SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog May 2022

STALKERWARE
An Acute and Pervasive Menace

STALKERWARE

In the summer of 2021 stories began to appear in the international media regarding the NSO Group's Pegasus spyware. While the invasive capabilities of Pegasus had long been known and its deployment by governments against dissidents suspected since at least 2016 (Marczak and Scott-Railton 5) it wasn't until the summer of 2021 that the prevalence and severity of Pegasus began to be widely reported on. On July 18th, 2021 The Washington Post in conjunction with 16 media partners released a report indicating that at least 37 smartphones "belonging to journalists, human rights activists, business executives and two women close to murdered Saudi journalist Jamal Khashoggi" had been infected with Pegasus spyware, believed to have been surreptitiously placed there by governmental customers of the NSO Group. Pegasus spyware allows for capturing and copying recordings from smartphone cameras and microphones, collecting location data and communication logs (Priest, Timberg and Mekhennet). For the international community these revelations signify a threat to individual digital dignity, civil rights and privacy. For victims of intimate partner violence (IPV), however, the sinister and invasive capabilities of spyware similar in nature to Pegasus has been a prevalent and acute threat for years in the form of "stalkerware".

Stalkerware is a subset of spyware, often performing the same covert functions but for the specific purposes of harassing and/or psychologically, physically or emotionally harming an intimate partner (Parsons et al. 18). According to Han et. al what makes stalkerware a special case of spyware is that the data that is collected from a victim's device is that that data is often "weaponize(ed)…to perpetrate further abuse," (2). For the purposes of this paper "stalkerware" will refer to spyware which is marketed as a tool for intimate partner surveillance (IPS) or has been verifiably utilized for that purpose; it will also refer solely to mobile phone-oriented Stalkerware apps unless otherwise noted. It is further important to note that this report will not be focusing on proprietary pre-loaded apps such as Apple's "Find my iPhone"; while these apps can certainly provide a means of IPS the focus of this report will be on third-party apps installed by an abuser on a victim's phone.

Stalkerware tools have become prevalent over the last several years and do not require sophisticated technical knowledge to utilize; they can be downloaded as any other mobile phone app and provide either in-app or web-based guides for operation (and often circumvention of mobile phone security features). Stalkerware's ease of installation and use are a significant factor in the pervasiveness of stalkerware in IPS and this is augmented by many stalkerware apps (particularly on Android OS) offering the ability to function without any

indications that they are running or even that they exist on a mobile device. Robust privacy regulations such as GDPR in the EU or the upcoming California Consumer Privacy Act (CCPA) in California exist to hold organizations responsible for the breach of an individual's digital privacy, but often perpetrators of cyberstalking are not subject to specific criminal charges relating to their cyberstalking; instead they are often charged with more legally familiar crimes related to traditional stalking. While a holistic approach to addressing stalkerware is needed to effectively combat the threat, legislation, law enforcement and prosecution of stalkerware-related crimes can be slow to materialize and difficult to enforce consistently. The critical components to addressing stalkerware should focus on both the front-line organizations and personnel that provide support to survivors of IPV and the tech companies that facilitate the distribution and functionality of these stalkerware apps.

In 2014 National Public Radio surveyed 72 domestic violence shelters in the United States and observed that 85% of domestic violence workers reported that they had assisted victims whom had been tracked by GPS. A 2015 article by University of Maryland School of Law scholar Danielle Keats Citron) cited a study by the National Network to End Domestic Violence that reported in 2012 that 54% of abusers in the United States tracked survivor's cell phones with stalking apps (1251). Australia's Domestic Violence Resources Centre Victoria reported in 2013 that a survey that they had conducted had found that 74% of those domestic abuse practitioners who responded reported that they had observed "tracking via applications" as occurring "often" amongst those victims whom they encountered (Parsons et al. 13). While these numbers are alarming, it is important to note that due to the covert nature of stalkerware, it is impossible to form a complete picture of the prevalence of stalkerware on IPS victim's mobile devices. The consequences of stalkerware in IPS can be profound and in at least three cases the stalkerware-enabled tracking has led to direct physical confrontation by an abuser, and in at least one case has led to the murder of an abuser's wife and two children (Keats Citron 16). Even in the absence of direct confrontation with an abuser facilitated by stalkerware, the simple knowledge by a victim of IPS of the level of control and surveillance by an abuser utilizing stalkerware can "present a reality where the perpetrator is omnipresent and deepen the victim's sense of isolation, fear and anxiety in everyday activities. Notably, this control can also severely undermine prospects for victim-survivors to seek outside help or support without additional fear of repercussion, often which includes threats and physical violence," (Parsons et al. 24).

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

Physical tracking of an IPS target is not the only capability of stalkerware apps. According to R. Chatterjee et al. several stalkerware apps also allow for remote activation of cameras and microphones and covert access to all communications (441). In the case of the stalkerware app known as "Cerberus", abusers were able to send spoofed text messages from the victim's phone number and remotely wipe and reboot the victim's phone (Harkin and Molnar 859). A 2019 study conducted by The Citizen Lab focused on the recording, access and monitoring capabilities of seven commercially available stalkerware applications (Cerberus, FlexiSPY, Highster Mobile, Hoverwatch, Mobistealth, mSpy, Teensafe and The TruthSpy) examined the capabilities of each app in regards to phone calls, SMS, Chat Apps, Phone Logs, Social Media, Stored Media, Web Traffic, Email, GPS, Contacts, Calendar, Keystrokes, Activate Microphone, Take Photos, Remote Access/Update, Block Phone Calls and Backup Data on Android devices. The findings were that while none of the stalkerware was capable of all of these actions, all were capable of at least two and FlexiSPY was capable of 13 (Parsons et al. 20-21).

Victims of stalkerware are also vulnerable to "secondary victimization", where the data that is collected is at risk of being accessed by unauthorized parties other than the abuser due to suboptimal cybersecurity configurations implemented by the stalkerware developers (Parsons et al. 56-57). The particularly sensitive data collected by these stalkerware apps means this data is highly sought after by cybercriminals, and the nature of many of the stalkerware developers' terms of service and privacy protocols are written in such a way they only the customer (more than often the abuser) is notified of data breaches (Parsons et al. 89). The updating protocols of the stalkerware apps present particularly significant cybersecurity vulnerabilities, with a Citizen Lab study indicating that of the 5 stalkerware apps examined (Cerberus, TheTruthSpy, mSpy, FlexiSPY and Hoverwatch) finding that update protocols are usually not sufficiently encrypted or protected, allowing for the possibility of "man-in-the-middle" attacks by motivated cybercriminals (Parsons et al. 56-57). Compounding this issue is the fact that stalkeware victims are generally unaware of the information being collected, and of the stalkerware developers that state their breach notification and data collection/security policies, they are focused solely on the customer (who is generally the abuser) and not the stalkerware victim (Parsons et al. 89). The Citizen Lab study cites Vice's Motherboard website as a source for a story involving two "hacktivists" breaching stalkerware developers FlexiSpy and Retina-X and finding customer account information, GPS locations of surveillance victims and photos and communications from the victim's phones (Cox and Franceschi-Bicchierai). While this information is difficult to substantiate independently, it is not difficult to imagine such breaches are a very real possibility as it pertains to the insufficient cybersecurity of stalkerware developers. Of similar concern is the fear that the stalkerware developers are improperly selling

or distributing the information to third-parties; in 2021 the FTC banned stalkerware provider Support King LLC and its CEO Scott Zuckerman from the surveillance market after an investigation into allegations that the company "…secretly harvested and shared data on people's physical movements, phone use, and online activities," (FTC).

In the case of Pegasus spyware it is alleged that the spyware was installed on the victims' phones remotely; this is too sophisticated for the average abuser with unsophisticated technical knowledge and beyond the technological capabilities of the apps themselves unless the victims phone is "rooted" or "jailbroken" as certain permissions need to be granted on the phone itself following installation (Amnesty 6, Chatterjee et al.448). Most often the case is that the stalkerware is installed on the victim's device by an abuser who is defined by Freed et al. as a "UI-bound adversary", meaning an "…authenticated user that interacts with a victim's device or account via standard user interfaces" (Freed et al. 1). This is often the case as abusers are often the legal owners of victims' phones and have access to them, allowing them the legal right and physical opportunity to install the stalkerware as they would any benign app from the app store (Freed et al. 4). Once the stalkerware is installed on a victim's phone via direct access and appropriate permissions are given, its icon can be hidden and its operations made undetectable from that point (particularly on Android devices, as will be explored later in this paper) (Chatterjee et al. 449). Depending on the particular stalkerware the abuser can then gain access to the information that is extracted from the victim's phone via a companion app downloaded to their phone or by accessing the stalkerware company's servers where the data is stored (Chatterjee et al. 449). Depending on the particular stalkerware control of a victim's device is often instigated through a stalkerware company's web portal or via sending an SMS text message to the victim's phone via a sent SMS message containing a keyword (the stalkerware can be configured to customize the keyword to something seemingly innocuous or to hide the notification of having received an SMS) (Chatterjee et al. 449). Further simplifying the process of compromising the mobile device of a victim with stalkerware some stalkerware companies such as FlexiSpy advertise the direct sale of mobile devices already pre-loaded with optimally configured stalkerware, including both "rooted" Android devices and "jailbroken" iPhone devices, allowing for greater invasive capabilities (Chatterjee et al. 448).

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

Stalkerware apps are significantly more effective when loaded onto a mobile device running the Android operating system as opposed to an iPhone running iOS (Harkin and Molnar 851). There are a variety of reasons for this disproportionate performance of stalkerware on the two different operating systems, largely owing to the Android OS being designed to facilitate a more "open" environment, while the Apple iOS is designed to facilitate a more "closed environment" (Harkin and Molnar 851). According to the Open Handset Alliance (OHA), a group of 84 technology experts who were involved in the development of the Android OS, this openness "(enables) everyone in our industry to innovate more rapidly and respond better to consumer's demands" (Harkin and Molnar 864). This greater openness allows for Android users to install third-party apps directly from the web without going through the proprietary Google Play app store (known as "sideloaded apps"), this circumventing any protections and verifications offered by the app store, and allows many third-party apps significantly more permissions to important components of the mobile device (Harkin and Molnar 859). These functionalities can be used to hide app icons, transmit information without notification, and circumvent ongoing and persistent notifications of suspicious behavior (Harkin and Molnar 865). The operating system of Android is open-source, allowing any interested party the ability to understand (and conversely manipulate) the security protections built into the design (Harkin and Molnar 865). In contrast Apple's iOS is designed as a "closed" operating system; it is impossible top hide an app icon once it is installed (with the closest alternative being to put it in a "drawer"), it is impossible to download apps from third-parties, it is designed to limit permissions to certain phone components, and it is designed to require persistent notification of "suspicious" behavior (Harkin and Molnar 859). Harkin and Molnar exemplified this difference in functionality by installing Trackview stalkerware on both iOS and and Android devices. On the iOS device, despite granting initial access to GPS data, the phone would send periodic reminders that the app was tracking the data with no way to turn them off; this is in contrast to the same app that was run on an Android OS device. In this instance the researchers were able to configure the phone to not send similar notifications (859). As mentioned previously, stalkerware functionality can be augmented by "rooting" an Android phone or "jailbreaking" an iPhone; technical processes that allow the owner of the phone to circumvent protections built into the operating systems and have greater control (Harkin and Molnar 860). While a jailbroken iPhone is able to run many stalkerware apps with the same functionality of a non-rooted Android phone, the process and continuing maintenance for jailbreaking an iPhone is technologically complicated and relies on a number of factors, such as running an outdated version of iOS (Harkin and Molnar 860).

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

For these reasons two of the major studies on the stalkerware ecosystem, Chatterjee et al. and Parsons et al., focus exclusively on stalkerware run on Androids while only briefly exploring the functionality of their counterparts on iPhones, although these studies do investigate the marketing of these apps to iOS users and the prevalence of these apps on the Apple App Store, which will be covered later in the paper. There are two important caveats to this discrepancy in stalkerware functionality on the two operating systems: iOS is not an inherently secure operating system. It is vulnerable to "iCloud capture", in which a perpetrator with the victim's iCloud username and password can extract large amounts of data from their phones remotely (Harkin and Molnar 860). It is important to note as well that the Pegasus spyware was remotely loaded into and functioned on non-jailbroken iPhones running iOS (Amnesty International 6). The second caveat is that the greater stalkerware capabilities on the Android OS are not the result of carelessness or lack of foresight on the part of Andoird developers; they are merely an unfortunate consequence of conscious design decisions that enable Android OS users greater customization and control of their mobile devices as opposed to adhering to the proprietary pre-rendered options of Apple devices. The purpose of this section is not to paint the Android OS as "deficient" as it provides its own benefits to the dignity, privacy and human rights of its users; for instance, Chinese dissidents are able to utilize Android devices to install VPNs and circumvent governmental control of the internet, which is not an option for Chinese Apple users (Harkin and Molnar 869).

Proprietary and third-party tools and policies for blocking, detecting and deleting stalkerware on mobile devices exist and are at least reasonably effective. A study by The Citizen Lab indicated that Google Play Protect, which is a proprietary Android process paired with Google Play, scans any apps before they are sideloaded into an Android phone and blocks their installation if they are flagged as malicious (Parsons et al. 56). The study found that in an attempt to sideload 4 stalkerware apps (including an older and newer version of the same app called TheTruthSpy) on an Android phone Google Play Protect is extremely effective, blocking all but the Cerberus app and the newest version of TheTruthSpy app (Parsons et al. 57). Upon repeating the experiment a few days later, the newest version of TheTruthSpy was blocked as well (Parsons et al. 57). The researchers indicated that they believe the only reason Cerberus wasn't blocked was because a version of it legitimately existed on the Google Play Store, unlike the other apps (Parsons et al. 58). While these are promising results, there is cause for concern; Google Play Protect can be turned off by the phone's user, which would allow any sideloaded apps to be installed on the phone. Were an abuser to have physical control of the victim's phone during the installation of the app (which is likely), they would be able to disable Google Play Protect (Parsons et al 56). This is somewhat mitigated by the fact that when Google Play Protect is reactivated, it scans the phone and notifies the user of the malicious sideloaded apps.

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

This is a significant and effective protocol, as it can alert the victim that they are being cyberstalked, detail exactly which apps are responsible, and instead of just deleting the app Google Play Protects leaves the option up the victim as deleting a stalkerware app carries significant risk of elevating the threat from their abuser (Parsons et al 56). The fact that the newest version of The TruthSpy wasn't initially detected is also of importance and indicated to researchers that by making insignificant changes to an app, they can reintroduce it to the customer in a way that it will be usable for a few days before Google Play Protect begins to recognize it as malicious; this seemed to be confirmed by a post on FlexiSPY's technical support website (Parsons et al. 46). Commercial antivirus products claiming the ability to detect spyware offered more of a mixed bag of results. Chatterjee et al. conducted an experiment wherein they utilized the antivirus aggregator VirusTotal and found that of the 60 antivirus engines examining 280 on-store apps and 23 off-store apps, only 8% of the on-store apps were flagged by at least three antivirus engines. The results were more promising for off-store (sideloaded apps) as most of the antivirus engines flagged the majority of the off-store apps, with one catching all of them (Chatterjee et al. 452) . The Citizen Lab ran a similar experiment with VirusTotal utilizing only off-store apps, where they compared the .apk files for stalkerware applications with previous VirusTotal data. Their findings were that all products were detected by anywhere from six to 34 security products (a 22.1% chance of detection), and that only three of the antivirus programs were able to detect four of the five examined stalkerware apps (Parsons et al. 54).

Stalkerware developers often market their products for more benign and legitimate purposes than overt stalking (Harkin and Molnar 869). These are referred to as "dual-use" apps and are presented as tools for monitoring children, locating lost or stolen mobile devices, or employee monitoring (Harkin and Molnar 869). According to Chatterjee et al. despite claims from stalkerware developers of benign purpose, many manipulate or legitimately utilize advertising and search engine optimization algorithms to ensure that there are suggested when users search for overt stalking terms, such as "spy on my spouse" or "read my boyfriend's text messages" (441). In one particularly egregious example of a stalkerware company surreptitiously promoting the stalking capabilities of their product, mSpy was found to have encoded concealed HTML text which advertised spousal spying on their website, which would make it so it was not observable by those viewing the website, but those terms would be considered by search engines (Parsons et al. 58) Chatterjee et al. also indicates that many of these companies do not offer any support or information for people who suspect they are victims of their stalkerware, and when customer service is contacted for that purpose they are generally ignored or given unhelpful advice (451).

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

The same study also indicated that when contacting a select group of 12 dual-use stalkerware companies which had displayed advertisements on IPS related search terms to explicitly ask if the program could be used for covert surveillance of a spouse, only one company (TeenSafe) admonished the researchers, 2 of the companies did not respond while 8 companies responded with a version of "no, they won't be able to tell". While many off-store (sideloaded) stalkerware apps are more direct about advertising their products as overt spyware, those that wish to function on the Google Play Store are careful to hide the capabilities of their products (but are not afraid to covertly advertise them as stalkerware and provide support to abusers who are looking to surveil an intimate partner) (Chatterjee et al. 450).

As noted earlier the FTC has recently taken action against a stalkerware developer, which could serve as an important milestone in the battle against stalkerware; more likely it will not as the FTC was investigating the company's improper handling of data rather then the capabilities and implications of its product. While lawmakers and law enforcement are critical components to combatting stalkerware, legislation is slow and uncertain and can not be counted on to rectify the problem. While the NSO Group has suffered sanctions and investigations into their deployment of Pegasus spyware this will do little to help IPS victims who are currently under stalkerware surveillance or at risk of becoming so. The critical approach to combatting stalkerware is to take a bottom-up approach and to spread detection awareness to those are victimized or likely to be victimized. It is also necessary to train and give resources to entities and individuals who provide assistance and support to intimate partner violence victims so that they can utilize their specialized support training in conjunction with low-level stalkerware detection and eradication techniques and do so in a way that will maximize the safety and security of the victims. Of similar importance is the interplay between these organizations and cybersecurity professionals and tech companies who have proven to be responsive and open to listening to and adapting to the suggestions of security researchers involved in stalkerware research (particularly Google). In need of greater consideration is also the societal normalization of surveillance apps ostensibly for the purposes of child safety or employee efficiency. While it is impossible to argue that these are important and effective use cases, there needs to be greater consideration by the public about the potentially catastrophic trade-off in terms of privacy that these apps can present.

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

Awareness of the cyberstalking threat by victims and potential victims is the initial component of a successful anti-stalkerware initiative. Not only should IPS victims know of some of the telltale signs of stalkerware technology being present on their mobile devices such as unusual battery drain, slow responsiveness or spikes in bandwidth usage (Chatterjee et al 451), they should also be made aware of how to check for the stalkerware and confirm its presence, or at least be aware of options as to where to go to have their device examined. Even if an individual does not notice any of the technical signs of potential stalkerware infection, being aware of the pervasiveness of stalkerware could prove to be the impetus that prompts victims to check their devices for stalkerware. As was explored earlier in this paper Google Play Protect provides highly effective detection and response to stalkerware applications that have been sideloaded onto an Android phone. Knowing how to check if Google Play Protect has been disabled (another potential indicator of stalkerware infection) and reactivate that protection would allow a victim of IPS to confirm and chronicle the use of stalkerware for later use in court and to eliminate the stalkerware from the from if that is the decision they make. In some cases the confirmation that stalkerware had been loaded onto their phone could serve as an important step for an IPS victim as victims who suspect the presence of stalkerware but are unable to confirm it can become isolated and self-doubting from wondering whether they are paranoid or not (Harkin and Molnar 854). It may be in many cases that victims of IPS believe that investigating or eradicating their phones in regards to stalkerware is a technologically advanced and intensive activity; as we have seen earlier in the paper this is not the case. Raising awareness towards the threat and prevalence of stalkerware, as well as detection and removal tactics (with a caveat regarding removal protocol that will be explored later) would go a long way towards empowering victims of IPS to taking concrete steps to investigate and confirm their situation and give them options to act.

Awareness among response and support organizations related to IPV survivors is a significantly important component of combatting stalkerware as well. IPV and IPS are inherently nuanced and complicated and there is no one-size-fits-all approach to addressing it or extracting victims. Response and support organizations such as shelters need to take into account a number of different factors when assisting a victim of IPV so as not to exacerbate or worsen the threat that they face, and their specialized training and experience can help to address some of the residual risk around detecting and removing stalkerware from an IPS victim's phone and allow them to better triage and effectively care for and protect IPS victims based on knowledge of what type of phone they have, whether they have Google Play Protect enabled, and what (if any) technical signs they have seen to indicate stalkerware infection.

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

As an example, an IPS trained professional could be made aware that the operating system utilized by an IPS victim is susceptible to GPS tracking and remote camera and microphone activation. This knowledge could inform assistance protocol, such as meeting at a secondary location and having the IPS victim leave their phone outside, or speak in coded language so as to not elevate the threat that the IPS victim faces by seeking assistance.

Cybersecurity professionals and researchers critical component of the stalkerware detection and eradication process by providing the technical means of these properties. However, it is important to note that many cybersecurity professionals may just see the problem in technical terms and lack the training and understanding to deal with the stalkerware in a way that is safe for the IPS victim (Freed et al. 15). Simply deleting the stalkerware app could place the IPS victim in greater danger, as the abuser's actions could elevate due to their knowledge that they have been discovered. Cybersecurity professionals can certainly help to raise awareness of the stalkerware problem, but may lack the nuanced understanding of the treatment, as many IPV victims still live with their abusers (Freed et al 15).

It is easy to say that "raising awareness" is an important priority for dealing with stalkerware, but difficult to put into meaningful action. As such it is important for federal, state, local, territorial and tribal governments to allocate resources into awareness and advertisement campaigns similar to those that exist for drunk driving. While the effectiveness of that particular campaign may be disputed, it is dissimilar to stalkerware in that it is informing the public of the consequences of an already understood phenomenon, as opposed to raising awareness for one that it not well understood or even known. This awareness campaign should be augmented by these governmental bodies forming committees composed of cybersecurity professionals, law enforcement, and abuse support entities so that each party can bring their expertise to the table and establish safe and efficient means of combating stalkerware. Support organizations should furthermore be incentivized to form ISAC or ISAO-like entities that allow for the free flow of information regarding threats and best practices.

It is important to note that in Chatterjee et al.'s report they indicated that they had contacted Google with their findings and found that Google had responded by limiting advertisement terms relating to stalkerware and removed some of the offending on-store apps from their app store.

John Ward – Cyberblog May 2022

STALKER WARE
An Acute and Pervasive Menace

This is a promising development and should be exploited in a systematic way, as opposed to waiting for independent studies to be conducted and submitted to Google. Google has the resources to conduct or commission these studies on their own and should be incentivized to conduct them at regular intervals and act on their findings. It would also be beneficial for the committees mentioned in the paragraph above to maintain communication with Google and similar companies so that they can share their experiences and findings in the hope of forcing change.

The purpose of these recommendations is not to discount the importance of legislative, federal and industry involvement in addressing the problem of stalkerware; these entities play a vital part. These recommendations are a recognition that the nature of the stalkerware problem presents real and potentially deadly acute threats to people on the ground and immediate action needs to be taken in their defense as opposed to waiting for significant action from top-down. Stakeholders at all levels need to work with government, lawmakers and CEOs to drive home the importance of addressing the stalkerware problem head-on but cannot afford to be inactive while doing so.

Works Cited

Chatterjee, Rahul, et al. “The Spyware Used in Intimate Partner Violence.” *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 441–458., https://doi.org/10.1109/sp.2018.00061.

Citron, Danielle Keats. “Spying Inc..” *Washington and Lee Law Review*, vol. 72, no. 3, 1 June 2015, pp. 1243–1282., https://doi.org/10.2139/ssrn.2568684.

Cox, Joseph, and Lorenzo Franceschi-Bicchierai. “'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market.” *VICE*, 19 Apr. 2017, https://www.vice.com/en/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x.

“Forensic Methodology Report: How to Catch Nso Group's Pegasus.” *Amnesty International*, 26 Apr. 2022, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

Works Cited

Freed, Diana, et al. "'A Stalker's Paradise.'" *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13., https://doi.org/10.1145/3173574.3174241.

Freed, Diana, et al. "'Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence." *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, 2019, pp. 1–24., https://doi.org/10.1145/3359304.

"FTC Finalizes Order Banning Stalkerware Provider from Spyware Business." *Federal Trade Commission*, 10 Mar. 2022, https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business.

Han, Yufei, et al. "Towards Stalkerware Detection with Precise Warnings." *Annual Computer Security Applications Conference*, 6 Dec. 2021, pp. 1–13., https://doi.org/10.1145/3485832.3485901.

Harkin, Diarmaid, and Adam Molnar. "Operating-System Design and Its Implications for Victims of Family Violence: The Comparative Threat of Smart Phone Spyware for Android versus IPhone Users." *Violence Against Women*, vol. 27, no. 6-7, 2020, pp. 851–875., https://doi.org/10.1177/1077801220923731.

Marczak, Bill, and John Scott-Railton. "The Million Dollar Dissident: NSO Group's Iphone Zero-Days Used against a UAE Human Rights Defender." *The Citizen Lab*, 23 June 2020, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Parsons, Christopher, et al. "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry." *The Citizen Lab*, 12 June 2019, https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

Works Cited

Priest, Dana, et al. "Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide." *The Washington Post*, WP Company, 19 July 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_4.

Shahani, Aarti. "Smartphones Are Used to Stalk, Control Domestic Abuse Victims." *NPR*, NPR, 15 Sept. 2014, https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

END OF BLOG