
Kirill Arbuzov

# Advanced spyware for mobile devices.

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Bachelor's Thesis

30 March 2023

## Abstract


| | |
|---|---|
| Author: | Kirill Arbuzov |
| Title: | Advanced spyware for mobile devices |
| Number of Pages: | 31 pages |
| Date: | 30 March 2023 |
| Degree: | Bachelor of Engineering |
| Degree Programme: | Information and Communication Technology |
| Professional Major: | Mobile Solutions |
| Supervisors: | Kimmo Sauren |


---


This thesis aims to investigate how advanced spyware for mobile devices are being installed, what sort of information spyware could extract and some countermeasures against it. The study will focus on spyware that is being produced legally by private security-oriented companies whose clients are various government agencies. Also the study includes analysis on who could be targeted with spyware. Lastly the study includes several suggestions on how to reduce attack surface and reduce consequences following spyware installation.

The study is done by investigating previously known victims of spyware. Because of the secretive nature of spyware producers and their clients combined with inability to access spyware, study relies completely on open-source information.

The thesis shows that spyware manufactured by offensive security companies is very advanced. Main goal of it is to be as stealthy as possible while gaining information that mass surveillance wouldn’t produce. Companies either discover or buy latest vulnerabilities in order to successfully install spyware on target's device. Despite all that there are several ways to either prevent unwanted installation of spyware or reduce harm that may be caused by gathered data.



Keywords: Spyware, Surveillance, Malware, Pegasus

# Tiivistelmä


| | |
|---|---|
| Tekijä: | Kirill Arbuzov |
| Otsikko: | Edistyneet vakoiluohjelmat mobiililaitteille |
| Sivumäärä: | 31 sivua |
| Aika: | 30 maaliskuuta 2023 |

| | |
|---|---|
| Tutkinto: | Insinööri (AMK) |
| Tutkinto-ohjelma: | Tieto- ja viestintätekniikka |
| Ammatillinen pääaine: | Mobile Solutions |
| Ohjaajat: | Kimmo Sauren |


---


Opinnäytetyön tarkoituksena on tutkia, miten mobiililaitteisiin tarkoitettuja edistyneitä vakoiluohjelmia asennetaan, sekä mitä tietoa ne pystyvät ottamaan talteen. Työssä tutkitaan vakoiluohjelmia, joita kyberturvallisuuteen erikoistuvat firmat tuotettavat laillisesti. Näiden vakoiluohjelmien käyttäjät ovat aina valtioiden turvallisuuspalvelut tai poliisit. Työssä myös tutkitaan kuka voi joutua vakoiluohjelman kohteeksi ja miten mahdollista vahinkoa voisi pienentää.

Tutkimus tehdään tutkimalla aiemmin tunnettuja vakoiluohjelmien uhreja. Koska vakoiluohjelman saaminen on melko mahdotonta sekä vakoiluohjelmien tuottajat ja heidän asiakkaidensa ovat salaperäisiä, tutkimus perustuu täysin julkisesti saatavissa oleviin tietoihin.

Opinnäytetyössä näytetään, että yksityisfirmojen luomat vakoiluohjelmat ovat erittäin edistyneitä. Niiden päätarkoituksena on mahdollisimman paljon sellaista tietoa, jota ei saa massavalvonnan avulla. Yksityisfirmat joko tai ostavat sellaisia haavoittuvuuksia, jotka mahdollistavat vakoiluohjelmien asentamisen. Tästä kaikesta huolimatta on olemassa keinoja, joilla voidaan joko kokonaan estää vakoiluohjelman asennus tai vähentää siitä aiheutuvan mahdollisen haitan.



Avainsanat: Vakoiluohjelmat, Valvonta, Haittaohjelmat, Pegasus

# Contents

## List of Abbreviations

| | |
|---|---|
| IMEI: | International Mobile station Equipment Identity. |
| IMSI: | International Mobile Subscriber Identity |
| IP: | Internet Protocol |
| KASLR: | Kernel Address Space Layout Randomization |
| RTCP: | Realtime Control Protocol |
| SRTCP: | Secure Realtime Control Protocol |
| FISA: | Foreign Intelligence Surveillance Court |
| OSI: | Open Systems Interconnection |
| TCP: | Transmission Control Protocol |
| UDP: | User Datagram Protocol |
| CDR: | Call detail record |
| NSA: | National Security Agency |
| CDR: | Call detail record |
| TAO: | Tailored Access Operations |
| OTA: | Over the air |

# 1 Introduction

Since smartphone revolution started about 15 years ago, their significance in everyday people's lives grew rapidly. It could be argued that their importance outgrew personal computers. We store more sensitive information on mobile devices such as banking applications, media, contacts, precise location information. Since the pandemic started, mobile phones were developed to work as identification for vaccination status. In future they could extend to work as standard identification document. During the pandemic, mobile phones used to track possible contaminations. Unlike personal computers, all mobile devices have several cameras and microphones, access to a precise location and other sensors like accelerometer. They tend to be almost always nearby. People who leave their houses without smartphones are suffering from condition called nomophobia – fear of being without your phone. All these characteristics made mobile devices perfect targets for surveillance industry.

The goal of research was to investigate spyware installation requirements, possible ways to detect spyware, and some practices to avoid and reduce impact of installed spyware.

The result shows that spyware is thoroughly designed advanced piece of software that has same characteristics as other applications like updates. From installation process to data gathering to possible uninstallation it is designed above all to be as stealthy as possible. Not only is it very hard to detect, it is also hard to prevent from installing as even most recent operational systems aren't safe.

# 2 Surveillance in mobile devices

Surveillance in the context of mobile devices and overall in technology can be divided into two sub-categories: mass surveillance and targeted surveillance.

## 2.1 Mass surveillance

Mass surveillance includes gathering, saving, analyzing & searching large amount of metadata produced by mobile devices. Metadata contains information about data, but not the content of data itself. In modern mobile devices metadata can be divided into telephony & Internet Protocol metadata.

According to United States Foreign Intelligence Surveillance Court (FISA) “metadata includes originating and terminating telephone number, mobile phone’s unique International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI), trunk identifier, telephone calling card numbers, time and duration of the call and cell site location data, location of cell tower with loudest (strongest) signal”. Signal strength is defined by cell tower and mobile device trusts. Metadata however does not contain content of a call or subscriber or customer name, address, financial information. [1, 2]

Internet Protocol (IP) metadata contains “access providers on each end of the communications, transport operators, core network operators, and providers of services”. Furthermore, browser’s cookies can contain large number of metadata, such as user preferences & settings, browsing activity, unique advertisement id. [1]

Even though metadata does not contain content of communication itself and may seem on surface less invasive, according to Edward W. Felten, a Professor of Computer Science and Public Affairs at Princeton University it can produce far better analysis that content of communication itself. [3]

The main reason for that is structure of metadata. People can speak different languages or use street slangs or even codewords that can be quite difficult to understand for people, let alone computers. Metadata is different. The structure of metadata makes it easy for computer to store and analyze it, especially combined with advanced link analysis programs. Advanced algorithms together with large datasets can reveal embedded patterns and relationships, including personal details. Metadata can reveal extraordinary amount of information.

Calling patterns can expose, based on phone's activity, when we are awake and sleep, religion based on activity on religious holidays, number of friends, sexual orientation, dating partner. Even people's social status can be determined with calling patterns. Per Economist: "People at the top of the office or social pecking order often receive quick call-backs, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organized (sic), such as Friday afternoons". [4]

Algorithms can analyze behavior based on CRDs and location information such as who target calls when he arrives, who else is in area at the time of target's arrival and who is leaving shortly after targets arrival. Who is travelling with target, who is travelling on specific days and what is pattern of travelling. Who is travelling to city A and immediately to city B.

Algorithms support behavioral profiling. Based on statistics they can profile standard behavior in certain region. They can also profile abnormal or suspicious behavior models for example, how courier tends to behave. Any deviation from standard behavior can be considered unusual. Unusual behavior includes for instance low use of mobile device or using it only for incoming calls, frequent SIM or device swapping or frequent power-off.

As figure 1 demonstrates, devices used by Al-Qaeda's Senior Leadership have more connections to unique cell sites than typically is seen in Pakistan. Reason for that is abnormal travel frequency, which is suspicious behavior. [5]

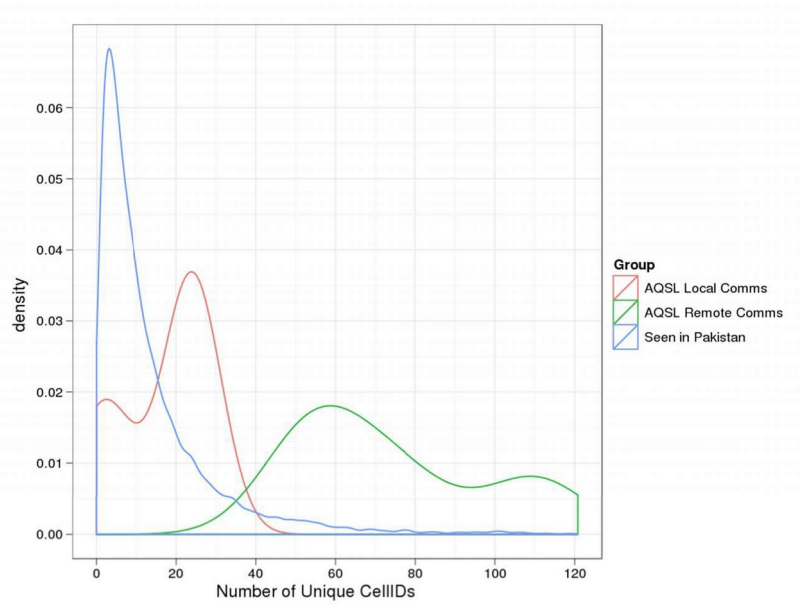


Figure 1. Amount of unique Cell Ids connections based on group. [5]

Another characteristic for mass surveillance is its low cost. For example, in United States CDR gathering program cost 100 million over three years. Adjusted for population, that's 10 dollars per person per year. [6]

## 2.2 Targeted surveillance

Unlike mass surveillance, that targets indiscriminately, is done automatically and is limited to metadata, targeted surveillance requires specific target, a name or an organization. It's not limited only to metadata, but includes actual content of private information, for example, content of phone call. This sort of surveillance is costly and is done against individuals who could be perceived threat to a state. [7]

### 2.2.1 Advanced spyware

In this study, "advanced spyware" term will be limited to a software that is legally manufactured by security-oriented companies. Those sorts of companies, like Italian "HackingTeam" or Israeli "NSO-Group" provide offensive security tools to government agencies across the world. Even though it is

software, some of spyware could be defined as weapons, requiring export license.

Besides spyware itself, they are

constantly researching vulnerabilities that would allow installation and functioning of spyware. Vulnerabilities could be also sold to private vendors like “Zerodium”, a broker that specializes on exclusive exploitations. While vulnerabilities also could be reported to product manufacturer and they tend to reward for them, private brokers offer higher reward, making it fiscally more attractive for individuals to sell them. [8]

Targets of such sophisticated spyware are meant to be dangerous criminals wanted by authorities. There is however, worrying trend, where government agencies have targeted journalists, human rights activists, judges, politicians, businessmen with sophisticated spyware. Because of the secretive nature of offensive security, there’s limited information about targets. One common dominator is that targets tend to pose threat to government. [7]

# 3 Installation of spyware

## 3.1 Vulnerabilities

Spyware installation, regardless of method, requires Operation System and sometimes software vulnerability. Software vulnerabilities are flaws that can cause undesired behavior of program, triggered by user or exploited. Software vulnerability, also known as bugs, can be related to performance, functionality or security. Once security related vulnerability is exploited, it can result to violation of security policies. [9, 10]

In the context of mobile spyware, zero-day vulnerabilities play key role. Zero-day software vulnerability means that zero days has passed since developer of said software has released patch to fix vulnerability. Very often developers are not even aware of the existence of these vulnerabilities. What worsens the

situation is those vulnerabilities are very expensive and private brokers, depending on vulnerability, are willing to pay millions of dollars. That encourages to sell vulnerability to brokers rather that report it to developers. [11]

### 3.1.1 Case study Trident

Trident (tri – thee & dentis- teeth) is a Greek god's Poseidon. Trident vulnerability consists of three smaller vulnerabilities that together combined have been used to remotely install Pegasus spyware on smartphone running iOS 9.3.3.

First part of Trident is Safari WebKit memory corruption vulnerability (CVE-2016-4657) that allows to execute JavaScript code outside of an iPhone's safari web browser's sandbox.

Second step is about finding kernel. Kernels are written in unsafe languages and therefore tend to offer large attack surface. One of solutions to secure kernel is address space layout randomization. Every time device is turned on, Kernel Address Space Layout Randomization (KASLR) assigns kernel to different address. Spyware installation requires kernel location. Vulnerability (CVE-2016-4657) leaks information that allows attacker to calculate kernel's location. After kernel has been located, spyware disables security features like code signing & removes browser's caches to cover tracks. Final steps are remounting system partition, writing spyware files to location /sbin/mount_nfs and removing configuration file /etc/nfs.conf. That will trigger OS to run /sbin/mount_nfs that contains spyware as root, with full privileges.

The last vulnerability (CVE-2016-4657) is gaining persistence so spyware will be turned on when booting. Spyware will check what version of iOS device is running. Depending on version there is a different method of installation. The priority is to prevent device from bricking. [12]

### 3.1.2 Case study NSO WhatsApp zero-click attack

Whenever the program runs, it needs memory to store data and sometimes it needs to copy data from one place to other. Typical C program memory is divided in five segments: text, data, BSS, heap & stack. WhatsApp vulnerability is related to VOIP stack. The stack is used for storing variables defined in functions & for storing data related to function calls.

Buffer overflow happens during data copying from source to destination. If program didn't allocate enough space for destination before copying data, that would cause buffer overflow. Some programming languages live Java can detect buffer overflow, while languages like C & C++ won't be able to detect buffer overflow. WhatsApp implemented SRTCP in C/C++, instead of Java. Buffer overflow may cause program to crash, however in certain circumstances it can allow to execute code. If program is running with privileges, attacker may be able to perform privilege escalation. [13]

In May 2019 WhatsApp has announced vulnerability (CVE-2019-3568) that allowed remote code execution via Realtime Control Protocol packets sent to target's phone. WhatsApp patched buffer overflow vulnerability by adding two size checkers that would check length of arguments against maximum allowed size of 1480 bytes.

Figure 2 shows the first size checker that was added at start of RTCP handler function. It would check against maximum size of 1480 bytes or 0x5C8 in hexadecimal number. Figure 3 shows additional length validation that the packet's length field doesn't exceed the length, right before a memory copy.

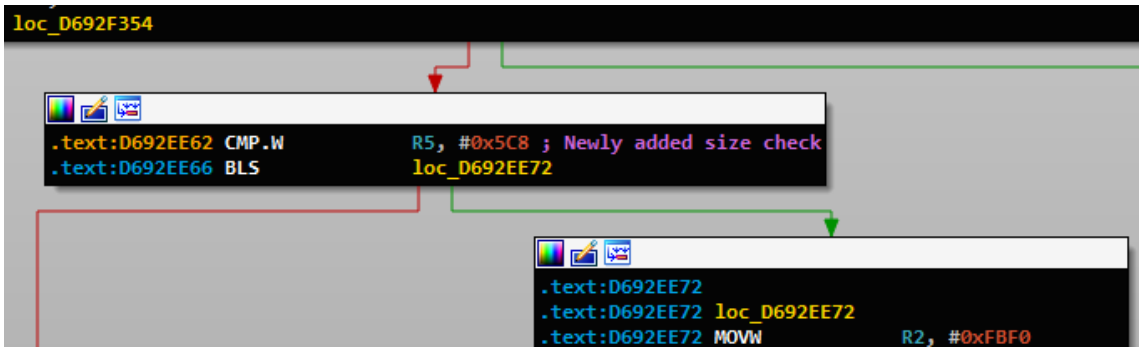

Figure 2. Added function checks that length argument doesn't exceed 1480 bytes (0x5C8). [14]

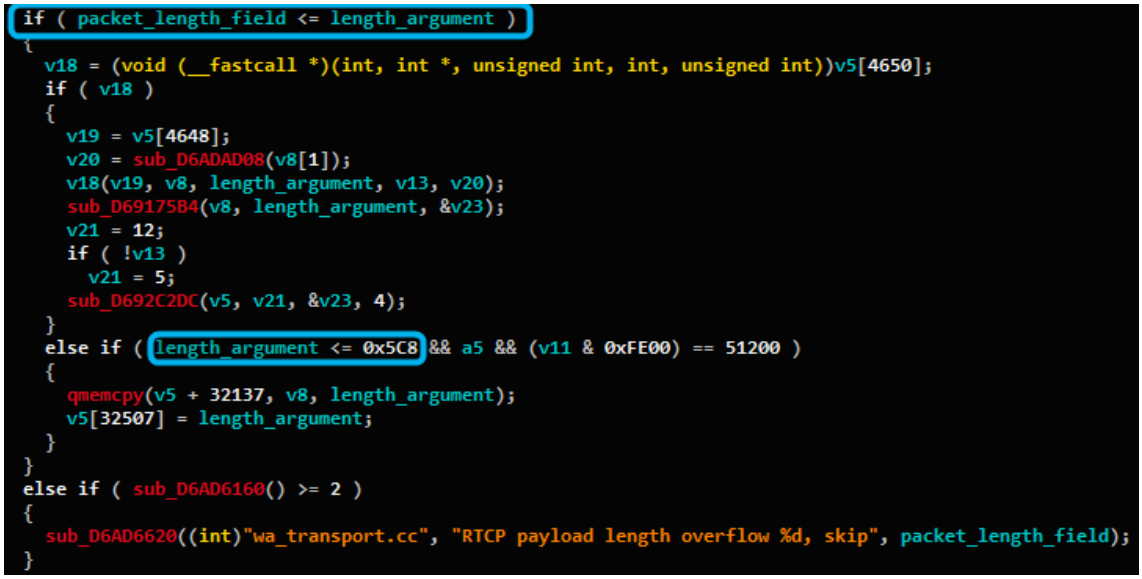


Figure 3. Additional length validation.

That function would trigger before and regardless of whether receiver would answer the call, making it zero-click vulnerability.

WhatsApp has publicly called out NSO group for using vulnerability against more than 1400 phones. [14, 15]

### 3.1.3 Case study iOS Forced Entry

Forced entry vulnerability CVE-2021-30860 was first discovered when unnamed Saudi activist had a suspicion that his iPhone was infected with malware and sent backup of iOS to Citizen lab. Further analysis, together with Apple, has yielded several files with .gif extension that were sent prior to being hacked by spyware.

The initial entry point for spyware on iPhone was iMessage application. iMessage had support for GIF animated images, however Apple wanted to make these animations loop continuedly, instead of only once. This was

achieved by rendering received file to a completely new GIF file using CoreGraphics API.

Coincidently CoreGraphics is also responsible for decoding PDF files. Mostly it is proprietary software managed by Apple, however it is implementing JBIG2 image codec designed to compress image. JBIG2 is opensource and therefore source code for it is available.

Just because a file has .gif extension, doesn't necessary mean that it is in fact a GIF image. NSO group used PDF file with .gif extension targeting vulnerability in Core-Graphics PDF parser. [16, 17]

## 3.2 Installation vectors

Installation of spyware is the most critical part of intelligence operation conducted on targets mobile device. Vulnerabilities can cost millions of dollars and single installation of spyware costs tens of thousands of dollars. Targets of such sophisticated spyware must be high value. Very often they're conscious that they could be a target of government agencies, or at least paranoid enough to be on guard. For these reasons installation must be planned carefully and tailored to the target. [17]

### 3.2.1 Remote installation

Remote installation allows to install spyware on target's device remotely and without limitations to the range. It can be done even from another country. There are two main methods of remote installation: Over-the-Air and Enhanced Social Engineering Message. Sometimes they're referred as "zero-click" and "single-click" installation methods.

Enhanced Social Engineering Message or more commonly referred as "single-click", requires for client to send hyperlink to targets device via any messaging or email application and for target to click on that link. After clicking that link, spyware will begin installation unbeknownst to the target and cannot be

stopped. Success ratio of target clicking that hyperlink is crucial part on process, therefore, content of message must appeal to target. [18]

Example of such installation vector is case Ahmed Mansoor - human right's activist based in United Arab Emirates. Mansoor has been on government's radar and has been jailed for supporting pro-democracy petition.

Figure 4 demonstrates SMS message with hyperlink that would trigger installation of spyware. Message was tailored in such way that human right advocate would be interested in it. Because Mansoor had trouble with government and in fact has been previously hacked, he did not click on it. Instead, he sent backup of his iOS to Citizenlab for analysis.


Figure 4. Tailored SMS messages sent to Mansoor: "New secrets about torture of Emiratis in state prisons". [18]

Figure 5 illustrates request made during spyware installation process, after clicking malicious hyperlink. Spyware was intentionally triggered to install in order to study it's abilities.

Figure 5. Requests made after following malicious link. [18]

Another case of single-click spyware being used is Rafael Cabrera, a Mexican journalist who has been reporting on Casa Blanca controversy that implicated Mexico’s president Peña Nieto's family.

On August 2015 Rafael posted tweet about receiving SMS message impersonating Mexican Uno TV channel with shortened Bitly hyperlink. Message included direct reference to the story that he wrote. While link was unactive, it did lead to domain names that were linked to NSO Group infrastructure. Also, director of Uno TV publicly responded that those messages were not sent by them.

Cabrera case follows the same pattern as Mansoor’s. As seen in figure 6 Cabrera also received messages with hyperlink to install spyware and these messages were also tailored to increase probability of target clicking the link.


Figure 6. Tailored Messages purporting to come from UNO TV. [18]

Lately most advanced spyware installation services started shifting towards vectors that don't require any interaction from targets called zero-click installation. Those installation vectors are network-based attacks and over-the-air (OTA) attacks. [7]

OTA installation, such as Enhanced Social Engineering Message, involves sending a message or making a call to targets device to trigger spyware installation. However installation process does not require any action from target, like clicking link, opening message or answering a call. Also, it is not limited by range, therefore it can be installed from anywhere. Only requirement is a telephone number, or an email address tied to a target's device. Installation is also completely invisible to the target in order not to raise any suspicions, making it most advanced installation vector. [7, 19]

Example of such sophisticated attack is previously mentioned WhatsApp zero-click, zero-day exploitation that can be used to install spyware without target ever knowing about it.

### 3.2.2 Close to target installation

If a target is using mobile device that does not have a telephone number or an email tied to it, it is possible to install spyware with Close to target installation vector. Close to target vectors requires proximity to target's device or even physical access, depending on installation vector. Those vectors are Tactical Network Element and Physical vector. [19]

Tactical Network Element, or network injection attack is a remote man in the middle type of attack vector. Up until 2018 NSO-Group's clients favored remote installation with the help vulnerabilities in messenger applications.

Figure 7 illustrates network injection attack process. Instead of using additional vulnerabilities in applications, target's device can be redirected to malicious website with either dedicated special equipment like IMSI-catcher, or actual cell tower that is compromised. [20]

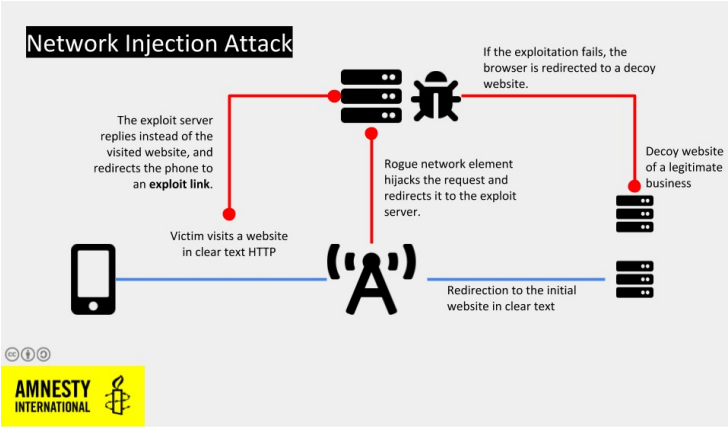


Figure 7. Diagram of network injection attack. [20]

Tactical network element installation requires proximity to target's device. Reason for that is installation vector requires tactical devices like rogue cell tower, also known as IMSI catcher or stingray.

Figure 8 shows a mobile rogue cell tower that could perform, amongst other things, network injection attack. Purpose of these sort of devices is to emulate cell tower tricking mobile devices nearby to connect to them. IMSI catchers tend

to have several modules on them that allow them to emulate multiple frequency bands like 3G, 4G etc. Once connection has been established, rogue cell tower can intercept and alter unencrypted mobile internet traffic. Network injection can happen when target is using any application that can trigger internet browser. Case in point Moroccan journalist Omar Radi who was targeted with Pegasus spyware while he was using Twitter app. While previewing link in his feed, network injection triggered Safari WebView to load malicious hyperlink, triggering installation. [19, 20]


Figure 8. Mobile rogue cell tower sold by NSO Group. [20]

Furthermore, network injection can be performed with the help of dedicated equipment placed at the mobile operator. Because clients of this sort of sophisticated spyware are government officials, they would have no problem legally accessing and deploying such methods. IMSI catchers can also work as mass surveillance method or disruption of service. [19]

### 3.2.3 Physical installation

If there is physical access to target's device, spyware "can be manually installed in less than five minutes". It would provide the same features as standard installation and would implement same method of data extraction. [19]

Physical access to device could be obtained while target is for instance crossing border or detained as the case was with Washington Post's journalist's wife Hanan Elatr. Her phone was targeted while she was in custody. [21]

Another, more covert option, is supply-chain interdiction, method favoured by United States National Security Agency (NSA). Within NSA, Office of Tailored Access Operations (TAO) would intercept network devices that were being headed to target and install malicious software or hardware. Afterwards equipment would be carefully repackaged and sent to original recipient. [22]

If mobile device were intercepted in similar scenario, spyware installation most likely be flawless. Furthermore, hijackers would gain access to unique International Mobile Equipment Identity, thus deanonymizing it before it even reaches owner.

## 3.3 Installation failure

Installation of spyware can fail for several reasons. The most probable in case of single-click installation vectors, is that target simply will not click malicious hyperlink. Targets of these attacks tend to be high value and therefore more careful. Some of them were previously targeted with spyware. This was the case with Ahmed Mansoor who instead of clicking hyperlink that he received via SMS message, turned backup of his iOS to Citizen lab for analyze.

Another cause for installation failure can be unsupported device or operational system. This is especially case with devices running Android operational systems. Apple's mobile devices are running same operational system - iOS, implementing only different versions of it. They are also using same hardware. General rule is, if one iPhone can be hacked, so can hundreds of millions of phones. The same rule does not apply to Android devices, however. Vendors of Android mobile devices can deploy different types of hardware or can have custom operational systems that are based on Android but tweaked enough for spyware not to trigger properly. Some Android based operational systems are even specifically hardened to enchase privacy & security. [11]

Lastly, regarding installation methods that implement internet browser vulnerabilities, some browsers do not share vulnerability and therefore are not supported. This is also the case that is more likely to occur with Android OS, where default internet browser can be changed. Although since iOS 14 it is also a possibility on Apple's devices. [19, 23]

# 4 Spyware features

## 4.1 Data collection

Once spyware is installed, it offers substantial amount of passive & active data collection that already existed on device of will be generated in future. In fact, it can collect more data of device that owner of compromised device. For instance, it allows voice calls to be recorded & saved. That is something that standard device will not offer due to legal reasons. Reason for that is privilege escalation that is performed during installation of spyware. In iOS devices process of acquiring elevated privileges is called Jailbreaking while on Android devices it is called Rooting – getting the same privileges as root user in Unix like systems, which Android is. [19, 24]

As figure 9 shows, spyware can collect textual, audio, visual and file & location information. Textual information can be SMS & other types of instant messages, email, calendar, call log, contact list, browsing history, favorite sites. Spyware can also monitor any changes in calendar & contact details and notify when changes are applied.


Figure 9. Data available for collection per NSO-Group's presentation. [19]

Audio information includes intercepted calls or active microphone recording, sometimes referred as "hot mic". Intercepted calls are saved on targets device and after completion sent to spyware servers. Real time microphone can be activated only when device is idle, and screen is turned off. When target turns device's screen, recording will be terminated without alerting target. Real time recording is automatically saved.

Visual information includes retrieving of photos from library, screen capture & active camera. Media files also contain metadata like date and time of photo. Furthermore, modern smartphones tend to store information of location where photo or video was taken by default. Active camera, just like with microphone, can be activated only in idle mode & without alerting target, for instance flash is disabled even if visibility is low.

Spyware can access & download documents, application databases and any other files on device that could be relevant.

Location information includes satellite positioning system information like GPS, cell tower identifier and wireless networks. In case if GPS is turned off, spyware can enable it and immediately turn it off after information is collected.

Furthermore, even if device is in airplane mode, it will still listen to any available networks nearby. [11, 19]

Spyware also collects general device information such as network & connection details and battery health. Network details are collected even if the device is in airplane mode as it is only preventing device from sending signals, not listening in. Battery information is very important as draining battery may raise suspicions. [19]

## 4.2 Data transmission

By default, spyware is sending collected data in real time, when connection is available and when battery level is above 5%. There are several instances when data transmission is either not possible or not optimal.

When transmission is not possible, spyware will collect information, encrypt, and store it in hidden location on targets device. Buffer is set to maximum of 5% of available space by default. In case of buffer reaching its limit, it will delete old information first. When network is available and data has been transmitted, buffer is cleared.

The preferred connection method is a wireless network as in many countries cellular data is charged by usage. To reduce footprint, spyware can compress data or focus on transferring only textual data via cellular network. When the device is roaming, transmission of data is done only by wireless network as roaming can be pricy and thus raise suspicions.

When internet network is not available, communication can be established and data can be extracted via SMS messages, but it is also suboptimal as SMS communication may appear in target’s billing report.

Communications are encrypted with symmetric encryption and anonymized. For anonymization, NSO-Group has implemented a network of anonymizers with nodes that are spread around the world. Although human rights organizations

such as Amnesty & Citizen lab was able to determine that some devices were communicating with NSO group related servers, end user has remained unidentified. [19]

Figure 10 shows proxy chain configuration that follows similar logic as NSO-Group's anonymized network. In this case, if client's traffic was intercepted, it would not reveal actual destination. Second and third proxy servers are not aware of source or destination, thus shielding destination's anonymity. [19, 25]

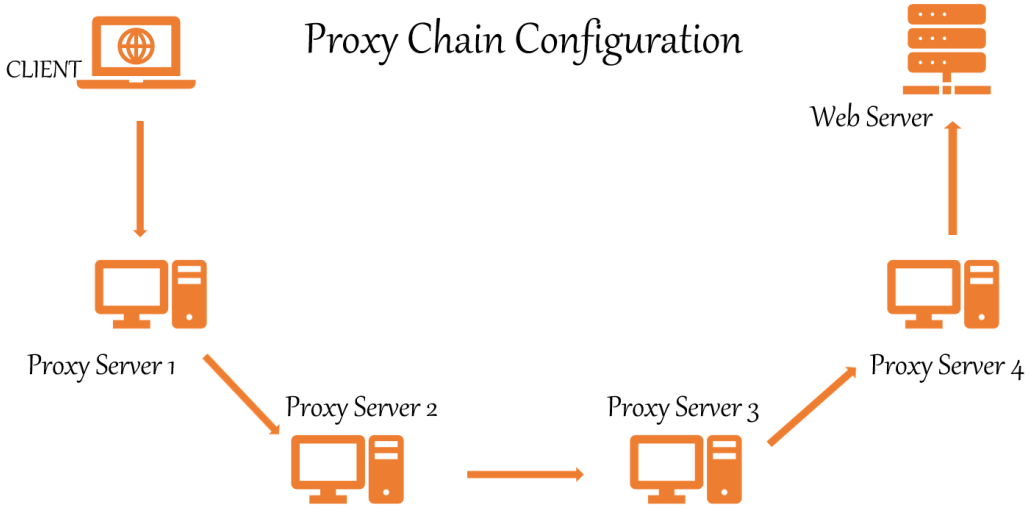


Figure 10. Diagram of proxy chain configuration. [24]

## 4.3 Data analysis

After extracting data from target's device, it needs to be analyzed and presented. For instance, if several targets are part of the same organization or type of threat, they can be grouped making it easier to monitor several targets.

Analysis includes several rules that spyware's client can define in advance for important events, that when take place, client will be alerted. Geofencing triggers alert either when target arrives or leaves certain location. Meeting detection feature can detect when two targets meet. Connection detection

notifies when either message or call is made to a specific receiver. Content detection is when specific word is used in message. [19]

### 4.4 Spyware maintenance

Just like any professionally made application, spyware also receives upgrades to either provide new functionalities or fix bugs. Upgrade requires internet connection and is invisible to target. Sometimes upgrade will require new installation of spyware.

An agent can also be uninstalled be user's single request and will not leave easily visible trace that it ever was installed. Uninstalling can be done with same methods as installation: remotely or physically. Usually removing spyware is invisible to targets, although sometimes it can result in device reboot.

Spyware contains self-destruct mechanism. In case of risk of exposure it will automatically self-destruct. Another scenario for self-destruction is agent not responding or communicating with servers for specific amount of time, set to 60 days by default. [19]

## 5 Defense against spyware

While the only definite method to defeat sophisticated mobile spyware like Pegasus is to not have equipment that can be targeted by it, there are some measures that can be taken either to reduce or prevent penetration.

### 5.1 Target audience

To understand how to counter spyware, one first would need to understand reasoning behind being targeted by sophisticated and costly attack. Advanced spyware installation requires serious vulnerabilities that would allow gaining root privilege and persistence on device. Exploits like that could either be found by entity specializing in providing spyware or bought from brokers specializing in

selling this sort of exploitations. Furthermore, they must be unknow to developer, who are constantly searching for vulnerabilities in their products. Combination of these factors makes spyware services expensive. Basic zero-click installation of spyware would require vulnerability that could cost up to 1.5 million dollars. Add persistence to that and price could bump to another million.

Figure 11 demonstrates payouts for exploitations provided to anyone who reports exploit. Zerodium is a broker that specializes in trading exclusive vulnerabilities. With such expensive exploitations, spyware services must be expensive too. In 2016 NSO-group charged $650,000 for installation & $500,000 service fee per 10 iPhone devices. Also, additional 17% a year maintenance fee is required to use all the infrastructure to retrieve, analyze & setup rules for data.

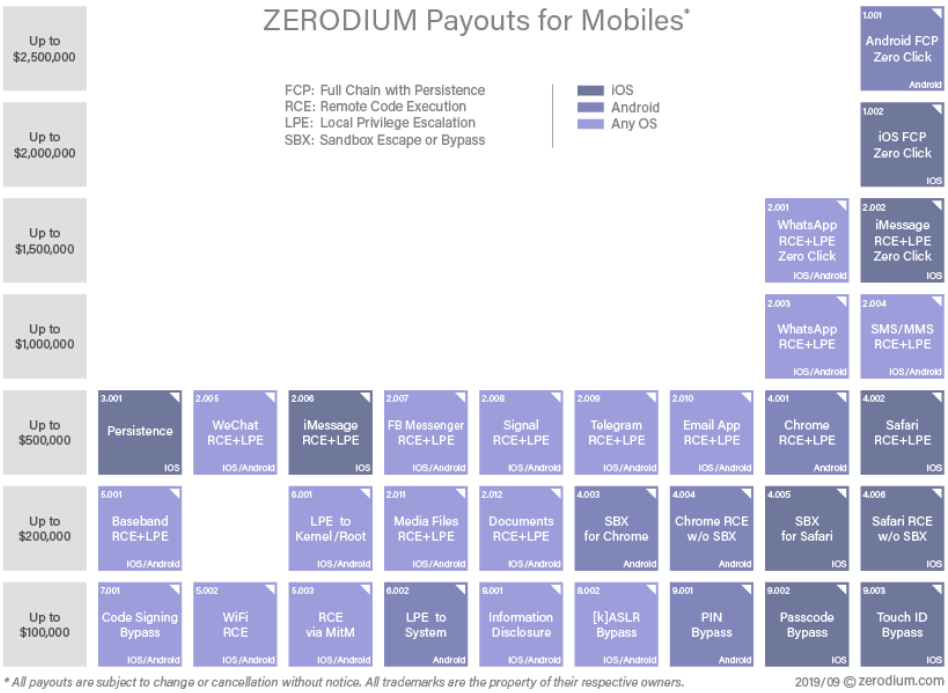


Figure 11. Payouts for mobile exploitations. Currently Android's exploits are more expensive more. [26]

Another thing to consider is nature of this sort of service. For instance, state of Israel, home country to the NSO-Group, requires export approval of Pegasus spyware, since it is labelled as a weapon and can be sold only to government clients only. [7, 27]

Taken expensiveness and clientele into consideration, targets of such sophisticated spyware are either posing threat or hold valuable information. Mercenary corporations that are providing these products justify it with fight against violent criminals. That is true to some extent. For example, first customer of Pegasus spyware was government of Mexico, who's primary target was boss of most powerful drug cartel at the time - Joaquín Guzmán. However, there is a tendency for using spyware for political reasons against journalists, activists, lawyers, judges & politicians. Previously mentioned journalist Rafael Cabrera was targeted for investigating corruption linked to president. Or Ricardo Raphael, journalist who investigated infamous disappearance of 43 students & teachers.

Same pattern is observed in other countries. Wife of Washington Post's journalist Jamal Khashoggi was targeted by Pegasus, who was murdered in Saudi Arabia's embassy in Istanbul. Owner of Washington Post and richest man at the time Jeff Bezos was also targeted with Pegasus. Among Finnish targets Ministry for Foreign Affairs confirmed that diplomats ware targeted with Pegasus by unknown state entity.

Targeting political opponents is not limited to countries that could be considered authoritarian. At least 65 Catalan jurists, activists and their immediate family members were targeted by Pegasus spyware, with circumstantial evidence pointing at Spanish government. Illegal cases of spyware use were also detected in Poland, Hungary, and Greece. Total of 14 EU members had purchased NSO technology. [8]

To summarize it, because of high cost & government only clientele, targets of sophisticated spyware are high value individuals. They can be violent or dangerous criminals who are threat to society. Or they could be individuals who are posing threat to current regime.

## 5.2 Preventive measures

Preventive measures are measures that will decrease probability of unwanted installation of spyware. Key element to prevent spyware installation is to decrease attack surface.

### 5.2.1 Anonymity

Anonymity is a “condition where entity can be recognized as distinct, but identity information isn’t sufficient to link to a known identity”. In other words, your actions can be seen, like visiting email service provider, but that email cannot be tied to you. [28]

In almost all notorious spyware attacks, like with Ahmed Mansoor, Rafael Cabrera, Omar Radi spyware was installed remotely. That type of attack vector requires identity tied to mobile equipment. That could be either an email address that is used on phone or IMS identity to send either SMS or perform WhatsApp call. Also, network injection attacks would require either IMS or IME identifiers to target correct device. By staying anonymous, only attack vector would be physical access to mobile equipment. [18, 22]

Not all countries allow anonymous purchase of prepaid SIM cards. Furthermore, identity call be discovered either by tracking with IMSI catcher or with geofence. In latter case authorities would contact OS developer, like Google that has knowledge of devices IME identifier. Once identity is blown, changing SIM card will be useless as IME identifier is tied to device itself. While it is possible to change IME identifier of equipment after obtaining elevated privileges thought Jailbreaking or rooting, in many countries it is forgery, including in Finland. [29, 30]

### 5.2.2 Traffic Encryption

Once device has been linked to targets identity, spyware application is usually installed remotely either with network injection attack or with the help of vulnerability in specific messenger application, like WhatsApp.

To perform man in the middle type of attack, like network injection, communication must be unencrypted – implementing HTT protocol. Using a virtual private network tunnel protocol decreases chances of man in the middle attack by implementing symmetric encryption of communication between mobile device and VPN service provider. While VPN uses less secure symmetric encryption for connection, handshake itself is done with asymmetric encryption. Unless VPN service provider or session is encryption key is compromised, connection is secure, and redirection should not be possible, if VPN service has also its own custom DNS servers. [31]

It should be emphasized that when using VPN, one is shifting trust to provide secure connection from internet service provider to a VPN provider. By any means it is not a simple solution to complicated problem.

First, virtual service providers can and have been breached attaining root access in the past. Another issue to keep in mind since clients of such sophisticated spyware tend to be official intelligence agencies. That means that, depending on how much power they hold, they could simply compel VPN service provider to cooperate. When the provider faces dilemma of compromising one user’s connection who pays for service 10 bucks or potentially having their business shut down or attacked, it may be not much of a choice. [32, 33]

### 5.2.3 Firewall

Remote installation of spyware always requires, that infected device downloads it and after downloading it, it must communicate with server in order to extract

data from device. If communication is blocked, there is no way for spyware to download and communicate to server. [19]

This is where firewall comes in. Firewall is a network security system that monitors and controls network traffic. It can be hardware, software or virtual. Dedicated hardware is recommended as it adds extra layer of security and doesn't consume client's resources. Firewall allows, blocks or redirects traffic based on set rules. Those rules depend on firewall layer in Open Systems Interconnection model (OSI). Generally modern, more advanced hardware firewalls operate on application-level, that is layer 7 in OSI model. [34]

There are basically two main firewall policies that dictate how traffic should be handled. First policy, sometimes referred as blacklist, is to deny traffic that has been specifically prohibited. This could be publicly available blacklists of malicious websites, or simply blocking unsecure HTTP protocol on port 80 or forcing it to redirect to safer HTTPS on port 443.

Another, more restrictive policy is to deny by default. That is to block all incoming and outgoing traffic unless it has specifically been permitted. This policy is more secure, but it will require constant adjustment. For instance, in order to user secure Signal messenger app, firewall must allow traffic from domain whispersystems.org and signal.org. Also, TCP 443 and all UDP port must be open. [35, 36]

Modern firewalls come with VPN capabilities. That allows phone to establish secure encrypted connection to firewall when not close by. Furthermore, firewall rules can be setup based on source. In order to filter by source, user will have to assign static IP address to specific device and assign restrictive rules for it. Also, rules may apply for specific VPN user. That will allow having other devices on same network with less restrictions if needed. [37]

### 5.2.4 Mobile applications

Previously mentioned exploits, like Trident, consisted of vulnerabilities in Safari's Webkit. Forced entry had vulnerability in iMessage. Also, WhatsApp had buffer overflow vulnerability. Network injection attacks are intended to trigger redirection to malicious site with default web browser. Common denominator among these attack vectors is that they're either done with the help of default or very popular applications. For instance, WhatsApp had 1,4 billion users. [11]

NSO group leaked presentation states that most common installation failures are due to unsupported device, operational system, or browser. Zerodium is offering pay-out for vulnerabilities in WeChat, Signal, Telegram, Chrome, Safari, WhatsApp, FB Messenger, iMessage & email application. [19]

Therefore, to decrease surface attack, all default and popular applications should be disabled or not installed in the first place. Also, it is suggested to avoid messenger applications that are tied to phone number, this is part or previously mentioned anonymity.

### 5.2.5 Operational system

Because there are basically only two major mobile operational systems, user would have to choose between iOS and Android. For a long time, privacy & security-oriented experts were recommending iOS devices for optimal security. There were mostly two reasons behind that logic.

Apple's business model, at least at the time, is not dependent on gathering information about devices users. They pride and advertise themselves as a company that protects customers' privacies. Where's devices that are running Android OS are gathering large amount of information that they're either selling to advertisers or provide to authorities.

Apple’s iOS is tightly controlled by Apple. Sideloading is disabled, customization is minimal, and Apple is notorious for providing updates for several years after release of device. Android on the other hand allows application sideloading, very customizable and updates depend on device manufacturer. [38]

However, when it comes to advanced spyware, thigs are not that black and white. To begin with, currently pay-outs for mobile device persistence exploits are more expensive on Android side. That would mean, penetrating Android with persistence is harder. Restarting device would mean losing surveillance application. [26]

Another thing to consider is iPhone’s target audience. Like previously stated, targets of such sophisticated spyware tend to be influential people themselves. People with higher net income favor iOS devices.

People with higher social status prefer devices made by Apple as figure 13 shows. Apple’s devices as secure as they are, face same problem that some of previously mentioned mobile applications. Their newest devices run on same operational system as previous that were developed by same developer. Same issue is with hardware as smartphones are running A-series bionic chips. Android is completely opposite because of its open-source code. Currently there are 25 Android-derived operational systems with active development status. Devices that run on different processors and different modifications of Android. Also, there are security & privacy-oriented Android based operational systems, most favored being GrapheneOS. [11]

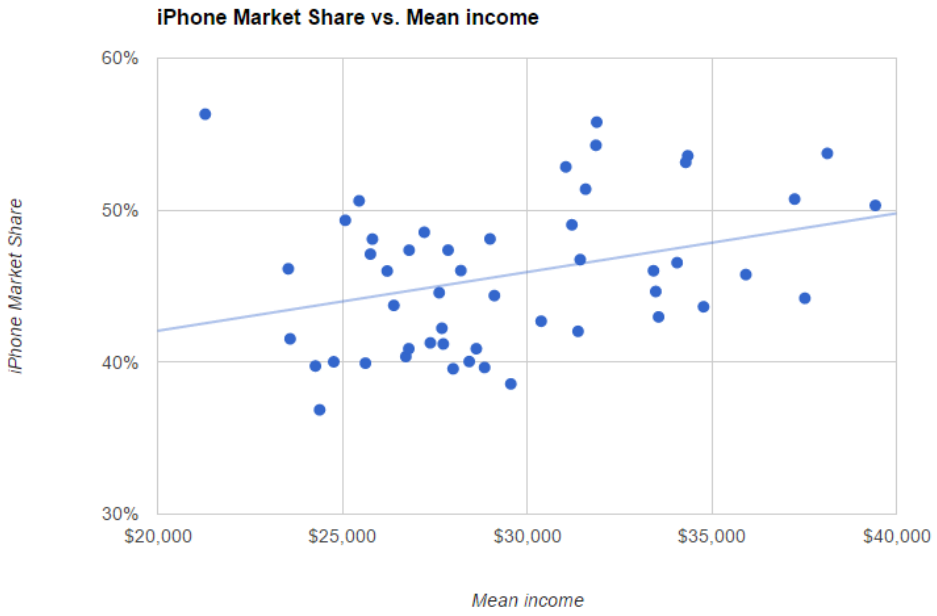


Figure 13. Correlation between mean income and iPhone's market share. [39]

Even though OS is based on Google's Android, all Google related services are missing from fresh install. Also, standard applications are replaced with security oriented. For instance, instead of Chrome, GrapheneOS is implementing Vanadium, which is more secure version of Chromium browser.

Hardened memory allocator is designed to be resilient against heap-related vulnerabilities, like WhatsApp's overflow vulnerability. Strengthened application sandbox is directed to combat privilege escalation. Enhanced verified boot hardens already well-known anti-persistence features. [40]

## 5.3 Attack mitigation

Attack Mitigation is the reduction in severity or seriousness of breach. Because no system is impenetrable one should prepare for possibility of mobile device being compromised. When dealing with spyware attack mitigation measures consist of reduction of information that can be extracted from device. [41]

### 5.3.1 Spyware detection

NSO group claims that its spyware is traceless, but as practice has shown, there are ways to determine whether device has been compromised.
First, there are domains that are tied to NSO infrastructure, like free247downloads.com. Even though Pegasus did wipe Omar Radi's web browser's history, it left Safari database intact, indicating visit to malicious site.

Then there are process names that are tied to Pegasus spyware. IOS maintains records of process executions that performed network activity in SQLite database. Ahmed Mansoor's & Omar Radi's mobile phones both contained references to "bh" process – bridgehead.

Spyware also disabled reporting of crash logs back to manufacturer. In iOS this is done in "com.apple.CrashReporter.plist" file. Alone alteration of this file is not necessary indicator of compromise, but rather a reason for concern.

Monitoring processes, databases, and logs can be time consuming so Amnesty International has created python script to check signs of Pegasus compromise called Mobile Verification Toolkit that scans logs, databases, installed apps, system analytics against list of malicious indicators. Question arises what happens when spyware is installed with new domain-, process-, account- & filenames. [42]

### 5.3.2 Hardware security

One sure method to reduce information that spyware could gather form mobile devices to physically remove certain hardware components from mobile device. Those components are cameras and microphones. A typical new mobile device has three cameras and microphones and can be either disconnected it unsoldered from board.

Logic behind such implementation is simple, if device is compromised with spyware, it won't be able to gather visual and audial information. If voice call is needed, external wired earbuds with attached microphone could be used for duration of the call. [43]

There are also phone vendors that specifically create smartphones with physical kill switches for certain hardware components. Those components tend to be modem, wireless network, Bluetooth, microphone, cameras, and sometimes headphone jack. [44]

### 5.3.3 Operations Security

Operations security is defined as a "process of identifying critical information and analysing friendly actions attendant to activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level". [45]

Because spyware has root privileges, it will be able to access data that device's owner isn't privileged to and before it is encrypted (see chapter 4.1). Users that could be targeted by sophisticated spyware, need to analyse what sort of consequences they would encounter if all their data would be compromised by adversary (Assume Breach Approach). If risk is too high, data being accessed and generated by mobile device need to be reduced. User might also need to re-evaluate content of communication, by asking themselves what would happen if communication were to become public? Lastly, data stored in counterpart's device need to be taken into consideration.

If user is using separate phone for secure communication, by default it must be turned off with removed battery and SIM card or stored in faraday bag that would block all signals. Secure phone must not be turned on near place of

residence or carried with other personal devices. Only communications that are allowed are with other secure phones, that would not reveal identity. [46]

# 6 Conclusions

The purpose of this thesis was to define what advanced spyware is, who the users of advanced spyware are, and who could be targeted with this sort of weapon. The study also concentrates on installation process, spyware features and how one could detect & prevent, or perhaps rather reduce the possibility of spyware installation on mobile device. It is good to bear in mind that we are dealing with limited information since both spyware providers and their clients operate in privacy.

This study shows that sophisticated spyware is developed by private security-oriented corporations that develop spyware and delivery methods. There are also private brokers who buy and trade vulnerabilities necessary for spyware installation. Clients of these companies are various government agencies, because it is legally considered to be a weapon. The targets vary from journalists to violent criminals to politicians & businessmen. A common dominator is that targets tend to be influential people one way or the other.

Based on the available information, installation process zero day and preferably zero click vulnerabilities to install spyware remotely without raising the target's suspicion. Once installed, spyware gains elevated privileges above the device's owner in order to access any information on mobile device. The priority is discretion, spyware will not send data when device is in roaming or has low battery level to avoid raising suspicion. It also has a self-destruct feature. Lastly this study provides tips on how to reduce the possibility of spyware installation. Anonymity is key, as spyware cannot be installed if there is no information about the target's device. Another thing to bear in mind is the mobile device's software & hardware. Since the business model of offensive security rests on one spyware being able to hack into hundreds of millions of devices, it is good practice to avoid going with the flow. To avoid popular mobile brands and popular apps is to reduce attack surface.

## References


1. Garcia, Arkaitz Gamino. Velasco, Concepción Cortes. Zamalloa, Eider Iturbe. Velasco, Erkuden Rios. Elejabarrieta, Iñaki Eguía. Lotero, Javier Herrera. Mansell, Jason. Ibañez, José Javier Larrañeta. Schuster, Stefan. 2015. Mass Surveillance Part 1 - Risks and opportunities raised by the current generation of network services and applications. European Parliament Think Tank. [online] Available at: https://europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf [Accessed 17 Sept. 2022].

2. Greenwald, Glenn. 2013. The Guardian. NSA collecting phone records of millions of Verizon customers daily. [online] Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Accessed 17 Sept. 2022].

3. Felten, Edward William. 2013. United States Senate. Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act. [online] Available at: https://www.judiciary.senate.gov/imo/media/doc/10-2-13FeltenTestimony.pdf [Accessed 17 Sept. 2022].

4. The Economist. Untangling the social web. 2010. [online] Available at: https://www.economist.com/technology-quarterly/2010/09/04/untangling-the-social-web [Accessed 17 Sept. 2022].

5. SKYNET: Applying Advanced Cloud-based Behavior Analytics. NSA. [online] Available at: https://cryptome.org/2015/05/nsa-skynet-intercept-15-0507.pdf [Accessed 18 Feb. 2023].

6. Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act. 2020. Privacy and Civil Liberties Oversight

Board. [online] Available at: https://irp.fas.org/eprint/pclob-cdr.pdf [Accessed 18 Sept. 2022].

7. Snowden, Edward. 2019. Joe Rogan Experience. Episode 1368. [online] Available at: https://youtu.be/efs3QRr8LWw [Accessed 1 Oct. 2022].

8. Mildebrath, Hendrik. Members' Research Service. 2022. European Parliamentary Research Service. Europe's PegasusGate Countering spyware abuse. [online] Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729397 [Accessed 2 Oct. 2022].

9. Ahmad, Nurul Haszeli. Aljunid, Syed Ahmad. Ab Manan, Jamalul-Lail. 2013. VULNERABILITIES AND EXPLOITATION IN COMPUTER SYSTEM – PAST, PRESENT, AND FUTURE. [online] Available at: www.researchgate.net/publication/287333829_VULNERABILITIES_AND_EXPLOITATION_IN_COMPUTER_SYSTEM_-_PAST_PRESENT_AND_FUTURE [Accessed 2 Oct. 2022].

10. Lin, Guanjun. Wen, Sheng. Han, Qing-Long. Zhang, Jun. Xiang, Yang. 2020. Software Vulnerability Detection Using Deep Neural Networks. [online] Available at: https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/9108283 [Accessed 8 Oct. 2022].

11. Snowden, Edward. 2019. Joe Rogan Experience. Episode 1536. [online] Available at: https://youtu.be/_RI82OQDoOc [Accessed 14 Jan. 2023].

12. Bazaliy, Max. Flossman, Michael. Blaich, Andrew. Hardy, Seth. Edwards, Kristy. Murray, Mike. 2016. Lookout. Technical Analysis of Pegasus Spyware. [online] Available at: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf [Accessed 9 Oct. 2022].

13. Du, Wenliang. 2017. Computer Security: A Hands-on Approach. Chapter4. [online] Available at: https://web.ecs.syr.edu/~wedu/seed/Book/book_du_toc.pdf [Accessed 15 Oct. 2022].

14. The NSO WhatsApp Vulnerability – This is How It Happened. [online] Available at: https://asyafaat.wordpress.com/2019/05/15/the-nso-whatsapp-vulnerability-this-is-how-it-happened [Accessed 16 Oct. 2022].

15. Claburn, Thomas. 2019. WhatsApp slaps app hacker chaps on the rack for booby-trapped chat: NSO Group accused of illegal hacking by Facebook. [online] Available at: https://www.theregister.com/2019/10/29/whatsapp_sue_nso_group [Accessed 22 Oct. 2022].

16. Marczak, Bill. Scott-Railton, John. Razzak, Bahr Abdul. Al-Jizawi, Noura. Anstis, Siena. Berdan, Kristin. Deibert, Ron. 2021. Citizenlab. FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild. [online] Available at: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild [Accessed 21 Oct. 2022].

17. Beer, Ian. Groß, Samuel. 2021. Google Project Zero. A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution. [online] Available at: https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html [Accessed 22 Oct. 2022].

18. Marczak, Bill. Scott-Railton, John. 2016. Citizenlab. The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. [online] Available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae [Accessed 29 Oct. 2022].

19. NSO-Group. 2014. Pegasus – Product Description. [online] Available at: https://www.documentcloud.org/documents/4599753-NSO-Pegasus [Accessed 23 Oct. 2022].

20. Amnesty International. 2020. Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group’s Tools. [online] Available at: https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools [Accessed 29 Oct. 2022].

21. Priest, Dana. 2021. The Washington Post. A UAE agency put Pegasus spyware on phone of Jamal Khashoggi’s wife months before his murder, new forensics show. [online] Available at: https://washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus [Accessed 12 Feb. 2023].

22. NSA Tailored Access Operations. 2010. [online] Available at: https://spiegel.de /media/11a9bd87-0001-0014-0000-000000035669/media-35669.pdf [Accessed 12 Feb. 2023].

23. Apple. 2021. Change the default web browser or email app on your iPhone, iPad or iPod touch. [online] Available at: https://support.apple.com/en-gb/HT211336 [Accessed 29 Oct. 2022].

24. Kaldani, Tamar. Prokopets, Zeev. Council of Europe. PEGASUS SPYWARE and its impacts on human rights. [online] Available at: https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8 [Accessed 29 Oct. 2022].

25. Jenifa, Ashlin. 2022. Anonymize Linux Traffic With ProxyChains and Tor. [online] Available at: https://geekflare.com/anonymize-linux-traffic [Accessed 30 Oct. 2022].

26. Zerodium Exploit Acquisition Program. 2022. [online] Available at: zerodium.com/program.html [Accessed 30 Oct. 2022].

27. Perlroth, Nicole. 2016. The New York Times. How Spy Tech Firms Let Governments See Everything on a Smartphone. [online] Available at: https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html [Accessed 5 Nov. 2022].

28. Garfinkel, Simson Leon. 2015. National Institute of Standards and Technology. De-Identification of Personal Information. [online] Available at: https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf [Accessed 12 Nov. 2022].

29. Damien, Christopher. Penzenstadler, Nick. USA Today. How police work with Google to obtain cellphone locatition data for criminal investigations. [online] Available at: https://eu.usatoday.com/in-depth/graphics/2022/09/08/police-use-google-location-data-cellphones-investigate-crimes/8005530001 [Accessed 6 Nov. 2022].

30. Criminal Code. 1996. Ministry of Justice, Finland. Chapter 33 Section 1. [online] Available at: https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039_20210433.pdf [Accessed 7 Jan. 2023].

31. VPN University. 2021. How VPN Encryption Works. [online] Available at: https://www.vpnuniversity.com/learn/how-vpn-encryption-works [Accessed 5 Nov. 2022].

32. Pcmag. Kan, Michael. 2022. NordVPN: Actually, We Do Comply With Law Enforcement Data Requests. [online] Available at: https://pcmag.com/news/nordvpn-actually-we-do-comply-with-law-enforcement-data-requests [Accessed 5 Nov. 2022]

33. Pcmag. Kan, Michael. 2019. TorGuard Hit by Hacks Involving Insecure Servers. [online] Available at: https://www.pcmag.com/news/nordvpn-torguard-hit-by-hacks-involving-insecure-servers [Accessed 5 Nov. 2022]

34. Checkpoint. What is a Firewall. [online] Available at: https://checkpoint.com/cyber-hub/network-security/what-is-firewall [Accessed 15 Jan. 2023]

35. Netgate. 2022. Firewall Rule Best Practices. [online] Available at: docs.netgate.com/pfsense/en/latest/firewall/best-practices.html

36. Signal. Firewall and Internet settings. [online] Available at: https://support.signal.org/hc/en-us/articles/360007320291-Firewall-and-Internet-settings [Accessed 24 Feb. 2023]

37. Miniserver. pfSense and OpenVPN: how to assign a fixed IP on remote client. [online] Available at: https://blog.miniserver.it/en/pfsense/pfsense-and-openvpn-how-to-assign-a-fixed-ip-on-remote-client [Accessed 15 Jan. 2023]

38. Kaspersky Lab. 2022. Mobile Security: Android vs iOS — which one is safer? [online] Available at: https://www.kaspersky.com/resource-center/threats/android-vs-iphone-mobile-security [Accessed 26 Nov. 2022].

39. Shaffer, Dan. 2016. Webfx. iPhones Dominate Smartphone Market Share for Internet Usage. [online] Available at: https://webfx.com/blog/internet/iphone-smartphone-market-share [Accessed 3 Dec. 2022].

40. GrapheneOS. Frequently Asked Questions. [online] Available at: https://grapheneos.org/faq [Accessed 26 Nov. 2022]

41. HYPR Corp. Security Encyclopedia. Mitigation. [online] Available at: https://hypr.com/security-encyclopedia/mitigation [Accessed 20 Mar. 2023].

42. Amnesty International. 2020. Forensic Methodology Report How To Catch NSO-Group's Pegasus. [online] Available at: https://amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus [Accessed 8 Jan. 2023].

43. Snowden, Edward. 2016. Vice. State of Surveillance with Edward Snowden and Shane Smith. [online] Available at: https://youtu.be/ucRWyGKBVzo [Accessed 04 Feb. 2023].

44. Ene, Andrei. 2020. Techthelead. PinePhone Comes With Six Physical Switches For Wi-Fi, Bluetooth And Others. [online] Available at: https://techthelead.com/phone-with-physical-switches-for-communication-functions [Accessed 9 Jan. 2023].

45. National Institute of Standards and Technology, Computer Security Resource Centre. [online] Available at: https://csrc.nist.gov/glossary/term/operations_security [Accessed 18 Feb. 2023].

46. GCHQ Covert Mobile Phones Policy. [online] Available at: https://s3.documentcloud.org/documents/1273603/gchq-covert-mobile-phones-policy.pdf [Accessed 18 Feb. 2023].