RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date: November 26, 2025
Number of pages: 42

MOBILE PHONES

THREAT LANDSCAPE SINCE 2015

TLP:CLEAR

Contents

SUMMARY

The ubiquity and systematic use of smartphones, along with the increasing number of features and data they handle, make them targets of interest for the acquisition of cyber intelligence.

These everyday devices exhibit multiple vulnerabilities as well as a significant attack surface across multiple layers of the device architecture. These vulnerabilities may reside within wireless interfaces, applications, operating systems, and even within hardware components.

The numerous communication protocols used, such as cellular network, Wi-Fi, Bluetooth and NFC, suffer from several weaknesses facilitating the interception of exchanged information, or even the alteration of data in order to deploy spyware code on the devices.

Operating systems and applications installed on the device may also constitute another intrusion vector for spyware deployment. Some sophisticated threats indeed exploit chains of 0-day vulnerabilities which do not require any user interaction to compromise the device, usually referred to as zero-click. The implants deployed after gaining access to the mobile phone are generally non persistent and leave only few traces on the compromised device. The sophistication of these infection chains and their stealth, as well as the absence of detection solutions significantly increase the difficulty of response efforts.

These elements show that mobile devices have a large attack surface that multiple offensive actors strive to exploit - sometimes deploying very advanced attack capabilities to successfully compromise a device.

Mobile phones can indeed be targeted by state-sponsored offensive actors in the course of espionage or surveillance operations, drawing upon resources developed internally or by the national defense and industrial base, or acquired externally from specialised companies known as Private Sector Offensive Actors (PSOA).

PSOAs can facilitate access to advanced capabilities for states which do not own these offensive technologies or for states wanting to complicate the process of attribution[1]. PSOAs thus contribute to the multiplication of threats sources and to the uncontrolled dissemination of mobile-oriented offensive tools, which increases the threat level on mobile devices.

In response to these threats, France and the United-Kingdom have launched consultations to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCIC) in November 2023, during the Paris Peace Forum[2]. This initiative has been named the Pall Mall Process during its formal launch in London in February 2024 and has lead to the production of a code of practices for states [1]. It promotes both an enhanced cooperation between manufacturers to reinforce the security of the mobile devices and to increase the information sharing on observed threats, and recommendations on the legal frameworks regulating the use and the marketing of CCICs.

Over the past three years, ANSSI has handled several cases of mobile phones compromised by an irresponsible use[3] of spyware targeting individuals holding positions within senior official

[1] While the process of imputation bind malicious activity to an intrusion set based on technical and contextual elements, the process of attribution bind an attack to a sponsor with a political or geopolitical objective.

[2] Annual event gathering heads of state and government, representative of international organizations and of civil society aimed at providing a cooperative space to promote reflection on collective action methods to address global challenges.

[3] The Pall Mall Process Code of Practice for States defines *irresponsible use* as a threat to the security, the respect for human rights and fundamental freedoms and the stability of cyberspace, or without guarantees or adapted supervision processes, or incompatible with applicable international law or the consensus United Nations framework on responsible State behavior in cyberspace.

authorities or within the executive committees of companies in strategic sectors. In the majority of those cases, ANSSI has observed that the devices targeted were the victims' personal mobile phones.

Furthermore, mobile phones are increasingly a prime target for cyber-crime actors. Their for-profit attacks involve less sophisticated malware and rely on social engineering methods to collect their victims' personal and professional data. Depending on its nature, the collected data may be reused to launch phishing campaigns or to gain access to a related information system. The opportunistic nature of these for-profit attacks means that cyber-criminal activites impact individuals and organisation without regard for their geographical localisation or economic sector.

i

How to react when receiving a threat notification

If you receive an alert (by emails, SMS, etc.) from a security vendor or from your mobile provider warning of a potential compromise of an account or device, it is recommended to avoid handling your phone and **contact CERT-FR** by email at **cert-fr@ssi.gouv.fr** or by phone at **3218** (free service + cost of a call) or +33 (0) 9 70 83 32 18.

1 FOREWORD

This Threat Landscape about Mobile Devices focuses on the threats targeting consumer smartphones.

It relies on incidents handled by ANSSI, on various reports published by official organizations, security vendors, non-governmental organization, as well as on relevant information from publicly available sources and offers an overview of the current state of knowledge on this type of threat.

This Threat Landscape first provides a technical analysis of the attack vectors and exploitation methods used to compromise mobile devices. It subsequently describes the known capabilities and objectives of some offensive actors. It does however not present an exhaustive view of all attacks against mobile devices but offers a selection of cases to illustrate the general observations on this threat. To accompany this overview, recommendations, which are regrouped and developed in a dedicated final section (4), are provided along the way. Their purpose is to help reduce the attack surface of these devices both for individual users (who are strongly advised to read and take into account the recommendations if they recognise themselves in one of the cases described hereunder) and for organisations and their Chief Information Security Officer (CISO).

i

Can I be targeted by a spyware?

Individuals dealing with topics which are either sensitive and/or in relation with the fundamental interests of the Nation may be targeted by sophisticated spyware in order to gather information that can be valuable for a foreign state. For instance, senior authorities in the civil service, elected representatives, executive committees of strategic companies, lawyers, journalists, militants or activists, dissidents or people close to those type of individuals may be targeted.

Conversely, the whole population may be victim of identifiers stealing or mobile device compromise by cyber-crime actors.

2 ON ATTACK OPPORTUNITIES: TECHNICAL VECTORS AND EXPLOITATION METHODS USED BY MALICIOUS ACTORS AGAINST MOBILE DEVICES

2.1 Attack surface related to wireless interfaces

Mobile interfaces are systems or protocols enabling communication between two devices, for instance between a base transceiver station (BTS) and a mobile phone. Data is thus exchanged using radio wave communication without any physical contact between the devices. As with most network protocol, unique identifiers are assigned to each mobile device to precisely identify each device. Mobile communication protocols, such as 2G, 3G, 4G, 5G, Wi-Fi, Bluetooth and NFC, all exhibit vulnerabilities exploitable by malicious actors.

Attacks targeting mobile wireless interfaces follow three main objectives:

- **Passive interception**: data interception executed in close proximity to the targeted device, with the intercepted data being mobile devices identifiers and the exchanged raw data,
- **Active interception**[4]: decryption of the exchanged data and communication hijack where the attacker is placed between the two devices, *e.g.* using an Adversary-in-the-middle (AITM) technique and information recording methods,
- **Data modification**: active interception involving communication hijacking and alteration in order to compromise a mobile device.

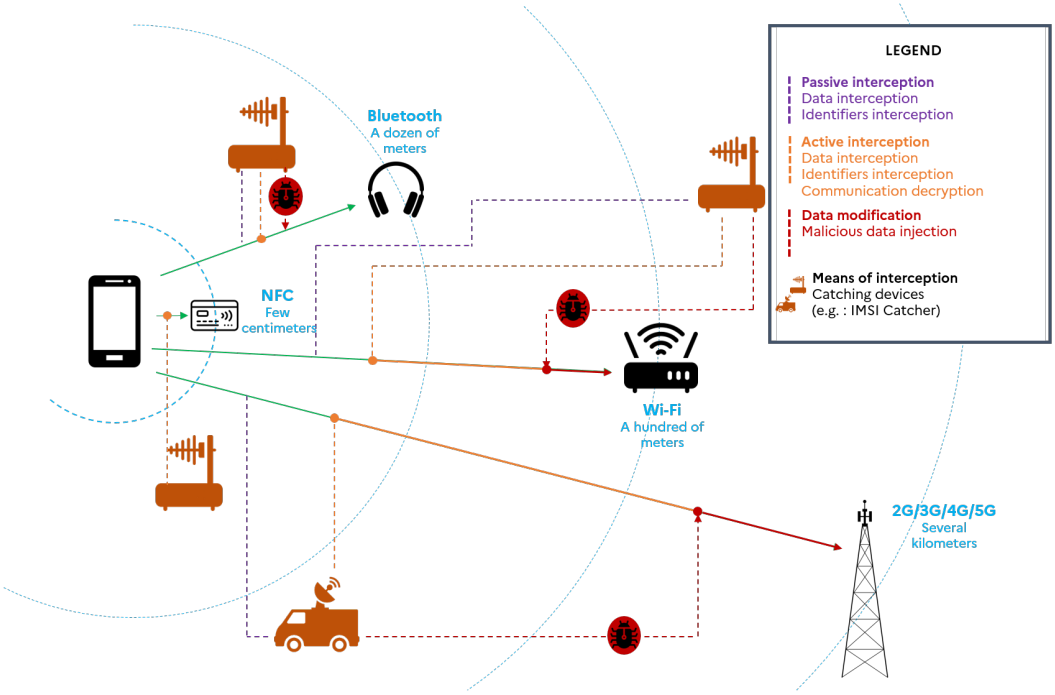

Figure 1: Attacks targeting several mobile interfaces

[4] Active interception emits radio signals and can thus be detected.

2.1.1 2G protocol exploitation

2G protocol is a communication technology specific to mobile phones[5] which main uses are voice communication, message exchange based on SMS protocol and access to the Internet[6].

SMS messages are not natively encrypted and, for voice communication, the security of exchanges over 2G protocol relies on a weak encryption algorithm[7] which has been publicly broken since 2010. Unlike 3G or 4G protocols, 2G protocol does not provide any authentication base transceiver stations for the devices [2]. In other words, there is no way for a mobile device to check the authenticity of a base transceiver station before connecting to it, allowing for AITM attack.

2G network is being gradually replaced with newer and more secure cellular standards[8], and is already decommissioned in many countries such as the United States or Japan[9]. It is however still in use to maintain a network coverage in areas where modern protocols are not yet available.

Weaknesses and backward compatibility in 2G protocol allow for a proximity interception capacity that is used by devices like IMSI catcher[10] to collect identities (IMSI, IMEI) of 2G, 3G and 4G mobile phones. Such devices impersonate the carrier's base transceiver station to disconnect the target from the legitimate network and reconnect it to the attacker-operated network, thus catching the voice calls, messages and location.

Such devices are now used by criminals who acquire them either through smuggling or foreign sales platform. Some of these attackers use it to acquire mobile phone numbers before sending them phishing message by SMS in targeted areas. According to Libération, in 2022 in Paris, a driver was arrested with an activated IMSI catcher in their car's trunk, planning on sending phishing messages related to Assurance Maladie[11] [3].

2.1.2 Exploitation of weaknesses in the Wi-Fi protocol

Wi-Fi is a set of wireless protocols connecting several devices close to each other within the same network. Wi-Fi networks, specifically the unsecured public ones, may exhibit vulnerabilities or weaknesses in their configuration that make them vulnerable to AITM attacks: an attacker may position itself between the user and the Wi-Fi access point to intercept, modify or gather sensitive information. Even though Wi-Fi network attacks impact a broader spectrum of devices than just mobile devices, several cases of Wi-Fi-enabled attacks on mobile phones were publicly documented over the past few years:

- **Exploitation of vulnerabilities or of configuration weaknesses**[12]**:** some PSOAs are selling solutions specifically built to compromise Wi-Fi-connected devices and intercept both the data exchanged on this protocol and the target's geolocation in real time. This method

[5] Released in the 90's, 2G protocol allowed for the first time to exchange digital rather than analog data.
[6] Internet communication over 2G has been integrated later with the GPRS protocol.
[7] The standard encryption algorithm for 2G is A5/1.
[8] Cellular standards are usually known as 2G, 3G, 4G and 5G.
[9] 2G network is scheduled to be decommissioned in France in 2026.
[10] An IMSI (International Mobile Subscriber Identification) catcher is a device used to gather mobile phones identifiers (IMSI, IMEI) on 2G, 3G and 4G. IMSI catcher are not operational with 5G because SUPI (Subscription Permanent Identifier), alternative to IMSI, is encrypted and not transmitted while establishing a connection. Attackers must use a SUCI (Subscription Concealed Identifier) catcher, where the unique identifier is derivated from SUPI.
[11] French national health service.
[12] There are many Wi-Fi configuration weaknesses, such as the use of outdated security protocols (*e.g.* Wired Equivalent Protocol (WEP)) or the absence of password to connect to a device.

of attack was used by a malicious actor in 2022 to redirect their target's communication towards the **Predator** spyware exploit chain[4, 5, 6].

- **Wi-Fi interception capabilities**: some PSOAs, such as the Israeli company MAGEN or the Emirati company STRATIGN, are developing and commercializing portable Wi-Fi interception systems designed to massively catch data exchanged on this protocol, without leaving any trace [7].
- **Fake Wi-Fi access points**: this type of attack relies on social engineering methods to persuade the user to connect to an attacker-operated network. Fake Wi-Fi access points can be used to intercept credentials by redirecting victims to phishing websites or injecting malware on the visited websites in order to compromise the phone [8, 9].

Recommendations on Wi-Fi usage

- Deactivate Wi-Fi when it is not in use.
- Disable automatic connection to known or open Wi-Fi networks.
- Do not connect to public Wi-Fi access points unless it is necessary and if so, use a VPN.

2.1.3 Exploitation of the Bluetooth protocol

Bluetooth is a wireless connection protocol allowing electronic devices to exchange data over a limited distance[13]. Compared to Wi-Fi, Bluetooth is meant for lower volumes of data exchanges between devices such a headsets, smartwatches, etc. This technology is also used to unlock cars and hotel room doors.

Any mobile phone with an activated Bluetooth interface is detectable. Any radio device within a dozen of meters is therefore able to catch its identifier. In 2021, a Norwegian researcher traveled 300 kilometers in 12 days with a homemade equipment logging Bluetooth interfaces and was able to follow the movements of devices with a Bluetooth interface activated [10]. Tracking technology using Bluetooth is already sold for surveillance purposes and also for commercial and marketing purposes such as following customers' movements in a store, a recreational area or public transportation [11, 12, 13, 14].

Vulnerabilities residing in a mobile device's Bluetooth interface can be exploited and used as initial vectors of intrusion. A Bluetooth interface can be exploited by simulating the connection of a device to inject malware. Cases where vulnerabilities, including vulnerabilities in the Bluetooth protocol, have been exploited in chain to achieve remote code execution on a mobile phone have been observed, for instance in the **Blueborne** case, where *Android* [15] devices were targeted and in the **Airbone** case, where *iOS* [16] devices were targeted.

The security level of a Bluetooth connection can vary widely and it is thus possible for a malicious actor to decrypt or even alter the contents of the communications exchanged on this protocol [17].

Recommendations on Bluetooth protocol usage

- Deactivate Bluetooth interface when not in use.
- Do not pair a mobile device to an unknown or a shared device.

[13] Depending on its power, Bluetooth technology can allow devices positioned dozens, and sometimes even hundreds of meters apart to connect to each other.

2.1.4 Exploitation of the NFC protocol

NFC protocol (Near-Field Communication) is a contactless proximity communication protocol used exclusively to exchange data over very short distances of a few centimeters at most. Data is thus exchanged in close proximity between two devices: one is active (mobile phone, payment terminal), the other is either active or passive (transportation pass or credit card). A passive device can be read by any nearby active device[14]. Most mobile devices are nowadays compatible with NFC protocol.

NFC protocol use may be hijacked directly *via* mobile phones. According to ESET, in 2024, a cybercrime actor ran an SMS phishing campaign, persuading users to click on a link which ultimately lead to the installation of the **NGate** malware. This code exploits the mobile phone's capacity to passively read data on the NFC protocol. Once a device had been compromised this way, the malware was able to read the data of any nearby payment card and to send it to the attacker who could then use it to process payments [18].

Recommendation on NFC protocol usage

- Deactivate NFC interface on the phone when not in use.

2.1.5 Other exploitation methods related to telecommunication providers

Some attack vectors are not directly linked to mobile devices but rather to telecommunication providers, whose organisational procedures can expose weaknesses which can in turn be exploited.

For instance, the SIM swapping scam consists in usurping the victim's identity to order a new, attacker-controlled SIM card from the victim's provider.. The attacker will therefore receive every SMS destinated to the victim, including the two factors authentication tokens (2FA) allowing the attacker to reset the victim's passwords [19]. Operators of the intrusion set Scattered Spider may have used SIM swapping along with their toolset since 2022. By gathering personal data about their victims, cyber-crime actors can achieve an identity theft and contact the victim's provider to get a new SIM card. Obtaining multi-factor authentication codes can also facilitate a later exfiltration of data from a desktop environment and, in some cases, even a deployment of ransomware[5, 20].

Comment: reinforcing providers' identity verification procedures in order to effectively confirm the identity of users remotely requesting a SIM card change could significantly reduce the risks of SIM swapping attacks [21].

Recommendation on multi-factor authentication

- Lock the SIM card with a PIN code.
- Change the default PIN code of the SIM card.
- Choose authentication application (TOTP) for multi-factor authentication.

[14] In other words, NFC does not involve any mutual authentication. In some cases, such as with phone payments, authentication is directly carried out by the mobile phone without recourse to the NFC protocol.

2.2 Attack surface of a mobile device

While early mobile phones were equipped with very minimal operating systems, they are nowadays comparable to desktop computers in terms of complexity and features. The hardware components of the device are mainly responsible for communication operations (see 2.1), whereas the software components are made up of two layers: the operating system and applications[15].

The operating system is directly installed by the phone vendor and manages the device, the hardware parts and user's data. The different layers of a mobile phone create a substantial attack surface that may be targeted on any step of the exploit chain.

2.2.1 Initial vectors of attack

The initial vectors of attack used by malicious actors to compromise mobile phones can target a network interface or directly the mobile device. As such, three methods with various complexity levels are observed to deploy malware on mobile phone:

- exploiting a zero-click vulnerability,
- inciting a user to click on a malicious link or file,
- installing malware while physically accessing the device.

In some cases, hardware components were directly compromised by the vendor, but supply chain compromise of mobile phone hardware is still limited today.

Recommendations on hardening the operating system

- Hardening the operating system is possible by disabling optional features and thus reducing the attack surface of the device. This is possible on *iOS* by turning on the *Lockdown Mode* or on *Android* by turning on the *Advanced Protection Mode*, available with *Android* 16.
- Always install as soon as possible updates for the operating system and applications.
- Do not delay the reboot of the device after an update.

Comment : ANSSI has independently tested the efficiency of "Lockdown Mode" to prevent the compromise of a device.

Exploitation of zero-click vulnerabilities

Applications which constantly synchronise may be vectors for the exploitation of so-called zero-click vulnerabilities which do not require any user interaction. Amongst these applications, instant messaging applications such as *iMessage* or *WhatsApp* are regularly targeted as they are installed on most mobile devices. A zero-click vulnerability is automatically triggered during data processing, for instance when a message or a call is received, before anything is even displayed on the phone. Compromising these applications is generally only the first stage of the exploit chain which purpose is to expose the device's data in its entirety[16]. The exploitation of several vulnerabilities as an exploit chain is generally necessary to bypass each application layer in order to deploy a spyware as close as possible to the core of the system. Figure 2 illustrates

[15] Applications are software which extend the features of the operating system and the device usages. It can be natively included to the operating system or installed by the user.

[16] An exploit chain is a sequence of vulnerabilities exploitation allowing an attacker to progressively take over a system.

how an exploit chain is executed on a mobile device, from the reception of the initial message to the full compromise of the device. Exploiting a zero-click vulnerability as an initial vector of attack is a sophisticated means of attack and has been documented for various exploit chain related to spyware like **Pegasus** since 2018 or **Triangulation** since 2019 [22, 23, 24].

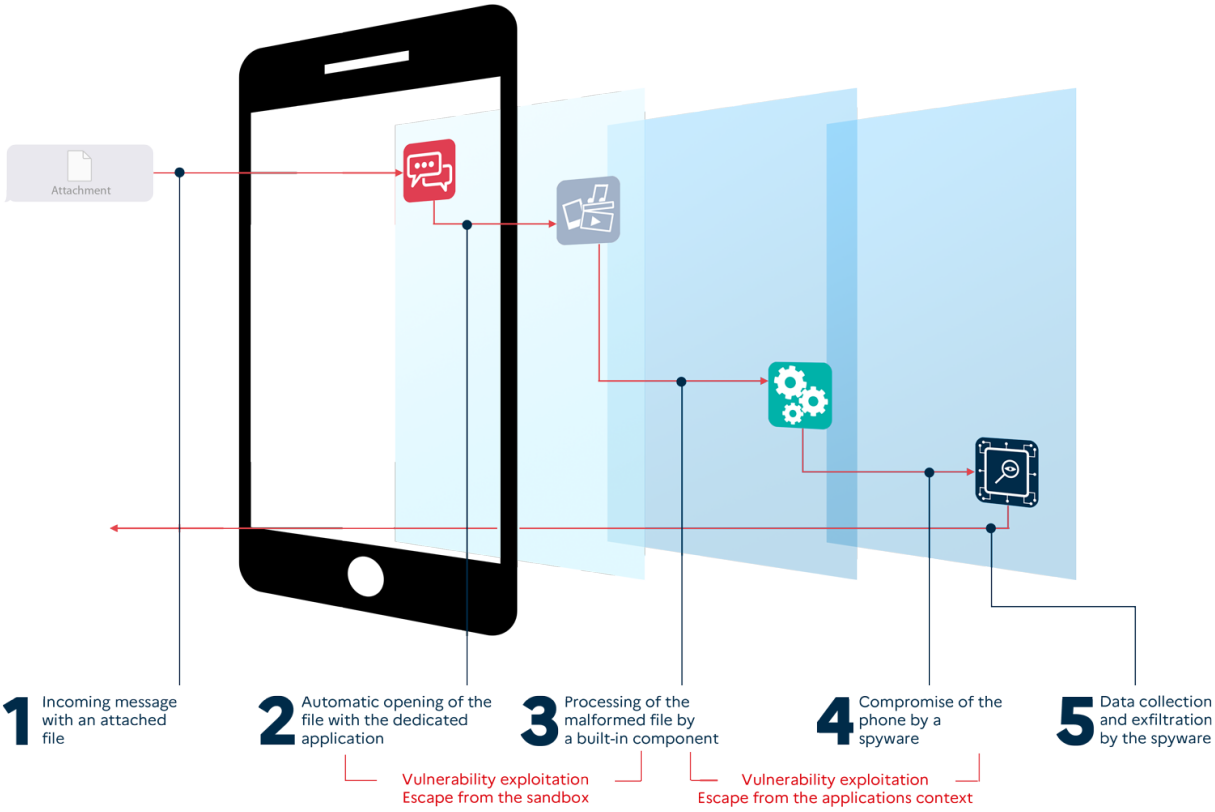

Figure 2: Overview of a zero-click exploit chain

Recommendations on messaging applications

- Deactivate the preinstalled messaging applications if not used.
- Deactivate the automatic reception of MMS messages.
- Avoid exchanging sensitive information via SMS and prefer messaging apps that use end-to-end encryption.
- Deactivate the automatic backup of chats within these applications.

Messaging applications are prime targets for this type of attack, but other native applications can also be targeted: for instance, *Calendar* on *iOS* has been used as zero-click initial vector in an exploit chain of the **Reign** spyware, documented by CITIZEN LAB [25].

Spyware deployed with the use of zero-click vulnerability are the most sophisticated threats targeting mobile devices. Spyware are usually very stealthy: they may conceal their incoming and outgoing communications through legitimate services as seen with the recent versions of **Pegasus** which use **iMessage** on *iOS* and exists only in the memory of the device so as to leave no trace of its presence [26]. This type of attack is however not usually persistent[17] and the attacker needs to re-compromise the device after each reboot. The non-persistent nature of those attacks

[17] A malware will use persistence mechanisms to stay on a compromised system even after a full reboot of the device.

complicates the detection of this type of spyware, as well as the digital investigation operations subsequently conducted on the infected devices.

Comment: Research on zero-click vulnerability is a complex subject and some companies and state organisations will prefer using other, less-complex attack vectors that are still undetectable by the user, such as accessing the victim's network either through cooperation with the victim's telecommunication provider or after compromising the provider's networks, as described in 3.1.1.1.

Recommendation on rebooting a mobile device

- Regularly reboot the mobile device.

Attacks using social engineering

Mobile phones can be compromised through social engineering[18] methods that trick the victim into downloading or clicking on a malicious payload sent either through social networks, SMS, e-mail or instant messaging applications. Since at least 2014, phishing campaigns targeting mobile phone users and associated with a reputedly Russian intrusion set have disseminated malicious payloads (files or links) through legitimate channels such as online forums, e-mails, social networks or messaging applications like *WhatsApp* or *Signal* to conduct espionage campaigns [27, 28, 29, 30].

Some PSOAs have also developed a network of fake profiles on social media platforms such as *Facebook* or *LinkedIn*. In 2024, META revealed that it had identified and subsequently taken down fake profiles used by PSOAs companies, used both to test their spyware and to conduct social engineering operations with the aim of compromising targeted users. This was for instance the case of the Spanish company MOLLITIAM SECURITY, which conducted a significant phishing campaign in Spain, Colombia and Peru in order to deploy the spywares **Invisible Man** and **Night Crawler** on behalf of its customers [31, 32].

Recommendation on phishing

- Do not click on links or open files embedded in unsolicited messages.
- Be vigilant when opening links received through QR codes.

Attacks relying on a physical access to the device

Some attackers will try to take advantage of a physical access to the mobile device to compromise it. Security vendors have documented several cases of compromise performed with the support of local law enforcement officers. For instance, in China, mobile devices have been compromised by spyware such as **EagleMsgSpy** [33] and **Massistant** [34]. The security vendor LOOKOUT has observed and documented the deployment in Iran of the **BouldSpy** surveillance tool between March 2020 and May 2023. This spyware was installed on at least 300 mobile devices belonging to minority groups, potentially under the supervision of the Islamic Republic of Iran police force: most of the targeted devices were initially compromised in the vicinity of police stations and border crossings, meaning that victims' mobile phones had likely been confiscated and physically compromised [35]. Lastly, the spyware **NoviSpy** may have been deployed on mobile phones belonging to Serbian activists during interrogation at police stations. In this

[18] Social engineering methods strive to exploit the trust or credulity of a user in order to incite them to trigger an action.

particular case, some of the mobile phones' unlock codes may have been obtained by observing the victims as they typed them into their devices [36].

Physical access to a device may also facilitate the gathering of the necessary information for a future remote compromise of this device. According to the Security Service of Ukraine (SBU), the preparation of a campaign associated with the reputedly Russian intrusion set Sandworm targeting *Android* devices belonging to the Ukrainian army might have been facilitated by the analysis of mobile phones recovered on the battlefield [37, 38].

Recommendation on the physical protection of mobile devices

- Do not connect a mobile phone to unknown USB ports and devices.
- Use a trusted USB data blocker when using an unknown USB port to charge a mobile device.
- Protect the phone's unlock password and use passwords composed by six alphanumeric characters.
- Completely turn off the mobile device when it has to be left unattended.

Hardware compromise during manufacturing

Mobile phones can sometimes present native features which expose vulnerabilities or which are even potentially malicious. In September 2021, the Lithuanian CERT revealed that several mobiles phones manufactured by the Chinese vendor XIAOMI were distributed with built-in censorship features which prevented the use of some words related to topics deemed sensitive for Chinese authorities[19], both in English and Chinese. These censorship features could be activated remotely by the vendor, even when they were not originally activated [39]. In 2025, KASPERSKY discovered counterfeit mobile phones imitating major brands distributed with the malware **Triada** pre-installed [40]. **Triada** is a stealer malware, exfiltrating data such as messaging credentials and cryptocurrency wallets credentials.

2.2.2 Exploitation of built-in operating system components

Although designed with a high level of security by design, the features and components integrated into a mobile device, including third-party components, are not immune to vulnerabilities and can be hijacked to perform malicious actions. Built-in operating system components are of interest for attackers as they are present in most mobile devices, resulting in attackers exploiting vulnerabilities and hijacking native features at any stage of the exploit chain, depending on the component.

Vulnerabilities residing in the native features of an operating system can be exploited in an exploit chain. For instance, several exploit chains of the **Pegasus** spyware relied on an exploit chain of 0-day vulnerabilities[20] impacting *iOS* native features and applications such as *HomeKit* (exploitation observed in 2024), *FindMy* (exploitation observed in 2022) and *Apple Wallet*[21] [41, 42, 43, 26]. Similarly, in 2021, the operators of the reputedly Russian intrusion set Nobelium might have targeted *iOS* users using an exploit chain based on a vulnerability residing in the *WebKit* rendering engine[22], allowing the attackers to exfiltrate credentials for social media platforms such as *LinkedIn*, *Gmail*, *Facebook* and *Yahoo* [29, 44].

[19] For instance, the expressions *Free Tibet*, *Democratic Movement* or *Longing Taiwan Independence* were censored.

[20] A 0-day vulnerability is not yet remediated at the time of its exploitation.

[21] *HomeKit* is used for home automation, *FindMy* is used to find the location of a device, and *Apple Wallet* is used for managing virtual cards.

[22] A rendering engine in a component responsible for displaying web content. In *iOS*, *WebKit* is the rendering enging built-in with the system and the most used in the applications displaying web content.

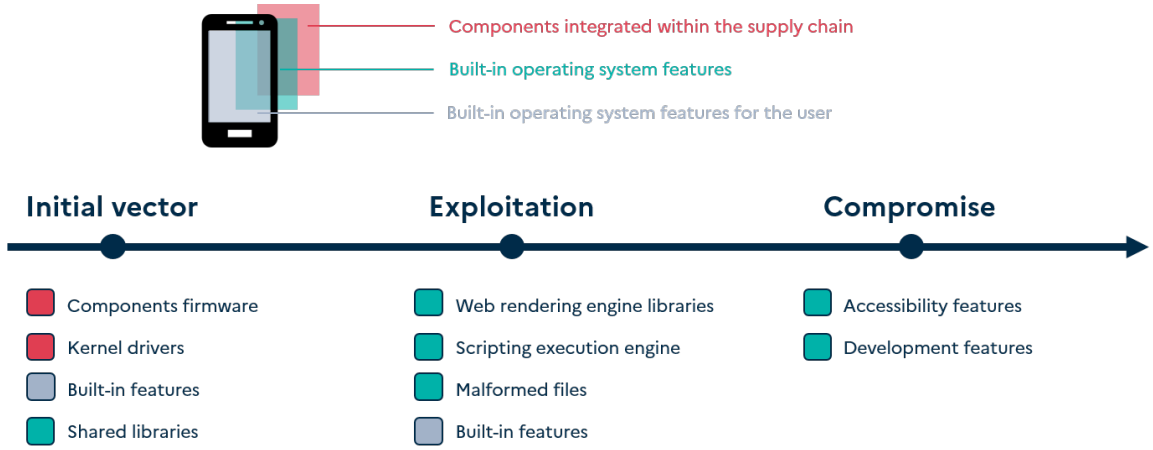

Figure 3: Examples of exploitation of OS built-in components in an exploit chain

Features provided natively by the operating system can be hijacked by attackers, especially in order to gain higher privileged rights.

For instance, **accessibility features** were initially provided to assist users with disabilities[23] and can be hijacked to gain access to specific resources such as the content displayed on the screen and data input from the keyboard. Some specific cybercriminal malware, such as **Crocodilus**, discovered in 2025, use these features to exfiltrate banking and cryptocurrency-related data [45].

Other **internal features**, such as those specifically designed for developers, are also used to perform malicious actions. For instance, the exploit chain associated with the spywares **Pegasus** and **Triangulation** rely on a calculus-dedicated framework on *iOS* to drop payloads [46, 47, 48].

Recommendations regarding built-in features

- Do not grant access to accessibility features to applications without a legitimate reason.

Lastly, third-party components integrated within the manufacturer's supply chain can also introduce vulnerabilities that can be exploited to compromise the device. These components can be hardware parts, such as electronic chips in a mobile device. The components can also introduce vulnerabilities when associated with vulnerable system drivers or software, for instance shared libraries (such as *CoreAudio* on *iOS* or *Skia* on *Android*). These third-party specific and sophisticated components are present in multiple devices manufactured by different vendors, and as such constitute prime targets to compromise a wide array of mobile phones.

> The baseband processor is a third-party chip natively integrated in a mobile operating system and found in all mobile devices. This component is required to interact with cellular networks as it manages radio protocols. In 2023, AMNESTY INTERNATIONAL described how the **Triton** module sold by the INTELLEXA consortium was used to achieve the zero-click compromise of mobile devices by exploiting vulnerabilities residing in the baseband processor. This module must be used in tandem with an IMSI catcher in order to compromise the victim [4].

Shared libraries are third-party software facilitating the development of applications[24] and are regularly exploited as an initial vectors of attack. Among shared libraries, those developed

[23] Accessibility features include screen reader and voice control, for example. The features are also available for developers to assist them to make their applications more accessible.

[24] Some features are directly provided by the operating system as software blob, usable by developers through internal interfaces.

to manage media formats (displaying pictures, playing video files) are a hotbed of exploitable vulnerabilities as a result of the wide variety of supported formats. In 2020, SAMSUNG has for instance patched a vulnerability that had been present in the *Qmage* codec since 2014 [49]. Vulnerabilities impacting shared libraries are regularly exploited in exploit chain, such as in 2023 by the spyware **Pegasus** [26].

Comment: Shared libraries can be found in all devices containing the same version of an operating system, which facilitates the exploitation of vulnerabilities by providing attackers with a similar attack surface on different devices. Widespread inclusion of third party libraries in mobile phone applications create a strong dependency on library developers for the release of security updates. This situation in turn creates a security risk for downstream vendors and users.

Recommendation on updating the operating system

- Always apply operating system updates as soon as possible when they are made available.

2.2.3 Attacks exploiting user-installed applications

Applications installed directly by the user are an important part of the usage of a mobile device. They are downloaded through applications stores, either official or alternative, and even sometimes manually, without using a store as intermediary.

The architecture of an operating system natively includes enhanced security measures such as application compartmentalisation, fine-tuned access management, limiting access to to the various layers of a device, including the user's data, and privilege management, restricting the execution privilege of applications.

Advanced memory protection

Another common vector for vulnerabilities can be found in the device's memory management, where errors introduced during the development phase can create exploitable vulnerabilities. To prevent any unwanted use of an equipment's memory, proactive measures such as MTE (*Memory Tagging Extension*) on *Android* or MIE (*Memory Integrity Enforcement*) on *iOS* have recently been implemented by manufacturers. These mechanisms limit the risks of malicious exploitation of memory management bugs.

These measures can however not guarantee the complete security of a mobile device: the legitimate applications downloaded by the user can also be exploited by attackers.

These attacks can be successful through the exploitation of vulnerabilities or the abuse of the application's features.

- **Vulnerabilities residing in legitimate applications installed by the user can be exploited and allow an attacker to simultaneously target *Android* and *iOS* operating systems** through common features in order to deploy specific malware.
  In 2019, a vulnerability registered as CVE-2019-3568 was found in the call processing mechanism in *WhatsApp* and was used to deploy the spyware **Pegasus**. This method was used on mobile phones running on both *Android* and *iOS* [42, 50]. Similarly, in 2024, CITIZEN LAB has documented the case of a zero-click vulnerability exploited to target *WhatsApp* in a campaign related to the spyware **Graphite**[25]. The attackers are believed to have added the victims to a *WhatsApp* group before sending a PDF document. The document was automatically processed by the victim's mobile phone, exploiting a vulnerability in the application and thus enabling the download and deployment of the spyware [51].

[25] The spyware **Graphite** is sold by the Israeli company PARAGON.

Comment: While versions of the WhatsApp application are specific to each operating system, both Android and iOS devices are exposed to this particular vulnerability. According to CITIZEN LAB, while the majority of reported victims used Android devices, at least one iOS user was notified of a compromise by APPLE.

Recommendation on unused applications

- Uninstall or disable applications which are never or rarely used.

- **Legitimate features can be directly exploited in attacks.** This is for instance the case with a particular feature allowing users to synchronise their messaging application accounts with third-party devices, which can be used by attackers to exfiltrate conversations.
  In 2024, in the context of intelligence-gathering operations associated to the invasion of Ukraine by Russia, both the reportedly Russian intrusion sets UNC4221 and UNC5792 conducted phishing campaigns inciting their targets to synchronise their *Signal* accounts with a third-party device [52]. In November 2024, a similar method was employed by the reportedly Russian intrusion set Callisto against targets supporting Ukraine and employed in the governmental, diplomatic, and research sectors, in order for the attacker to gain access to the victims' WhatsApp accounts [28].

Although applications stores implement security measures to detect malicious behaviours, they can be bypassed to deploy malwares.

In 2025, KASPERSKY uncovered a password-stealing malware targeting cryptocurrency wallets. This malware was integrated in applications[26] available on the *Android PlayStore* and the *iOS AppStore* [53].

Even when they are available on official application stores, some applications can leak sensitive data and abuse the permissions granted by the user in order to collect their information. Although less intrusive than a spyware, these applications still allow to collect data such as the list of contacts and the location of the user. Permissions abuse has notably been observed through the case of the Spanish football championship's official application, which used its permission to access both the mobile phone's microphone and location to actually control undeclared public broadcasts of matches [54].

A malware can be deployed by downloading *ex post* the malicious code or by directly trojanising new releases of a legitimate application. In the first case, the malicious code is not present in the application when installed but is downloaded during the application's first run. This method has been for instance used by the banking malware **SharkBot** [55]. In the latter case, the new version of the application downloaded when the application is updated directly contains the malware and installs it on the mobile phone[27]. This was for instance the case with the **AhRat** Trojan, which was deployed through a *Google Play Store* update in 2022, one year after the release of the initial application [56].

Recommendations regarding permissions granted to applications

- Verify and manage the permissions granted for each application.

Another method favoured by attackers striving to compromise mobile devices involves enticing users to download applications containing backdoors.

[26] Including for instance a food delivery application exclusively used in Indonesia and in the United Arab Emirates.

[27] This technique is also known as "versioning".

- **This type of attack can rely on fake copies imitating legitimate applications and assuming their names.** The security vendor LOOKOUT documented attack campaigns observed between 2015 and 2019 where the malware **Monokle**[28] may have been delivered through a trojanized version of popular messaging and utilitarian applications [57]. Similarly, between 2014 and 2016, a legitimate military application embedding the *Android* version of the malware **XAgent** [27, 58] was distributed through social media platforms used by Ukrainian soldiers by the operators of the Russian military-related intrusion set APT28.

Recommendations regarding the applications installation sources

- Do not install applications from sources other than the official application stores.

- **Lastly, the installation of specific applications can be made mandatory for the population in some States in the course of domestic surveillance operations. These applications might act as a backdoor to the mobile devices.** The Chinese government is believed to force the installation of specific applications to some or all of its citizens, potentially for control and surveillance purposes. The application *Xuexi Qiangguo*[29] has for instance been mandatory for the members of the Chinese communist party since early 2019 and collects the user's personal data such as their location, consumer habits, health data, etc. [59, 60].
  In other countries, the national legal framework can restrict the available applications, *de facto* forcing the installation of a specific application. In 2025, Russia has for instance approved the development of a messaging application by the government. The resulting application, *Max*, is developed by VKONTAKTE, a subsidiary of the state-owned company GASPROM [61]. To facilitate its adoption, audio and video call features present in other messaging applications such as *WhatsApp* and *Telegram* have been blocked on the Russian territory by the telecommunication supervising State agency ROSKOMNADZOR. Installation of the application *Max* is also mandatory for every mobile phone prior to its distribution in Russia [62]. Even though no malicious code has been found in the application, the absence of end-to-end encryption and the harvesting of personal data personal might allow authorities to use *Max* as a surveillance tool [63].

3 ON THE CAPABILITIES DEPLOYED AND OBJECTIVES PURSUED BY ACTORS TARGETING MOBILE DEVICES

3.1 Data collection and surveillance operations

While the attack opportunities against mobile devices described *supra* (see 2) can be developed and operated directly by states maintaining advanced offensive capabilities, they can also be acquired through private companies. The market for privately-owned and operated surveillance capabilities has indeed been on the rise since 2010 and some of those specialised companies can

[28] The development of this spyware is tied to the Russian company SPECIAL TECHNOLOGIES CENTER LLC (STC).
[29] With 100 million downloads, its name may be translated as *Studying and strengthening the nation*.

provide governments and intelligence agencies with sophisticated spyware, whereas other will sell less advanced capabilities such as stalkerware[30] to private companies and individuals.

3.1.1 State-sponsored operations

3.1.1.1 Offensive capabilities can be directly developed or purchased

Mobile devices exploitation capabilities can be developed directly by a state or through contractors, or developed by and purchased from specialised foreign companies.

These companies finance major research and development projects, giving rise to new offensive tools such as ADINT (see 3.1.1.1) which complicate the exploit chain and raise the global threat level. Moreover, the use of off-the-shelf capabilities by some states, including tools and techniques used in the cybercriminal world, further complicate the imputation process.

Lastly, some states enlist the help of Internet Service Providers (ISP) in their internal surveillance activities, facilitating the deployment of spyware and intercepting communications right on the cellular network's backbone.

Capabilities can be developed in-house by the state and also by national contractors

Offensive capabilities used to target mobile devices for espionage and surveillance operations can be developed by state services and by a national offensive cyberwarfare ecosystem exclusively providing their tools to the state. This is for instance the case in China, the United Arab Emirates (UAE) and in Russia [27, 57, 68].

This bears witness to the fact that states are willing to maintain in-house offensive capabilities, usually on sovereignty grounds, which require a significant financial and human investment.

Since 2014, the UAE government has been working on the diversification of its investments and developing technologies designated as strategic for its national sovereignty, as shown by the creation of the company DARKMATTER. DARKMATTER has been accused by the REUTERS press agency of facilitating attacks targeting activists and foreign officials [68].

The Chinese offensive security ecosystem

The Chinese offensive security ecosystem is particularly focused on the development of offensive capabilities targeting mobile devices. The Chinese ecosystem is composed of multiple contractors supplying the cyber units of the People's Liberation Army (PLA), the Ministry of State Security (MSS) and the Ministry of Public Security (MPS). Several companies have developed malware for the operators of reputedly Chinese intrusion sets, including for instance WUHAN CHINASOFT TOKEN INFORMATION TECHNOLOGY CO., LTD.. Some of those companies, like the company I-SOON, are suspected of directly operating these intrusion sets [33, 64].

The Chinese offensive security ecosystem is also composed of vulnerability research teams, such as Pangu Team. Comprising offensive security experts specialised in mobile devices, vulnerability research teams often participate in China-based vulnerability research competitions like the Tianfu Cup. During the 2021 edition of the competition, Pangu Team successfully achieved remote code execution through a 1-click exploit code on an iPhone 13 Pro with IOS version 15 [65].

The Chinese ecosystem also develops and produces offensive tools able to target multiple platforms. For instance, the operators of the reputedly Chinese intrusion set BrazenBamboo might have developed the **LightSpy** malware family which can target multiple operating systems: *iOS*, *Android*, *Windows* and *macOS*, in order to collect the target's location and record their voice calls on VoIP [66, 67].

[30] Stalkerware is a type of malware that can be installed on a mobile device, generally when physically accessing the device. Stalkerware allows an attacker to remotely track the device's location and access the user's data such as messages and photos, without the user's knowledge.

Capabilities can be purchased from PSOA companies

While in some countries offensive cyberwarfare companies are directly integrated to the state's supply chain, others companies, mostly operating out of Europe, Israel and India, market their services to governmental customers around the world, thus facilitating the acquisition of offensive technologies for states lacking the resources and for those who want to hinder the imputation process of their offensive operations[31].

The number of companies developing and selling spyware has consistently risen in the years since the 2010 decade.

Some companies like NSO GROUP and INTELLEXA provide intrusive spyware relying on different exploit chain. The spyware **Pegasus** was observed in the course of offensive campaigns using 1-click vulnerabilities, particularly in Serbia and in Mexico, and also in the course of more sophisticated campaigns relying on zero-click vulnerabilities [36, 74]. The exploit chain used in an attack depends on the customer and their resources, as well as on the target's location[32].

Risks of dissemination of offensives capabilities

The company HACKING TEAM, operating out of Milan between 2001 and 2010, was responsible for the development of various spyware such as **Galileo**[a] which was sold to several states. In 2015, over 400 GB of data belonging to the company were leaked by a hacktivist, revealing that these tools were being sold to and used by authoritarian states for civil surveillance purposes. In the following days and months, the HACKING TEAM leak gave rise to the exploitation of 0-day vulnerabilities residing in ADOBE FLASH PLAYER by reputedly Russian, Chinese and North-Korean threat actors [70]. Offensive tools exposed from the HACKING TEAM networks have been used by other threat actors during many years, like for instance the remote surveillance platform **Galileo** which was used to compromise state targets and especially diplomatic personnel, at least between 2016 and 2019 [71, 72]. A malware composing this platform may also have been used by the operators of the reputedly Russian threat actor Callisto [72, 73]. A disclosure of technical capabilities from a PSOA can therefore lead to a proliferation of its offensive tools which are then reused by other offensive actors, finally leading to a heightened threat level.

[a] Depending on the sources and the period, **Galileo** was also known as either **Da Vinci** or **RCS** or *Remote Control System* [69].

The Israeli ecosystem is now one of the most developed in the PSOA sector, both in terms of number of companies and in terms of capabilities offered by those companies [75]. Members of the executive committees of the companies of this ecosystem often share the same background, which is also used as a recruitment pool[33]. These companies export their products through either foreign subsidiaries, joint ventures with local companies and resellers in countries with lax regulation, such as the UAE. Access to new markets can also be unlocked through foreign investments for these companies [78].

Capabilities can be purchased from vulnerability brokers

Some PSOAs have specialized themselves in the development and marketing of 0-day vulnerabilities to offensive actors. Less visible than other companies operating in the same sector, these intermediaries are however an essential part of the digital surveillance supply chain and can be found all around the world.

Comment: These PSOAs companies tend to favour geographical locations with attractive corporate tax allowances and lax regulations.

[31] Some states use surveillance tools developed and marketed by companies rather than their own capabilities in order to make the imputation process harder. One sponsor for an operation may use several spyware concurrently or successively in order to keep its anonymity.

[32] Attacks can be more complex to achieve when the target of an attack is located in a different country than the customer, especially when the cooperation of local telecommunication companies is required.

[33] For instance, the Unit 8200 of the Israeli army, dedicated to technological intelligence, is a recruitment pool for the Israeli ecosystem [76, 77].

Exploit codes developed by these companies might be used by reputedly state-sponsored actors already operating their own capabilities. For instance, between November 2023 and August 2024, the operators of the reputedly Russian intrusion set Nobelium might have used an exploit chain relying on vulnerabilities similar to the ones exploited by the PSOAs companies INTELLEXA and NSO GROUP [44].

Comment: The similarities between these exploit chain illustrate the risk of proliferation of offensive tools stemming from the relative ease with which offensive tools can be acquired. This particular case also raises concerns on how the offensive actors gained access to the exploit chain, as they might have identified them on a mobile device already compromised by INTELLEXA or NSO GROUP, or directly purchased the vulnerabilities through the same broker.

During the November 2023 Paris Peace Forum, France and the United-Kingdom have launched consultations to address the issues of proliferation and irresponsible use of CCICs. The Pall Mall Process, as these consultations have been called since their formal introduction in February 2024 in London, has lead to the publication of a code of practice for states [1]. In order to address these threats, it promotes an enhanced cooperation between manufacturers to reinforce the security of mobile devices and to increase information sharing on observed threats; it also recommends an evolution of the legal framework regulating the use and the sales of offensive capabilities.

Capabilities can be acquired through cooperation or compromise of advertising data (ADINT) brokers

Advertising-based intelligence or ADINT is characterized by the either large-scale or targeted delivery of advertisements to one or more targets for profiling and geolocation purposes. A real-time bidding system provides profiling data on users (age, gender, hobbies, location, socioeconomic group, etc.) to advertisers, allowing them to buy advertisement space on website and application targeting a specific public. This system is exploited by ADINT operators who present themselves as legitimate advertisers on bidding platforms to collect profiling data for surveillance purposes. ADINT operators can then exploit the massively collected data on a population of interest and precisely target an individual as well. This new data collection method is currently on the rise and widely advertised by many PSOAs benefiting from a still very imprecise legal framework in this area [79, 80].

ADINT providers are believed to work closely with buying platforms (*Demand Side Platforms* or DSP)[34] and some might even now operate the same capabilities internally [81, 82]. Cooperation with DSP and in-house DSP capabilities limit the risks of exposure for ADINT providers as they do not depend on an autonomous DSP and do not have to systematically justify their use of the data.

Comment: As well as collaborating with the companies owning the profiling data, state-sponsored actors might also directly compromise these companies and collect their data to support future espionage and surveillance operations.

Recent innovations in ADINT-based technologies combining targeted advertisement with vulnerability exploitation are reportedly enabling attacks on both mobile devices and computers. Commercial offensive tools such as **Sherlock**, **Patternz** or **Alladin**, respectively developed by the companies INSANET, ISA SECURITY and INTELLEXA, are reported to already offer this new technology [83, 84].

[34] The buying platforms own the data required for user profiling

Recommendation on advertisement profiling

- Remove and/or renew the advertising identifier.

Capabilities can be acquired through Internet Service Providers (ISP)

Inclusion of Internet Service Providers (*ISP*) in offensive operations enables and facilitates data collection straight from the cellular network's core for offensive actors.

As an example, the **Predator** spyware developed by INTELLEXA can be deployed on targeted mobile devices through a zero-click compromise when a local ISP's network is used in the attack. Specifically, this attack relies on the deployment of the two malware modules known as **Jupiter** and **Mars**. More precisely, **Jupiter** is deployed upstream with the hosting provider's complicity, right between the certificate authority and the websites visited by the victim and collects the target's certificates and encryptions keys. These are then sent to **Mars** in order to decipher, alter and redirect the intercepted communication [4]. The zero-click exploit chain of **Predator** is described in Figure 4.

Comment: ANSSI observed that in 2020 ***Pegasus*** *was deployed by a national customer in their own country to redirect Internet traffic towards malicious duplicates of legitimate websites with the active contribution of a national ISP.*

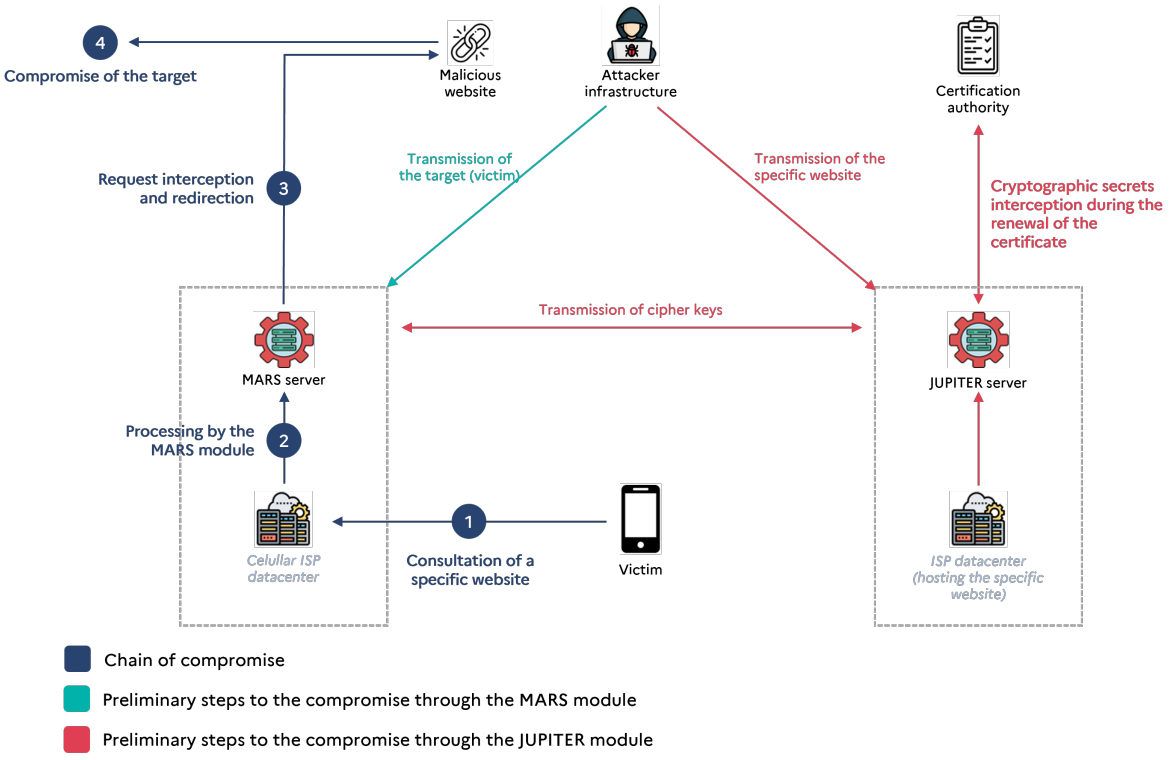

Figure 4: Summary of the zero-click exploit chain relying on the **Jupiter** and **Mars** malware modules ahead of a full deployment of the **Predator** spyware

Besides relying on local ISP, some offensive actors can also exploit weaknesses affecting telecommunication networks to facilitate their operations. The company TYKELAB has for instance in 2022 reportedly exploited vulnerabilities in the networks belonging to small telecommunication

providers operating out of Pacific islands to discreetly inject large amounts of data towards multiple targets worldwide. The company allegedly exploited vulnerabilities enabling geolocation and interception of voice calls on targeted mobile devices without leaving any trace on the devices. TYKELAB is registered as a telecommunication provider and a subsidiary of the Italian PSOA company RCS LAB [85].

Recommendation on using a mobile device in a foreign country

- When travelling abroad, it is recommended to apply the recommendations found in this document.
- When the object or location of a trip abroad is deemed sensitive, it is recommended to use a separate mobile phone.

Capabilities can include cybercriminal tools

In 2024, versions of the cybercriminal tools **Hydra** (a trojan horse-type malware) and **CraxsRat** (an *Android*-targeting remote access tool) were reportedly used against supposedly military personnel in Ukraine whose targeting is generally associated with an intrusion sets aligned with Russian state interests [30, 86].

Comment: Using tools generally associated with the cybercriminal ecosystem in the course of espionage operations illustrates the adaptability of some offensive actors who are able to reuse codes in different contexts. ANSSI cannot assess how the codes have precisely been acquired. They might have been purchased or obtained for free on cybercriminal marketplaces or forums.

3.1.1.2 Offensive capabilities can be operated for espionage and surveillance purposes

ANSSI, or other C4 members (depending on the victim's choosing), is regularly asked to analyse suspected compromise of mobile phones after their owners received a security notification from vendors such as APPLE. The positions held by those individuals demonstrate that offensive actors leverage mobile phone compromises to obtain sensitive data relating to French national interests. This is especially true where the phone owners have repeatedly received security notifications, showing a precise and persistent targeting of French personalities.

State-sponsored espionage campaigns targeting mobile devices sometimes appear related to national and international events. As an example, offensive operations lead by the operators of the Nobelium intrusion set have targeted the Mongolian government between 2023 and 2024, probably in relation to Vladimir Putin's State visit in Mongolia which took place in September 2024 [44, 87].

ANSSI has also handled cases of compromised mobile phones belonging to members of the executive committee of companies operating in strategic economic sectors.

Spyware can also be used for economic and industrial espionage purposes. Twelve European Union representatives and prominent figures sharing a declared interest on illegal fishing issues have for instance been targeted between February and June 2023 by allegedly Vietnamese

offensive actors[35] through messages sent from a fake *Twitter* account[36] [88].

Recommendations on mobile phone use in a professional environment

- Separate professional and personal use on mobile devices.
- When discussing sensitive topics, store the mobile phones in another room at a safe distance

State-sponsored espionage campaigns against mobile devices can also occur in times of high intensity conflicts. Mobile devices belonging to Ukrainian military forces have for instance been targeted by operators of reportedly Russian or Russian-aligned intrusion sets in the context of the Russian annexation of Crimea and of the subsequent Russian invasion of Ukraine starting February 2022 [27, 52]. Armed forces increasingly rely on mobile devices to exchange tactical information (military communication, geolocation, etc.), in turn attracting the interest of offensive actors.

Several reputedly State-sponsored intrusion sets, some with links to China, Iran and Russia, have already been observed in use against ethnic minorities and individuals regarded as dissidents (NGO, journalists, lawyers, human rights defenders). Some reportedly Chinese intrusion sets have been used for many years to target individuals deemed by the Chinese government as dissidents or dangerous for the stability of the regime [89]. CHECK POINT RESEARCH also wrote in February 2021 that the reputedly Iranian intrusion set known as Domestic Kitten (also called APT-C-50) has been used to target more than 1200 persons including dissidents, Kurdish minority members and supporters of the Islamic State [90]. This intrusion set has been active since at least 2017 and relies on the use of the **FurBall** spyware to target its victims. In 2021, a similar campaign was observed where the *Android* spyware **Pineflower** was deployed by the intrusion set UNC788[37], reputedly linked to the Iranian Islamic Revolutionary Guard Corps [91].

Spyware are also massively used to target journalists and figures of the civil society. In 2025, CITIZEN LAB reported on the use of the **Graphite** spyware, developed by the Israeli company PARAGON, through *WhatsApp* to compromise victims in Italy. A report published by the Italian parliament on June, 5th 2025 demonstrated the responsibility of the Italian intelligence services in the use of **Graphite** against two Italian members of the NGO MEDITERRANEA SAVINGS HUMANS [51, 92, 93].

3.1.2 Corporate-sponsored operations

Some PSOAs such as the Israeli company BLACK CUBE offer mobile-specific spyware to companies in litigation, albeit less sophisticated ones than the malware provided by other PSOAs described earlier [94, 95]. Other PSOAs offer even less sophisticated tools but have a large workforce at their disposal used to provide specific services to a vast array of customers including major companies and private intelligence agencies. This threat is less visible and mostly underestimated.

[35] Vietnam has been warned in 2017 by the European Union with a "yellow card" over insufficient action to fight illegal fishing, as the Vietnamese fish exports generate more than 750 millions Euros of revenue each year. Had a "red card" been voted, Vietnam would have been barred from exporting its fish production to the European Union and would have provoked a major loss of revenue for Vietnam [88].

[36] In this case, the attacker replied to tweets of interest using the profile "@joseph_Gordon16", directly calling out to the targeted figures and systematically attaching to their tweets a link leading to a malicious website which ultimately enabled a compromise of the mobile phone used by the victims to visit *Twitter*.

[37] This intrusion set is also known as TA453 or APT42

For instance, the Indian company BELLTROX was created in 2013 and is presenting itself as an *ethical hacking company*, when it actually provides its customers with a wide array of offensive capabilities oriented towards strategic business intelligence [96]. Its customer base is believed to be mostly composed of mainly western companies looking to spy on their competitors. Known victims are mostly located in the United States and in Europe and belong to various economic sectors: finance, pharmaceuticals, media, energy. In 2015, the CEO of BELLTROX Sumit Gupta has allegedly been indicted for the compromise of *Skype* and messaging accounts belonging to employees of an US company which appear to have been mandated by one of its competitors [97] . The intrusion set associated with BELLTROX is publicly known as **Dark Basin**. It has been used against a variety of victims, which is typical of a mercenary intrusion set. More than 13,000 targets have reportedly been compromised by **Dark Basin** between 2013 and 2020 [98].

3.1.3 Privately-sponsored operations in the course of litigation or for revenge

A stalkerware is a software which can be installed on mobile devices, allowing a third-party to track the location of the device and to access its messages, phone calls and social media profiles without the user's knowledge.

In order to avoid getting blocked on applications stores, stalkerware are usually marketed as parental controls and remote employee monitoring solutions. These applications, which supposedly require the user's agreement to be installed, are actually set to be invisible and undetectable[38] [99]. According to KASPERSKY, in 2023, nearly 31 000 users of mobile devices may have been targeted by stalkerware, including 330 cases in France [100]. stalkerware are particularly seen in cases of domestic violence where they facilitate the controlling and abusive behaviour of the abuser [101]. As the deployment of these offensive tools often requires a physical access to the targeted device, the abuser is often part of the victim's family, or social or professional circle.

Besides the privacy and consent concerns raised by stalkerware, this type of tool also create serious security issues as they often contain multiple vulnerabilities while accessing and storing sensitive data. ESET has for instance identified more than 150 known vulnerabilities in 58 *Android* stalkerware, creating serious security risks for the victims. The most commonly observed vulnerability in stalkerware is the plaintext exchange of data over the http protocol without any additional security, which can facilitate an AITM attack [99] leaking both the victim and the abuser's data. In February 2025, a data leak causes by development errors affected millions of victims of the stalkerware Spyzie, CocoSpy and Spyic, leaking their messages, pictures, call logs and other sensitive data [102, 103].

3.2 Other objectives motivating offensive operations

ANSSI has not yet handled any case of profit or destabilisation-motivated mobile phone compromise. Mobile devices are clear targets of interest of cybercriminals who can opportunistically exploit their weaknesses for profit. That is, cybercriminal will compromise devices belonging to both individuals and companies without targeting a specific victim profile. Destabilisation oriented attacks are on the other hand an uncommon occurrence even though the consequences on the targeted population are significant.

[38] It is actually more complicated to install these tools on *iOS* as either the *iCloud* password of the user is required or the phone has to be jailbroken in order to successfully install them [99].

3.2.1 Attacks pursuing a destabilisation objective

Hacktivist groups have operated destabilisation-oriented operations against mobile devices to cause a panic, notably by compromising applications programming interfaces (API). For instance, on November, 15th 2023, the pro-Palestinian hacktivist group AnonGhost claimed on its *Telegram* channel having successfully exploited a vulnerability in the API of the Israeli application *Red Alert* used to send real-time notifications of incoming missile attacks against Israel. This alleged attack might have allowed AnonGhost to send fake messages to 10 000 to 20 000 users of the application alerting of an imminent nuclear attack against Israel[39] [104].

Another example can be found in the 2022 compromise of the Russian ridesharing application *YandexTaxi* by the hacktivist collective Anonymous and the pro-Ukrainian hacktivist group IT Army of Ukraine, bringing about a gathering of every single available Moscow taxi at the "Hotel Ukraina" [105]. Both of these cases demonstrate that attacks against mobile phones can be leveraged to cause a panic among the targeted population to support a political claim.

3.2.2 For-profit attacks against mobile devices

The ubiquity of mobile devices and the personal data they store make them a prime target for cybercriminals [18]. Cybercrime-oriented malware are generally developed to collect banking data to misappropriate the victim's funds or collect and sell the victim's data to other cybercriminal actors [106]. Dissemination methods for cybercriminal codes can vary from phishing campaigns to cloning legitimate applications.

Cybercriminal codes targeting mobile devices can be used to remotely control a mobile phone, record the text input and collect SMS messages as well as collect banking and cryptocurrency wallets credentials, as is the case with the *Android* malware **Copybara** [107]. The collected credentials are then either directly reused or sold to other criminal actors [108, 106]. As is already the case with malware targeting computers, these codes are either developed by cybercriminals or acquired through cybercriminal markeplaces[40].

Cybercriminal groups already known to compromise desktop environments have been observed turning to mobile environments. In January 2025 for instance, the cybercriminal actor TA2727 has deployed the infostealers **LummaStealer**, **Marcher** and **FrigidStealer**, respectively targeting *Windows*, *Android* and *macOS* [109] to steal credentials.

Mobile devices can also be used by attackers as a first step towards compromising desktop environments. For instance, since 2023 the cybercriminal group Scattered Spider has been using sophisticated SMS and voice phishing attacks to collect 2FA tokens. The tokens are reused by the attackers against information systems to deploy ransomware and collect data [20].

Comment: ANSSI has yet to observe a case where a mobile phone is compromised specifically with the aim of later compromising a desktop environment. Mobile devices could well become targets of interest in for-profit attacks: mobile environment present many technical opportunities for compromise and store valuable data, which could generate a high return on investment for malicious actors. In the light of this threat, it then appears crucial to maintain a high security level when a mobile fleet is integrated in a corporate information system.

[39] This operation took place in the context of a large hacktivist campaign against Israel and its sponsors after October, 7th 2023.

[40] Malware sold and bought through cybercriminal networks is called "malware-as-a-service".

4 RECOMMENDATIONS

Recommendations on Wi-Fi usage

- **Completely deactivate Wi-Fi interface** on the phone when Wi-Fi is not needed, to avoid any connection to fake networks.
- *Note: On iOS, turning-off Wi-Fi must be done by using the Settings application; the Control center parameter is indeed only disconnecting from the network without turning off the interface.*
- **Deactivate automatic connection to the known networks** already saved in the phone, including private networks.
- **Avoid as much as possible to connect the mobile device to public networks**. When it cannot be avoided, a VPN must be used to encrypt the information passing through the public network. The VPN must use cryptography protocols such as IPSec[a] or TLS[b] and must be controlled by the user in order to guarantee the confidentiality of communications.

[a] https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-ipsec
[b] https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-tls

Recommendations on Bluetooth protocol usage

- **Completely deactivate the Bluetooth interface** on the mobile phone when a Bluetooth connection is not required. Please note that with *iOS*, turning off Bluetooth must be done by using the *Settings* application; the *Control center* parameter is actually only disconnecting the paired devices without deactivating the Bluetooth interface.
- **Do no pair the mobile device to uncontrolled or shared devices**, to avoid any exploitation or data leak through theses.

Recommendation on NFC protocol usage

- **Deactivating the NFC interface** on the device helps avoiding the interception of payment card data in case of a compromise. Please note it is only possible to deactivate the NFC interface on *Android*.

Recommendation on multi-factor authentication

- **Lock the SIM card with a PIN code** and **change the default code**. A SIM card that is locked and protected by a PIN code cannot be used in an alternative device, which limits the attacker's ability to obtain two-factor authentication codes (2FA).
- **Using authentication application** (**TOTP**) helps prevent the hijacking of an online account protected by a two factor authentication in case of the theft of a SIM card or of a SIM swapping scam.

Recommendations on hardening the operating system

These hardened modes for the operating systems add many limits on media formats, hyperlinks embedded in messages and network protocols.
Note: These parameters are recommended for individuals who might be targeted by sophisticated threats. Some features of the devices used on daily basis might not work properly[a]*, and as such the activation of the hardened modes may be limited to some specific time period (business travel, trips abroad, sensitive political or commercial climate).*

- On *iOS*, hardening the operating system is possible using the *Lockdown Mode*[b]. It has been available since *iOS* 16 released in 2022. Some features are impacted such as messaging (blocking attachments and embedded links), web browsing (restriction of certain display technologies and media). It is however possible to manually exclude some applications and websites from this mode in order to ensure that they function normally.
- On *Android*, hardening features can be enabled through the *Advanced Protection Mode*[c], which has been available since *Android* 16 released in 2025. Impacted features are messaging (spam filtering), automatic lock and restart in certain circumstances, and blocking installation of applications without using an official store.

[a] For instance, on *iOS* and *Android* Wi-Fi connection to open networks or to network with obsolete security features is no longer automatic and the deactivation of 2G means that there will be no connection available in areas only covered by 2G
[b] https://support.apple.com/105120
[c] https://security.googleblog.com/2025/05/advanced-protection-mobile-devices.html

Recommendations on messaging applications

- **Deactivate the preinstalled messaging applications if not used**, because these ones, by their ubiquity on every mobile devices, are an initial vector of choice for the attackers.
- **Deactivate the automatic reception of MMS messages**, to avoid the processing of them without any action of the user.
- **Avoid exchanging sensitive information via SMS** and **prefer messaging apps that use end-to-end encryption** to ensure the confidentiality of the exchanges.
- Deactivate the automatic backup of chats within these applications.

Recommendation on the reboot of the device

- **Reboot the device**. The complete shutdown of the device stops every processes and removes every software residing only in memory, such as a memory-based non-persistent spyware. When the device is restarting, the memory-based spyware will not be executed. The deletion of a spyware does not however protect from a reinfection using the same, previously-used vector.
- **Power off then power on the device without using the reboot feature** as some spyware are able to simulate a reboot to deceive the user.

Recommendation on phishing

- **Do not click on links or open files** embedded in unsolicited messages. In any doubt, it is advisable to verify the legitimacy of the message by using another channel than the one used in reception.
- **Be vigilant when links received through QR codes are opened**. QR codes do not allow to visually identify the link's target and might be used by criminals to perform a redirection towards malicious payloads.

Recommendation on the physical protection of mobile devices

- **Do not connect the phone to unknown devices**[a].
- **Use a trusted USB data blocker** when charging the mobile phone on an unknown USB port cannot be avoided. This tool filters the internal connection of an USB port and only allows the flow of electrical power as needed to charge up the device. USB data blockers might however be themselves attack vectors and it is recommended to avoid using unverified blockers such as those that can be offered during a conference.
- **Protect the device with a strong password**. Mobile devices increasingly require entering the unlock password to transfer data through physical ports and a strong one will limit the risk of compromise using this method. It is also recommended to **avoid using biometric authentication** (facial recognition and fingerprints) to prevent the possibility of unlocking a mobile device without knowing its password.
- **Completely turn off the device** when leaving it unattended cannot be avoided. Many features are disabled on the phone when turned on as long as it has not been unlocked once after being turned off, thus considerably reducing the phone's attack surface.

Note: Android's Advanced Protection Mode[b] *disables USB data transfer when the phone is locked, allowing only electrical charge. It is also the default behavior on iOS where connecting the mobile phone to a USB port or device is only possible when the mobile phone is unlocked.*

[a] For instance public charging stations
[b] Released with Android 16

Recommendations regarding built-in features

- **Be vigilant when access to accessibility features is requested** and when an application seems suspicious, **remove it**. Access to the accessibility features by an applications is not possible without the explicit consent of the user, materialised by a confirmation message appearing at the first run of the application .

Recommendation on updating the operating system

- **Always apply operating system updates** as soon as possible when they are made available to patch the vulnerabilities impacting components and security mechanisms.

Recommendation on unused applications

- **Uninstall or disable applications which are never or rarely used** (such as applications related to travels, events, games, social media, etc.). These applications create an unnecessarily large attack surface on the mobile device. On *iOS* and *Android* it is possible to remove the software without removing the data:
- *iOS*: *Settings* → *General* → *iPhone Storage* then click on each application to offload and select *Offload App*.
- *Android*: *Settings* → *Apps* then click on each application to archive and select *Archive*.

Recommendations regarding permissions granted to applications

- **Verify the permissions granted for each application** installed on the device. In the recent version of *Android* and *iOS*, these information are centralised in the settings menu:
  - *Android*: *Settings* → *Security and privacy* → *Permissions manager*
  - *iOS*: *Settings* → *Privacy*
- **Manage the permissions granted for each application** when it is possible. Thus, when a permission does not seem to be necessary and does not impact the application's functioning, it is advised to remove it.
- **Avoid applications that appear to be asking for excessive permissions** when a new application is about to be installed.

Recommendations regarding the applications installation sources

- **Do not install applications from sources other than the official application stores**, especially when the applications can be directly downloaded from a third-party source or through an alternative store. Official stores are more closely watched than the latter, limiting the risks of downloading a trojanised application.

Recommendation on advertisement profiling

Remove and/or renew the advertising identifier following this procedure:

- *Android*: *Settings* → *Security and privacy* → *Privacy* → *More privacy settings* → *Ads* → *Delete Advertising ID* or *Reset Advertising ID*
- *iOS*: *Settings* → *Privacy* → *Apple Advertising* then turn-off *Personalised Ads*

Recommendation on using a mobile device in a foreign country

- When travelling abroad, it is recommended to apply the recommendations found in this document.
- When the object or location of a trip abroad is deemed sensitive, it is recommended to use a separate mobile phone.

Recommendations on mobile phone use in a professional environment

- **Never use a personal mobile device for work-related tasks**. Thus, even if the personal mobile phone is compromised, the attacker will not be able to access or use work-related data.
- **Remove all electronic device from the room when discussing sensitive topics.** Mobile devices must also be removed from meeting rooms. Shutting down a mobile phone's wireless connections, for instance when turning on the *Airplane Mode*, is not an adequate measure to ensure the security of sensitive talks as it does not prevent a spyware from recording the discussion and eventually transferring it to the attacker when wireless connections are turned on again.

Recommendations for organisations

These recommendations are specific to business mobiles devices.

On mobile fleet management

- **Use an MDM software to manage a business mobile fleet**[a] and apply the recommendations detailed in this document. An MDM software enables a centralised management of business mobile phones with essential features such as remote update deployment and application permissions management.
- When a business phone is lost or stolen, **remotely reset the device and its data using the MDM software** to prevent any risk of an attacker exploiting the data stored on the phone (such as VPN certificates and messaging accounts credentials) to gain access and compromise the corporate network. Revoke and renew the credentials on the corporate networks following loss or theft of a mobile device.

On the use of Bluetooth connections

- **Never use Bluetooth devices when a communication is deemed sensitive.**

On the use of Wi-Fi networks

- **Establish a list of authorised Wi-Fi networks through the MDM softare** in order to limit the risk of seeing a business phone connecting to an unknown and potentially malicious Wi-Fi network.
- **Never hide the network's name** (ESSID[b]) when deploying a Wi-Fi network, to prevent malicious connection attempts.

When travelling abroad

- **Avoid the use of local cellular networks** when in a foreign country. For voice calls, **opt for "Wi-Fi call" using a known and controlled IPSec VPN and rely on secure messaging applications** rather than SMS messages to exchange text messages.

[a] Mobile Devices Management
[b] Extended Service Set Identification

5 GLOSSARY

ISP Internet Services Provider. 21

0-day A vulnerability exploited before any corrective measure is available. 3, 13, 19

1-click An exploit chain requiring an action from the user. 18, 19

2FA Two factors authentication. 9, 25, 26

ADINT A contraction of ”advertising” and ”intelligence”, ADINT is a data collection method relying on advertisement; it relies on either large-scale or targeted delivery of advertisement to one or more targets with the aim of profiling, tracking and locating them. 18, 20

AITM An Adversary-in-the-middle attack is a type of attack where an attacker position themselves between networked devices, allowing them to effectively intercept the exchanged data. 6, 7, 24

base transceiver station An equipment used to connect mobile devices to a cellular network. 6, 7

CCIC Commercial Cyber Intrusion Capabilities are privately-operated offensive cyber capabilities enabling an attacker to penetrate a network owned by an individual or an organisation to disrupt, alter, degrade, destroy the targeted network and/or collect their data. 3, 20

exploit chain Vulnerabilities exploited successively in a chain, enabling an attacker to gradually gain access and take over a network. 8, 10, 11, 13–15, 18–21

IMEI The International Mobile Equipment Identity is a unique numeric identifier attributed to each mobile device. 7

IMSI The International Mobile Subscriber Identity is a unique numeric identifier attributed to each user on a cellular network. 7

IMSI catcher An IMSI catcher is a device or a technical set-up which simulates a base transceiver station and intercepts the International Mobile Subscriber Identity attributed to the nearby mobile devices before transferring them further to the network base station. 7

intrusion set A set of tactics, techniques and procedures associated with a specific theat actor or a group of threat actors. 3, 9, 12, 13, 16, 18, 20, 22–24

PSOA A Private Sector Offensive Actor is a privately-operated offensive actor offering and/or performing actions aiming to penetrate a network owned by an individual or an organisation to disrupt, alter, degrade, destroy the targeted network and/or collect their data. 3, 7, 8, 12, 19, 20, 22, 23

stalkerware A software deployed on mobile devices enabling a third party to track the geolocation of a device and to gain access to the messages, voice calls and social media profiles without the user’s knowledge. 18, 24

zero-click An exploit chain that does not require any action from the user. 3, 10–12, 14, 15, 19, 21

6 REFERENCES

[1] Ministère de l'Europe et des Affaires étrangères. *Processus de Pall Mall : code de bonnes pratiques à destination des États, pour lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché (avril 2025)*. April 2025.
URL: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/processus-de-pall-mall-code-de-bonnes-pratiques-a-destination-des-etats-pour.

[2] Dare Abodunrin, Yoan Miche, and Silke Holtmanns. *Some Dangers from 2G Networks Legacy Support and a Possible Mitigation*. September 2015.
URL: https://ieeexplore.ieee.org/document/7346872.

[3] Libération. *SMS frauduleux et Imsi-catchers : les dessous d'une escroquerie dernier cri*. June 2025.
URL: https://www.liberation.fr/societe/police-justice/imsi-catchers-et-sms-frauduleux-les-dessous-dune-escroquerie-dernier-cri-20230423_TNQT6AJF65EGVP5BZBJ62VSQZM/.

[4] Amnesty International. *Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products*. October 2023.
URL: https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

[5] Bleeping Computer. *T-Mobile Says New Data Breach Caused by SIM Swap Attacks*. December 2021.
URL: https://www.bleepingcomputer.com/news/security/t-mobile-says-new-data-breach-caused-by-sim-swap-attacks/.

[6] Al-Estiklal. *Tal Dilian — A Former Career IDF Intelligence Officer Turned Spy Technology Entrepreneur*. July 2022.
URL: https://www.alestiklal.net/en/article/tal-dilian-a-former-career-idf-intelligence-officer-turned-spy-technology-entrepreneur.

[7] Intelligence Online. *Magen, la start-up qui chamboule l'interception Wifi*. December 2015.
URL: https://www.intelligenceonline.fr/surveillance--interception/2015/12/16/magen-la-start-up-qui-chamboule-l-interception-wifi,108117226-art.

[8] Australian Federal Police. *Man Charged over Creation of 'evil Twin' Free WiFi Networks to Access Personal Data*. June 2024.
URL: https://www.afp.gov.au/news-centre/media-release/man-charged-over-creation-evil-twin-free-wifi-networks-access-personal.

[9] Legend. *Sébastien Lecornu, Ministre Des Armées : Attentats Déjoués, Tout Ce Qu'on Ne Sait Pas (Nucléaire, Etc.)* March 2025.
URL: https://www.youtube.com/watch?v=H0D4a_O_bxY.

[10] NRK. *Someone Could Be Tracking You through Your Headphones*. September 2021.
URL: https://nrkbeta.no/2021/09/02/someone-could-be-tracking-you-through-your-headphones/.

[11] NOTUS. *War Zone Surveillance Technology Is Hitting American Streets*. April 2024.
URL: https://www.notus.org/technology/war-zone-surveillance-border-us.

[12] The New York Times. *In Stores, Secret Bluetooth Surveillance Tracks Your Every Move*. June 2019.
URL: https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

[13] The Walt Disney Company. *Privacy At The Walt Disney World Resort, The Disneyland Resort, And Aulani, A Disney Resort & Spa, And On Disney Cruise Line Vacations - Frequently Asked Questions About Bluetooth® Technology*. April 2023.
URL: https://privacy.thewaltdisneycompany.com/en/resortble/.

[14] Libération. *Les panneaux de pub du métro tracent-ils les téléphones des usagers ?* March 2019.
URL: https://www.liberation.fr/checknews/2019/03/25/les-panneaux-de-pub-du-metro-tracent-ils-les-telephones-des-usagers_1717316/.

[15] Armis. *BlueBorne Cyber Threat Impacts Amazon Echo and Google Home*. November 2017.
URL: https://www.armis.com/blog/blueborne-cyber-threat-impacts-amazon-echo-and-google-home/.

[16] Oligo Security. *Airborne: Wormable Zero-Click RCE in Apple AirPlay Puts Billions of Devices at Risk*. April 2025.
URL: https://www.oligo.security/blog/airborne.

[17] Tristan Claverie and José Lopes Esteves. *BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols*. May 2021.
URL: https://ieeexplore.ieee.org/document/9474325.

[18] WeLiveSecurity. *NGate Android Malware Relays NFC Traffic to Steal Cash*. August 2024.
URL: https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/.

[19] Action Fraud Police UK. *Alert – How You Can Be Scammed by a Method Called SIM Splitting*. September 2014.
URL: https://www.actionfraud.police.uk/alert/alert-how-you-can-be-scammed-by-a-method-called-sim-splitting.

[20] CISA. *Scattered Spider*. November 2023.
URL: https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf.

[21] ANSSI. *État de la menace ciblant le secteur des télécommunications*. December 2023.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/.

[22] Vice. *They Got 'Everything': Inside a Demo of NSO Group's Powerful iPhone Malware*. September 2018.
URL: https://www.vice.com/en/article/inside-nso-group-spyware-demo/.

[23] Google Project Zero. *A Deep Dive into an NSO Zero-Click iMessage Exploit: Remote Code Execution*. December 2021.
URL: https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html.

[24] Kaspersky. *Operation Triangulation: iOS Devices Targeted with Previously Unknown Malware*. June 2023.
URL: https://securelist.com/operation-triangulation/109842/.

[25] Citizen Lab. *Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers*. April 2023.
URL: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[26] Google Project Zero. *Blasting Past Webp*. March 2025.
URL: https://googleprojectzero.blogspot.com/2025/03/blasting-past-webp.html.

[27] Crowdstrike. *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units*. December 2016.
URL: https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[28] Microsoft Threat Intelligence Center. *New Star Blizzard Spear-Phishing Campaign Targets WhatsApp Accounts*. January 2025.
URL: https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/.

[29] Google Threat Analysis Group. *How We Protect Users from 0-Day Attacks*. July 2021.
URL: https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

[30] CERT-UA. *Attempts of cyber attacks on military systems using malware for mobile devices*. September 2024.
URL: https://cert.gov.ua/article/6280563.

[31] META. *Adversarial Threat Report: Countering the Surveillance-for-Hire Industry & Influence Operations*. February 2024.
URL: https://transparency.fb.com/sr/Q4-2023-Adversarial-threat-report.

[32] Wired. *This Secretive Firm Has Powerful New Hacking Tools*. June 2021.
URL: https://www.wired.com/story/phone-hacking-mollitiam-industries/.

[33] Lookout. *Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus*. December 2024.
URL: https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware.

[34] Lookout. *Lookout Discovers Massistant Chinese Mobile Forensic Tooling*. July 2025.
URL: https://www.lookout.com/threat-intelligence/article/massistant-chinese-mobile-forensics.

[35] Lookout. *Lookout Discovers Android Spyware Tied to Iranian Police Targeting Minorities: BouldSpy*. April 2023.
URL: https://www.lookout.com/blog/iranian-spyware-bouldspy.

[36] Amnesty International. *"A Digital Prison" Surveillance and the Suppression of Civil Society in Serbia*. December 2024.
URL: https://securitylab.amnesty.org/latest/2024/12/a-digital-prison-surveillance-and-the-suppression-of-civil-society-in-serbia/.

[37] SBU. *SBU Exposes Russian Intelligence Attempts to Penetrate Armed Forces' Planning Operations System*. August 2023.
URL: https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system.

[38] CISA. *CISA and International Partners Release Malware Analysis Report on Infamous Chisel Mobile Malware*. August 2024.
URL: https://www.cisa.gov/news-events/alerts/2023/08/31/cisa-and-international-partners-release-malware-analysis-report-infamous-chisel-mobile-malware.

[39] Recorded Future. *Lithuanian Government Warns about Secret Censorship Features in Xiaomi Phones*. September 2021.
URL: https://therecord.media/lithuanian-government-warns-about-secret-censorship-features-in-xiaomi-phones/.

[40] Kaspersky. *Triada: A Trojan Pre-Installed on Android Smartphones out of the Box*. July 2025.
URL: https://www.kaspersky.com/blog/trojan-in-fake-smartphones/53331/.

[41] Citizen Lab. *Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*. April 2023.
URL: https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/.

[42] Google Project Zero. *FORCEDENTRY: Sandbox Escape*. March 2022.
URL: https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html.

[43] Donncha O'Cearbhaill and Bill Marczak. *Exploit Archaeology: A Forensic History of in-the-Wild NSO Group Exploits*. September 2022.
URL: https://www.virusbulletin.com/conference/vb2022/abstracts/exploit-archaeology-forensic-history-wild-nso-group-exploits/.

[44] Google Threat Analysis Group. *State-Backed Attackers and Commercial Surveillance Vendors Repeatedly Use the Same Exploits*. August 2024.
URL: https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/.

[45] Threat Fabric. *Exposing Crocodilus: New Device Takeover Malware Targeting Android Devices*. March 2025.
URL: https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices.

[46] Kaspersky. *Operation Triangulation: The Last (Hardware) Mystery*. December 2023.
URL: https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/.

[47] Amnesty International. *Forensic Appendix: Pegasus Zero-Click Exploit Threatens Journalists in India*. December 2023.
URL: https://securitylab.amnesty.org/latest/2023/12/pegasus-zero-click-exploit-threatens-journalists-in-india/.

[48] Google Threat Analysis Group. *Buying Spying: How the Commercial Surveillance Industry Works and What Can Be Done about It*. February 2024.
URL: https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

[49] Google Project Zero. *MMS Exploit Part 1: Introduction to the Samsung Qmage Codec and Remote Attack Surface*. July 2020.
URL: https://googleprojectzero.blogspot.com/2020/07/mms-exploit-part-1-introduction-to-qmage.html.

[50] Zimperium. *WhatsApp Buffer Overflow Vulnerability: Under the Scope*. June 2019.
URL: https://zimperium.com/blog/whatsapp-buffer-overflow-vulnerability-under-the-scope.

[51] Citizen Lab. *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*. March 2025.
URL: https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/.

[52] Google Threat Intelligence Group. *Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger*. February 2025.
URL: https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger.

[53] Kaspersky. *SparkCat Crypto Stealer in Google Play and App Store*. February 2025.
URL: https://securelist.com/sparkcat-stealer-in-app-store-and-google-play/115385/.

[54] ESET. *Spain's La Liga App Uses Fans' Phones to Detect Illegal Soccer Broadcasts*. June 2018.
URL: https://www.welivesecurity.com/2018/06/12/spains-la-liga-app-phones-detect-illegal/.

[55] Google Cloud. *Threat Horizons - August 2023*. August 2023.
URL: https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf.

[56] ESET. *Android App Breaking Bad: From Legitimate Screen Recording to File Exfiltration within a Year*. May 2023.
URL: https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/.

[57] Lookout. *Monokle*. July 2019.
URL: https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf.

[58] ANSSI. *Ciblage et compromission d'entités françaises au moyen du Mode Opératoire d'Attaque APT28*. April 2025.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-006/.

[59] Cure53. *Analysis-Report "Study the Great Nation" 08.-09.2019*. September 2019.
URL: https://cure53.de/analysis_report_sgn.pdf.

[60] CNN. *Chinese Communist Party Propaganda? There's an App for That*. February 2019.
URL: https://www.cnn.com/2019/02/15/asia/china-xi-jinping-communist-party-app-intl.

[61] BBC News. *Russia targets WhatsApp and pushes new 'super-app' as internet blackouts grow*. September 2025.
URL: https://www.bbc.com/news/articles/ce9rj2145jgo.

[62] Reuters. *Russia orders state-backed MAX messenger app, a WhatsApp rival, pre-installed on phones and tablets*. September 2025.
URL: https://www.reuters.com/technology/russia-orders-state-backed-max-messenger-app-whatsapp-rival-pre-installed-phones-2025-08-21/.

[63] Politico. *Russia's answer to WhatsApp: Kremlin puts a spy in every new phone*. September 2025.
URL: https://www.politico.eu/article/russia-app-max-data-privacy-concerns-whatsapp-kremlin-china/.

[64] Natto Thoughts. *I-SOON: Another Company in the APT41 Network*. October 2023.
URL: https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

[65] Natto Thoughts. *The Pangu Team—iOS Jailbreak and Vulnerability Research Giant: A Member of i-SOON's Exploit-Sharing Network*. February 2025.
URL: https://nattothoughts.substack.com/p/the-pangu-teamios-jailbreak-and-vulnerability.

[66] Kaspersky. *iOS Exploit Chain Deploys LightSpy Feature-Rich Malware*. March 2020.
URL: https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/.

[67] Volexity. *BrazenBamboo Weaponizes FortiClient Vulnerability to Steal VPN Credentials via DEEPDATA*. November 2024.
URL: https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/.

[68] Reuters. *'Karma': Inside the Hack Used by the UAE to Break into iPhones of Foes*. January 2019.
URL: https://www.reuters.com/investigates/special-report/usa-spying-karma/.

[69] Vice. *Hacking Team Gave Spyware Demos to Police Agencies Across the Nation*. July 2015.
URL: https://www.vice.com/en/article/hacking-team-gave-spyware-demos-to-police-agencies-across-the-nation/.

[70] The Hacker News. *Zero-Day Flash Player Exploit Disclosed in 'Hacking Team' Data Dump*. July 2015.
URL: https://thehackernews.com/2015/07/flash-zero-day-vulnerability.html.

[71] ESET. *New Traces of Hacking Team in the Wild*. March 2028.
URL: https://www.eset.com/gr-en/about/newsroom/press-releases-1/new-traces-of-hacking-team-in-the-wild/.

[72] BBC News. *Hackers Targeted Foreign Office Data*. April 2017.
URL: https://www.bbc.com/news/technology-39588703.

[73] F-Secure. *The Callisto Group*. April 2017.
URL: https://labs.withsecure.com/content/dam/labs/docs/callisto-group.pdf.

[74] Citizen Lab. *New Pegasus Spyware Abuses Identified in Mexico*. October 2022.
URL: https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

[75] Atlantic Council. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. September 2024.
URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

[76] Citizen Lab. *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*. July 2021.
URL: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[77] Le Monde. *« Projet Pegasus » : comment la société israélienne NSO Group a révolutionné l'espionnage*. July 2021.
URL: https://www.lemonde.fr/projet-pegasus/article/2021/07/19/projet-pegasus-comment-la-societe-israelienne-nso-group-a-revolutionne-l-espionnage_6088692_6088648.html.

[78] TechCrunch. *Israeli Spyware Maker Paragon Bought by US Private Equity Giant*. December 2024.
URL: https://techcrunch.com/2024/12/16/israeli-spyware-maker-paragon-bought-by-u-s-private-equity-giant/.

[79] Intelligence Online. *L'ADINT, planche de salut du cyber israélien*. May 2023.
URL: https://www.intelligenceonline.fr/surveillance--interception/2023/05/26/l-adint-planche-de-salut-du-cyber-israelien,109977613-art.

[80] Intelligence Online. *Offensive ADINT Is Israeli Cyber Sector's New Secret Weapon*. February 2024.
URL: https://www.intelligenceonline.com/surveillance--interception/2024/02/15/offensive-adint-is-israeli-cyber-sector-s-new-secret-weapon,110159842-eve.

[81] Forbes. *Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps*. December 2020.
URL: https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/.

[82] Bloomberg. *Your Ad Data Is Now Powering Government Surveillance*. May 2023.
URL: https://www.bloomberg.com/news/articles/2023-05-11/surveillance-company-turns-ad-data-into-government-tracking-tool.

[83] Haaretz. *Israel Tried to Keep Sensitive Spy Tech Under Wraps. It Leaked Abroad*. April 2024.
URL: https://www.haaretz.com/israel-news/security-aviation/2024-04-11/ty-article/.premium/israel-tried-to-keep-sensitive-spy-tech-under-wraps-it-leaked-abroad/0000018e-c948-d480-a99e-cf5f24900000.

[84] Irish Council for Civil Liberties. *Europe's Hidden Security Crisis*. November 2023.
URL: https://www.iccl.ie/digital-data/europes-hidden-security-crisis/.

[85] Lighthouse Reports. *Revealing Europe's NSO*. August 2022.
URL: https://www.lighthousereports.nl/investigation/revealing-europes-nso/.

[86] Google Threat Intelligence Group. *Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives*. October 2024.
URL: https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives.

[87] France 24. *La visite de Vladimir Poutine en Mongolie, "un pied de nez" lancé à la CPI*. September 2024.
URL: https://www.france24.com/fr/europe/20240903-la-visite-de-vladimir-poutine-en-mongolie-un-pied-de-nez-lanc%C3%A9-%C3%A0-la-cpi.

[88] Mediapart. *L'incroyable puissance des armes de surveillance de Nexa et Intellexa*. October 2023.
URL: https://www.mediapart.fr/journal/international/071023/l-incroyable-puissance-des-armes-de-surveillance-de-nexa-et-intellexa.

[89] Crowdstrike. *CrowdStrike 2025 Global Threat Report*. February 2025.
URL: https://www.crowdstrike.com/explore/2025-global-threat-report.

[90] Checkpoint. *Domestic Kitten – An Inside Look at the Iranian Surveillance Operations*. February 2021.
URL: https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/.

[91] Emiel Haeghebaert. *UNC788: Iran's Decade of Credential Harvesting and Surveillance Operations*. October 2021.
URL: https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf.

[92] The Guardian. *Italian Government Approved Use of Spyware on Members of Refugee NGO, MPs Told*. March 2025.
URL: https://www.theguardian.com/world/2025/mar/27/italian-government-approved-use-of-spyware-on-members-of-refugee-ngo-mps-told.

[93] Citizen Lab. *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*. June 2025.
URL: https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/.

[94] The Guardian. *Ronan Farrow on Surveillance Spyware: 'It Threatens Democracy and Freedom'*. November 2024.
URL: https://www.theguardian.com/tv-and-radio/2024/nov/23/ronan-farrow-surveilled-documentary.

[95] Intelligence Online. *Black Cube au secours de Beny Steinmetz contre Vale*. May 2020.
URL: https://www.intelligenceonline.fr/renseignement-d-affaires_premier-cercle/2020/05/27/black-cube-au-secours-de-beny-steinmetz-contre-vale,108407256-bre.

[96] Citizen Lab. *Dark Basin: Uncovering a Massive Hack-For-Hire Operation*. June 2020.
URL: https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/.

[97] The Guardian. *Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones*. December 2019.
URL: https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

[98] Reuters. *Exclusive: Obscure Indian Cyber Firm Spied on Politicians, Investors Worldwide*. June 2020.
URL: https://www.reuters.com/article/technology/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1FI/.

[99] ESET. *Android Stalkerware Vulnerabilities*. May 2018.
URL: https://web-assets.esetstatic.com/wls/2021/05/eset_android_stalkerware.pdf.

[100] Kaspersky. *Kaspersky 2023 Report on Stalkerware*. March 2024.
URL: https://securelist.com/state-of-stalkerware-2023/112135/.

[101] FranceInfo. *Des victimes de violences conjugales racontent le cyberharcèlement exercé par leur conjoint*. August 2023.
URL: https://www.francetvinfo.fr/societe/violences-faites-aux-femmes/temoignages-j-etais-comme-une-bete-traquee-des-victimes-de-violences-conjugales-racontent-le-cyberharcelement-exerce-par-leur-conjoint_6005945.html.

[102] TechCrunch. *Exclusive: Stalkerware Apps Cocospy and Spyic Are Exposing Phone Data of Millions of People*. February 2025.
URL: https://techcrunch.com/2025/02/20/stalkerware-apps-cocospy-spyic-exposing-phone-data-of-millions-of-people/.

[103] TechCrunch. *Spyzie Stalkerware Is Spying on Thousands of Android and iPhone Users*. February 2025.
URL: https://techcrunch.com/2025/02/27/spyzie-stalkerware-spying-on-thousands-of-android-and-iphone-users/.

[104] Cyber News. *Red Alert, Israel's Rocket Alert App, Breached*. November 2023.
URL: https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/.

[105] HackRead. *Anonymous Hacked Russian Yandex Taxi App Causing a Massive Traffic Jam*. September 2022.
URL: https://hackread.com/anonymous-russian-yandex-taxi-app-hacked/.

[106] Intel 471. *Mobile Malware - Underground Perspective*. November 2023.
URL: https://intel471.com/resources/whitepapers/mobile-malware-underground-perspective.

[107] ZScaler. *Technical Analysis of Copybara | ThreatLabz*. August 2024.
URL: https://www.zscaler.com/blogs/security-research/technical-analysis-copybara.

[108] Team Cymru. *Coper / Octo: Team Cymru's Mobile Mayhem Conductor*. March 2024.
URL: https://www.team-cymru.com/post/coper-octo-a-conductor-for-mobile-mayhem-with-eight-limbs.

[109] Proofpoint. *An Update on Fake Updates: Two New Actors, and New Mac Malware*. February 2025.
URL: https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware.

[110] ANSSI. *Hygiène numérique des téléphones mobiles*. April 2025.
URL: https://cyber.gouv.fr/publications/hygiene-numerique-des-telephones-mobiles.

November 26, 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr