No Place to Hide: Privacy Exposure in Anti-Stalkerware Apps and Support Websites

Philippe Mangeard, Xiufen Yu, Mohammad Mannan, Amr Youssef

Concordia University
Montreal, Quebec, Canada
{p_mangea,y_xiufe,mmannan,youssef}@ciise.concordia.ca

Abstract. Stalkerware is malicious software found in mobile devices that monitors and tracks a victim's online and offline activity. This harmful technology has become a growing concern, jeopardizing the security and privacy of millions of victims and fostering stalking and Intimate Partner Violence (IPV). In response to this threat, various solutions have emerged, including anti-stalkerware apps that aim to prevent and detect the use of monitoring apps on a user's device. Organizations dedicated to assisting IPV victims have also enhanced their online presence, offering improved support and easy access to resources and materials. Considering how these tools and support websites handle sensitive personal information of users, it is crucial to assess the privacy risks associated with them. In this paper, we conduct a privacy analysis on 25 anti-stalkerware apps and 323 websites to identify issues such as PII leaks, authentication problems and 3rd-party tracking. Our tests reveal that 14/25 apps and 210/323 websites share user information with 3rd-party services through trackers, cookies or session replay. We also identified 44 domains to which sensitive data is sent, along with 3 services collecting information submitted in forms through session replay.

1 Introduction

A recent report [19] published by the Bureau of Justice Statistics revealed that approximately 1.3% (3.4 million) of all U.S. residents age 16 or older were victims of stalking in 2019. Intimate Partner Violence can take various forms, from physical violence to psychological harm, and can occur in several contexts including households, and long distance relationships. As indicated by a 2022 Kaspersky report [13], there is an undeniable correlation between online and offline abuse; 25% of surveyed people confirmed experience of IPV, and 24% confirmed incidents of cyber-stalking within their relationship. Such experiences can lead to severe emotional distress and physical harm with extreme cases being homicides (15% of the 2020 homicides in Canada were committed by spouses or former intimate partners [2]). Given the serious nature of stalking, its growth in the past few years [3] and its detrimental effects on victims, there are a variety of physical and online resources available to help victims, especially against digital

tools fostering abusive behaviors like stalkerware. In today's digital era, anti-stalking websites/apps help victims to prevent, identify, report, and respond to stalking incidents.

Anti-viruses or anti-malware apps are generally widely known as they offer a large set of services regarding malware mitigation, but other apps claim to focus on protecting the user from stalkerware specifically, and can be found more easily than other general detection tools when looking for stalking-related keywords on app markets. Victims suspicious that a stalkerware could be installed on their phone might be more likely to download an app claiming to be specifically conceived for this case. Through our work, we aim to understand whether and how user data privacy is ensured in detection apps, as well as their reliability in combating stalkerware. Additionally, we examine websites that provide online resources and support materials to IPV victims. These resources may include hot-line numbers, support center addresses, chat rooms, and general guidelines for various victim situations. Considering that these websites may be accessed by individuals in danger, it is crucial to carefully assess how they handle private user information to prevent exposing sensitive data to unauthorized parties or networks. Our focus is to identify 3rd-party trackers and potential leaks of personally identifiable information (PII), as they pose a threat to the anonymity that should be inherent to these websites.

Numerous studies related to anti-malware apps have been conducted, notably on new malware detection methods and rogue mitigation apps being hidden malware [6, 11, 15, 22]. Other work in spyware detection [16] does not focus on mobile environment. Similarly, privacy issues on websites have been extensively analyzed, with large scale studies of privacy protection on the web, including specific areas like government websites [23] and hospital websites [29]. Han et al. [11] developed a framework specifically designed for stalkerware detection, using active learning on the in-store app description to classify the stalkerware's capabilities. This method is efficient against potentially harmful apps available on the Play Store without the help of a threat list, but is unfit for apps downloaded from other sources. The specific case of anti-stalkerware apps, however, has not been thoroughly studied yet. More specifically, their privacy footprint and effectiveness have not been measured. The same applies for IPV victims helping websites.

In this paper, we perform a privacy and security study on 25 anti-stalkerware Android apps and 323 victim support websites. Out of 25 Android apps, we downloaded 18 from the Google Play Store and 7 from a Chinese website dedicated to downloading Chinese apps.[1] We chose to look at Chinese apps because of their unique app ecosystem, which is arguably the second largest after the Google Play Store one. We divided our analysis into three parts, each addressing a specific challenge: (i) Identifying privacy issues that could jeopardize user anonymity, such as the collection and distribution of Personally Identifiable Information, (ii) Identifying security issues that could enable malicious actors to gather user data or compromise user accounts, and (iii) Understanding the func-

[1] http://www.downcc.com

tionality of these apps and evaluating their effectiveness in detecting stalkerware. Our research contributions and findings encompass the following:

1) We design analysis frameworks to identify privacy related issues in apps and websites, and use them to assess the privacy footprint of 25 anti-stalkerware apps for Android devices and 323 IPV victim support websites. We detected 1206 third-party scripts in IPV victim support websites, 603/1206 (50.0%) of them were identified as known trackers.
2) Our privacy analysis reveals that 14/25 apps transmit data to 3rd-party services, including sensitive information like device ID or GPS location in 4 cases. 13 apps are also found using trackers for advertisements or user experience purposes. We also identify 44 distinct 3rd-party domains that tested apps communicate with during user interaction. 210/323 (65.0%) of victim support websites include 3rd-party trackers. We list 40 unique 3rd-party hosts that gather the user's browsed web pages and the keywords used in the Search functionality. We detect 3 session replay services (Yandex, Hotjar and Clarity) on 17 victim support websites, which apparently collect usage information, user PII and other sensitive data (when a data submission form is available). Our analysis also reveals that the Chinese tracker hm.baidu.com collects users sensitive information on 2 Chinese websites.
3) 2/4 apps incorporating a login feature with account management use dangerous authentication practices, which could lead to account takeover in one of these cases. One anti-stalking website uses HTTP protocol for their online chat service, exposing users' names, emails and messages.
4) We identify one company developing a stalkerware (KidsGuard) and an anti-stalkerware (ClevGuard), promoting both apps on their website and publishing their mitigation tool on the Google Play Store. The anti-stalking tool detects the malicious app but requires a premium subscription to see it. We also observe 3 apps from separate companies using the same detection framework on their back-end infrastructure when scanning the phone.

2 Related Work

Anti-stalkerware apps. Fassl et al. [10] compared the users' reviews of 2 anti-stalkerware apps to understand users' perception and the apps' capabilities. They also performed reverse engineering to understand their detection features. Their results suggests that app capabilities do not correspond to the users' expectations. In order to detect spyware systems, Qabalin et al. [22] employed machine learning algorithms to create a multi-class classification model for network traffic, which achieved good detection accuracy. Kaur et al. [15] proposed a hybrid approach of description analysis, permission mapping and interface analysis to detect malicious applications in Android. The works mentioned above deal with spyware detection, instead of privacy and security issues related to such detection methods. In addition to academic research, the specific topic of stalkerware also caught the attention of people in the industry. ESET research group published a white paper [25] which analyzed Android stalkerware vulnerabilities. A

group of collaborators also compiled all information about known stalkerware apps and built the Stalkerware-indicators [8] GitHub repository to make the detection of spyware easier in both Android and iOS systems. Another detection solution, TinyCheck [14] is currently in development by Kaspersky to assist non-technical individuals to detect stalkerware on their device. Because of its early development stage, the tool currently lacks features thus making it less effective than more standard solutions. However, its main end goal quality would be to allow stalkerware detection without installing or interacting with anything on the compromised phone, thus making it harder for the stalker to notice that the victim is being suspicious.

IPV victim support websites. Eterovic et al. [9] conducted a review of the technologies used by stalkers and technologies used against stalkers. They pointed out the following possible future research directions: improving existing privacy and anti-stalker techniques as well as developing methods to detect stalking behavior on social media and blogging platforms. Samarasinghe et al. [23] performed a privacy measurement on government websites and Android apps. They found numerous commercial trackers on these services; 27% of government Android apps leak sensitive information to 3rd-parties. Senol et al. [24] performed a measurement of data exfiltration from online forms. Their study showed that users' email addresses were collected by 3rd-parties before form submission and without giving consent on both US and EU websites. Similarly, password on 52 websites were found to be leaked to 3rd-party session replay scripts. Yu et al. [29] analyzed the privacy issues on hospital websites and observed that users credentials were sent to session replay services. Ischen et al. [12] investigated the privacy issues of chatbots used on websites. Their results showed that users are more inclined to share personal information with a human-like chatbot rather than with a machine-like chatbot.

Other relevant work. Several other recent studies also explored topics related to IPV technologies and victims, although not directly the privacy implications of victim-support apps and websites. For example, Chatterjee et al. [5] studied the intimate partner stalking (IPS) spyware ecosystem, and identified several hundred of such IPS-relevant apps (from app stores and beyond). The authors showed that existing anti-virus and anti-spyware tools mostly fail to identify these dual-use apps as a threat. More recently, Almansoori et al. [1] identified 854 dual-use apps available on the Google Play Store, many of which do not provide English descriptions and cannot be found via English search queries (i.e., available in other languages, which are not as well-monitored by Google as the apps in English). Liu et al. [17] analyzed 14 Android apps outside of Google Play, and studied the mechanisms used for spying. ESET [25] performed a comprehensive security analysis of 86 stalkerware applications, and reported several critical vulnerabilities in the apps that may allow victim data compromise via other third-party attackers.

Beyond stalkerware apps, Stephenson et al. [27] identified how various common IoT devices (32 types in total) including home thermostats, smart speakers, cameras, smart toys, and Bluetooth item trackers, can be abused by IPV attack-

ers. From interviews with 20 IPV victims of such IoT abuse, in another study, Stephenson et al. [26] identified various instances of abuse cases involving such devices. Ceccio et al. [4] evaluated commercial devices and apps that claim to detect such spy IoT devices, and found that these detectors are very ineffective in real-world abuse scenarios.

3 Methodology

3.1 Anti-Stalkerware Apps

We conduct our analysis of solutions against stalkerware apps with three goals in mind: evaluating data privacy and identifying security issues of stalkerware detection tools available for Android, as well as assessing their effectiveness in a realistic context. To collect apps we look through the Google Play Store and web-based Android app databases for keywords such as "anti-stalkerware", "anti-stalking", "stalk detector", as they would be most probably used by a victim looking for such apps. We gather a sum of 25 victim support apps, with 18 from the Google Play Store, and 7 from Chinese app markets. See Figure 1 for our methodology diagram.

Privacy and security analysis. We focus our analysis on 4 distinct vectors through which users' security and privacy could be violated. We chose these specific vectors as they represent a threat to the user's anonymity, which is crucial in the context of IPV and stalkerware detection.

Authentication mechanisms. In cases where the app offers a login feature and account management functionalities, we identify the mechanisms used for authentication and verify their security. Such methods include username & password validation, session management and authentication tokens. We examine network traffic related to user login to check if credentials are properly secured and sent. We also look at how the user session is kept alive over time and if token replay attacks allow unauthorized users to hijack the user's account.

Personal Identifiable Information (PII) leaks. Apps can sometimes upload information about the device they are installed on, or the device's user. If such personal data is transmitted without proper encryption, pieces of information such as names, addresses, phone numbers or IMEI number could be extracted by attackers and used to identify, track or impersonate individuals. These leaks can be unintentional or malicious, in cases where the app transmit data to other parties without the consent of the user. Unintentional leaks can be caused by faulty security protocols during uploads, or accidental exposure through error messages or debug logs.

Third-party libraries. Through static code analysis, we identify 3rd-party libraries used by anti-stalking apps. Then, by examining the traffic generated by user interactions, we can discern requests related to first-party and 3rd-party libraries. Like with PII leaks, these 3rd-party libraries used by the app could be a threat to the user's privacy by accessing device information or personal data. We identify the presence of libraries and trackers and verify the data they collect

through static code analysis and traffic monitoring. We then compare them to a list of well-known trackers (Easylist) for classification.

Insecure custom encryption. In addition to potentially insecure implementations of standard encryption channels (like HTTPS), some apps use non-standard protocols, additional channels and encryption layers. We used ThirdEye [21] to identify custom encryption used by the apps and assess their security.

Effectiveness Tests. Proper functioning of anti-stalkerware apps is crucial to the safety of IPV victims, it is thus important to assess the effectiveness of such apps and verify that they are not being wrongfully advertised as "highly effective spyware detectors". We tested the reliability of anti-stalkerware solutions by manually installing each app on a purposefully compromised Android device and verifying whether the app could flag the installed stalkerware. Each app is tested against 10 different free stalkerwares. We utilize only free stalkerware apps for our test to avoid purchasing such apps due to ethical concerns about supporting stalkerware companies. Among the 10 chosen stalkerware apps, *iKeyMonitor* and *AndroidSpy* are treated as special cases, as they provide weekly builds of their app's package. The APK available on their website is recompiled every week with a different package name. This effectiveness test allows us to identify the different detection mechanisms used by anti-stalkerware apps as well as the amount of details they give about detected apps. This includes information such as the permissions required by the detection app to function properly, or flags assigned to potentially dangerous apps giving details to the user (e.g., labelling the detected app as a stalkerware or just a malware). We note that our tests do not include any attempt to trick the anti-stalkerware apps, by changing the stalkerware package names or signature. However, the inclusion of weekly built apps approximates this behaviour.

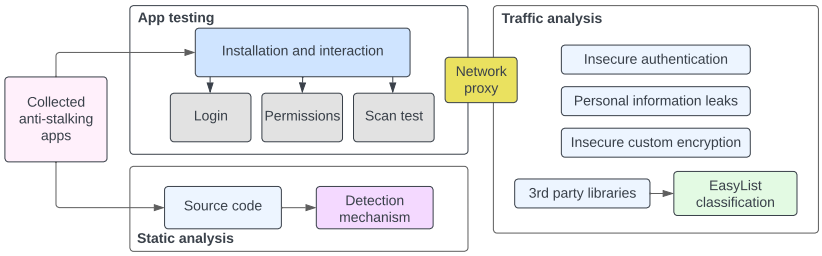

Fig. 1: Privacy analysis methodology of anti-stalkerware apps

3.2 Privacy Analysis of Victim Support Websites

Our methodology comprises three key elements. We collect the URLs of anti-stalking websites through keyword searches such as "anti-stalking", "stalking victims" or "stalking support" in both Google and Baidu search engines. We then use OpenWPM [20] to crawl the websites, which saves crawled information in a SQLite database. We then filter it through Easylist and EasyPrivacy [7] to categorize 3rd-party scripts/cookies and check whether there are session replay

services on the websites or not. We manually fill online forms on those websites to identify users' sensitive information leaks; see Figure 2.

Collecting Victim Support Websites. We start with the resources mentioned on the stopstalkerware website[2] which includes 25 domains in 13 different countries. We then manually extended our victim support website collection by searching for keywords, like, "anti-stalking", "stalking victims", "stalking support" and "stalking help". In total, we collect 323 victim support websites; including 120 from China, 77 from Canada, 34 from the USA, 22 from Europe, 14 from Hong Kong, 13 from the UK, 12 from South America, 7 from Australia, 24 others from Egypt, Turkey, Malaysia, Russia, Ukraine, India and 1 from the UN. This set might not be exhaustive but it includes the most relevant websites that we were able to find online. Note that the collect 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 or non-profit organizations. Chinese websites are collected on Google and Baidu, however if we search keywords related to anti-stalking or domestic violence for China, most of the results tend to be news reports rather than websites or resources directly related to the topic. We choose Women's Federation's websites[3] for our Chinese dataset. The Women's Federation is a women's rights organization divided in subgroups across China, providing online resources for each city. They offer guidelines for victims of domestic violence or any form of IPV. In total, we collect 108 Women Association websites and 12 online legal support websites in China.

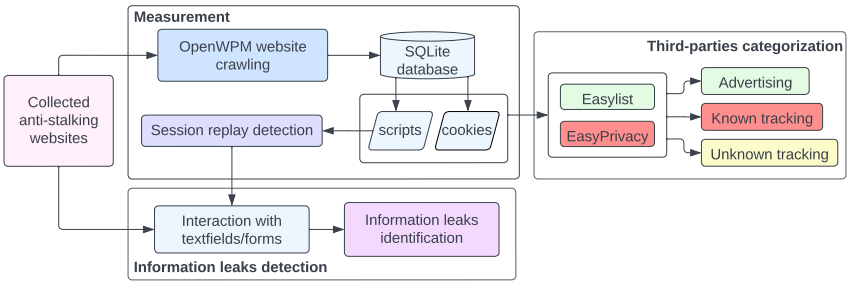

Fig. 2: Privacy analysis methodology of victim support websites

Privacy Measurements. We configure OpenWMP [20] web privacy measurement framework with 10 parallel browser instances in headless mode. We explicitly enable OpenWPM instrumentations for HTTP requests, Javascript, cookies, DNS requests, callbacks and page navigations. We use a physical machine running Ubuntu 22.04 LTS for our measurements in Feb. 2023. A total of 323 victim support websites are crawled using OpenWPM from a North American university

[2] https://stopstalkerware.org/resources
[3] www.bjwomen.gov.cn, hnflw.gov.cn, www.sxwomen.org.cn, www.womenvoice.cn

campus. We save the crawling result in a SQLite database for further analysis. The saved information contains both stateful (i.e., scripts/cookies), and stateless forms of tracking metrics. We then examine the saved tracking scripts/cookies for 3rd-party domains, i.e., domains of scripts/cookies that do not match the domain of the websites that they are on.

We use filtering rules [7] that block 3rd-parties to identify three categories of 3rd-party domains: ad-related 3rd-parties blocked by EasyList; known trackers blocked by EasyPrivacy; Unknown trackers, or any 3rd-party service that is not blocked by either lists. We manually browse those websites to find pages containing user-filled forms, which include registration/login, contact-us, and search. We tested 220 unique URLs of such web pages on victim support websites.

4 Results

4.1 Results of Victim Support Apps Analysis

Tested apps gathered on the Google Play Store are listed in Table 3. We refer to their common names (or company names) in the following sections. For Chinese apps, we refer to their package names.

Authentication and session management. Out of the tested 25 anti-stalkerware apps, only 4 of them allow the user to register an account and login with their credentials (Protectstar AntiSpy and Clevguard on Google Play, as well as cn.lslake.fangjianting and uni.UNI1898B51 on Chinese app markets). Protectstar uses API calls to perform actions, and authenticate as a specific default user when no account is used. This user account called "psapi" is automatically logged into by the app on launch, using seemingly hard-coded credentials to request a session token. This session token appears to be usable for any regular API call, except the ones reserved for getting premium subscription licenses and account management. On the other hand, the Chinese app uni.UNI1898B51 assigns session tokens on login that are not modified nor deleted after logging out. Even though a new token is generated if the user logs in again, an attacker could replay this token even after a user disconnected from their account and call the API on their behalf. The second Chinese app, cn.lslake.fangjianting, allows login through either Tencent QQ or Wechat and thus leaves authentication responsibility to these apps.

Encryption mechanisms and PII leaks. Upon manual inspection of the network traffic generated by anti-stalkerware apps, we identified 3 cases where data is being sent to 3rd-party hosts. Com.arcane.incognito shares hardware and OS information with Facebook, data including memory usage, OS version or the phone's model, whether the device is rooted or not, and if it is identified as an emulator. We also noticed the user's email being sent to a first party host (incognitotheapp.zendesk.com), even though the app does not feature user accounts. Skibapps also shares hardware information like the device type, alongside OS type and version, only this time to Adloox. The app spyware.detector.remove.antihacker communicates with Yandex, a Russian ad

provider, and sends hardware information along with the google_aid (advertising ID), device-id (IMEI or MEID) and userid.

In addition to these manual checks, we gathered network traffic from all 25 anti-stalkerware apps using ThirdEye [21], and identified 21 additional instances of user/device information being shared to 3rd-party hosts by 14 apps. The data includes 13 cases disclosing the phone model, 4 with OS information, and others sharing cookies or tokens. We identified 3 first-party destination hosts (for Foxbyte Code, Incognito and Cb Innovations), the others being 3rd-party; see Table 1.

Table 1: Information shared per app to 3rd-party services.

App	Item	Destination address
cn.lslake.fangjianting	build	pangolin.snssdk.com (custom encryption)
Foxbyte Code	build	www.foxbytecode.com
com.txjjy.fjtjc	build	pangolin.snssdk.com (custom encryption)
Clevguard	cookie	apipdm.imyfone.club
com.yyyx.fjtws	cookie	fjt.4fqp.com
Incognito Security Solutions	device-email	incognitotheapp.zendesk.com
cn.lslake.fangjianting	model	ulogs.umeng.com
Cb Innovations	model	firebase-settings.crashlytics.com
Certo	model	certo-scan-results-ingestion.azurewebsites.net
Cyber Tor	model	cdn.liftoff-creatives.io
Malloc Privacy	model	firebase-settings.crashlytics.com
Protectstar Antivirus	model	firebase-settings.crashlytics.com
com.txjjy.fjtjc	model	privacy.viterbi-tech.com
com.txjjy.fjtjc	model	ulogs.umeng.com
World Globle	model	adtubeservices.co.in
World Globle	model	cdn.liftoff-creatives.io
com.yyyx.fjtws	model	ulogs.umeng.com
Coolrepairapps	model	yastatic.net
cn.lslake.fangjianting	token	tool.sqcat.cn (custom encryption)
Mahika Developers	token	graph.facebook.com

Third-party libraries. Since all anti-stalkerware apps in our analysis are free, most of them rely on 3rd-party ad providers and trackers to generate income. Others offer premium versions of their app with additional features, but still make the device scan available for free. During the course of our analysis, we kept track of each request being sent to a 3rd-party and compiled all of them into Table 2. We can see the majority of apps use Google APIs (e.g., 11 using Firebase) for various reasons. However, specific apps like spyware.detector.remove.antihacker send data to unique known tracking/advertisement companies like Yandex, adjust or Doubleclick (owned by Google). We also notice the presence of Facebook hosts in 3 apps, 2 of them specifically reaching graph.facebook.com, often used to get data in or out of the platform (in our case, both requests were sending data to Facebook).

Out of 121 separate get requests for .js files found in the apps' network traffic, we found 95 are used by "advertisers" according to EasyList. The other 26 URLs were unknown to the blocklist we used for comparison, but we then manually identified 3 domains associated with Yandex (in spyware.detector.remove.antihacker), and 5 related to a Chinese advertisement platform (pglstatp-toutiao.com, hosted by ByteDance).

Table 2: Number of anti-stalkerware apps reaching 3rd-party hosts

Destination host	**#App**
Google	18
DoubleClick	7
Umeng, app-measurement.com, cdn.liftoff-creatives.io, s0.2mdn.net	3
graph.facebook.com, dt.adsafeprotected.com, fw.adsafeprotected.com, impression-east.liftoff.io, mobile.adsafeprotected.com, my-api.protectstar.com, pan-golin.snssdk.com, rr4—sn-gpn9-t0as.gvt1.com, sf3-fe-tos.pglstatp-toutiao.com, static.adsafeprotected.com, toblog.ctobsnssdk.com, api-access.pangolin-sdk-toutiao.com	2
adexp.liftoff.io, adtubeservices.co.in, Android.bugly.qq.com, api.revenuecat.com, app.adjust.com, app.viterbi-tech.com, assets.mintegral.com, click.liftoff.io, cdnjs.cloudflare.com, dsum-sec.casalemedia.com, ec2-18-116-59-188.us-east-2.compute.amazonaws.com, fjt.4fqp.com, ib.adnxs.com, lf6-ad-union-sdk.pglstatp-toutiao.com, maps.wikimedia.org, privacy.viterbi-tech.com, settings.crashlytics.com, sf3-ttcdn-tos.pstatp.com, techcrunch.com, tnc3-bjlgy.snssdk.com, tool.sqcat.cn, us01.rayjump.com, www.facebook.com, www.lslake.cn, yastatic.net	1

Detection methods and effectiveness. From the effectiveness tests, we found that 15 out of 25 anti-stalking apps could detect at least one malicious app; see Table 3. Surprisingly, 10 out of 25 anti-stalkerware apps (i.e., 7 Chinese apps and 3 Google Play Store apps) completely failed to detect any of the stakerware apps; these 10 apps are omitted in the result table. Overall, stalkerware apps present in open source threat lists and featured in online web articles were the most detected, with TheTruthSpy being found by 13 out of the 25 mitigation tools and CatWatchful by 11 out of 25. Only 4 tools flagged the weekly build of iKeyMonitor as suspicious, but none identified it as a stalkerware. Similarly, AndroidSpy was flagged in 6 cases, but only once as a malware. 7 tools reported apps with risky permissions, but Malloc Privacy and Incognito needed the stalkerware to be entirely configured (not just installed and disabled) to flag it.

10 anti-stalkerware apps required a total filesystem access (READ, WRITE and MANAGE_EXTERNAL_STORAGE permissions) and 6 of them requested media access only (among which 3 of them were requesting total access as well). Notification access is required by 11 apps. This is mostly to send notifications rather than to analyze them, as many apps use them to warn the user that a scan is in progress, or that a problem has been found. These permissions are all required by apps performing application signature checks.

Other anti-stalkerware apps function by monitoring the phone's main tools (e.g., camera, microphone, GPS) and sending a notification when an app uses either of these. One app (World Globle Apps) from the Google Play Store claims to use this "active" detection method, recording camera, microphone and GPS usage and alerting the user if it is accessed by another app. However it raised only 1 flag when one stalkerware was being configured (warning that the camera was being used). This means that this anti-stalkerware needs to be on the phone before the malicious app is installed. Other than that, no alerts were raised, even after multiple hours of phone usage. Unlike Google Play Store apps, all Chinese ones implement this monitoring method and thus require related permissions. Access to camera and microphone was requested by 7 apps, and GPS usage was needed in 6 apps. App usage access was only requested twice. This detection

mechanism didn't prove to be the most efficient, even if it detects stalkerware upon installation, as the abuser would be the one seeing the notification.

During our analysis, we noticed that 4 different apps use the exact same back-end framework to perform their malware scan (Protectstar Antispy, Protectstar Antivirus, Cb Innovations and Foxbyte Code). We note that only the first two apps are developed by the same company. When scanning the device, these apps send two batches of information to an API responding with a list of identified threats. The first batch contains package names of apps installed on the phone, the second one contains their cryptographic hashes. This means that the actual comparison of installed apps to the malware database is done remotely.

Additionally, we found that the company developing com.clevguard.guard also offers on their website a "parental control" app that is advertised as a remote monitoring tool (in other words, a stalkerware). The anti-stalkerware developed by ClevGuard hides most of its functionalities behind paywalls. The free version displays the number of detected threats but does not give information about flagged apps. We tested this anti-stalkerware against the spyware developed by the same company. Even though the free version prevented us from seeing the name of the flagged app, the fact that it detected one threat confirmed that it was not ignoring it.

Table 3: Anti-stalkerware apps detection results. ●: flagged as stalkerware. ▨: flagged as malware. ○ : flagged because of critical permissions detected. ⊙ : flagged because of trackers detected. ◐: Combination of permissions and trackers. 👤: Flagged as a hidden/fake system app. Empty: not flagged

Company name (package name)	Version	SpyPhoneLabs	Mobilespy	TheTruthSpy	Snoopza	OwnSpy	CatWatchful	iKeyMonitor	MeuSpy	Cerberus	AndroidSpy
Malloc Privacy (com.mallocprivacy.antistalkerfree)	2.49	○	⊙	●	○	◐	●	⊙	○	●	
World Globle Apps (com.world.globle.mobileantistalker.rs)	1.0.3								○		
Incognito Security Solutions (com.arcane.incognito)	3.0.0.15		●	○	○	○	●		○	○	○
Protectstar antispy (com.protectstar.antispy.android)	5.0.3	●		●	▨	●	●				
Cb innovations (com.cbinnovations.antispy)	2.0.1	●		●	▨	●	▨			●	▨
Protectstar antivirus (com.protectstar.antivirus)	1.2.5	⊙		●	▨	●	●		▨	●	
Certo (com.certo.Android)	2.1.2	●		●		●	●		●	●	
Own effect (com.owneffect.spyware.detector)	1.0.4		○								
Foxbyte Code Inc. (com.foxbytecode.spywarescanner)	1.4	▨		●	▨	▨	▨		▨	▨	
Coolrepairapps (spyware.detector.remove.antihacker)	5.0.0.1	▨	⊙	⊙	○	◐	○	◐		▨	○
Skibapps (com.skibapps.antispyforAndroid)	3.43	●		●	▨	●	▨		▨	●	👤
Lighthouse (net.hobbyapplications.privacyscanner)	1.8.29	●	●	●	○	○	●	○	○	●	○
Mahika Developers (com.whotrackmyphonemhk)	1.0.6	○	○	○	○	○	○	○	○	○	○
Safety Apps (com.spyscanner.spyware.antispywaredetector)	3.0			👤		○			👤	○	
Cyber Tor (com.cyber genius.cyber tor)	5.6			👤		○				○	

4.2 Results of Victim Support Websites Analysis

Third-party tracking JavaScript/cookies. We found that 169/323 (52.3%) of victim support websites include at least one known 3rd-party tracking script;

31/323 (9.6%) victim support websites use 3rd-party tracking cookies. The proportion of websites with 3rd-party tracking cookies is much lower than websites with 3rd-party tracking scripts. This might be because the EasyList Cookies list we used[4] does not include extensive rules for cookies on Chinese websites.

To better understand 3rd-party scripts/cookies, we grouped them into three categories. We found that 53/1206 (4.4%) 3rd-party scripts were flagged as advertising; 603/1206 (50.0%) 3rd-party scripts were identified as known trackers; 550/1206 (45.6%) were not recognized by Easylist [7], we labelled them as unknown trackers. Similarly, 49/694 (7.1%) 3rd-party cookies were identified as advertising cookies; 266/694 (38.3%) 3rd-party cookies were categorized as known trackers; 379/694 (54.6%) were unknown trackers.

We listed the top-10 domains of tracking scripts and tracking cookies. We can see that the top tracking scripts are googlemanager.com (107/323 (33.1%)), google-analytics (115/323 (35.6%)), Facebook (30/323 (9.3%)) and Baidu (25/323 (7.7%)). We observed Baidu tracker only on Chinese websites; see Figure 3. Top tracking cookies are addthis.com (10/323 (3.1%)), clarity.com (6/323 (1.9%)), and demdex.net (8/323 (2.5%)). Addthis is used for a free social bookmarking service integrated in websites, making sharing content across social web; clarity.ms is Microsoft session replay service [18]; Sharethis collects data on user behavior advertising and analytics; see Figure 4.

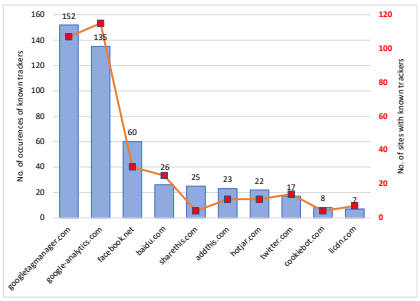

Fig. 3: Top-10 known tracking scripts on victim support sites.

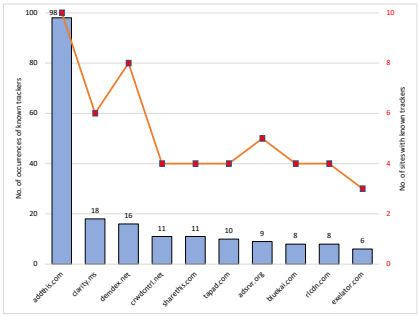

Fig. 4: Top-10 known tracking cookies on victim support sites.

Third-party hosts tracking users' operations. We also listed some 3rd-party hosts that track web pages victims browse and the keywords used in the websites search functionality (if available); see Table 4. We found 7 hosts belonging to Google (www.google-analytics.com, www.google.ca, googleads.g.doubleclick.net, www.googleadservices.com, analytics.google.com, adservice.google.com, and ssl.google-analytics.com); 2 hosts owned by Twitter (syndication.twitter.com, analytics.twitter.com); and 3 Chinese hosts (hm.baidu.com, sp0.baidu.com, analytics.tiktok.com). We observed that hm.baidu.com and sp0.baidu.com only

[4] https://easylist.to/

tracks Chinese websites while analytics.tiktok.com tracks 5 Canadian websites along with 1 South Africa website.

Online chat tracking. We noticed that the online chat service on three websites (diamondlaw.ca, lawyersuae.com, dubaipolice.gov.ae) tracked users. Diamondlaw.ca is a law firm with physical offices in Canadian provinces including British Columbia, Ontario and Alberta, which offers legal services related to stalking. The website employed chat-api.intaker.com for customer online chat service. However, the customer online chat service tracks the user's navigation through the website. Similarly, lawyersuae.com and dubaipolice.gov.ae, both UAE websites, use online chat services tracking the victims' page navigation (on their websites). Lawyersuae.com uses gateway.botstar.com for online chat while dubaipolice.gov.ae used api.livechatinc.com.

Table 4: Third-party hosts tracking users' operations in more than 10 different websites

Third-party Host	**#Sites**
www.google-analytics.com	130
www.google.ca	52
googleads.g.doubleclick.net	42
www.facebook.com	37
www.googleadservices.com	26
hm.baidu.com	25
www.youtube.com	23
analytics.google.com	15
syndication.twitter.com	13
m.addthis.com	11
px.ads.linkedin.com	11

We found that two Chinese websites for online legal support (user.maxlaw.cn and www.66law.cn) leak users' information to hm.baidu.com. Both websites claim that users do not need to worry about the information they provide, because all data is encrypted, so they can provide as much detailed information as possible for online legal support. Although user's sensitive data is encrypted, it is sent to hm.baidu.com without the user's consent through a tracking pixel with the url *hm.baidu.com/hm.gif*. The script from s.canddi.io tracks the functionalities of mailing list subscription and contact on www.suzylamplugh.org; as a result, victims' first name, last name, email, message title 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/last name, email, organization, subject, message) is 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 tracking cookies. We examined the validity duration of top-10 tracking cookies, and found that clarity.ms set cookies on 4 victim support websites were valid for more than 1000 years. Known tracking cookies that expire within 1 to 5 years were addthis.com (90), clarity.ms (4), sharethis.com (8) and adsrvr.org (9); see Table 5.

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 includes user interactions on a website such as typed inputs, mouse movements, clicks, browsed pages, tapping and scrolling events. During this process, users' sensitive information can be exposed to 3rd-party servers that host session replay scripts. We identified 3 session replay services in the analyzed 323 victim support websites: Clarity on 6 websites (Canada (4), UAE

Table 5: The top-10 known tracking cookies and their expiry periods (m=month, y=year).

		Cookie Expiry Duration			
Tracker	**#Sites**	**<1m**	**1m-1y**	**1y-5y**	**>1000y**
addthis.com	98		8	90	
clarity.ms	18	6	4	4	4
demdex.net	16		16		
crwdcntrl.net	11		11		
sharethis.com	11	3		8	
tapad.com	10		10		
adsrvr.org	9			9	
bluekai.com	8		8		
rlcdn.com	8		8		
exelator.com	6		6		

(1), USA (1)), Hotjar on 9 websites (Canada (4), USA (3), South-Africa (1), UK (2), India (1)) and Yandex on 2 in Russia; see Table 7.

We found that 2 victim support websites in Russia expose victims' information to Yandex [28] 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. Users are asked to fill an online form for support; all the victims' sensitive information in the form is sent to Yandex, including, name, email address, phone number, year of birth, location, the presence of minor children, reasons to contact, who inflicts violence as well as a custom message. The other website, i.e., nasiliu.net provides legal assistance, psychological help and support to victims. We noticed that when victims use the website's search engine, searched keywords are collected by Yandex. Users' names and email addresses are also leaked through money donations; see Table 6. Note that safehorizon.org includes two session replay services: Hotjar and Clarity. Clarity initializes 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 is uploaded to o.clarity.ms. Hotjar uses web sockets to transfer collected data to ws4.hotjar.com. Both session replay services collect elements and web pages that users interacted with, as well as mouse events.

HTTP plaintext traffic. We observed that 4 websites use HTTP protocol for their core functions; these include connectnetwork.ca www.tandemlaw.ca, www.alberta.ca and www.dfac.ae. On www.alberta.ca, users are required to fill in their email, first and last name, location data, gender and age group to create an online chat server account. However, the chat registration (provided by the 3rd-party domain m2.icarol.com), use HTTP, exposing all provided information to any on-path attacker. The online chat service (www.chat.dfwac.ae/Customer/Start) for the Dubai Foundation for Women and Children (DFWAC) used the HTTP protocol. Victims are required to enter name, email and questions before sending a chat request. Victims sensitive information (e.g., name, email, and chat logs) is leaked because of the use of

Table 6: Sensitive information leaks in victim support websites

Website	Country	Leaked data	Feature	Destination	Cause
wcons.net	Russia	Name, email address, birthyear, phone number, location, minor children presence, custom message, name of the abuser	Report a crime	mc.yandex.ru	Session Replay
		Keywords	Search		
nasiliu.net		Name	Donate		
lawyersuae.com	UAE	Keywords	Search	botstar.com	Online Chat
dubaipolice.gov.ae				api.livechatinc.com	
diamondlaw.ca	Canada			chat-api.intaker.com	
suzylamplugh.org	UK	Name, email address	User Sign-in	s.canddi.io	Tracker
		Name, email address, phone number, job title, company name, custom message	Contact		
workplacesrespond.org	USA	Name, email address, company name, custom message	Contact	go.futurewithout-violence.org	
www.maxlaw.cn	China	Chat messages	Online Chat	hm.baidu.com	
www.66law.cn				hm.baidu.com	
www.dfac.ae	UAE	Name, email address, chat messages		www.chat.dfwac.ae	HTTP
www.alberta.ca	Canada	Name, email address, location, gender, agegroup	Online Chat sign-in	m2.icarol.com	

Table 7: Session replay services (SRS) on victim support websites.

SRS	Websites
Yandex	wcons.net (Russia), nasiliu.net(Russia)
Hotjar	getsafeonline.org (USA), safehorizon.org (USA), onlineharassmentfieldmanual.pen.org (USA), domesticshelters.org(USA, CAN), canadianwomen.org (CAN), member.psychologytoday.com (USA), lawrato.com (India), mysupportspace.org.uk (UK), legalwise.co.za (South-Africa)
Clarity	legaladviceme.com (UAE), getsafeonline.org (USA), diamondlaw.ca (CAN) calgarydefence.com (CAN),ualberta.ca (CAN),lawcentralalberta.ca (CAN)

HTTP. We found that 72/120 (60.0%) of websites in China only support HTTP protocol, they however do not handle sensitive information (no forms to fill).
The use of third-party services for core functionality. We observed two websites (safehorizon.org and rainn.org) in the USA using a 3rd-party service for the sign-up functionality. Safehorizon.org utilizes go.pardot.com for this functionality, consequently sending user's email address, first and last name to 3rd-party servers We noticed that three websites in Canada (canadianlabour.ca, iheartmob.org and www.kruselaw.ca) use a 3rd-party service during user sign-up, leading to victims' sensitive information being sent to the 3rd-party domain, instead of the website's domain. Consequently, on canadianlabour.ca, victims' first and last name, email address, phone number and location data are sent to actionnetwork.org; their first and last name, email address and country are also sent to the same address when asking for support on iheartmob.org.

5 Conclusion

The limited number of efficient anti-stalkerware app makes it difficult for users to rely on such tools. In addition, based on our experiments, more than half of the analyzed apps share sensitive data to other parties and use tracking services for advertisement. Similarly, 65% of the websites dedicated to IPV victim support use 3rd-party trackers, with 8% of them collecting PII. It should be noted, however, that using only free stalkerware apps for our tests might not give a thorough picture of anti-stalkerware effectiveness, as premium stalkerware apps could use more advanced techniques to evade detection. Our analysis provides a lower bound of the help these solutions can provide, and makes it easy to extrapolate to a larger testing set the effectiveness of apps that fail to detect free stalkerware. Testing such paid apps would provide more insights into this problem. Detection tools providers and developers should be aware of the data gathered by 3rd-party libraries and avoid using them for their apps and/or websites; it is crucial to ensure that no PII is used or collected by these apps. Improving the detection rate should also be a priority. We recommend using multiple trusted, up-to-date package name databases (like Echap's repository of stalkerware indicators [8]) and relying more on local analysis rather than cloud-based ones. Similarly, anti-stalkerware websites' developers should ensure that 3rd-party scripts they use are not performing any user tracking. As victims' data is highly sensitive, these support websites should avoid using any tracking services, like session replay services. Finally, we hope that our work provides insight for developers to improve these platforms and make them as safe and useful as possible for IPV victims in need of help.

6 Acknowledgements

This research was funded by the Office of the Privacy Commissioner of Canada (OPC), we thank them for their trust and support.

References

1. 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.
2. A. Armstrong and B. Jaffray. Homicide in Canada. *Juristat: Canadian Centre for Justice Statistics*, 2020.
3. K. Bracewell, P. Hargreaves, and N. Stanley. The consequences of the covid-19 lockdown on stalking victimisation. *Journal of Family Violence*, pages 1–7, 2020.
4. R. Ceccio, S. Stephenson, V. Chadha, D. Y. Huang, and R. Chatterjee. Sneaky spy devices and defective detectors: The ecosystem of intimate partner surveillance with covert devices. In *USENIX Security Symposium*, Anaheim, CA, USA, Aug. 2023.
5. R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.
6. M. Conti, G. Rigoni, and F. Toffalini. Asaint: a spy app identification system based on network traffic. In *Proceedings of ARES '20*, pages 1–8, 2020.
7. EasyList. EasyList, 2023. online article (2023). https://easylist.to.
8. Echap. Stalkerware indicators of compromise, 2022. https://github.com/AssoEchap/stalkerware-indicators.
9. B. Eterovic-Soric, K.-K. R. Choo, H. Ashman, and S. Mubarak. Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review. *Computers & security*, 70:278–289, 2017.
10. M. Fassl, S. Anell, S. Houy, M. Lindorfer, and K. Krombholz. Comparing user perceptions of anti-stalkerware apps with the technical reality. In *SOUPS 2022*, pages 135–154, 2022.
11. Y. Han, K. A. Roundy, and A. Tamersoy. Towards stalkerware detection with precise warnings. In *Annual Computer Security Applications Conference*, pages 957–969, 2021.
12. C. Ischen, T. Araujo, H. Voorveld, G. van Noort, and E. Smit. Privacy concerns in chatbot interactions. In *Chatbot Research and Design, CONVERSATIONS 2019*, pages 34–48. Springer, 2020.
13. Kaspersky. New kaspersky stalkerware report confirms the link between online and offline violence, 2022. https://www.kaspersky.com/about/press-releases/2022_new-kaspersky-stalkerware-report-confirms-the-link-between-online-and-offline-violence.
14. KasperskyLab. Tinycheck, 2021. https://github.com/KasperskyLab/TinyCheck.
15. P. Kaur and S. Sharma. Spyware detection in android using hybridization of description analysis, permission mapping and interface analysis. *Procedia Computer Science*, 46:794–803, 2015.
16. E. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. Kemmerer. Behavior-based spyware detection. In *Usenix Security Symposium*, page 694, 2006.
17. E. Liu, S. Rao, S. Havron, G. Ho, S. Savage, G. M. Voelker, and D. McCoy. No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*, 1:1–18, 2023.
18. Microsoft Clarity. Microsoft clarity, 2023. https://clarity.microsoft.com.
19. B. of Justice Statistics. Stalking victimization, 2019. https://bjs.ojp.gov/library/publications/stalking-victimization-2019.
20. OpenWPM. OpenWPM, 2023. https://github.com/openwpm/OpenWPM.
21. S. Pourali, N. Samarasinghe, and M. Mannan. Hidden in plain sight: Exploring encrypted channels in android apps. In *Proceedings of the 2022 ACM SIGSAC CCS*, pages 2445–2458, 2022.
22. M. K. Qabalin, M. Naser, and M. Alkasassbeh. Android spyware detection using machine learning: A novel dataset. *Sensors*, 22(15):5765, 2022.
23. N. Samarasinghe, A. Adhikari, M. Mannan, and A. Youssef. Et tu, brute? privacy analysis of government websites and mobile apps. In *Proceedings of the ACM Web Conference 2022*, pages 564–575, 2022.

24. A. Senol, G. Acar, M. Humbert, and F. Z. Borgesius. Leaky forms: A study of email and password exfiltration before form submission. In *USENIX Security Symposium*, pages 1813–1830, 2022.
25. L. Stefanko. Android stalkerware vulnerabilities, May 2021. https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_android_stalkerware.pdf.
26. S. Stephenson, M. Almansoori, P. Emami-Naeini, and R. Chatterjee. "it's the equivalent of feeling like you're in jail": Lessons from firsthand and secondhand accounts of iot-enabled intimate partner abuse. In *USENIX Security Symposium*, Anaheim, CA, USA, Aug. 2023.
27. S. Stephenson, M. Almansoori, P. Emami-Naeini, D. Y. Huang, and R. Chatterjee. Abuse vectors: A framework for conceptualizing IoT-enabled interpersonal abuse. In *USENIX Security Symposium*, Anaheim, CA, USA, Aug. 2023.
28. Yandex. Yandex, 2023. https://metrica.yandex.com/about.
29. X. Yu, N. Samarasinghe, M. Mannan, and A. Youssef. Got sick and tracked: Privacy analysis of hospital websites. In *2022 IEEE EuroS&PW*, pages 278–286. IEEE, 2022.