (3.64%) third-party scripts were for advertising, 378/742 (50.94%) cannot be identified by Easylist, we treated them as unknown trackers. Similarly, there were 143/395 (36.20%) tracking cookies on the anti-stalking websites, 35/395 (8.86%) third-party cookies were advertisers, 217/395 (54.94%) were unknown trackers; see Figure 8. We listed the top-10 domains of tracking scripts and tracking cookies. We can see that the top tracking scripts were from Google (googlemanager, google-analytics), Facebook and Baidu. We only observed Baidu tracked Chinese websites; see 9. Top tracking cookies were addthis.com, sharethis.com, and rlcdn.com, all of which were included less than seven websites. Addthis is used for a free social bookmarking service integrated in websites, making sharing content across social web. Sharethis collects data on user behavior advertising and analytics; see Figure 10.

We listed 36 third-party hosts included on anti-stalking websites that tracked web pages that users browsed; see Figure 10. The hosts also collected users input in the Search text field if the websites have Search functionality. Hm.baidu.com only tracked websites in China. A Tiktok host, i.e., analytics.tikto.com was found to be included in a South Africa website (legalwise.co.za).

Online chat tracking. The websites lawyersuae.com and dubaipolice.gov.ae had online

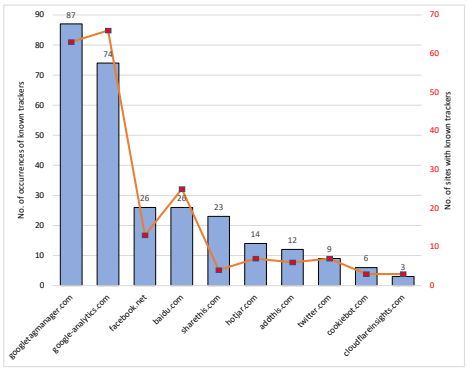

Figure 9: Top-10 known tracking scripts on anti-stalking sites - the bars show the number of occurrences of known tracking scripts (vertical axis to the left), while the line chart shows the number of anti-stalking websites with known tracking scripts.

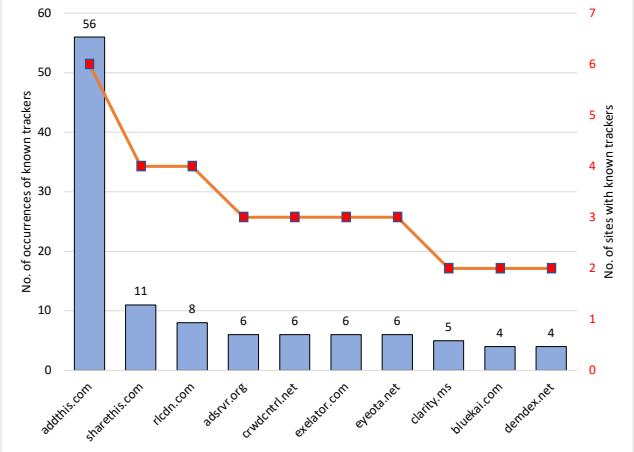

Figure 10: Top-10 known tracking cookies on anti-stalking sites - the bars show the number of occurrences of known tracking cookies (vertical axis to the left), while the line chart shows the number of anti-stalking websites with known tracking cookies.

Third-party Host	#Sites
www.google-analytics.com	79
www.google.ca	29
googleads.g.doubleclick.net	27
hm.baidu.com	25
www.facebook.com	19
www.googleadservices.com	15
www.youtube.com	13
syndication.twitter.com	7
m.addthis.com	6
px.ads.linkedin.com	5
analytics.google.com	4
l.sharethis.com	4
bam.nr-data.net	4
l.sharethis.com	4
ssl.google-analytics.com	3
adservice.google.com	3
t.sharethis.com	3
api.livechatinc.com	3
track.hubspot.com	3
analytics.twitter.com	2
fndrsp.net	2
d.adroll.com	2
brain.foresee.com	1
hexagon-analytics.com	1
plausible.io	1
dc.services.visualstudio.com	1
events.api.secureserver.net	1
bat.bing.com	1
cms.piwik.pro	1
10037187.fls.doubleclick.net	1
ec.editmysite.com	1
r4kfygnqdf-1.algolianet.com	1
p.leads5050.com	1
secure.gaug.es	1
analytics.tiktok.com	1
sp0.baidu.com	1

Table 10: Third-party hosts tracking users' operations

chat service which tracked every web pages victims browsed. Lawyersuae.com used gateway.botstar.com for online chat while dubaipolice.gov.ae used api.livechatinc.com.

Information leaks through tracking. We found that two Chinese websites for online legal support user.maxlaw.cn and www.66law.cn leaked users' information to hm.baidu.com. The two websites claimed that users do not need to worry about the information they provide, because all the data is encrypted, so they can provide as much detailed information as possible for online legal support. Although users' sensitive data is encrypted, it is sent to hm.baidu.com without users' consent. However, all the information filled by users was collected by hm.baidu.com. Interestingly, hm.baidu.com used hm.baidu.com/hm.gif when tracking users, as if it was only sending a picture, but in fact, it was collecting users' sensitive information. The script from s.canddi.io tracked the functionalities of subscription and contact in the website www.suzylamplugh.org; as a result, victims' first name, last name, email, subject and message were disclosed to s.canddi.io. The website www.workspacesrespond.org provides help to victims of domestic and sexual violence in the USA. All the private information filled in the contact web page (e.g., first name, last name, email, organization, subject, message) was sent to the workspacesrespond server as well as to another non-profit organization (go.futurewithoutviolence.org), apparently another anti-violence organization; however, this information sharing is not visible to users.

Expiration of third-party tracking cookies. We also examined the cookie validity duration, and found that 1/395 (0.25%) known tracking cookies set on anti-stalking websites, were valid for more than 1000 years, e.g., clarity.ms (1). Known tracking cookies that expire between 1 year and 5 years were addthis.com (42), sharethis.com (8), and adsrvr.org (6); see Table 11.

		Cookie Expiry Duration			
Tracker	**#Sites**	**<1m**	**1m-1y**	**1y-5y**	**>1000y**
addthis.com	56	-	5	51	-
sharethis.com	11	3	-	8	-
rlcdn.com	8	-	4	4	-
adsrvr.org	6	-	-	6	-
crwdcntrl.net	6	-	6	-	-
exelator.com	6	-	6	-	-
eyeota.net	6	3	-	3	-
clarity.ms	5	2	1	1	1
bluekai.com	4	-	-	4	-
demdex.net	4	-	4	-	-

Table 11: The top-10 known tracking cookies and their expiry periods (m=month, y=year).

5.4.2 Session Replay

We found that 2 anti-stalking websites in Russia exposed victims' information to Yandex [49] session replay servers. One of the websites is wcons.net (i.e., the Consortium of Women's Non-Governmental Associations website), which provides legal support for victims of domestic violence in Russia. Victims were asked to fill an online form for support; all the victims' sensitive information in the form was sent to Yandex, including, name, email, telephone, year of birth, address (country, city, region), the presence of minor children, reasons

to contact, who inflicts violence as well as message (to describe more information). The other website, i.e., nasiliu.net provides legal assistance, psychological help and support to victims. We noticed that when victims searched something on the website, the searched keywords was collected by Yandex; when users donated money to the website, users' name and email were leaked to Yandex. Note that safehorizon.org included two session replay services: Hotjar and Clarity. Clarity initialized scripts from www.clarity.ms/eus-sc/s/0.7.2/clarity.js to track users' interactions with the DOM elements on a web page and the collected data was uploaded to o.clarity.ms. Hotjar used web socket to transfer the collected data to ws4.hotjar.com. We observed that the two session replay services collected the elements and web pages that users interacted with, in addition to mouse events. See Table 12.

SRS	**Websites with SRS**	**Country**
Yandex	wcons.net, nasiliu.net, nasiliu.net	RU(2)
Hotjar	mysupportspace.org.uk,getsafeonline.org, safehorizon.org,legalwise.co.za,lawrato.com member.psychologytoday.com, Onlineharassmentfieldmanual.pen.org	ZA(1), UK(2), USA(3), IN(1)
Clarity	legaladviceme.com getsafeonline.org	UAE(1), USA(1)

Table 12: Session replay services on anti-stalking websites. SRS: Session replay service

5.4.3 HTTP Plaintext Traffic

The online chat service (www.chat.dfwac.ae/Customer/Start) for the Dubai Foundation for Women and Children (DFWAC) used the HTTP protocol. Victims were required to enter name, email and questions before sending a chat request. Victims sensitive information (e.g., name, email, questions, and chat content) was leaked via HTTP. We found that 72/120 (60.00%) of websites in China only supported HTTP protocol.

5.4.4 Use Third-party Service for Core Functionality

We observed that there were two websites in the USA using a third-party service for the sign-up functionality. Safehorizon.org utilized go.pardot.com for sign-up. Consequently, first name, last name and email were sent to third-party servers.

6 Recommendations

In this section we provide some recommendations that can help IPV victims avoid stalkerware apps from being installed on their devices and/or detect the ones that could have been installed without their consent. We also add some suggestions for various web/payment service providers that can be abused to operate the stalkerware ecosystem. Finally, we also add recommendations for IPV help website maintainers and Android OS developers.

- Keep your phone up close and under surveillance at all times to prevent any unwanted person from accessing it and potentially installing malicious apps. Stay aware whenever someone else could have potentially used your phone, even with your consent. Use

strong passwords or PIN codes and avoid sharing them with other people to prevent unwanted use.

- Watch out for potential indicators of compromise, including: abnormal (increased) battery consumption, unexpected pop-ups, performance drops, suspicious app duplicates or with blatantly important name ("Wi-Fi", "Sync manager", a second "Settings" apps), green dot icon at the top of the screen (indicating that the phone is recording), and any other strange behaviour from the phone. If you observe any such behaviors, seek help from a qualified organization or professional.

- A common denominator to all stalkerware apps is that they require Google Play Protect[9] to be disabled in order to stay undetected. Regularly check that the Protect feature of Google Play is active. If disabled, this would indicate that someone have tampered with the phone. This feature can also be used to easily detect apps that were not downloaded from the Play Store.

- Keep the phone updated to its latest version, as many stalkerware apps are not updated regularly and could lose compatibility with newer system versions. Using dedicated anti-stalkerware tool could also help verify the presence of a malicious app, but keep in mind that apps installation can be monitored by the stalkerware itself, meaning that the stalker could be notified that the victim is suspicious.

- Another possible scenario (although one that we have not encountered during our analysis), would be the stalker sending a malicious link to the victim, tricking them into installing a malicious app without knowing that it is a stalkerware app. Always be cautious of links leading to app downloads, especially from unknown sources. Monitoring apps are often disguised as legitimate apps, and can be downloaded from outside the Play Store. Always verify the legitimacy of the source they download apps from.

It is also important to keep potential victims educated about the existence of stalkerware apps, and how to protect themselves against such tools. Awareness campaigns can be conducted through social medias, school programs or community events to teach users how to prevent, avoid or detect early signs of stalking.

Fighting against stalkerware websites can also lower the amount of monitoring apps in circulation. Advertisement platforms such as Google Ads should establish clear policies or blacklists to detect and block advertisements on stalkerware websites, as well as content promoting such applications. Similarly, domain providers, payment services, and web hosting platforms have proven to effectively prevent access to malicious websites when reported.

Anti-stalkerware websites, where victims go for seeking help in their vulnerable times, should avoid any use of third-party trackers and services. Such use can unfortunately help unwanted parties to track victims on other services, collect sensitive information (PII, and details of a victim's situation e.g., by session replay services), or even monetize their situation. The use of ads, and third-party code libraries (regularly used to reduce development burdens) should be restricted on these very sensitive websites.

Operating systems, such as Android OS can also play a role in various ways. For example, enforcing PIN/unlock requirement for sensitive configuration updates (e.g., disabling Play Protect), warning users periodically that such changes have been made (e.g., once a day), and disabling blatant and constant information collecting apps such as stalkerware (almost no legitimate apps would behave the same way).

[9] `https://support.google.com/googleplay/answer/2812853?hl=en`

7 Conclusion

We provided a systematic experimental privacy and security analysis of currently available stalkerware apps. Vectors through which vulnerabilities found in stalkerware apps could be exploited by malicious actors, targeting the IPV services, IPV abusers, and IPV victims, are also studied. We also examined the effectiveness of anti-stalkerware applications to assess their ability to detect monitoring apps on Android devices. Measurements of web tracking on websites that provide help for IPV victims are also performed, along with exploration of features provided by online services that are used by IPV app providers.

We identified 83 stalkerware apps and websites, out of which 2 can be found on the Google Play Store, and 81 are available outside of regular app markets. Many invasive capabilities offered by these apps were enumerated and experimentally verified to clearly identify the severe privacy risks posed by them. Additionally, well-known third-party web services that also help supporting the IPV ecosystem were identified. We also found 29 apps/services are vulnerable to various exploitable attacks, including broken authentication mechanisms, insecure storage of sensitive data, and other attack vectors exploitable by external attackers.

In addition, we measured 323 anti-stalking websites and analysed for possible privacy exposures. We found that 210/323 (65.02%) anti-stalking websites included third-party trackers, and identified 40 unique third-party hosts tracking users' operations on these websites. We also found that 19 anti-stalking websites included session replay service and observed that users' sensitive information was sent to a session replay server when they report violence online. We observed that two websites leaked very sensitive information due to the use of HTTP protocol, and the chatbot service on three websites tracked users.

References

[1] Adam Cotter. Intimate partner violence in Canada, 2018: An overview. *Juristat: Canadian Centre for Justice Statistics*, pages 1–23, 2021.

[2] Shelly Clevenger and Mia Gilliam. Intimate partner violence and the internet: Perspectives. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pages 1333–1351, 2020.

[3] Christo El Morr and Manpreet Layal. Effectiveness of ict-based intimate partner violence interventions: a systematic review. *BMC public health*, 20(1):1–25, 2020.

[4] Janneke M Schokkenbroek, Wim Hardyns, and Koen Ponnet. Baby don't hurt me: Victimization and perpetration experiences of offline and online intimate partner violence. In *Annual Meeting of the Belgian Association of Psychological Sciences*, 2021.

[5] Sarah Taylor and Yan Xia. Cyber partner abuse: A systematic review. *Violence and victims*, 33(6):983–1011, 2018.

[6] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1893–1909, 2020.

[7] Flavia Fascendini and Kateřina Fialová. Voices from digital spaces: Technology related violence against women. *Association for Progressive Communications (APC)*, 2011.

[8] Almansoor, Majed and Gallardo, Andrea and Poveda, Julio and Ahmed, Adil and Chatterjee, Rahul. A global survey of android dual-use applications used in intimate partner surveillance apps. In *Proceedings on Privacy Enhancing Technologies Symposium*, Lausanne, Switzerland, June 2022.

[9] Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M. Voelker, and Damon McCoy. No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. In *2023 Privacy Enhancing Technologies Symposium*, Lausanne, Switzerland, June 2023.

[10] L. Stefanko. Android stalkerware vulnerabilities, May 2021. `https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_android_stalkerware.pdf`.

[11] Avast. Use of stalkerware and spyware apps increase by 93% since lockdown began in the uk, 2021. `https://press.avast.com/use-of-stalkerware-and-spyware-apps-increase-by-93-since-lockdown-began-in-the-uk`.

[12] Heather L Storer, Eva X Nyerges, and Sherry Hamby. Technology "feels less threatening": The processes by which digital technologies facilitate youths' access to services at intimate partner violence organizations. *Children and youth services review*, 139:106573, 2022.

[13] OpenWPM. OpenWPM, 2023. `https://github.com/openwpm/OpenWPM`.

[14] Catherine Wyburn. The consumer spyware industry: An Australian based analysis of the threats of consumer spyware, 2019. `https://accan.org.au/grants/completed-grants/1435-risks-impacts-and-accountability-in-the-consumer-spyware-industry`.

[15] Diarmaid Harkin, Adam Molnar, and Erica Vowles. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture*, 16(1):33–60, 2020.

[16] Shivang Desai. A new wave of stalkerware apps, 2019. `https://www.zscaler.com/blogs/security-research/new-wave-stalkerware-apps`.

[17] Rachel Gibson. Countering tech abuse together, 2018. `https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-ZakorzhevskyG.pdf`.

[18] Joshua Dalman and Valerie Hantke. Commercial spyware-detecting the undetectable, 2015. `https://www.blackhat.com/docs/us-15/materials/us-15-Dalman-Commercial-Spyware-Detecting-The-Undetectable.pdf`.

[19] Szymon Sidor. Android: apps can take photos with your phone without you knowing., 2014. `https://rstforums.com/forum/topic/79016-android-apps-can-take-photos-with-your-phone-without-you-knowing/`.

[20] Zack Whittaker. Xnspy stalkerware spied on thousands of iphones and android devices, 2022. `https://techcrunch.com/2022/12/12/xnspy-stalkerware-iphone-android/`.

[21] Diana Nadine Moreira and Mariana Pinto Da Costa. The impact of the covid-19 pandemic in the precipitation of intimate partner violence. *International journal of law and psychiatry*, 71:101606, 2020.

[22] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.

[23] Balaji Palanisamy, Sheldon Sensenig, James Joshi, and Rose Constantino. Leaf: A privacy-conscious social network-based intervention tool for ipv survivors. In *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)*, pages 138–146. IEEE, 2014.

[24] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, 2019.

[25] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise" how intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–13, 2018.

[26] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. SoK: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 247–267. IEEE, 2021.

[27] Shivang Desai. Why you shouldn't trust "safe" spying apps!, 2018. `https://www.zscaler.com/blogs/security-research/why-you-shouldnt-trust-safe-spying-apps`.

[28] Asher Langton. Stalking stalkerware: A deep dive into flexispy, 2019. `https://blogs.juniper.net/en-us/threat-research/stalking-stalkerware-a-deep-dive-into-flexispy-2`.

[29] Michael Robinson and Christopher Taylor. Spy vs spy: Spying on mobile device spyware, 2020. `https://media.defcon.org/DEF%20CON%2020/DEF%20CON%2020%20presentations/DEF%20CON%2020%20-%20Robinson-Spy-vs-Spy.pdf`.

[30] Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M Voelker, and Damon McCoy. No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*, 1:1–18, 2023.

[31] Krebson. For 2nd time in 3 years, mobile spyware maker mspy leaks millions of sensitive records, 2018. `https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/`.

[32] Waqas. Company that sells spyware to domestic abusers hacked, 2018. `https://www.hackread.com/company-that-sells-spyware-to-domestic-abusers-hacked/`.

[33] Rithvik. Cerberus acknowledges data breach, states some usernames and encrypted passwords stolen, 2014. https://www.droid-life.com/2014/03/26/cerberus-data-breach.

[34] Joseph Cox. Hacker steals customers' text messages from Android spyware company, 2018. https://www.vice.com/en/article/qvm44m/hacker-steals-text-messages-android-spyware-company-spyhuman.

[35] Paul Lewis. Huge data leak shatters the lie that the innocent need not fear surveillance, 2021. https://www.theguardian.com/news/2021/jul/18/huge-data-leak-shatters-lie-innocent-need-not-fear-surveillance.

[36] Bushra Sabri, Maria Hartley, Jyoti Saha, Sarah Murray, Nancy Glass, and Jacquelyn C Campbell. Effect of Covid-19 pandemic on women's health and safety: A study of immigrant survivors of intimate partner violence. *Health care for women international*, 41(11-12):1294–1312, 2020.

[37] Echap. Stalkerware indicators of compromise, December 2022. https://github.com/AssoEchap/stalkerware-indicators.

[38] Matthias Fassl, Simon Anell, Sabine Houy, Martina Lindorfer, and Katharina Krombholz. Comparing user perceptions of anti-stalkerware apps with the technical reality. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 135–154, 2022.

[39] Parmjit Kaur and Sumit Sharma. Spyware detection in android using hybridization of description analysis, permission mapping and interface analysis. *Procedia Computer Science*, 46:794–803, 2015.

[40] Majdi K Qabalin, Muawya Naser, and Mouhammd Alkasassbeh. Android spyware detection using machine learning: A novel dataset. *Sensors*, 22(15):5765, 2022.

[41] KasperskyLab. Tinycheck, 2021. https://github.com/KasperskyLab/TinyCheck.

[42] Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the monetization ecosystem of stalkerware. *Proceedings on Privacy Enhancing Technologies*, 4:105–119, 2022.

[43] Jadx. Dex to java decompiler, 2023. https://github.com/skylot/jadx.

[44] Google. Developer program policy: September 16, 2020 announcement, 2020. https://support.google.com/googleplay/android-developer/answer/10065487?hl=en.

[45] Frida. Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers, 2023. https://frida.re.

[46] EasyList. EasyList, 2023. online article (2023). https://easylist.to.

[47] Coalition Against Stalkerware. Coalition against stalkerware, 2022. https://stopstalkerware.org/resources.

[48] Microsoft Clarity. Microsoft clarity, 2023. https://clarity.microsoft.com.

[49] Yandex. Yandex, 2023. https://metrica.yandex.com/about.