Intellexa and Cytrox: From fixer-upper to Intel Agency-grade spyware

blog.talosintelligence.com/intellexa-and-cytrox-intel-agency-grade-spyware

Vitor Ventura December 21, 2023

By Vitor Ventura

Thursday, December 21, 2023 11:00

Threat Spotlight

By Mike Gentile, Asheer Malhotra and Vitor Ventura.

Editor's note: This blog post is a public version of a talk presented at LabsCon 2023 on Sept. 22, 2023. You can watch a recording of the talk here. Some of the intelligence presented at LabsCon was later confirmed by an Amnesty International blog post released on Oct. 6, 2023.

- Cisco Talos has a new, in-depth analysis of timelines, operating paradigms and procedures adopted by spyware vendor Intellexa (previously known as Cytrox).
- Talos' analysis revealed that rebooting an iOS or Android device may ***not*** always remove the Predator spyware produced by Intellexa. Persistence is an add-on feature provided by Intellexa for their implants and primarily depends on the licensing options chosen by a customer.

- Intellexa knows if their customers intend to perform surveillance operations on foreign soil.
- Two years after its first public exposure, Intellexa's Predator/Nova spyware solution continues to be undetected by anti-virus solutions. Public reporting on Intellexa's operations has had little to no impact on their ability to conduct and grow their business across the world.
- Almost all publications on malicious operations conducted using Intellexa's spyware consist primarily of malicious domains as indicators of compromise (IOCs). Talos assesses that the disclosure of such domains, managed by the customers, has little to no effect on Intellexa's operations and enables them to preserve their malware implants due to a lack of technical disclosures.
- After many users patched against the exploit chains used by Intellexa as of December 2021, the spyware vendor started shipping a new exploit chain to at least one new customer in early 2022 that covered the same and more recent versions of the Android operating system.

In May 2023, Cisco Talos published the first ever in-depth technical report on Intellexa's spyware solution named Alien and Predator, showing its inner workings and demonstrating the highly complex software architecture decisions required to make such spyware work properly on the Android operating system. This research also sheds light on several other aspects of the commercial spyware space, like plausible deniability, the impacts of widespread media exposure and recruitment issues.

During the LabsCon 2023 cyber threat intelligence conference, Talos presented the operational risks inherent to the commercial spyware landscape, using Intellexa as a use case.

This research delves into the history of the Alien/Predator line of implants, illustrating how a run-down spyware seller, Cytrox, was bought and transformed into an intelligence agency-grade spyware vendor: Intellexa.

Implants' persistence is an add-on in Intellexa's offering

Leaked commercial proposals from the Intellexa Alliance have shown that prices per infection are increasing every year, along with the capabilities of the company's technological solution. Rebooting the device is no longer a means to remove the implants from an infected device.

In 2021, Predator spyware couldn't survive a reboot on the infected Android system (it had it on iOS). However, by April 2022, that capability was being offered to their customers. Since then, no reports have been published detailing such a mechanism, as there is no reason to believe it has become obsolete. It still doesn't survive a factory reset, but it is fair to assume that this specific capability will become available, literally breaking all trust in the device beyond recovery.

Intellexa's product development journey

Cytrox was first created in North Macedonia in 2017, and at the time, built Android-based malware. In 2018, Cytrox was acquired by WiSpear and then in 2019 Nexa Technologies, WiSpear (and Cytrox) and Senpai Technologies teamed up to create the Intellexa Alliance, a commercial spyware company that, according to public reports, sells commercial spyware to multiple customers without regard for their potential targets and the spyware's misuse.

Senpai Technologies is a company specializing in OSINT and persona creation based out of Israel, while WiSpear, also based in Israel, specializes in Wi-Fi interception. Nexa Technologies (now called RB 42) is a French-based company whose main focus is remote surveillance and security services.

Immediately after the consolidation of all these firms under Intellexa in May 2019, the revamping of Predator began, which at the time, was their flagship spyware for Android. This can be confirmed on the artifacts left on the malware binary due to the use of static library compilation at build time.

By April 2020, the revamp was finished and the malware was ready to be deployed on Android. In May 2020, the developers began working on an iOS "solution" which we assess with medium confidence was a port of Alien/Predator from Android to iOS. Our assessment is based on the fact that the engine that drives the high-level components of the Predator system is similar, if not identical, to the point where some Android artifacts, detailed in the following sections, can be found on the iOS sample.

Evolution timeline

Pricing model

Building commercial spyware is a sophisticated and research-driven process. It involves meticulously circumventing, bypassing and exploiting security controls put in place by mobile applications/packages and Operating Systems such as Android and iOS. Combining such potent software into a package with zero or one-click zero-day exploits

makes it a highly reliable offensive “solution” – and that is exactly what makes it expensive. As early as 2016, The New York Times reported that the NSO Group charged $650,000 for every 10 infections, with an additional $500,000 for initial setup. Multi-year deals between the NSO Group and Mexico were estimated to be around $15 million – and this was back in 2013.

Fast forward five years to 2021, and another disclosure from The New York Times details the proposal brochure for Intellexa’s Predator framework offering their solution for a whopping 13.6 million Euros for:

- 20 concurrent infections.
- One-click exploit for initial access.
- Predator C2 and administrative hardware and software.
- Project plans, documentation, etc.
- 12 months of warranty support.

Proposal (snipped) defining price and items

Leaked documents from 2022 show that the Nova platform, which is Intellexa's data-gathering module, was priced at 8 million Euros in 2022. Price tags of 13.6 million or even 8 million Euros is a hefty sum. However, this reinforces the fact that commercial spyware such as those from Intellexa is neither for the common man nor for petty crimeware operators. These solutions are meant for customers with deep pockets and such expenses can only be incurred by state-sponsored agencies.

The pricing model also shows the technological evolution of the product. Based on the leaked proposal dates in July 2022, Intellexa had already incorporated boot survivability into the Android solution. It also increased the support for Android to 18 months. At this

point, it is unclear if this is the direct result of Intellexa's development and research capabilities, or if these are based on exploits acquired that ultimately would result in having such capabilities.

The original persistence mechanism on iOS was the exploitation of the original vulnerability during the boot process by loading the malicious HTML page stored locally. As such, the newly introduced Android persistence mechanism can simply be based on a similar method.

Plausible deniability

Intellexa's commercial proposals are designed to create plausible deniability. These clauses extend from the infrastructure responsibilities to the delivery methods. This is a key aspect of Intellexa's business model, the goal is to avoid a bad reputation and to claim they are not responsible for what their customers do with their "product" — they claim that they don't even know who the victims are.

Proposal (snipped) defining responsibilities

The leaked proposals show that the infrastructure and anonymization are the responsibility of the customer. From a deniability point of view, this enables the claim that Intellexa doesn't know *how* victims are being targeted. From the operational risk perspective, such clauses also shield Intellexa from any responsibility in the event of a public exposure connecting malicious operations back to the vendor.

Delivery method method

The delivery of Intellexa's supporting hardware is done at a terminal or airport. This delivery method is known as Cost Insurance and Freight (CIF), which is part of the shipping industry's jargon ("Incoterms"). This mechanism allows Intellexa to claim that they have no visibility of where the systems are deployed and eventually located. This exact scenario was seen being put into practice when, according to a LighthouseReports investigation, Intellexa sold their solution to the Sudanese government.

Source: https://www.lighthousereports.com/investigation/flight-of-the-predator/

Even if we take into consideration the proposal's terms such as, "Installation and configuration at customer designated facility…" and the "Standard training course ……," it still does not mean that Intellexa might know where the hardware is located since everything can be done remotely or even without their personnel knowing where the customer's "solution" is physically located.

Intellexa does have first-hand knowledge of if their software is being used to conduct surveillance operations targeting phone number prefixes other than their customers' country of origin and possibly their jurisdiction. This knowledge is a consequence of the licensing model. Any sale is limited to a single phone country code prefix, but for an additional fee, the customer can license the usage of the solution in additional countries without geographic limitations.

Business risks

Human resources

Commercial spyware companies don't seem to have any kind of problem recruiting highly specialized human resources to develop their solutions. This was evidenced by the LinkedIn profiles of several highly specialized engineers. In one example, the NSO Group in June had just recruited new, highly specialized engineers from an intelligence military unit.

During the development of the iOS implant, Intellexa hired an iOS expert vulnerability researcher who had previously worked for the NSO Group. The timing of the hire indicates that the firm needed to integrate the implant with the exploit chain to deploy it reliably on iOS devices.

Snippet of the iOS security expert Curriculum Vitae

Such "experts" can be found working for and actively hunting for jobs regularly at other commercial spyware vendors too. For example, a quick search by Talos showed that just in September 2023, the NSO group had hired another security researcher with the same research background:

Example of employment history

And there are several examples like that. The highly skilled researchers will move from one company to another in the same line of business supplying a constant flow of human resources as needed.

Target operating system support

New operating system releases don't seem to make a considerable impact on the Predator solution. Intellexa now supports OS versions going back 18 months on Android and 12 months on iOS from their last supported version, which may not be the latest. Google releases approximately one new version per year just like Apple. But, the Android OS may consist of beta versions months before general availability. This gives plenty of lead time to Intellexa and their exploit suppliers to develop new exploit chains to use as initial attack vectors.

It is important to understand that the Alien/Predator implants themselves don't need to change much between operating system releases. They are written to be as generic and modular as possible, and the modules that need to be specific to an OS version and/or capability are written in Python, which can easily be updated and deployed on the fly via a customer's infrastructure.

The components that are more sensitive to operating system updates are the initial access vectors and the persistence mechanisms. These capabilities often rely on exploits that can be patched or new mitigation techniques may render them useless.

Vulnerability exploits chain patching

This is the most sensitive and least controlled part of any commercial spyware solution. Still, one may think that there is a high impact on the operational capability of a commercial spyware vendor, but the reality seems to prove the impact is low, or medium at most.

Exploit brokers and exploit research companies, sell full or partial exploit chains as a subscription model where the customers are entitled to workable replacements if the purchased chain is patched.

The timeline of events shows that it took Intellexa, at most, six months (probably less) to obtain and integrate a new fully operational exploit chain into their solution, after their Android previous one was patched in Nov 2021. This is confirmed by the fact that, in May 2022, their platform was being shipped to a new customer in Sudan, according to the Lighthouse report.

Overall, this demonstrates that exposing the vulnerabilities used by commercial spyware vendors, although extremely important, does not impose much of a risk on them. In fact, that risk is transferred onto the exploit brokers and vendors.

This has caught the attention of the Biden-Harris administration, to the point that the Intellexa Alliance was added to the Entity List for "*...determination that the companies engaged in trafficking in cyber exploits used to gain access to information systems…*" In practical terms, U.S.-based companies that deal in exploits cannot do business with the Intellexa galaxy of companies. This means that Intellexa will have to procure its exploits from companies in other regions, which for the time being, doesn't seem to be a problem. However, if the United Kingdom and the European Union take similar actions, the market will become smaller, making it much harder for these companies to acquire their initial attack vector.

The lack of impact from public exposure

The public exposure of commercial spyware companies creates awareness and has gained the attention of governments and regulating bodies. Such disclosures have also been successful at attributing malicious operations conducted by regimes against human rights activists, journalists and civilian dissidents, indicating the lack of a moral compass of many of Intellexa's "customers."

However, exposing regimes conducting these operations seems to have little effect on these companies' abilities to make money. It may increase the costs by making them buy or create new exploit chains but these vendors appear to have seamlessly acquired new exploit chains, enabling them to remain in business by jumping from one set of exploits to another as a means of initial access. A majority of public disclosures in the commercial spyware space focus on the political aspects of the operations along with listing malicious domains and infrastructure but fail to tear open the inner workings of the malware themselves. The domains and infrastructure exposed in a disclosure are owned and operated by spyware customers themselves, often in silos, meaning that exposing one operation typically may have no impact on all the other customers. However, the risk of exposure will always be primarily based on the efforts put by the customer into their anonymization chain.

Such disclosures may have a substantial impact on the regimes (“customer”), but they fail to impose costs on the spyware vendor themselves. What is needed is the public disclosure of technical analyses of the mobile spyware and tangible samples enabling public scrutiny of the malware. Such public disclosures will not only enable greater analyses and drive detection efforts but also impose development costs on vendors to constantly evolve their implants.