STRATEGIC REPORT

TLP:CLEAR

Predators for Hire: A Global Overview of Commercial Surveillance Vendors

Maxime Arquillière, Coline Chavane, Félix Aimé and TDR team, September 2025

sekoia

Table of Contents

Introduction

Between November 2023 and July 2024, the Russia-nexus intrusion set **APT29**, a group operated by the Russian foreign intelligence service SVR, was observed by Google's Threat Analysis Group (TAG) using exploits that are extremely similar to those previously used by **commercial surveillance vendors (CSV)**, particularly Intellexa's Predator spyware. This cyber espionage campaign illustrates how exploits developed or exploited by **CSVs** can persist beyond their initial operational use, highlighting one dimension of the risks associated with the proliferation of commercial spyware.

Commercial surveillance vendors are private companies or a groupement of companies that develop, maintain and sell spyware to clients, usually government agencies. CSV activities can include vulnerability research or acquisition, exploits development, digital forensics, command and control infrastructure or client training, all of them usually included or upsold in the full package. Beyond proliferation, the **risks** posed by commercial spyware **are multiple**. Documented use of commercial spyware by state actors have shown surveillance campaigns targeting dissidents, civil society activists and journalists. Such activities erode democratic processes, threaten freedom of expression, and enable politically motivated repression. In addition, CSV poses a **systemic threat to privacy** as spyware often results in collection of personally identifiable information (PII) and personal data without effective judicial oversight, creating risks of human rights violations. Commercial spyware can also be seen as **dual-use technology** under export control regimes, blurring the line between lawful investigative tools and instruments of oppression.

This report provides an overview of the **commercial surveillance vendors ecosystem between 2010 and 2025**, analysing their spyware offerings, business models, client base, target profiles, and infection chains.

Sekoia.io is monitoring CSV infrastructure in an effort to protect individuals against potential cases of misuse. In order to ensure the continuity of this monitoring, Sekoia.io ***will stop publishing Indicators of Compromise related to these infrastructure.*** *If you are interested in discussing this threat, please contact the TDR team at this address: tdr@sekoia.io.*

Sekoia.io is dedicated to protecting individuals against spyware threats and supports initiatives such as the Pall Mall Process led by France and the United Kingdom. The ***Pall Mall Code of Practice*** *for States to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities, issued in April 2025, can be found here.*

Key Takeaways

> Commercial surveillance vendors (CSV) have been thriving since at least 2010, benefiting from the pressing need **from authoritarian regimes** to acquire rapid and **ready-to-use surveillance tools** to contain the **Arab Spring** popular movement.

> In 2016, CSV started to **industrialise their products**, shifting from isolated technical components to **fully integrated solutions.** However, this development led to growing attention to the use of spyware by governments, shedding light on **cases of human rights violations.**

> After multiple exposures of the use of spyware in **an unlawful and repressive way** by NGOs and journalists, CSV faced a veritable **legitimacy crisis.** In response, they have been indicted by government and judicial courts, which considered these companies as **responsible** for selling their products to authoritarian states.

> Still, the surveillance market has remained **highly lucrative**, with commercial surveillance vendors making important benefits through the selling of their surveillance products.

> The **persistence** of CSV activity despite scandals has been made possible by the **complexification of their structures**, making it more challenging to identify specific business branches responsible for operating or selling the spyware.

> In addition, CSV relied on the **strategy of rebranding** to restore their image after public exposure, and to hide the tracks left by their business with autocratic regimes.

> Today, CSV have become **stealthier**, despite some variants in terms of how they **advertised** their surveillance activity. Indeed, some of them still publicly expose their expertise in intelligence gathering.

> The **infection chain** of private spyware used by CSV clients usually follows a similar structured process. However, differences exist regarding the possibility to use various vectors of infection. The most sophisticated ones being **zero-click and one-click infections.**

> **Detecting smartphone compromise** has then become increasingly challenging. However, security and hygiene protocols can still help to mitigate the risks of an infection.

Definitions

In this report, the term **spyware**, understandable as commercial spyware, refers to a specific type of software designed to covertly access and exfiltrate data from digital devices without the consent or knowledge of the user, for purposes of individual surveillance. It excludes mass surveillance capacities through signal intelligence or communication interception.

Commercial surveillance vendors (CSVs) are private companies or a group of companies that develop, maintain and sell spyware to clients, usually government agencies. CSV activities can include vulnerability research or acquisition, exploits development, digital forensics, command and control infrastructure or client training, all of them usually included or upsold in the full package.

CSV clients are defined here as governmental entities, including law enforcement agencies, intelligence services, and, in some cases, actors operating with partial or no formal state oversight.

Vulnerability brokers are individuals or organisations that research, identify, and develop exploits for software vulnerabilities, including operational system (OS) to sell them, either directly to **CSVs** or to clients developing offensive cyber capabilities. In this paper, vulnerability brokers will not be considered as CSV, but rather as suppliers for companies offering surveillance services.

Study perimeter and limitations

This report exclusively focuses on commercial surveillance vendors, their spyware and their activities between **2010 and 2025.** It excludes **hack-for-hire operations** - where private actors offer tailored intrusion services without developing or selling specific surveillance products -, and **Initial Access Brokers** (IABs), whose function is to provide access to compromised systems, not necessarily in the context of individual cyber surveillance. State-sponsored strategic cyber espionage campaigns are also excluded from the scope.

This report is **based on open-source information** and may be subject to limitations and bias inherent in open source data availability. So far, only large and important CSVs have been exposed through investigative journalism, NGOs' technical reports, cyber security vendors' or government publications. Therefore, this paper does not claim to offer an exhaustive view of the entire surveillance vendor ecosystem, particularly regarding entities operating at a smaller scale or with exclusive clients.

The geographical focus also reflects a **Euro-Atlantic perspective**, resulting from reliance on open-source reporting from Europe-based or North American research entities. Activities of vendors operating in other regions, particularly **Chinese surveillance vendors**, are underrepresented due to a lack of open-source data or publications.

Understanding cyber threats from commercial surveillance vendors

Commercial spyware poses a unique threat due to both their nature and intended use. Designed for sale, these tools are marketed as legitimate solutions to help law enforcement in preventing crime by enabling access to sensitive data such as messages, calls, photos, emails, and browsing history. Their **primary targets are mobile phones** - as these devices constantly accompany users and serve as hubs for personal communication. Others also have Desktop branches, such as Candiru (known as **Karkadann**), which has been active since at least 2020.

While democratic countries often regulate the use of spyware through legal frameworks designed to protect citizens' rights and prevent mass surveillance, these safeguards typically apply only to nationals and can be weakened or dismantled by shifts in authoritarian governance. In many other countries, such protections are nonexistent, leaving populations vulnerable to unchecked surveillance.

Numerous reports by NGOs and investigative journalists have exposed the **misuse of commercial spyware by authoritarian regimes**. These tools, instead of serving public safety, have been deployed to monitor, intimidate, and repress political opponents, business executives, activists, and journalists. The *Project Pegasus* (2021), for instance, revealed that the NSO Group's Pegasus spyware was used in countries like Saudi Arabia, India, Mexico, Morocco, and Hungary - often without legal oversight. In some cases, those targeted faced severe consequences, including disappearance or death.

Chapter 1 - History of the development of Commercial surveillance vendors

For a better understanding of the current CSV ecosystem, it is essential to have a look at the history of the first reported commercial spyware. As previously mentioned, our focus will begin in 2010, as this marks the emergence of the first significant CSVs of the decade - even though some companies may have existed earlier.

Commercial spyware development: a chronological overview (2010–2025)

Between 2010 and 2025, CSVs have evolved from niche suppliers of surveillance technologies into a multi-actor ecosystem with international clients. This chapter tries to identify key temporal phases shaping this evolution and a hypothetical political and economic context, though the example of a non-exhaustive list of CSVs.

2010-2015. Emergence of early commercial spyware

The **2010-2015** approximate era was marked by the emergence of early vendors in a context of geopolitical instability and the development of cyber capabilities for surveillance and intelligence gathering.

The **Arab Spring**, a series of popular protests which occurred in many Arabic countries (Tunisia, Egypt, Libya, Yemen, Syria, …) from December 2010 to 2013, created a demand from authoritarian governments for repression tools. As the Arab Spring was **at the time interpreted as** partly enabled by the popular access to new communication and **information technologies** (social networks and blogs), many countries with limited cyber capabilities had an urgent need to acquire rapid and ready-to-use surveillance and repression solutions. The emergence of this need was reinforced by some of the **first cyber operation revelations**, notably Stuxnet in 2010 and Snowden's disclosures in 2013, which drew the attention of many states to the strategic value of cyber tools for political surveillance and consolidating power. In this context, some of the first commercial spyware designed for individual cyber espionage such as FinFisher (Gamma Group) and Remote Control System (Hacking Team) gained interest.

For instance, **FinFisher** (also known as FinSpy) is a commercial spyware developed by the commercial surveillance vendor **Gamma Group**, which was designed to enable remote access and data exfiltration across desktop and mobile platforms. It was reportedly acquired in July 2012 and used by security services in countries such as Egypt and Bahrain to monitor activists and political opponents during and after the Arab Spring.

In the same period, the Italian surveillance vendor **Hacking Team** provided its **Remote Control System (RCS)** (also known as *Da Vinci* or *Galileo* software) to various Arab governments, including Morocco and Saudi Arabia. According to a 2015 report from the NGO Privacy International, RCS enabled regimes to conduct surveillance on political dissidents, journalists, and activists. In July 2012, members of *Mamfakinch*, a Moroccan citizen media platform established during the February 20 Movement (Moroccan Arab Spring moment) were targeted with phishing emails containing malicious Word macros embedded with Hacking Team's RCS spyware.

Of note, the need for surveillance, espionage and repression solutions were large, not only focusing on individual targeting but also for mass surveillance. For example, Libya authorities purchased ***Eagle***, a software sold by the French company Amesys, part of the Bull Group. Eagle was designed for nationwide internet monitoring, using Deep Packet Inspection (DPI) to intercept communications including emails, web traffic, instant messaging, and VoIP calls. After being prosecuted for complicity of torture and enforced disappearances, Bull Group sold Amesys activities to Nexa Technologies, now part of the Intellexa consortium known for its Predator spyware.

2016-2021. Industrialisation of commercial surveillance vendors

Between 2016 and 2021, the CSV ecosystem showed a significant process of **industrialisation and professionalisation, leading also to a greater exposure of their activity**. This evolution was visible in vendor offerings, which shifted from isolated technical components to **fully integrated solutions**. Early CSVs focused on supplying singular tools, such as spyware implants or traffic interception modules, whereas **new actors like NSO** have been selling a turnkey solution for government agencies. These solutions include the full infection chain (intrusion vector, command and control infrastructure, data exfiltration) with user-friendly interfaces featuring dashboards, multilingual support, and geolocation capabilities. CSVs were also marked by the emergence of structured international sales departments with vendors participating in specialised professional shows.

2016 marked a pivotal moment in the evolution of commercial surveillance vendors with the exposure of sophisticated mobile spyware that can be deployed without any victim action. In August 2016, the NGO Citizen Lab and the company Lookout Security exposed the use case of Ahmed Mansoor, an United Arab Emirates (UEA) human right activist whose iPhone was targeted by a 1-click intrusion vector which, if clicked, would have exploited a 0-day vulnerability on iOS to install Pegasus. The public exposure of the **Pegasus spyware** developed by the Israel-based company **NSO Group**, which later was observed using zero-click (0-click) technique (see explanation in Part 3), showed that CSVs had begun to adopt intrusion capabilities once thought to be the exclusive domain of state-sponsored actors—most notably, the use of exploits that does not require any action from the targeted individual. According to multiple international press articles, the sophistication of the 0-click technique was likely enabled by the recruitment by CSVs of former members of Unit 8200, a division of the Israeli Military Intelligence Corps (AMAN), regarded as one of the foremost technical and cyber-offensive intelligence units in the world.

Suspicious "1-click" text message received by Ahmed Mansoor in August 2016

Between 2016 and 2021, other Israel-based commercial surveillance vendors, with ties to ex-member of 8200 unit, or other Israeli cyber warfare units were exposed. For instance, **Paragon Solutions**, the company selling **Graphite Spyware** was founded in 2020 by Ehud Schneorson, an ex-commander of 8200. Paragon was and is still advertised as a tool for law enforcement units capable of remotely breaking into encrypted instant messaging communications (WhatsApp, Signal, Facebook Messenger or Gmail) with persistence capabilities. **Candiru** is another CSV with suspected ties to ex-members of cyber offensive units of Israeli intelligence agencies. Candiru was founded in 2015 by Eran Shorer and Yaakov Weizman. According to Haaretz, the largest shareholder is Isaac Zack, who has been its chairman since the beginning and was also a founder of NSO Group. **DevilsTongue**, Candiru's spyware dubbed by Microsoft, also exploits 0-day vulnerabilities in various operating systems (iOS, Windows and Chrome OS). Such capacities require sophisticated techniques typically associated with cyber intelligence units. Last, the consortium company **Intellexa**, known for its **spyware Predator** widely used for surveillance and repression of journalists, dissidents and activists, was founded in 2019 by Tal Dilian, an ex-commander of a military unit for cyber espionage (different from 8200).

2021-2024. Legitimacy crisis

Starting in 2021 and until nowadays, commercial surveillance vendors faced a legitimacy crisis due to a series of investigative reports from NGOs and cybersecurity vendors, data leaks, and journalistic investigations that exposed the misuse of commercial spyware by government entities. Although most CSVs advertised their products as tools for lawful surveillance by law enforcement entities, **multiple reports** highlighted the **deployment of private spyware against journalists, activists, and political figures**. Research based on open source data indicated that autocracies are more likely than democracies to rely on CSV, raising serious concerns about human rights violations and the lack of effective regulatory oversight.

In July 2021, **Amnesty International** published the *"Forensic Methodology Report: How to Catch NSO Group's Pegasus"*, exposing operational security mistakes left by Pegasus spyware on iOS and Android devices. This report was part of the **broader "Pegasus Project"**, an investigative initiative coordinated by Forbidden Stories, in collaboration with Amnesty and a consortium of 80 journalists from 17 media organisations across 10 countries. Among the use case examples, the Pegasus Project revealed that phone numbers belonging to senior French government officials, including President Macron and at the time Prime Minister Philippe, were part of potential surveillance targets by a client of NSO Group, reportedly identified as the Kingdom of Morocco. The affair contributed to raise awareness within European states and EU institutions regarding the proliferation of commercial spyware. However, despite being publicly exposed by the *Pegasus Project*, the NSO continued to maintain government clients, even in the European Union.

In addition, other NGOs such as **Citizen Lab**, which is based at the University of Toronto, have conducted investigations on the Predator spyware, sold by Cytrox, part of the Intellexa consortium. In December 2021, they published *"Pegasus vs. Predator"*, a report disclosing the targeting of Ayman Nour, an Egyptian opposition figure, whose iPhone was simultaneously infected with both Pegasus and Predator. Later, in October 2023, the **European Investigative Collaborations** (EIC) network, in association with Amnesty, published the *"Predator Files"* investigation**,** uncovering the use of Predator to target civil society members, politicians, and officials across multiple countries.

Beside NGOs, **targeted companies** and **cybersecurity vendors** also began publishing cyber threat intelligence reports on commercial spyware such as Google Threat Analysis Group (TAG) with their *"Buying Spying"* report, detailing the operations of approximately 40 CSVs and pointed up that CSVs were responsible for half of all known zero-day exploits targeting Google products and Android devices since mid-2014. Meta also published a "Threat Report on the Surveillance-for-Hire Industry" where they exposed a mix of CSV services for both individual targeted surveillance and wider surveillance through Meta services (Facebook, WhatsApp). Alongside other cybersecurity vendors, Sekoia.io also investigated commercial spyware, notably the C2 and spearphishing infrastructure used by clients of Candiru and Predator spyware.

Chapter 2 - The current state of Commercial surveillance vendors

Despite sanctions having reputational and financial impacts on exposed CSVs, the latest found techniques allowed them to continue their activity. Today, the market of CSVs has therefore remained particularly lucrative and fruitful. Several types of players are well-established, managing to sell their products at high prices and to many clients.

A particularly lucrative and complex market

The market of CSVs is challenging to follow as many of these companies rebrand over time and/or remain discrete on their intelligence activities, but also because this ecosystem has integrated new players, whose expertise can be complementary with CSVs services and products. However, public and leaked information confirmed that this market has remained **particularly lucrative**.

In 2011, documents of **Gamma Group** were leaked, indicating that the price to deploy the **FinFisher** spyware on a targeted device (also called "the activation") was 1100 euros. In 2015, the Italian company **Hacking Team** also suffered from a data breach, disclosing the price for activating its Remote Control System spyware, which was a little bit less than 1 million euros. Regarding **Candiru**, 2020 documents showed that the deployment of its spyware (whose customers are tracked under the intrusion set named Karkadann) costs 6 million euros. In 2022, **Intellexa** documents leaked, revealing that the price proposal for using Predator on up to 100 mobile phones was 8 million euros. In addition to being very lucrative, documents of major leaders of the sector dating from 2011 to 2022 demonstrate that the price for spyware use is in a **constant rise**. This is partly due to the increased cost of acquiring vulnerabilities and exploits, but also to the important number of clients looking for spyware.

A broad demand leading to opportunities for both large and small market players

The data provided above came from some of the major leaders of the CSV market, but other actors, such as **Cy4gate,** a large Italian company, or **Paragon,** a smaller Israeli actor, also make important deals, indicating the profitability of the surveillance industry.

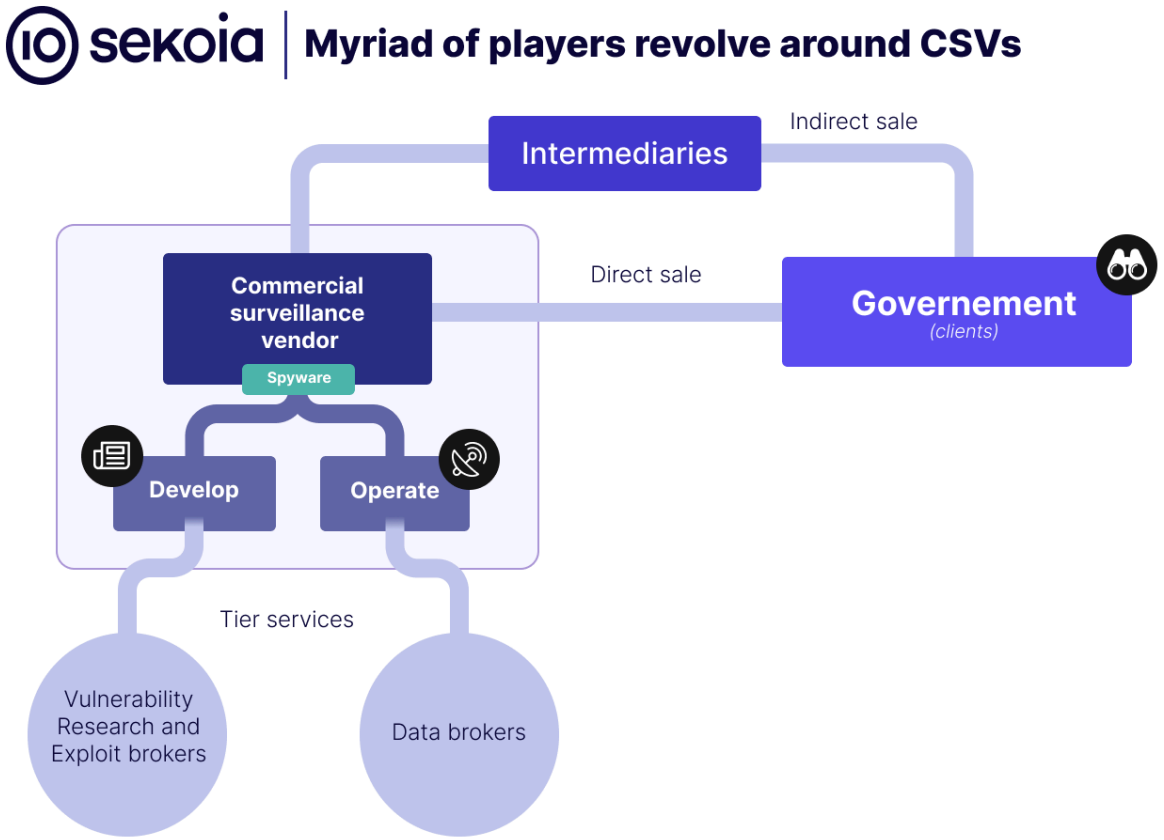
During the year 2024, Cy4gate reached 72 million euros of sales. The same year, the spyware company Paragon signed a contract of 2 million dollars with the US Immigration and Custom Enforcement.

The large demand can be explained by the fact that some governments rely on several types of spyware from different companies. That is the case of Italian prosecutors, which rely on various suppliers for their investigations. A same device can also be the target of several types of spyware, supposedly used by different governments which do not communicate between them. It was the case in 2021 with Ayman Nour, an Egyptian politician in exile, who was targeted by both Predator and Pegasus.

As a consequence of the unstable global economic context of the last few years, the budget of government entities has declined. This has led European CSVs to **export abroad to conquer new market shares**, thereby preserving the profitability of surveillance activities.

This large market is also **complex** as different types of actors are involved. First, CSVs can rely on third parties to access vulnerabilities and exploits to infect devices with their solution. **Vulnerability**

researchers, as well as **exploit developers and brokers**, can be called on to provide new vulnerabilities and exploits to ensure the continuity of a surveillance operation against specific targets.



In addition, services of **data brokers** and **investigative/big data analytics platforms** can also be leveraged to enhance the targeting of specific individuals and create custom lures to infect them with the malicious payload. **OSINT tools** can also be used for this purpose. It explains why companies providing OSINT solutions have been increasingly represented among the associated sponsors from the **2023 edition and beyond of the ISS World Forum**, an international forum taking place each year in the Middle East, Europe, Asia, North and Latin America and sponsored by NSO Group.

The ISS World

Trade fairs like the ISS World function as strategic meeting points for intelligence agencies, law enforcement, and high-level government officials. Deals concluded at such events have occasionally involved circumventing sanctions to supply embargoed states.

Several participants and sponsors of the ISS World have been involved in selling and operating spyware for repressive states, leading to violations of human rights. This is the case of the **major sponsors and associated sponsors of the event**, NSO Group, but also of Candiru, Intellexa, eSurv, Babel street, RCS, VoyagerLabs, *etc.*, which were present during previous editions from 2023 and onwards.

The particularity of the ISS World compared to other military forums, such as Milipol, is that its access is reserved exclusively for investigators from private companies, government employees, law enforcement agencies and security and surveillance products' suppliers, prohibiting journalists and NGOs from covering the event. It makes this event and the activity of its participants all the more opaque.

2021 & 2025 ISS World Brochures

In addition to the suppliers, which participate indirectly to the activity of CSVs, we identified three categories of CSVs. These categories are based on the way their surveillance activities are advertised.

Indeed, looking at some known-leaders of the industry like **Intellexa, NSO Group,** and **Candiru**, the way their activities are advertised differs completely. **NSO Group** has a website mentioning it

provides "cyber intelligence for global security and stability". On the other hand, **Candiru** and companies associated with Intellexa like **Cytrox** or **Intellexa Ltd.** do not have any website to advertise their services.

The stealthiness of some actors compared to others is interesting to distinguish to understand the different CSVs' strategies to promote their solutions, while limiting the information available about their activities.

Typology of CSVs based on spyware promotion

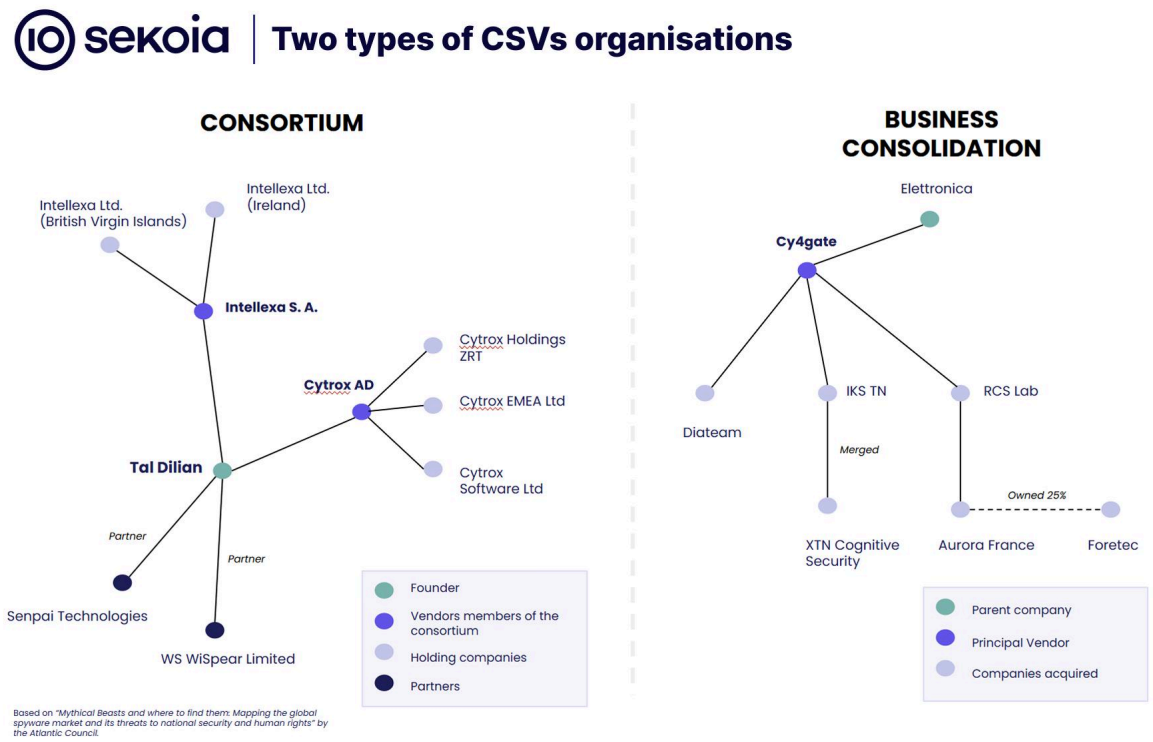
	Advertised CSV	Advertised CSV, but keep surveillance activities discrete	Stealthy CSV
DESCRIPTION	Companies publicly promoting their surveillance expertise **online or at international forums**.	Companies publicly offering **cybersecurity services**, while keeping surveillance tools hidden. Surveillance tools and operations can be either hidden or delegated to another sister company.	Companies linked to state-used spyware with little to **no online presence**. Most information about them comes from NGO reports documenting malicious activity tied to their tools.
TYPES OF PRODUCTS ADVERTISED	Surveillance, Intelligence services, Digital Forensics, Interception solutions	Cybersecurity solutions, Big Data analysis, OSINT, Consulting, IT Network	N/A
EXAMPLES OF COMPANY	NSO Group, Negg Group, RCS Lab, ClearTrail, Cy4Gate	Nexa Technologies/RB 42, Paragon, Innova	Candiru, Intellexa Ltd, WiSpear, Wintego

Despite these three categories, CSVs are **becoming more and more complex structures**, following a **process of consolidation**, blurring the lines between the different actors of this ecosystem. Gathered under a parent company or within a consortium, CSVs are increasingly mixed into a network of businesses, which can have different expertise related to security solutions.

For instance, the Italian spyware company **Cy4gate** - and its parent company Electtronica - have successively acquired companies in the branch of security and cybersecurity, making more complex the scope of its activity, as well as its distribution pipelines. In 2022, Cy4gate took control of **RCS Lab**, one of its principal rivals on the Italian intelligence market. RCS Lab had a distribution pipeline in France through the **Aurora France** company, which is under the parent company Aurora. Aurora owned 25% of the French judicial interception service provider **Foretec** in 2022. Therefore, this Cy4gate acquisition enabled the Italian company to penetrate more easily the French market of interception.

In 2022, Cy4gate also acquired **Diateam**, a French cybersecurity company and author of a simulation platform called *HYbrid NEtwork SIMulation* on behalf of the French Direction Générale de l'Armement (DGA).

This process of consolidation continued with Cy4gate's acquisition of the Italian company IKS TN in 2023, which has successfully merged with XTN Cognitive Security. XTN Cognitive Security developed a platform and has expertise in anti-fraud solutions.



The unclear role of intermediaries

With public exposure and scandals associated with CSVs' activities, as well as restrictions on license policies for export, cases of **spyware companies relying on intermediaries** have emerged.

These intermediaries constitute a *"grey zone"* and can endorse several roles, from **being the relays of spyware products** to bypass restrictions on license's export to certain countries, to **pieces of the infrastructure** supporting surveillance operations.

For instance, in 2021, the Swiss company **Toru Group** served as an intermediary for the sale of spyware to Bangladesh by the company **Passitora** (which used to be called WiSpear, which is part of the Intellexa consortium).

In 2025, activity related to the use of Predator was identified despite repeated public exposure and US sanctions. Predator is a spyware developed by **Cytrox**, which is part of the **Intellexa consortium**.

Predator operators rely on a multi-tier infrastructure. The first three layers were already observed in earliest campaigns and serve to obscure the origin of the attack. Based on 2025's observations, a fourth layer has been added to reinforce the anonymization of Predator customers. A fifth layer was also identified. It is a set of servers owned by a Czech company, **Foxltech s.r.o**., which has never been identified as part of the Intellexa consortium by the past. The owner of this company, Michal Ikonomidis, has been linked to Dvir Horef Hazan, the owner of several companies, three of which have received payments from the Intellexa consortium. Even if the role of the fifth layer remains unclear, it sheds light on the involvement of **companies that are not formally part of the Intellexa consortium** in Predator's infrastructure.

Persistence despite public exposure and scandals

Despite the legitimacy crisis faced by CSVs since 2021, the latest managed to maintain their activity using different techniques. First, CSVs exposed publicly for selling their products to repressive states violating human rights have been forced to stop their activity completely and to rebrand under another name, reusing the same technology and even reemploying the same team.

For instance, Amesys employed this **strategy of rebranding** following the 2007 Libyan scandal. After being accused of complicity of torture for selling its spyware under the name of "Project Eagle" to the Libyan government of Kadhafi, Amesys was bought by the group Bull. Bull was owned in majority by shareholders gathered among Crescendo Industries and I2E holdings. One of the ancient sales directors of Amesys had some parts into these two holdings and sold them to buy Amesys and the intellectual property of its software to launch two new companies: Nexa Technologies, based in France, and Advanced Middle East Systems (AMESys), based in Dubai. In 2014, the original company Amesys totally disappeared and was replaced by these two companies.

In addition to rebranding, CSVs used other techniques to blur the lines between their non controversial and controversial activities. By controversial activities, we mean selling surveillance software to countries which are known to conduct repression against their own population, journalists, political opponents, minorities and activists. Among these techniques is the creation of a complex network of companies, making it difficult to determine which company is responsible for which activity. For instance, taking the case of the founder of **Nexa Technologies** and **AMESys**, journalists found evidence that Nexa was used to send surveillance technologies and software to AMESys, which were then received and operationalised to be used by the final client, the government of Egypt.

In 2022, Nexa Technologies was bought by **Flandrin Technologies**. The parent company of Flandrin Technologies is ChapsVision. The same year, Flandrin Technologies acquired two other companies, Deveryware Group and Ockham Solutions SASand its branch SCO Ockham, illustrating the **process of consolidation** mentioned previously.

Growing challenges for governments and regulators

Since 2021, the commercial surveillance vendor ecosystem is facing a legitimacy crisis (see Chapter 1), due to a series of investigative reports, legal actions, exposition of infrastructure and diplomatic initiative, all of them condemning the misuse of commercial spyware for unlawful surveillance. The crisis has different consequences for CSVs, from bankruptcy to adapt their activity and rebrand to avoid legal sanctions and restore their image.

In May 2025, a California court ordered NSO Group to pay $167 million in damages to Meta, which accused the company of exploiting a vulnerability in the video call function of WhatsApp to deploy the Pegasus spyware and surveil nearly 1400 user accounts. This lawsuit reflects the ongoing legitimacy crisis faced by commercial spyware vendors since 2021. High-profile **legal actions** (such as those by Meta and Apple) and **public exposure** via user alerts and reports (from Google, Meta, Apple) have heightened political awareness about the risks these tools pose to civil rights and freedoms.

In Europe, this issue has prompted both investigations and public debate. A 2022 European Parliament report and subsequent conferences have highlighted abuses, including a March 2025 event led by MEPs Hannah Neumann and Saskia Bricmont, which focused on the use of **Graphite spyware** (developed by Israeli firm **Paragon**) by Italian intelligence services against journalists and dissidents.

In the United States, the Commerce Department added **NSO** and **Candiru** to its Entity List in 2021, and **Intellexa** followed in 2023. These designations demonstrate that, although states are the main customers of these tools, some governments are willing to take measures to reassure the public and reaffirm democratic values.

Yet, such actions can also reveal troubling ambiguities. Italy, for example, was flagged by Meta for deploying **Paragon spyware against journalists critical of Prime Minister Giorgia Meloni**. The Italian government denied the allegations and claimed to have reached out to Meta regarding the

targeting of at least 90 individuals. Meanwhile, Paragon reportedly cut off Italian access to its platform.

To obscure their involvement, some governments use **proxies, intermediaries, or brokers** to acquire spyware tools. Transactions often take place at international trade shows such as ISS World (with a European edition held annually in Prague) or events like the Italy–United Arab Emirates Business Forum, organised by government ministries from both countries. Although access to these events is increasingly restricted, past editions of ISS World suggest that the primary sponsors are CSVs already implicated in human rights abuses.

Democratic governments, especially in the European Union, have **sent conflicting signals about curbing spyware**, publicly enforcing strict regulations while simultaneously enabling the industry through regulatory loopholes and weak enforcement. Many EU-based companies—such as RCS Lab, MSAB, and DSIRF—develop and export intrusive surveillance tools, often to countries with questionable human rights records. Firms like Intellexa bypass EU export controls by setting up subsidiaries in member states with lax oversight, like Cyprus or Bulgaria. Moreover, EU institutions have at times financed surveillance projects abroad without proper risk assessments. Domestically, several EU countries have also deployed commercial spyware, including Pegasus, often without sufficient accountability. These patterns show that **surveillance abuses are not limited to authoritarian regimes**—democracies, too, exploit or overlook the misuse of spyware when oversight mechanisms are weak.

Chapter 3 - Techniques and infection chain process for commercial spyware

The infection chain of private spyware used by CSV clients usually follows a similar structured process. It begins by selecting the target and a delivery vector, then it continues with the execution of a vulnerability exploit to install the spyware on the device. Once installed, the malware communicates with the operator through a command-and-control infrastructure to exfiltrate relevant data for surveillance purposes. In addition, some spyware toolkits include features to uninstall and cover their tracks.

Reconnaissance and target selection

The initial phase of the infection chain is often the least visible, with CSV clients identifying their high-value targets with a mix of pre-surveillance information and open-source intelligence. The objective of this **reconnaissance** phase is often to gather information on the target's device ecosystem (operating system, browser version), behavioural patterns, and **communication apps**. Information is extracted from online sources, such as misconfigured social media accounts, open-source or private services, or can even be obtained from extracted data from another target,

for example, the contact list of a previously targeted individual. The point of reconnaissance is to assess the attack surface available to choose the most efficient intrusion vector.

Intrusion vectors

Once the attack surface is identified, multiple intrusion vectors can be used to deliver the payload.

One click exploit (1-click). The target is lured into clicking a malicious link in a message received by email, messenger app (WhatsApp, Signal, iMessage, *etc.*), a targeted advertisement or any website the target usually reads via a **watering hole attack** - local news website, specialised forum. A 1-click exploit can leverage malicious files such as weaponized invitations, images, any file format which can be interpreted by the smartphone operating system. To better lure the target, attackers often impersonate one of the target contacts or peers, for example another member of a NGO.

For instance, in the aftermath of a civil rights activist's arrest in an authoritarian state, information about the incident is likely to circulate rapidly within activist networks, particularly in search of legal assistance. Adversaries can exploit this context by impersonating a known peer - such as another prominent activist - and sending the target a malicious message that references the arrest. By leveraging the urgency and emotion of the event, the attacker increases the likelihood that the target will engage with the content, thereby triggering the 1-click exploit.

That was the case of Ahmed Mansoor. In 2016, the Emirati human rights activist was targeted by Pegasus spyware through a spear-phishing attack. He received SMS messages containing links that promised information about detainees tortured in UAE prisons. If clicked, the malicious link would have chained previously unknown iOS vulnerabilities, (CVE-2016-4657 - remote code execution, CVE-2016-4655 info disclosure, and CVE-2016-4656, elevation of privileges), collectively dubbed "Trident".

Zero click exploit (0-click). A 0-click exploit requires no user interaction. The target's device is compromised automatically with the reception of a specially crafted message or data packet — often via instant messaging apps (WhatsApp, iMessage…), but also email, or push notifications. These exploits typically abuse vulnerabilities in the parsing or rendering of content by the targeted application or operating system, enabling code execution without the user opening or interacting with the message. This method significantly reduces the risk of detection and failure, as it does not rely on preemptive social engineering.

For instance, an attacker may craft a malformed image, a contact list vCard, or message payload that triggers the exploit chain upon delivery. If the target is a journalist covering sensitive topics, the spyware operator might exploit a vulnerability in the messaging app used to contact sources. Once the vector message is delivered - often deleted automatically to avoid traces—the device is silently compromised, granting the attacker remote access without alerting the victim.

In January 2025, WhatsApp accused the Israeli company **Paragon** of targeting nearly 100 journalists and civil society members with their commercial spyware Graphite, using a 0-click exploiting WhatsApp's automatic content preview feature. Once the phone number of the target is acquired, it

is silently added to a WhatsApp group, where a malicious PDF is sent. As WhatsApp processes the file to generate a preview, a zero-day vulnerability is triggered, allowing Paragon's Graphite spyware to be installed.

Another example of a zero-click vulnerability exploited in the wild was recently discovered by iVerify. This vulnerability — a use-after-free affecting the Nickname Update functionality of the imagent (iMessage) process — was reportedly exploited by Chinese threat actors to target key individuals in the U.S. According to iVerify, as it used iMessage, the exploitation required only the victim's Apple ID or phone number.

In addition, commercial surveillance vendors have reportedly explored alternative zero click attack surfaces such as on the **baseband, Bluetooth, and Wi-Fi stacks**. Exploits in the baseband layer, which rules cellular communication, can enable remote compromise signals without user interaction, often bypassing the main operating system entirely. Bluetooth vulnerabilities, particularly in protocol parsing, have enabled proximity-based attacks without pairing. Similarly, Wi-Fi stack flaws can allow "over-the-air compromise" without requiring network connection. These vectors require most of the time a physical proximity and specific hardware equipment such as IMSI catcher for baseband attacks.

Physical access. A physical access exploit involves the manual compromise of a device through direct interaction, typically requiring the attacker to obtain temporary or permanent physical possession of the target's phone, laptop, or external media. This method may be used in border crossings, police custody, or covert operations where devices can be discreetly handled or swapped. Once the device is in hand, the attacker can install spyware via USB injection tools, removable media such as SD cards, or debugging interfaces like JTAG (Joint Test Action Group) or DFU mode (Device Firmware Update).

In some cases, authorities facilitate this access by seizing and tampering with devices during detentions or inspections. For instance, the Israeli vendor **Cellebrite**, known for its mobile forensic product Universal Forensic Extraction Device (UFED) used by client police authorities, was reported to be used by Serbian authorities in an Amnesty International paper from December 2024. UFED itself is not classified as spyware and appears to be employed within a legal framework, particularly in cases where a police access to the device is obtained. However, following the unlocking and data extraction through UFED requested by the Serbian authorities, Cellebrite operators installed their commercial spyware **NoviPsy**, aimed at conducting individual surveillance of civilian activists and journalists. In February 2025, following Amnesty's publication, Cellebrite announced they stopped working with Serbian authorities.

Detecting smartphone compromise

Detecting whether a smartphone has been compromised is inherently complex, as mobile operating systems (mostly Android and iOS) are significantly closer to users than traditional desktop systems. Nevertheless, complementary detection methods exist, each relying on different mechanisms.

Detection via Live Network Traffic Analysis

Malware implants mostly rely on network communication to receive commands. By intercepting a smartphone's network traffic, it is possible to identify anomalies—such as regular beaconing to a newly registered domain, or to a server using a free or self-signed certificate, especially when no browsing activity is occurring on the device. These kinds of behaviours, alongside traditional indicators of compromise, can be flagged by tools such as SpyGuard.

SpyGuard is a tool designed to intercept Wi-Fi traffic in search of network anomalies that may indicate the presence of spyware on a smartphone. Its detection engine can also be used offline to analyse PCAP files, such as those obtained from IMSI catcher captures conducted in a controlled environment.

However, SpyGuard tool does have limitations. For example, a sophisticated implant may choose which network interface to use for communication, refrain from any activity for several hours after connecting to a new Wi-Fi network, or implement geofencing-limiting communication when located outside of predefined 'safe' geographic zones.

Detection via System Backups, Logs, and Diagnostics (Sysdiagnose)

Other tools focus on analysing system logs and diagnostic data to detect anomalies - for example, irregularities in running processes or, in some cases, traces of network activity such as suspicious domains or IP addresses.

Apple's system diagnostic tool, Sysdiagnose, can reveal signs of compromise such as process crashes linked to exploitation attempts, unknown or suspicious processes, or - more recently - suspicious network connections by parsing the output of system commands like netstat. Sysdiagnose is particularly useful as it can be triggered by the user without any external device and then sent to a third party for expert analysis, enabling the search for anomalies or indicators of compromise.

Other technologies also exist, such as the Mobile Verification Toolkit (MVT), released in 2021 by Amnesty International's Security Lab. However, such tools need to make dumps containing a lot of PII and rely solely on known indicators of compromise (IOCs) rather than heuristics. While this approach helps reduce false positives, it also limits the ability to detect previously unknown or undocumented threats.

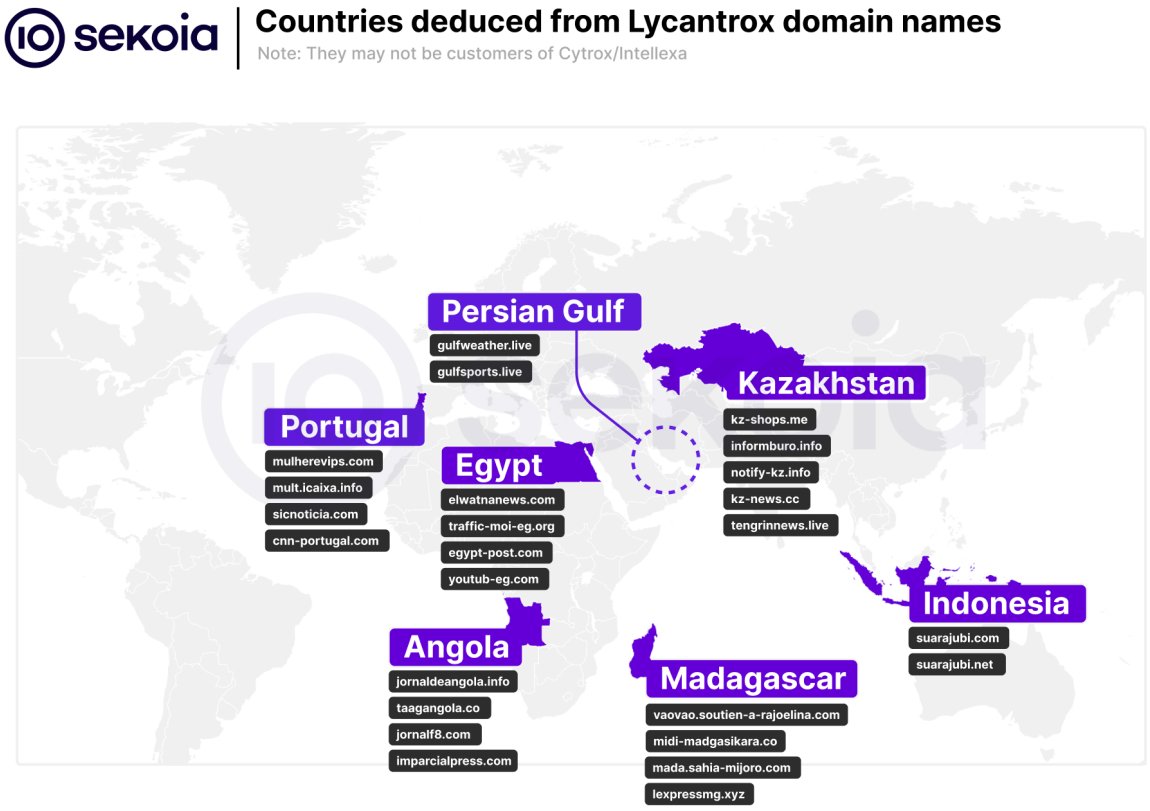
Last advice: take a look at your emails.

Several vendors now issue alerts to users who have been targeted by state-sponsored threat actors. Apple, for example, has been sending threat notification messages since 2021 from addresses such as: threat-notifications@apple.com or threat-notifications@email.apple.com. The reception of messages from these senders in your email, iMessage, or log files can serve as an indication that your device may have been compromised in the past. Such a finding should be investigated promptly in order to collect further evidence.

Delivery and command-and-control infrastructure

No matter the malware and its capabilities deployed on the victim phone, the attack still needs a command-and-control (C2) infrastructure to send instructions and receive extracted data. Those relays can be attacker-registered domains or compromised legitimate domains. In some cases, the attack also needs delivery domains, that usually typosquat legitimate websites identified as sources of interest for the targeted individuals.

Typosquatted delivery servers. It refers to registered malicious servers that exploit common typographical errors made when typing or reading a legitimate website URL. They differ by just a single character, misspelling, or common typographical mistake - for example replacing "l" with "i", or adding/removing a letter, or playing with TLD “gov.uk” to “gov.uk.com”. In our previous publications about Intellexa’s Predator commercial spyware, we were able to observe typosquatted delivery servers likely registered by clients of Predator spyware, mimicking legitimate websites from their countries. They aim at luring the victim into clicking / connection to the malicious server and ultimately receiving the payload.



Over time, and after a few publications exposing their operation security mistake, **we noticed a significant increase in the number of generic malicious domains** which do not give indications on targeted entities and possible customers of Intellexa surveillance solutions. **That is why, at Sekoia.io, we decided to publish no more IOCs in our publication, but rather sharing them with parties involved in detection or potential victims.**

Command-and-control servers. They can be compromised legitimate servers or attacker-registered, used to send instructions and receive extracted data. For example, still regarding Predator spyware, the infrastructure used by Intellexa customers consisted of VPS hosted in several autonomous systems, with each user running their own instances of VPS and managing their own domain name related to it. Operation security mistakes or registration patterns allow us to track such infrastructure. For the Predator example, since each Intellexa customer manages its own instance, registration patterns or OPSec depend on the customer and not Intellexa itself. This allowed us to track some infrastructures by looking at the services listed on the instances, most of the time there are two open ports, the SSH used for the administration and a 443 managed by Nginx.

Security and hygiene protocols

While keeping a phone updated is still recommended, it won't be enough protection for such threats. It is important to understand there are no bullet proof solutions. The best one can do is to adopt mitigation strategies, and follow security hygiene protocols to diminish the attack surface, and the impact of a compromise.

Routine usage

Still, it is imperative to keep your phone updated: activate auto-update and check your version regularly to protect from known exploits. Some legacy services such as 2G can be abused by IMSI catcher if they are not disabled. Additional steps can be implemented to reduce the attack surface of your phone: disable unused services (such as bluetooth, location, Wi-Fi, Airdrop) and activate them only when required. For iOS, the “Lockdown mode” can also contribute to lowering your exposure by blocking quality of life gadgets that are often used as an infection vector.

To connect to the internet, use VPN when possible. Once online, tame your curiosity, 1-click attack is a popular vector: never tap links or attachments unless you initiated the request, even from known contacts. Reboot your phone often to purge non-persistent implants, it will force the attacker to trigger another infection. If possible, leverage separate phones for different usages: one for personal activities, another one for work and burner phones for traveling.

When traveling

When crossing borders, it’s not rare for customs to temporarily seize your belongings, such as laptops and phones. Once seized or lost, consider your phone as compromised. Bringing a burner phone when traveling can significantly reduce the impact. Another advantage of burner phones is the smaller contact list, which will limit pivots for subsequent compromise. Remember to activate your burner far from home, on a different Wi-Fi, and if possible, connect it to the least amount of social media possible.

Conclusion

Commercial surveillance vendors (CSVs) have flourished amid strong demand from government actors seeking tools to monitor high-profile targets. Although these companies typically market their products as intended strictly for law enforcement purposes, numerous investigations by NGOs and journalists have revealed widespread misuse. These cases suggest that spyware abuse is not an isolated occurrence but a systemic issue within the industry.

As a result, the CSV ecosystem has expanded significantly since the emergence of the first firms specializing in targeted surveillance, evolving into a highly lucrative sector. The consolidation of key actors within the surveillance market further illustrates the sector's sustained and growing profitability.

In response to increasing sanctions and export controls, CSVs have adopted increasingly sophisticated strategies to evade regulation. These include rebranding, forming consortiums or holding groups, and establishing new subsidiaries with similar names across multiple jurisdictions.

The absence of effective political and regulatory safeguards has left spyware targets more exposed than ever, as infection techniques have grown more covert and resilient. Vendors now deploy a broader range of attack vectors, rely on stealthier command-and-control (C2) infrastructures, and exploit zero-day vulnerabilities with increasing frequency.

In response, NGOs, journalists and cybersecurity companies continue to investigate and expose violations of human rights caused by the use of CSV' spyware. For instance, Citizen Lab and Amnesty International regularly published reports based on individual notification. Esra'a Al Shafei has created the platform surveillancewatch.io to list surveillance entities, their role and their targeting. Reporter Sans Frontières collaborated with Sekoia.io and others NGOs to collect phishing emails and payloads to analyse. Lookout regularly published investigation reports on mobile threats, while Sekoia.io has been documenting malicious campaigns attributed to Cytrox and Candiru.

Sekoia.io is dedicated to protecting individuals against spyware threats and supports initiatives such as the Pall Mall Process led by France and the United Kingdom. The ***Pall Mall Code of Practice*** *for States to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities, issued in April 2025, can be found here.*

About Sekoia.io TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

About Sekoia.io

Sekoia.io is the European cybersecurity technology company, leading provider of detection and response solutions boosted by AI and Cyber Threat Intelligence. By combining threat anticipation through knowledge of attackers with automation of detection and response, the Sekoia AI-SOC platform provides security teams a unified view and total control over their information systems. Its open approach and interoperability with third-party solutions enable organizations to take full advantage of their existing technologies.

Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

www.sekoia.io

Find more publications on blog.sekoia.io

Please don't hesitate to provide your feedback on our publications by clicking here.
You can also contact us at tdr@sekoia.io for further discussions.