© Colin Foo

October 6, 2023

Predator Files: Technical deep-dive into Intellexa Alliance’s surveillance products

On 5 October 2023, a major global investigation – the “Predator Files” – was published exposing the proliferation of surveillance technologies around the world and the failure of governments and the European Union (EU) to properly regulate the industry. The Security Lab at Amnesty International is a technical partner in the “Predator Files”, a project coordinated by the European Investigative Collaborations (EIC) media network into the **Intellexa alliance**, the makers and marketers of the **Predator** spyware. As part of this collaboration, the Security Lab has reviewed technical documentation, marketing material and other records obtained by Der Spiegel and Mediapart – who are part of EIC – which shed light on the ecosystem of surveillance products offered by the Intellexa alliance.

The Intellexa alliance is an evolving group of companies and brands that have been involved in developing and marketing a wide range of surveillance products including advanced spyware, mass surveillance platforms, and tactical systems for targeting and intercepting nearby devices. The corporate entities of the alliance span various jurisdictions, both within and outside the EU. The exact nature of links between these companies is shrouded in secrecy as corporate entities, and the structures between them, are constantly morphing, renaming, rebranding, and evolving.

In the same vein, the products marketed by Intellexa have been rebranded and renamed numerous times, as various Intellexa alliance entities have worked together to combine product development and marketing activities. This report provides an overview of the distinct products and "attack vectors" offered by this surveillance alliance, including a product glossary to help clarify the analysis where multiple product names were used to describe the same product line over time. This report does not endeavour to describe every product in exhaustive detail, but rather to provide an overview of known or significant products. The goal of this research is also to provide an understanding of the potential impact of the described attack techniques, without making a judgement on the effectiveness of individual products, since marketing material can often overstate the effectiveness of commercial products.

Technical specifications and marketing material from surveillance vendors is often kept secret. The resulting information asymmetry prevents defenders in the cybersecurity industry and at-risk civil society groups from understanding the full scope of threats that they face. The aim of this research is to provide concrete information about surveillance capabilities available from this one vendor in the commercial surveillance market. We hope that this report can be a resource for the cybersecurity community and major mobile device and technology vendors. Our recommendations section outlines possible **mitigations and detections** which can help **protect potential civil society targets and the wider internet ecosystem** from some of the attack vectors described here.

Surveillance Industry Glossary

Term	Definition
Spyware	*Spyware* is software which enables an operator to gain covert access to information from a target computer system or device.

Commercial spyware	*Commercial or mercenary spyware* are surveillance products developed and sold by corporate actors to governments to conduct surveillance operations. So called “end-to-end” commercial spyware systems provide a full system for device infection and data collection. Components of these systems include the exploits used to install the spyware, a spyware agent which runs on the target device after infection and backend systems to gather and analyse the collected surveillance data.
Spyware agent	A *spyware agent* (or implant) is the final software code installed on a computer or phone after it has been successfully infected. The agent is responsible for collecting data from the device, activating sensors such as microphones and cameras, and uploading this data to the spyware operator.
Software vulnerability	A *software vulnerability* is a technical flaw or weakness in a software component or piece of code which can be exploited by an attacker to bypass security defences.
Exploit	An *exploit* is a piece of software or code which takes advantage of (or exploits) one or more software vulnerabilities to gain access to a device. On modern mobile devices ex-

	ploits must bypass numerous layered security defences and can be highly complex. A full exploit chain targeting latest device versions can sell for millions of euros.
Baseband	A mobile *baseband* is the hardware and software components in a mobile phone which are responsible for communicating over a radio interface with a mobile phone cell tower or base station.
Zero-day	A *zero-day vulnerability* is a software flaw which is not known to the original software developer and for which a software fix is not available. A zero-day exploit taking advantage of this flaw can successfully target even fully patched and updated devices.
Vector	*Vector* is a surveillance industry term for the different pathways or techniques which can be used to deliver an exploit to a target device. These include so called *1-click* and *zero-click* vectors.
1-Click	A *1-click* attack requires action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including

	spoofing legitimate websites or news articles. If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device.
Zero-click	A *zero-click* attack is a surveillance industry marketing term for any vector which can infect a device without requiring a user action, such as clicking on a link. *Fully remote* zero-click attacks allow infection over the internet, often by exploiting flaws in popular messaging apps such as iMessage or WhatsApp. Non-remote or *tactical* zero-click attacks can silently infect devices where the attacker has privileged network access or is in physical proximity to the target.
Network injection	*Network injection* is a technique where internet data packets are injected in the internet traffic of a target to block, intercept or manipulate their traffic.
Man-in-the-middle (MiTM)	A *man-in-the-middle* is an attacker who can read, modify, and block the network traffic from a target. A MiTM capability can be used to censor the target or perform network injection attacks.

Man-on-the-side (MOTS)	A *man-on-the-side* is an attacker who can read and monitor network traffic but is not able to directly block or modify the traffic. This situation is common when an attacker has access to a copy or mirror of traffic sent over a fibre optic link. Network injection attacks can also be performed from this network position.
Tactical infection	A *tactical infection* vector allows an attacker to attack devices in close physical proximity. Malicious Wi-Fi networks and mobile base stations can be used to silently redirect a nearby target to an exploit link. Attackers can also exploit vulnerabilities in cellular baseband software and Wi-Fi interfaces to infect nearby devices using radio packets sent over the air.
Strategic infection	*Strategic infection* is a marketing term referring to network injection systems deployed at an ISP (internet service provider) or national internet gateway which can be used to deliver spyware. These systems can intercept unencrypted requests sent by a target and silently redirect their device to an exploit link.
SS7	*Signaling System Number 7* is a set of signalling protocols and standards used in telephone networks to perform actions such as call-estab-

	lishment, routing, and roaming between national and international mobile phone providers. The protocol was designed without modern security defences and has been exploited by commercial surveillance vendors to enable various attacks including location tracking and communications interception.
Distributed Denial of Service (DDoS)	A *Distributed Denial of Service* is an attack aimed at disrupting a website or network by overloading the system with too much traffic or too many requests. This attack can result in a website being unavailable to legitimate visitors.
Avatar	An *Avatar* is a fake identity or online account which is used to gather information from online platforms or to interact with a targeted user. These seemingly real profiles can be used to send targeted attack links or to spread information online through social media or messaging services.

Spyware – Zero-clicks and 1-clicks

There is an ongoing high-stakes race between the vendors of smartphones and other devices we rely on and actors who are invested in subverting these systems for surveillance purposes. Mercenary spyware companies continuously develop and refine their tactics to adapt to expanding security mitigations introduced by vendors, to evade detection and to diversify their offering for customers with different operational and legal requirements.

For many years, researchers and security practitioners publicly observed so called ‘1-click’ attack vectors. Although the specifics vary between different types of attacks and exploits, the common characteristic of 1-click attacks, as demonstrated by their name, is the requirement for the target to unwittingly perform an interaction which triggers the exploitation process. To ensure the target initiates the process, attackers typically need to employ some form of ‘social engineering’. For example, a common ‘1-click’ attack vector involves delivering a malicious link via email, SMS or instant messenger apps with a tailored message to trick the victim into clicking on the malicious link. Just one click can be enough to deliver an exploit for their mobile browser.

As well as requiring interaction from the target, 1-click attacks also often leave behind visible traces which are useful for researchers and security practitioners to discover the **attempted attack**, and possibly even reconstruct which particular mercenary spyware system was involved in the attack.

The past five years saw the advent of so-called “zero-click” attacks. Such attacks – by definition – do not require any action on behalf of the target. The absence of tell-tell links also makes it much more difficult for a target to learn of the attack attempt without an in-depth forensic analysis of their device. Fewer traces and forensic evidence also make it exceedingly difficult for any independent authorities to investigate cases of abuse of these products. This lack of independent oversight capability for advanced attacks including ‘zero-clicks’ also makes it more difficult, if not impossible, to reconcile the use of these tools with human rights requirements.

For these reasons ‘zero-click’ has become the tactic of choice for mercenary spyware companies and their customers. Higher reliability, lower risk of discovery, and situational adaptability have made zero-click attacks an in-demand cyber *passe-partout*, and an ongoing challenge for digital defenders and technology vendors alike.

These attacks can come in different forms and target different network and software attack surfaces. In the last few years, several zero-click exploit chains have been **discovered** leveraging vulnerabilities in messaging platforms such as **iMessage and WhatsApp**, which can be used as the entry point to fully compromise the device. For example, a vulnerability in image parsing code, reachable in Apple’s iMessage image preview feature, can be used to silently deliver a first-stage attack to an unsuspecting target. Without any link to click, the target is unlikely to notice that anything untoward has happened.

Due to increased scrutiny from security researchers and technology vendors like Apple and Google, the development of full zero-click exploit chains which enable full system compromise are becoming ever more costly to develop and more fragile to maintain. Public pricing lists from a major exploit broker offer up to $2.5 million USD for a full chain, although information available to the Security Lab from industry sources suggests the true cost to a government wishing to buy such a full-chain capability off-the-shelf is more than double this price, if such a full chain is available.

Recent explosive reporting **from Haaretz** has revealed how cyber-surveillance companies are racing to subvert and exploit the already invasive digital advertising ecosystem to target and infect mobile devices globally using ad-network powered "zero-clicks". Spyware companies are borrowing hyper-targeting techniques from the already rights abusing ad-tech industry to enable their customers to infect targets as they are simply browsing a legitimate website. These new developments add urgency to the human rights case for banning the surveillance-based advertising model, which already undermines a number of human rights, even before being paired with highly invasive mercenary spyware.

As long as government demand for such invasive spyware tools and resulting profits from the mercenary surveillance industry remain high, we will continue to see a drive towards exploiting the essential shared internet infrastructure that the public relies on.

However, these "remote zero-click" attacks are not the only tactic that researchers and security practitioners have observed recently. Attackers with privileged access to a target's mobile or Wi-Fi network can leverage this vantage point to automatically redirect the target to an infection page. This tactic is commonly referred to as a "network injection".

Companies like **Hacking Team** and **FinFisher** pioneered the commercialisation of network injections over a decade ago. While early systems often involved **injecting malicious executable files**, current generations of these tools have evolved to use increasingly advanced exploits and vectors in response to generational change in mobile security and other network protocols.

Surveillance companies have productised a range of tactical equipment to mimic cell towers and to infiltrate Wi-Fi networks and even covert network equipment to physically install upstream in mobile networks and Internet service providers. Ultimately, they all aim to intercept the traffic generated by the target device, typically HTTP, hijack it, and then silently redirect the targets' web browser to an exploitation site. In this way, attackers can leverage more common 1-click exploits in browsers such as Chrome and Safari, but still silently infect a target without needing user interaction.

For example, while reading through their social media feed, a user might decide to read an article from a legitimate local news website, and inadvertently get their phone infected as a result. Just opening one HTTP link to the news website could give the attacker the split-second opportunity needed to redirect to a spyware infection page. The network injection attack and the subsequent exploitation **can happen automatically** and there is nothing, other than perhaps navigating over a VPN, that the target could have done to prevent it.

Because of this, network injection-based products have become lucrative options in mercenary spyware companies' offerings, appealing especially to customers who have legal or coercive power over a country's telecommunications infrastructure. While such systems may be operationally complex to install initially, once deployed, a surveillance operator can easily integrate with new infection solutions which create an ongoing threat.

Intellexa's spyware and attack vectors

The Intellexa alliance has built and commercialised a comprehensive suite of tactical and zero-click network injection products – marketed under the Intellexa brand – which accompany the sale of their flagship spyware, Predator. In the following section we detail the technical capabilities of Predator itself, and the wide range of supporting Intellexa products designed to deliver the Predator spyware to targeted mobile devices through the interception and subversion of mobile networks, Wi-Fi and the internet.

Our aim in this analysis is to provide concrete information to policy makers, product vendors, security researchers and civil society to help understand and develop defences against these dangerous attack vectors.

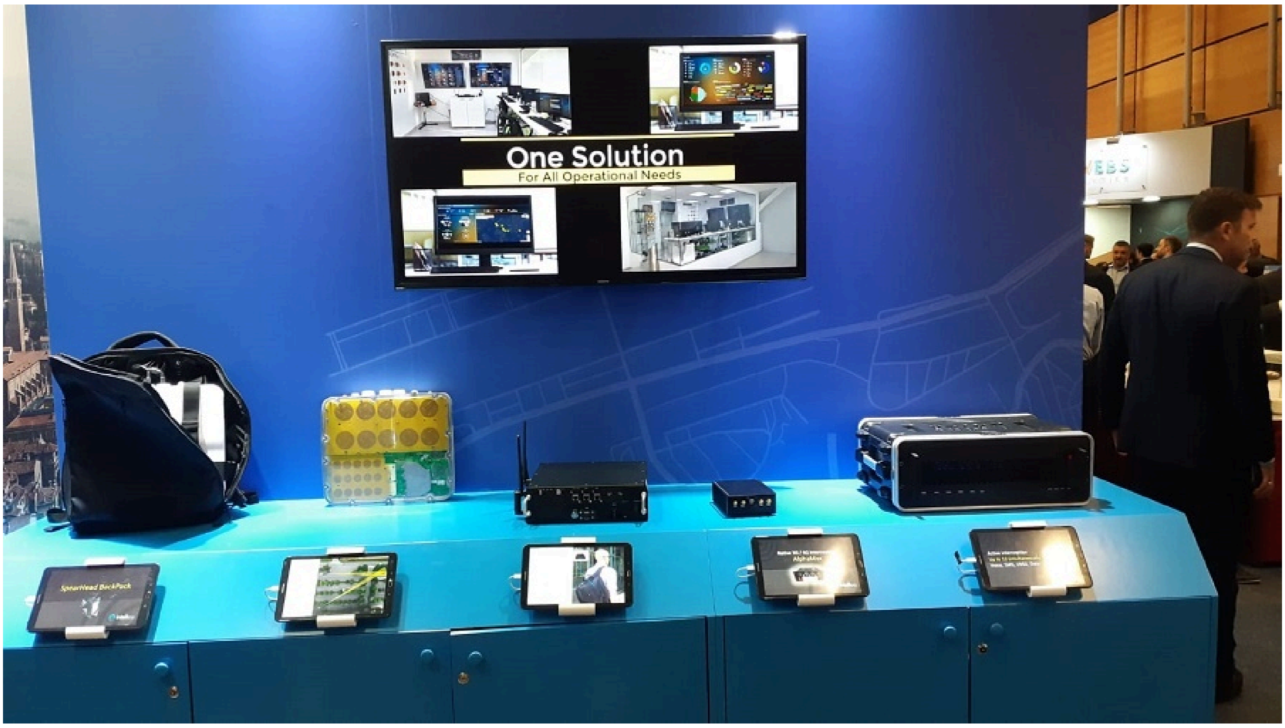


Figure 1: Exhibit of Intellexa's range of interception and OSINT products from an industry trade fair.

Predator – A highly invasive spyware ecosystem

The Security Lab's analysis of brochures and technical documents provided by EIC provides new insight into how this spyware functions on a technical level and the methods by which it infects targets' devices. Much of this information is published today for the first time as part of the "Predator Files".

The Intellexa alliance's mobile spyware, mostly commonly known as "Predator", is a form of highly invasive spyware that by default gains total access to all data stored or transmitted from the target's device, and that is designed to leave no traces on the target device, which would render any independent audit of potential abuses impossible.

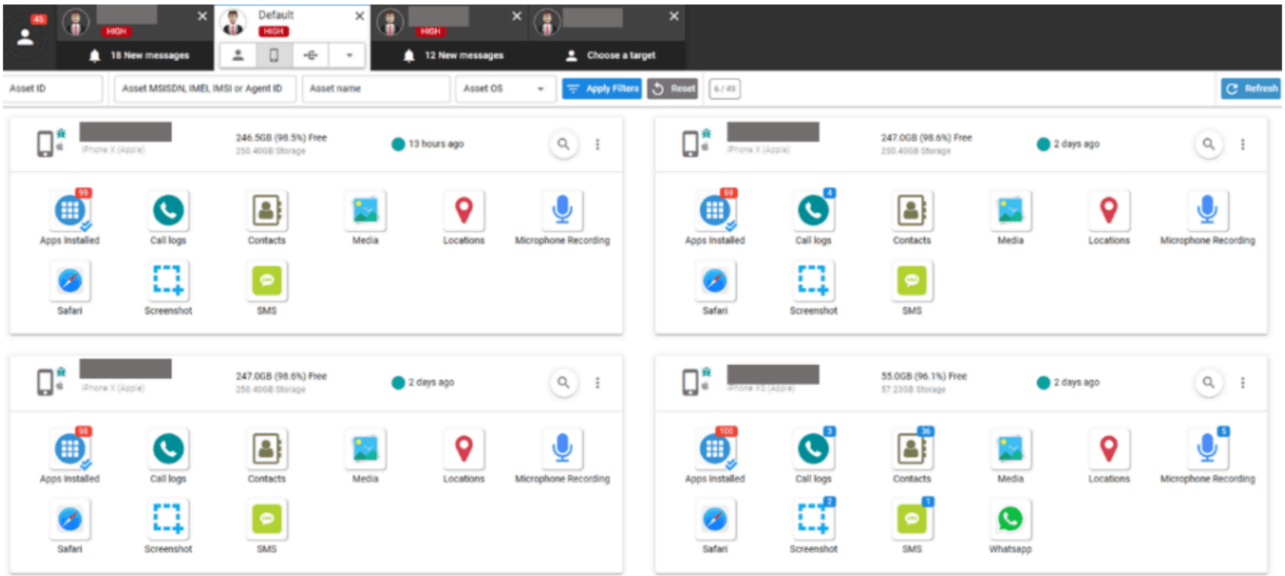


Figure 2: Intellexa Predator spyware interface (source: EIC documents)

Predator spyware infections are managed via a web-based system which Intellexa terms the “Cyber Operation Platform”. Spyware operators can also use this interface to initiate attack attempts against a target phone, and if successful, to retrieve and access sensitive information including photos, location data, chat messages and microphone recordings from the infected device. The full Predator system includes a number of distinct software and infrastructure components. These include the spyware agent itself, which is installed on the target’s device, and the software exploits and attack vectors necessary to install the spyware covertly on the target’s phone.

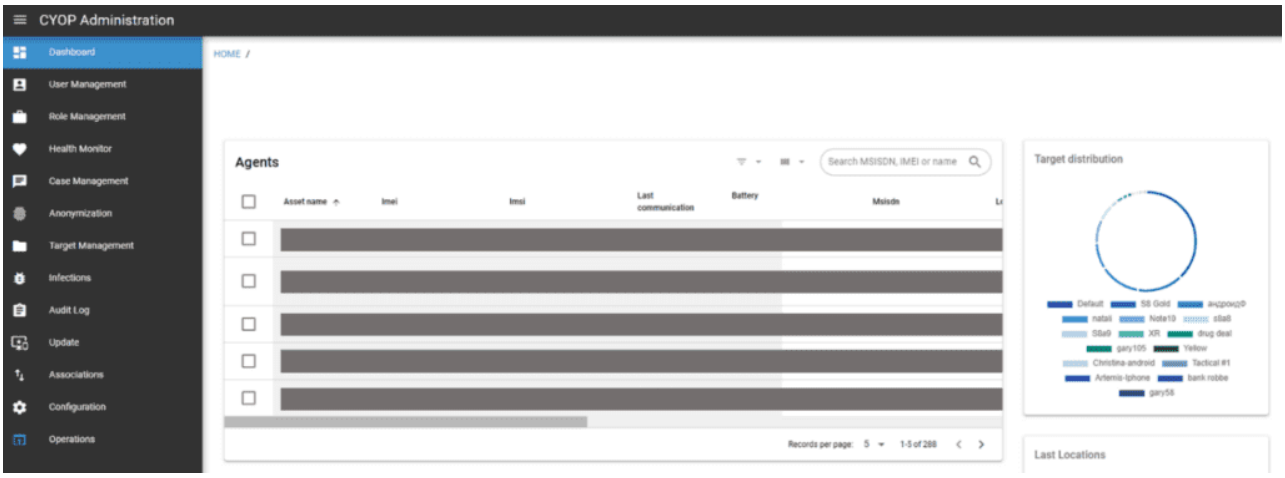


Figure 3: CyOP – Cyber Operations Platform (source: EIC documents)

The alliance has used several marketing names since 2018 to describe its mobile spyware products including ‘Green Arrow’ for their Android spyware agent and ‘Red Arrow’ for their iOS spyware agent. More recently, Intellexa has marketed its spyware system as ‘Predator’ and ‘Helios’, among others. In this report, we refer to this overall mobile spyware product as Predator as we believe all of these product names refer to the same set of broadly related spyware technology originally developed by the North Macedonian company Cytrox, which later became part of the Intellexa alliance.

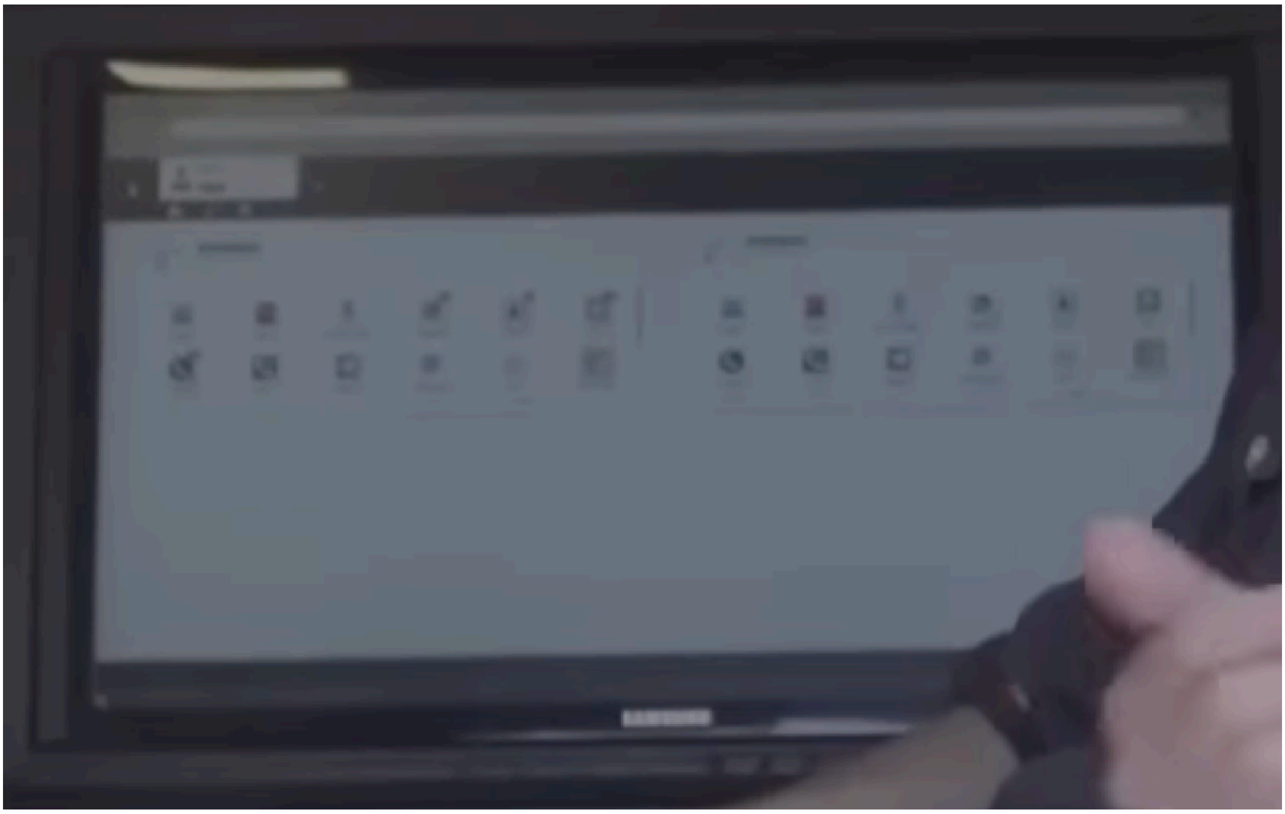


Figure 4: Predator interface shown in 2019 “spy van” interview (Forbes)

The Predator user interface documented publicly for the first time in the “Predator Files” is structurally and visually similar to an earlier Predator interface briefly shown in Intellexa’s infamous “spy van” during a **2019 Forbes interview** between Thomas Brewster and Intellexa founder Tal Dilian.

Predator network architecture

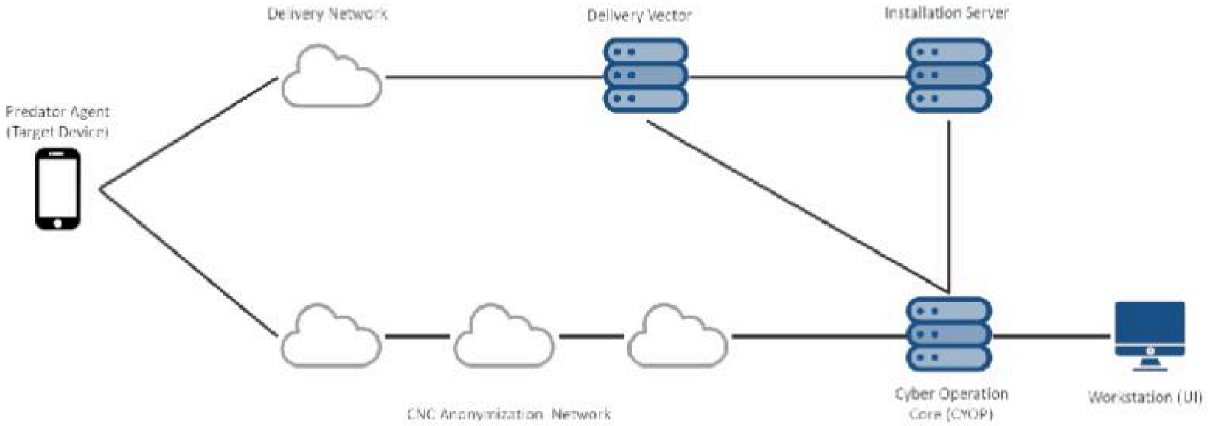

Delivery Network
Delivery Vector
Installation Server
Predator Agent (Target Device)
CNC Anonymization Network
Cyber Operation Core (CYOP)
Workstation (UI)

Figure 5: Predator high-level server architecture (source: EIC documents)

The “Predator Files” disclosures reveal how exploit code and spyware payloads are delivered to the target device from what Intellexa terms its “installation server”. Once a phone is infected with the Predator agent, it connects to the command and control (CNC) network where the operators can issue commands to the Predator spyware agent, such as to retrieve certain files or to activate the microphone.

As shown in the Predator architecture diagram (Figure 5), exfiltrated data is also transferred back from the infected device via the CNC anonymisation network with the aim of obscuring the location and identity of the spyware operator, making it more difficult for researchers to identify the source and nature of the attacks.

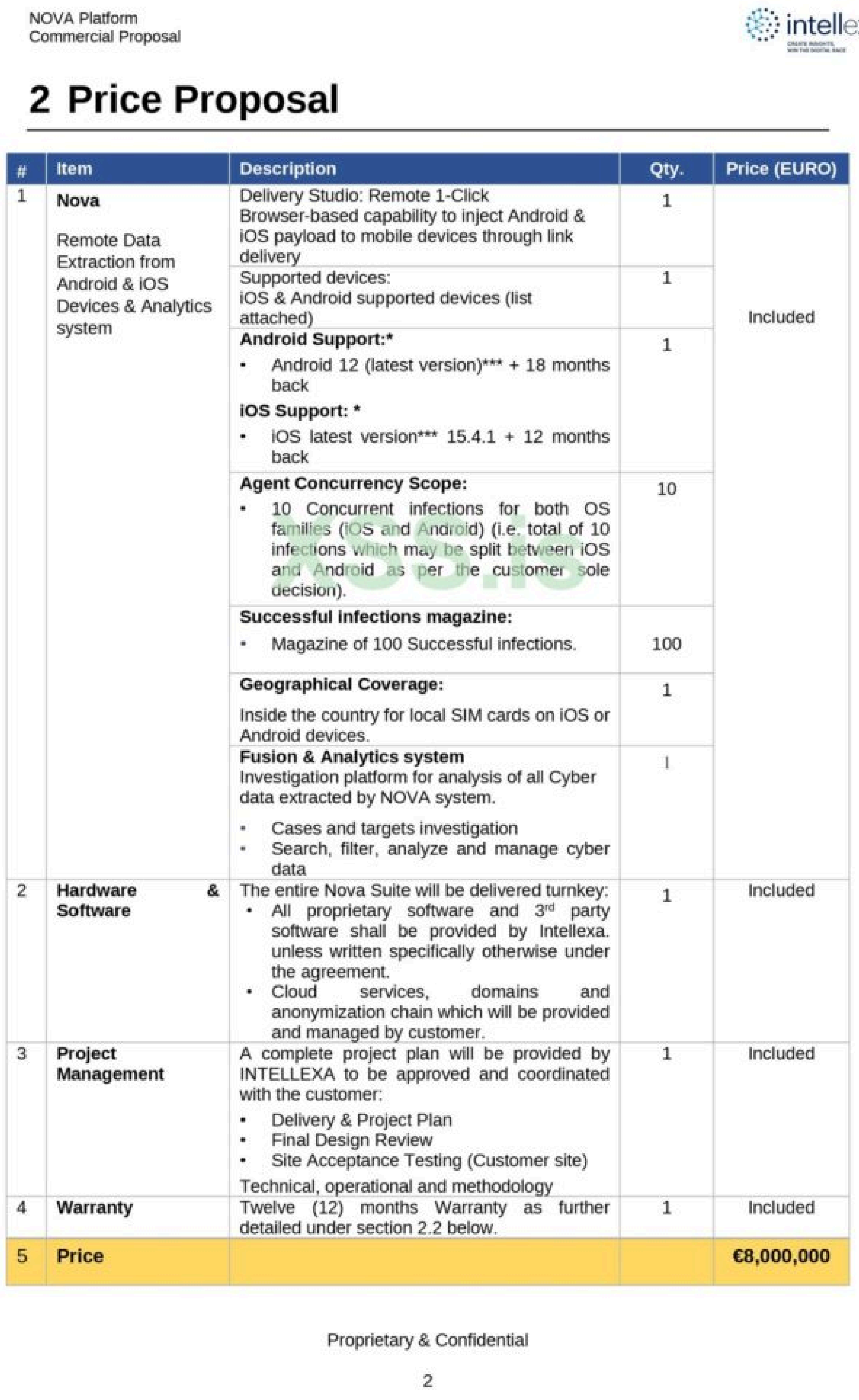
Pricing of mercenary spyware

Multiple leaked commercial proposals for the Predator spyware system provide insights on the economics of the end-to-end mercenary spyware industry. The New York Times **published** a 2021 commercial offer for Predator in December 2022. A more recent commercial offer for ‘NOVA’, an Intellexa alliance combined spyware and data analysis system, was leaked on the XSS.is cybercrime forum in 2022 and later **republished online**.

While commercial demand is one factor in spyware pricing, these leaked proposals also provide a proxy metric to evaluate the difficulty of attacking modern smartphones and building a maintainable commercial product capable of conducting such attacks.

The commercial offerings license a base system with the Predator Android and iOS surveillance agents along with optional add-ons. These commercial add-ons include the ability to target devices outside the customer’s country, to maintain an infection of a device between reboots (termed “persistency”) and to increase the “magazine” limiting the total number of successful infections allowed in the system.

This 2022 commercial proposal only advertises 1-click attacks, with 10 concurrent live agents (simultaneously infected devices) and 100 successful infections. The offer is restricted to domestic targeting only. A series of trainings for future operators of the spyware system is also included in the proposal.



NOVA Platform
Commercial Proposal

intellexa

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

Proprietary & Confidential

2

Figure 6: Leaked 2022 commercial offer with geographic, concurrency and magazine limits (XSS.is cybercrime forum).

Persistency is offered through an additional license for €3 million euro with support for both iOS and Android, although the 2022 proposal cautions that the persistent infection would not survive a factory reset and would not prevent version updates on the device. Additionally, if international targeting is required, the “Nova international” add-on is available for an additional 1.2 million euro which would give access to 5 additional countries to be mutually agreed upon, with no geographic limitation of target location.

The 2022 proposal also includes a condition that “Delivery is subject to export and/or import control certification by the relevant European authorities, as applicable”.

In the earlier 2021 proposal published by the New York Times, a separate add-on for an additional “magazine” with 100 successful infections was priced at €900,000. From this commercial licencing we can infer a lower bound cost per infection of at least €9000 euro per successful infection for this particular spyware system. This cost per infections is likely to increase each year as the challenge of developing and maintaining reliable exploit chains for modern mobile devices becomes increasingly difficult. While the cost of these attacks tools and individual attacks is significant, we are not yet at the point where these tools are economically unfeasible for States to deploy against civil society and human rights defenders.

Attack vectors

Both previously published commercial proposals and additional material available in the “Predator Files” investigation focus on 1-click attacks using malicious links. Indeed, the 2022 Predator commercial proposal explicitly describes the product as a “remote 1-click browser-based capability to inject Android and iOS payload to mobile devices through link delivery”.

However, in the following section we will demonstrate how such 1-click attack capabilities can be integrated with other surveillance systems to enable more covert and dangerous infection options. One Intellexa alliance document outlines its various approaches for delivering these attacks to the target. These include:

- Strategic ISP infection – described as “0-click through HTTP browsing”.
- Tactical infection (WiFi and GSM) – described as 0-click through HTTP browsing.
- Avatars platform – anonymous accounts or “bots” on social media or instant messaging apps can be used to send 1-click links to targets.

Mars – Infection through network injection

Description:

The Intellexa "Mars" product is a network injection system installed at mobile operator ISPs which allows a Predator customer to silently redirect targeted users to a Predator infection server after browsing any HTTP web page. This enables a 1-click browser exploit to be used as a "zero-click".

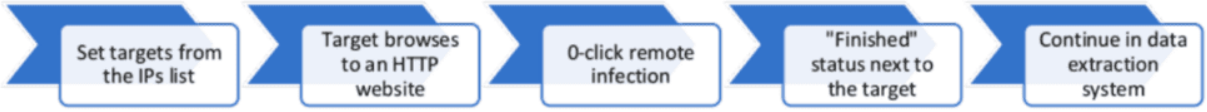

Set targets from the IPs list
Target browses to an HTTP website
0-click remote infection
"Finished" status next to the target
Continue in data extraction system

Figure 7: Mars "zero-click" infection – operational flow (source: EIC documents)

Technical Analysis:

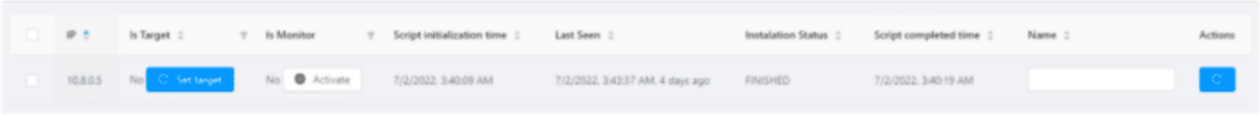
Network injection systems rely on the targeted user eventually opening a link to any legitimate unencrypted HTTP URL. The network injection system can respond to the original HTTP request with a HTTP redirect containing a to a 1-click browser exploit link which infects the device without further user action. Network injection systems in effect allow 1-click exploits to be used as no-interaction pseudo zero-clicks.

Such a system is not truly remote as it requires the target's internet traffic to be transferred over a network that the spyware operator can monitor. As more websites deploy HTTPS encryption, potential targets will tend to make fewer unencrypted HTTP requests, resulting in network injection systems taking longer to successfully inject and redirect a target.

The Mars solution consists of two distinct components: a physical Mars server deployed at each Mars-enabled mobile internet service provider (ISP), and a Mars administration system used by the surveillance operator to define targets and launch attacks across the Mars enabled ISPs.

In the Mars product specifications, Intellexa acknowledges that the product "requires full cooperation from the ISP for the integration and operation", as such these types of network injection systems can only be used to target devices domestically in a country or devices which are roaming with traffic being forwarded through the Mars-enabled ISP.

The reviewed Mars product documentation describes targeting of devices based on a static IP address assigned to the target subscriber rather than based on a phone number (or MSISDN). Targeting based on a phone number would require closer integration between the Mars system and the mobile operator's identity and user account systems which may make Mars deployment more complex.



□	IP	Is Target	Is Monitor	Script initialization time	Last Seen	Instalation Status	Script completed time	Name	Actions
□	10.8.0.5	No Set target	No ● Activate	7/2/2022, 3:40:09 AM	7/2/2022, 3:43:37 AM, 4 days ago	FINISHED	7/2/2022, 3:40:19 AM		

Figure 8: Administrator interface to target IP addresses.

Each mobile ISP must assign a static internal IP to the potential targets identified by the operator. The MARS operator can then enable targeted redirection and infection of devices connected through the system.

The cooperating ISP must also set up forwarding rules on the ISP gateway router to forward traffic from the predefined target IP addresses to the Mars system for traffic collection and manipulation. In the described scenario, the Mars system would act as a man-in-the-middle (MITM) inline system rather than a man-on-the-side (MOTS) system.

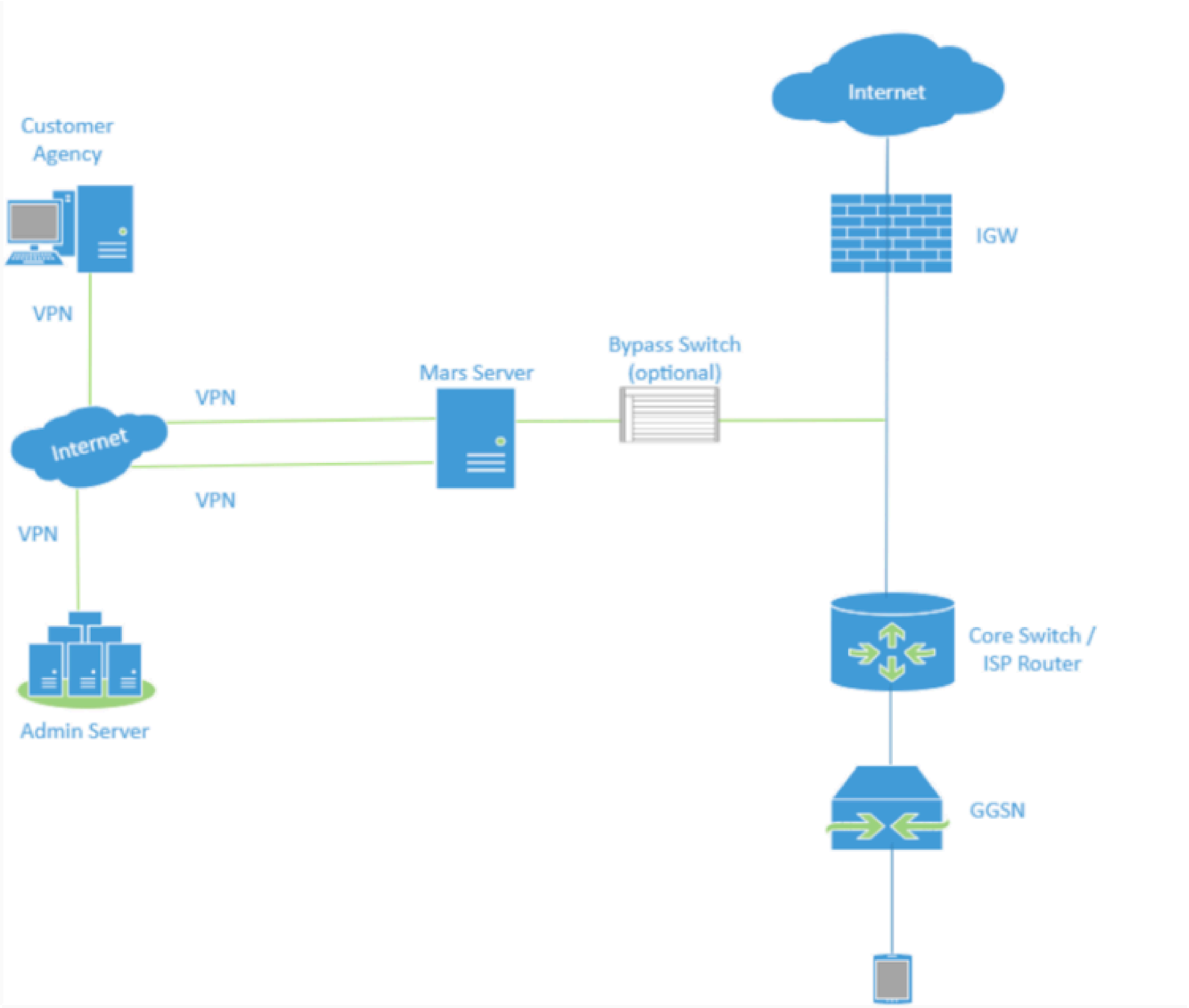


Figure 9: Network architecture for MARS system

Previous investigations have shown that the ISP-level (strategic) network injection infrastructure has been used to infect targeted mobile users with advanced spyware tools. In 2019, Amnesty International documented network injection attacks being used in Morocco to infect **human rights defenders** and **journalists** with NSO Group's Pegasus spyware.

The **Citizen Lab documented** a functionally similar system being used to target a political opposition figure in Egypt with Intellexa's Predator spyware in September 2023. The Citizen Lab investigation determined with "high confidence" that the network injection system used to deliver Predator infection links in Egypt was a Sandvine PacketLogic device. Earlier network measurements and research showed that Sandvine systems capable of network injection have been deployed in Egyptian networks since at **least 2018**.

From initial research, the Mars system offered by the Intellexa alliance appears to be a different product to the Sandvine system identified in Egypt. However, more research is needed to characterise this system, its original manufacturer and to identify Mars systems deployed in the wild.

Jupiter – Mars add-on enabling injection on encrypted traffic

Description:

The Intellexa alliance "Jupiter" product is an add-on for the Mars network injection system. The product documentation available as part of the "Predator Files" claims the system allows surveillance operators to also perform network injection into targets' encrypted HTTPS traffic. The product is only able to inject "pre-enabled" domestic websites.

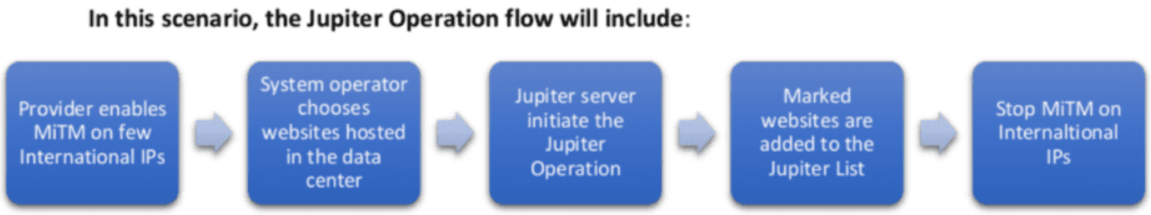

In this scenario, the Jupiter Operation flow will include:
Provider enables MiTM on few International IPs
System operator chooses websites hosted in the data center
Jupiter server initiate the Jupiter Operation
Marked websites are added to the Jupiter List
Stop MiTM on Internaltional IPs

Figure 10: Operational flow of Jupiter system (source: EIC documents)

Technical Analysis:

The Jupiter documentation states that "*SSL encryption has left intelligence agencies with no solution for interception and infection during SSL traffic".* The Jupiter system aims to subvert the HTTPS ecosystem to also enable network injection attacks on some encrypted traffic.

The product material explains that interception is limited to "local websites" hosted at an ISP in the customer country. The Jupiter hardware needs to be installed on a hosting providers network gateway or an ISP upstream from the domestic hosting provider where the local target website is running. Once Jupiter is installed, the operators need to perform a "one-time procedure", called a "Jupiter Operation", which involves redirecting traffic for the target website from "specific international IPs" allowing the target website to be enrolled into the system. A diagram of the combined Mars and Jupiter systems is shown in Figure 11.

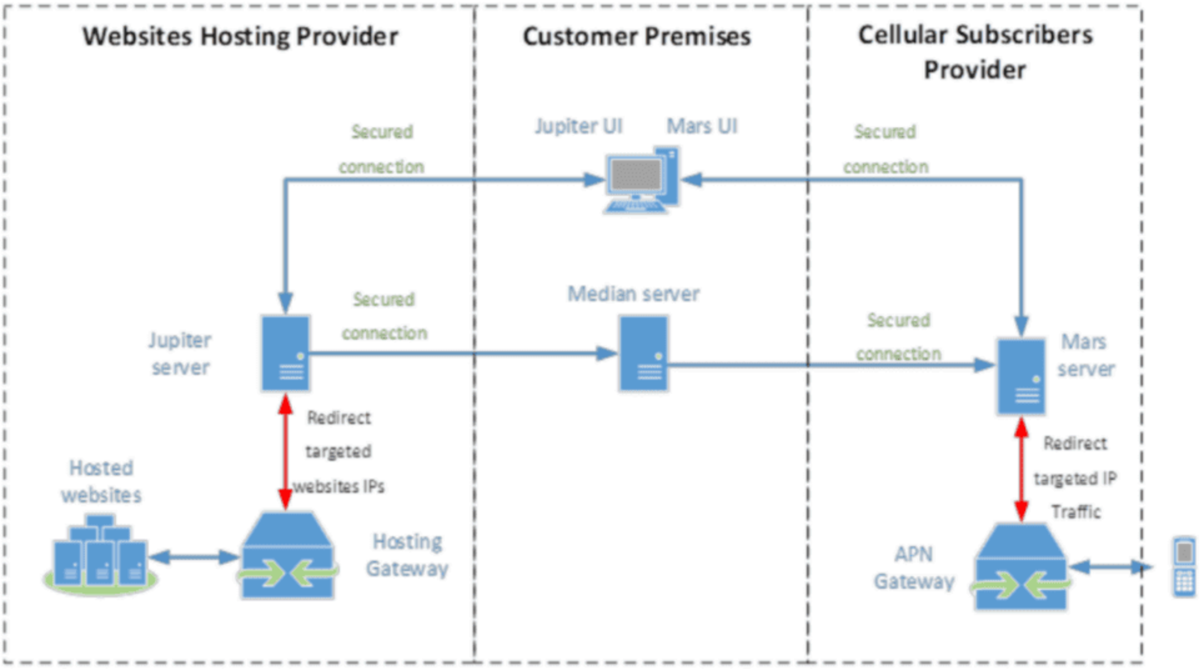


Figure 11: Network diagram of Mars and Jupiter systems for network injection (source: EIC documents)

Each local website that the "Jupiter Operation" is performed on will be added to the "Jupiter List" and becomes "approved for infection for a certain duration". A "median server" is responsible for communications between the Jupiter and Mars servers and maintains the "Jupiter List".

This technical documentation suggests that the Jupiter system relies on using a man-in-the-middle network position to obtain a valid TLS certificate for the targeted local website. Certificate authorities allow a number of challenge types to validate that an entity requesting a TLS certificate indeed controls the domain in question. These challenges include a "HTTP challenge" which verifies that a specific validation file is available on a website at a particular URL path, and a TLS challenge which checks that a website returns a specifically formatted TLS certificate.

With the Jupiter system installed at the hosting provider, the Jupiter customer can man-in-the-middle verification requests sent from the international IP ranges used by the TLS certificate authorities to verify the domain verification challenge. As the attacker chosen certificate authority receives a valid challenge response, it will allow the certificate request and in turn issue a valid TLS certificate to the Jupiter operator which is a valid and trusted for the target website.

The TLS certificate issued during the "Jupiter Operation" can then be loaded in the "Median server" and in the "Mars systems" installed at each mobile operator

ISP. Once the certificate has been issued, the Mars operator can actively man-in-the-middle encrypted HTTPS requests sent from a target to the local website without further interaction with the hosting provider network. This man-in-the-middle position can then be used to network inject browser exploit code inside the connection to the legitimate website.

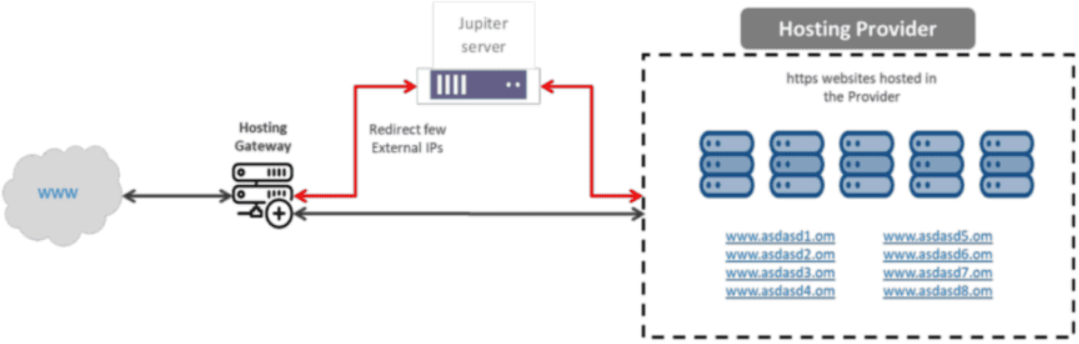


Figure 12: "Jupiter Operation" process involving temporary redirection of some external IPs (source: EIC documents)

Triton – Samsung baseband zero-click

Description:

Triton is a zero-click tactical infection product which can be used to compromise Samsung devices in a range of hundreds of meters through their cellular baseband.

Long-range Agent Delivery to Mobile Devices

GSM BaseBand 0-click target acquisition

Figure 13: Triton – Baseband target acquisition (source: EIC documents)

Technical Analysis:

The Triton system is a tactical infection vector which the Intellexa alliance's marketing material claims can infect many recent models of Samsung devices including "the latest models with the latest operating system versions". The system appears to target vulnerabilities in baseband software used in Samsung devices which allows infection with the Predator spyware with “no interaction with the target” or the need for the target to use a browser or any other app.

The attack involves a number of distinct steps. First, an IMSI catcher is used to downgrade target Samsung devices from 5G, 4G or 3G to the legacy 2G protocol. The documentation explains that the downgrade attack can be performed with an Intellexa alliance IMSI catcher product or with a third-party IMSI catcher which supports such downgrade attacks.

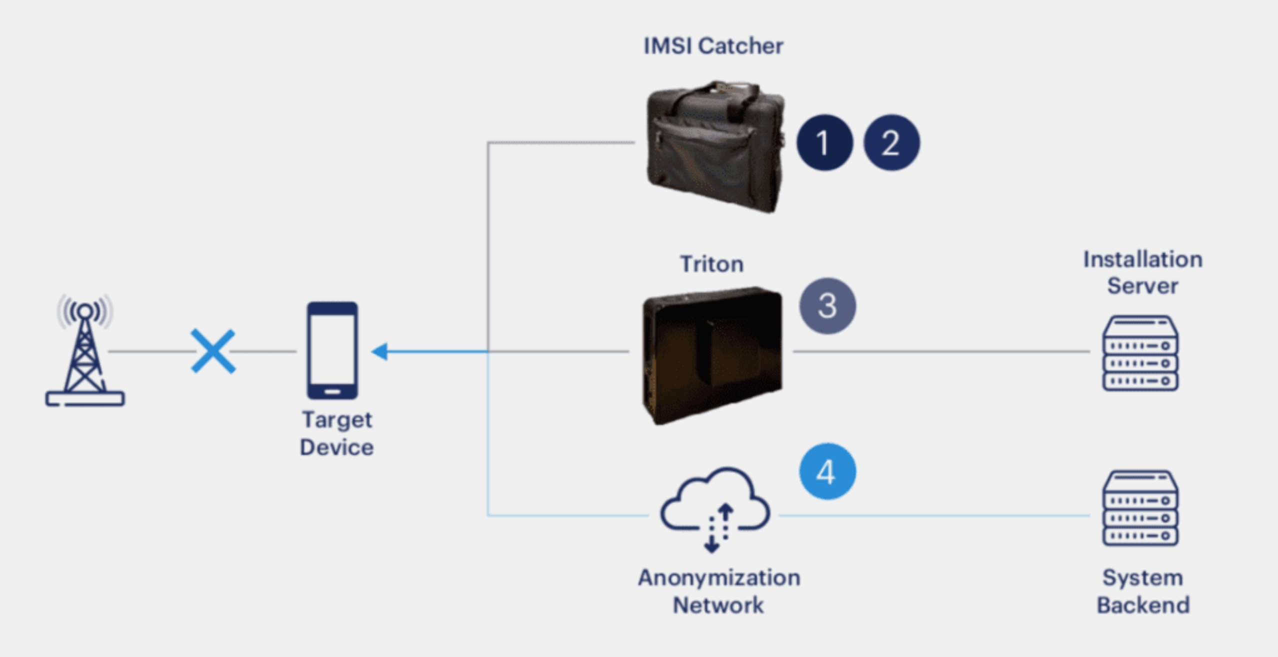


Figure 14: Diagram from Intellexa Triton marketing material

Once the target phone is downgraded to 2G, a separate 2G base station transceiver (BTS) – likely a software defined radio integrated with the Triton product – is used to deliver the attack payload over a ‘specific 2G radio channel’. The sales brochure claims the full spyware agent installation can take up to 3 minutes and be performed over distances ranging up to hundreds of meters.

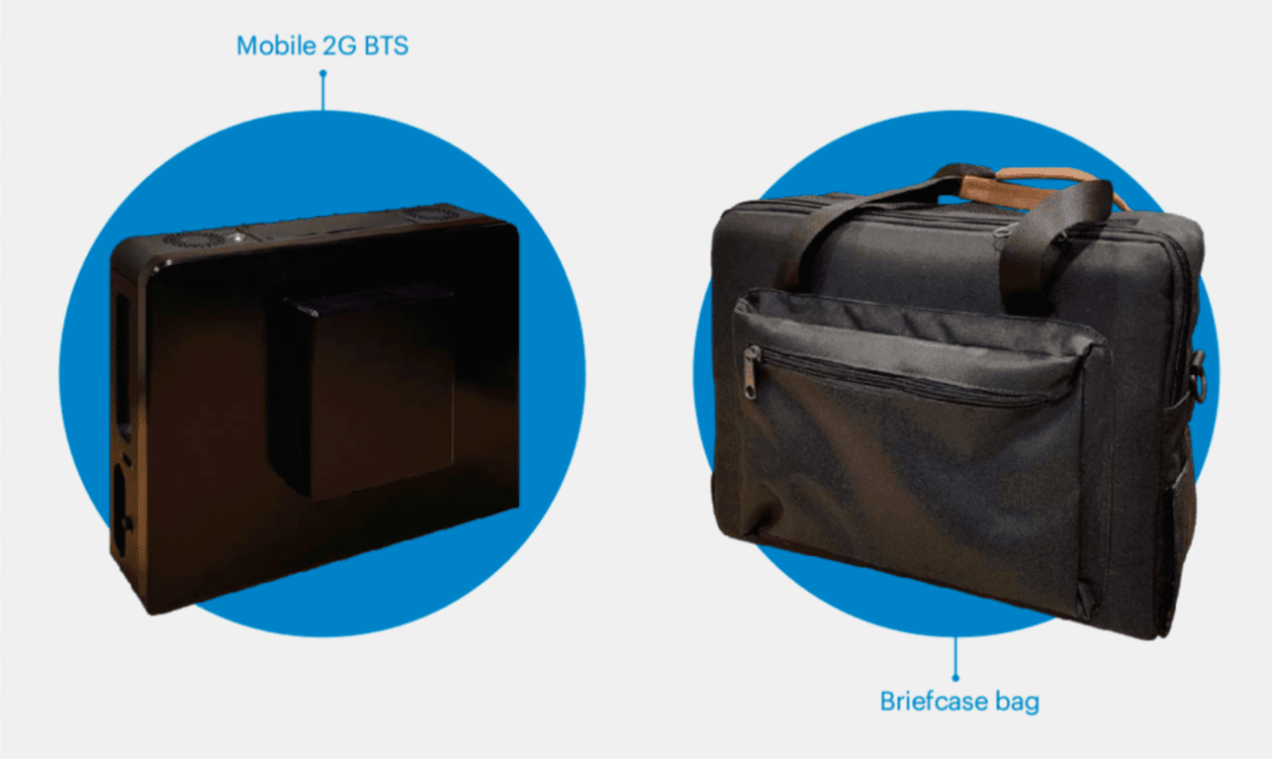


Figure 15: Diagram from Intellexa Triton marketing material

In March 2023, Google Project Zero **published research** documenting numerous fully remote zero-click vulnerabilities uncovered during their analysis of the Samsung Exynos baseband chipset and firmware used in many recent Samsung devices.

The Intellexa brochure claims that the Triton attack is effective against many recent models of Samsung devices. Based on the description of the affected device models and version, it is likely that Triton also targets vulnerabilities in the Exynos baseband software and in particular its 2G networking code. Unfortunately, the documentation available during this investigation does not include enough technical details to pinpoint the exact vulnerability or attack surface exploited by this product. It is unclear if Triton exploits a memory corruption vulnerability or if the baseband is manipulated to trigger a browser and pivot to a 1-click browser attack.

SpearHead – Wi-Fi interception and infection

Description:

SpearHead is a range of Wi-Fi interception systems originally developed by WiSpear is a member of the Intellexa alliance. SpearHead products allow target identification and geo-location, traffic interception, and network injection to deliver spyware payloads.

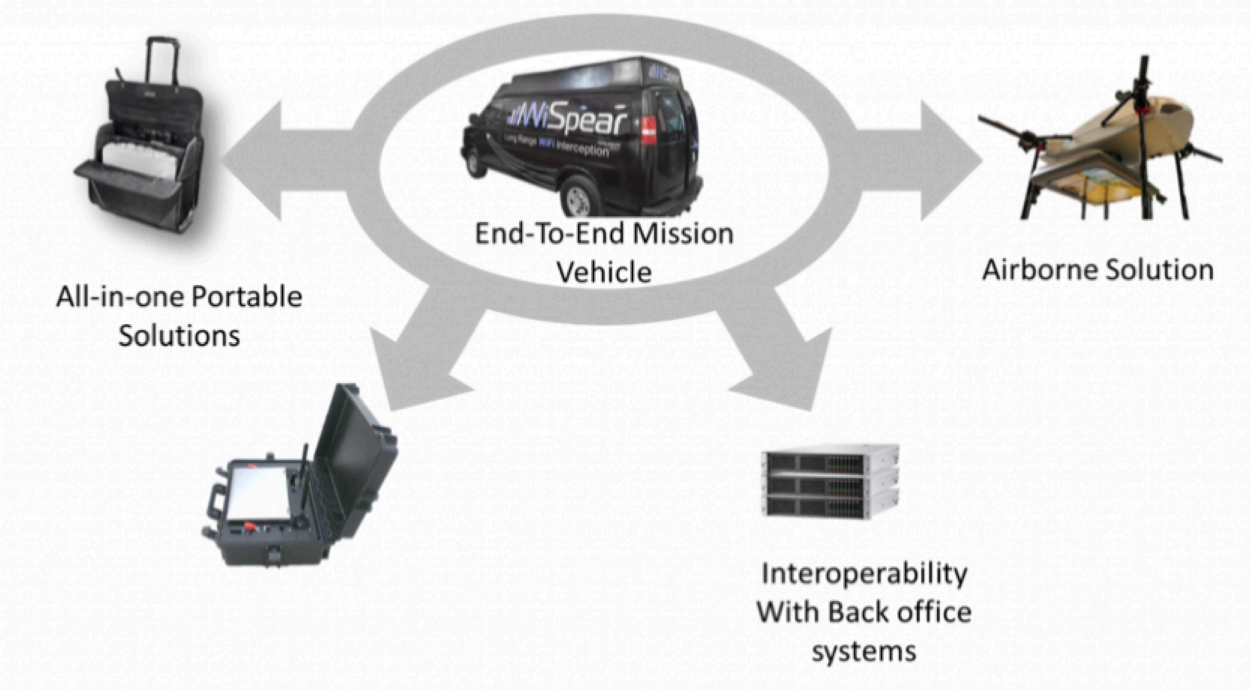

WiSpear
Long Range WiFi Interception
End-To-End Mission Vehicle
All-in-one Portable Solutions
Airborne Solution
Interoperability With Back office systems

Figure 16: Older public graphic containing WiSpear products (Source: public WiSpear image)

Technical Analysis:

EIC documents and **previous reporting** outline a range of SpearHead products which can be carried in a briefcase, mounted on a drone or installed in a **"surveillance van"**, the SpearHead 360. Intellexa alliance brochures claim the system is built around a Wi-Fi radio unit with a "digital adaptive beam-forming antenna" which allows for Wi-Fi signals to be "accurately geo-located based on direction of arrival (DoA) calculations".

The vehicle-based SpearHead 360 system can also be paired with the backpack or drone mounted SpearHead to create "ad-hoc tactical networks" which, according to the marketing material, can be used to triangulate and accurately geo-locate the exact location of emitted Wi-Fi signals over large distances.

In addition to Wi-Fi geolocation, the system also advertises methods for "advanced manipulation of WiFi communications and protocols" and multiple strategies to perform man-in-the-middle attacks which they term "active WiFi interception". The SpearHead systems promises integration with "back office systems" such as password cracking clusters which can allow for the brute-force calculation of Wi-Fi passwords where the network password is unknown. The system also includes a feature which uses "WiFi protocols to extract the device's IMSI". This feature may involve exploiting a publicly known information leakage flaw in **WiFi calling (VoWifi) implementations**.

The Intellexa material claims that their Wi-Fi interception systems is fully integrated with multiple "infection and data extraction systems" such as Intellexa's Predator. The SpearHead Wi-Fi interception devices can be used to perform network injection attacks on connected Wi-Fi devices and redirect to 1-click spyware infection links.

Alpha-Max – GSM interception and infection

Description:

Alpha-Max is a 3G/4G interception system originally developed by the Nexa group and marketed by the Intellexa alliance. Advertised features include the ability to identify handset identifiers (such as the target IMSI), listen to calls, block and modify text messages and intercept the data connection of any potential target in its vicinity.

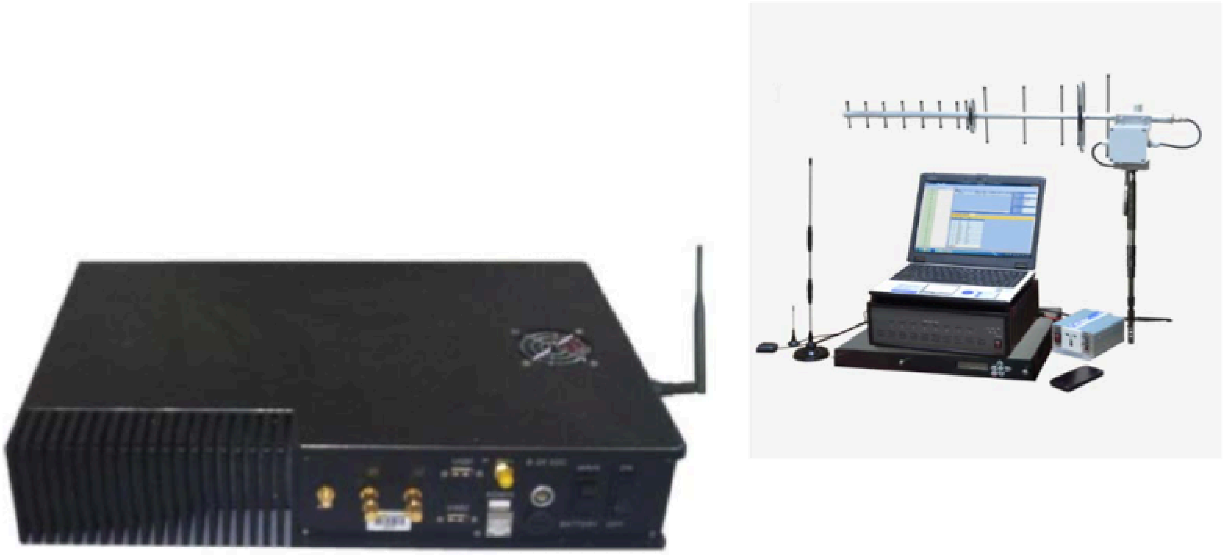


Figure 17: Tactical GSM interception systems in the ALPHA product line (source: DISCLOSE)

Technical Analysis:

The marketing material, which – based on described software versions – appears to have been written in 2019 and explains that the Alpha-MAX surveillance system works on the principle of mobile roaming. It consists of two integrated components, a 4G IMSI catcher and a 3G mobile base station (referred to as an eNodeB). Due to what was described as a “lack of 4G roaming agreements” at the time, target devices must first be downgraded from 4G to 3G using a built-in IMSI catcher.

The Alpha-Max system must be connected to the international SS7 network through a dedicated system called the “Alpha-Max provider system” that allows routing of calls, data and text messages. The documentation also says that, at the time, the provider system is “delivered with existing connectivity”, done through several Mobile Network Operators (MNO).

When the target is connected to the Alpha-Max 3G base station it authenticates to the virtual mobile network provider of the Alpha-Max. This allows the device to continue to communicate normally while allowing the operator to intercept the traffic.

In the 3G protocol the handset authenticates the cell tower, and it is no longer possible for an attacker to spoof an arbitrary mobile operator. The Alpha-Max system uses the legitimate network roaming feature and collaboration with mobile network operators to trick the device into roaming to another network. The backend signalling (SS7, and likely Diameter) connection allows the attacker-linked mobile network operator to send roaming requests to the targets’ home mobile operator and to **request the necessary cryptographic keys** to authenticate the handset.

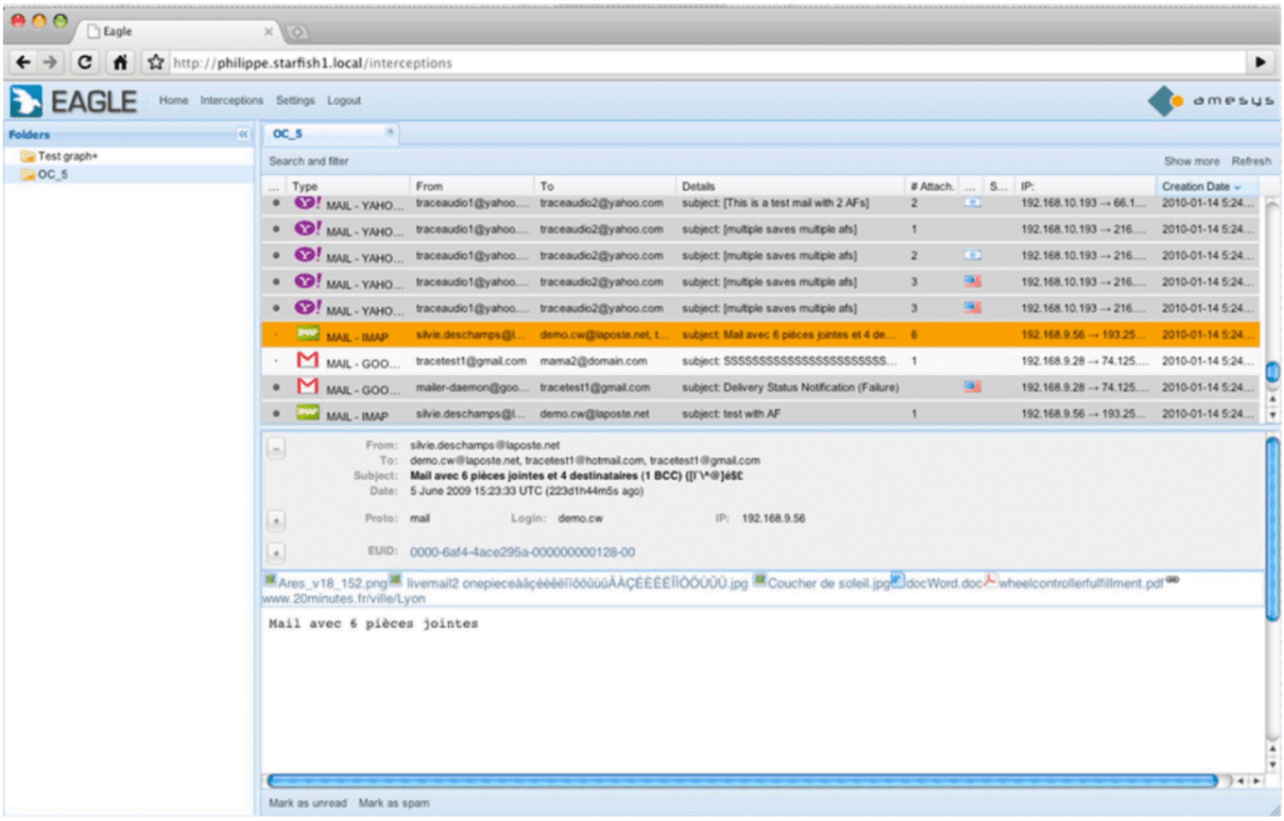
In a disclaimer, the product material explains that the “Alpha-Max is working based on roaming, all target mobile phones must be capable of roaming (i.e. roaming enabled). If not roaming enabled, this specific SIM card cannot be a target intercepted by the Alpha-Max”.

As with previous products, the Alpha-Max system is also advertised with spyware injection integration. The brochure describes how EPSILON, a “man-on-the-side” (MOTS) system can be used to manipulate target IP packets, perform a network injection into the targets traffic, and ultimately “place malware on the target’s phone”.

Mass surveillance: wiretapping to encrypted metadata analysis

While encryption of networked communications has become ubiquitous in many regions over the last decade, before that, large portions of Internet traffic was transmitted unencrypted and without protection. Until 2010 major email providers like Gmail and Yahoo did not employ any in-transit encryption at all for user content and served their websites over plain HTTP. In this environment, passive bulk interception technologies where highly effective, and for years were a cornerstone of the early digital surveillance industry's product offering.

Numerous surveillance companies built and sold mass telephone and internet systems which were deployed to intercept traffic on a whole-country level. These allowed governmental operators to select and monitor at will telephone communications, web traffic, email or messaging alike.



...	Type	From	To	Details	# Attach.	...	S...	IP:	Creation Date
●	MAIL - YAHO...	traceaudio1@yahoo....	traceaudio2@yahoo.com	subject: [This is a test mail with 2 AFs]	2			192.168.10.193 → 66.1...	2010-01-14 5:24...
●	MAIL - YAHO...	traceaudio1@yahoo....	traceaudio2@yahoo.com	subject: [multiple saves multiple afs]	1			192.168.10.193 → 216....	2010-01-14 5:24...
●	MAIL - YAHO...	traceaudio1@yahoo....	traceaudio2@yahoo.com	subject: [multiple saves multiple afs]	2			192.168.10.193 → 216....	2010-01-14 5:24...
●	MAIL - YAHO...	traceaudio1@yahoo....	traceaudio2@yahoo.com	subject: [multiple saves multiple afs]	3			192.168.10.193 → 216....	2010-01-14 5:24...
●	MAIL - YAHO...	traceaudio1@yahoo....	traceaudio2@yahoo.com	subject: [multiple saves multiple afs]	3			192.168.10.193 → 216....	2010-01-14 5:24...
·	MAIL - IMAP	silvie.deschamps@l...	demo.cw@laposte.net, t...	subject: Mail avec 6 pièces jointes et 4 de...	6			192.168.9.56 → 193.25...	2010-01-14 5:24...
·	MAIL - GOO...	tracetest1@gmail.com	mama2@domain.com	subject: SSSSSSSSSSSSSSSSSSSSSS...	1			192.168.9.28 → 74.125....	2010-01-14 5:24...
●	MAIL - GOO...	mailer-daemon@goo...	tracetest1@gmail.com	subject: Delivery Status Notification (Failure)				192.168.9.28 → 74.125....	2010-01-14 5:24...
●	MAIL - IMAP	silvie.deschamps@l...	demo.cw@laposte.net	subject: test with AF	1			192.168.9.56 → 193.25...	2010-01-14 5:24...

From: silvie.deschamps@laposte.net
To: demo.cw@laposte.net, tracetest1@hotmail.com, tracetest1@gmail.com
Subject: **Mail avec 6 pièces jointes et 4 destinataires (1 BCC) ([|'\^@]é$£**
Date: 5 June 2009 15:23:33 UTC (223d1h44m5s ago)

Proto: mail Login: demo.cw IP: 192.168.9.56

EUID: 0000-6af4-4ace295a-000000000128-00

Ares_v18_152.png livemail2 onepieceàâçèéêëîïôöûüùÀÂÇÈÉÊËÎÏÔÖÙÛÜ.jpg Coucher de soleil.jpg docWord.doc wheelcontrollerfulfillment.pdf
www.20minutes.fr/ville/Lyon

```
Mail avec 6 pièces jointes
```

Figure 18: Interface of the Amesys EAGLE dee packet inspection surveillance system

The Amesys EAGLE deep-packet inspection technology was first documented in 2006 and marketing material describes its ability to parse and analyse a range of network protocols including web browsing and email traffic. The EAGLE DPI system integrated with GLINT, which was a product that Amesys describes as a "global strategic system" for collecting and analysing telephone and network traffic in bulk for entire countries. Amesys, whose products were later integrated into the Intellexa alliance, also marketed a set of portable and tactical products including SMINT. SMINT was a transportable computer which could be connected to a target IP network to monitor and collect traffic. Marketing brochures previously published by Wikileaks show that Amesys also offered the SMINT system with additional EAGLE probe modules to integrate ADSL, WiFi and satellite sensors.

Nexa Technologies was founded in 2012 and took over the surveillance business of Amesys and their existing product lines. The new business entity also renamed the core mass surveillance product EAGLE to the new CEREBRO brand. The new CEREBRO mass surveillance product was integrated with a range of sensor “probes” including the ALPHA series of over-the-air GSM interception products, GAMMA for telephone monitoring, IOTA for internet traffic collection, SIGMA for satellite interception and the OMEGA open-source intelligence system.

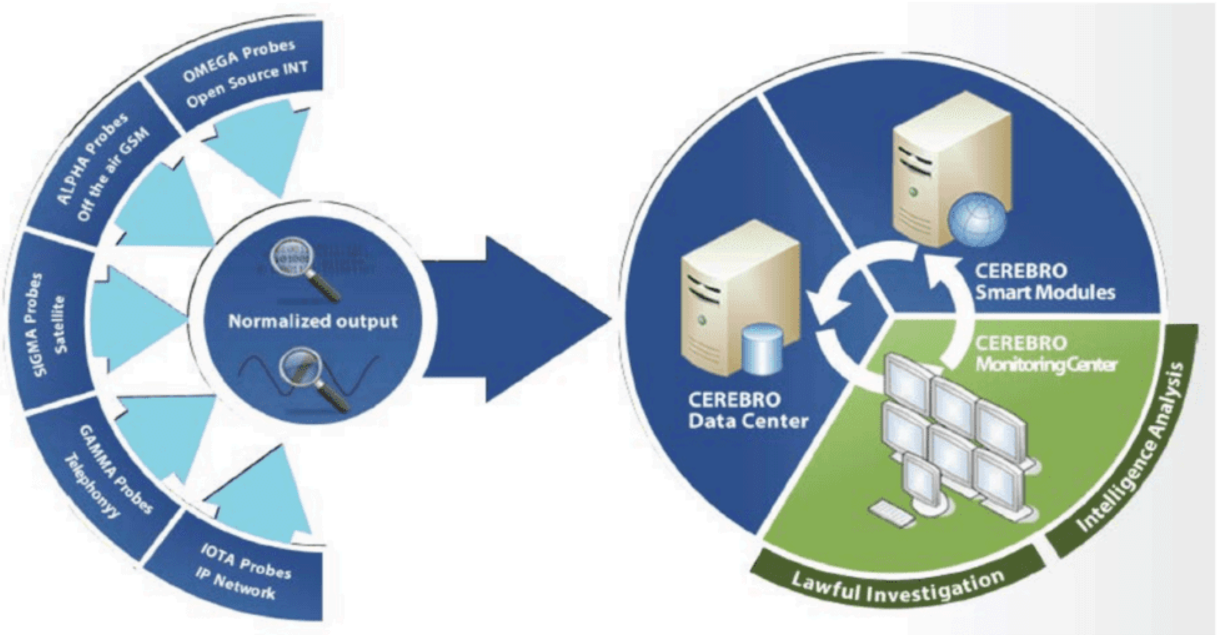


Figure 19: CEREBRO monitoring system and supported probes (published by DISCLOSE)

The golden age of internet mass surveillance technologies such as EAGLE and CEREBRO later faced critical challenges. In 2013, Edward Snowden’s groundbreaking disclosures exposed the unchecked global interception of Internet traffic by the National Security Agency of the United States and its allies. In response, technology vendors and major platforms demonstrated new commitment to rolling-out strong encryption in their products and services. Within a short number of years, the usage of HTTPS by major websites skyrocketed. Today, for example, large parts of web traffic are encrypted by default.

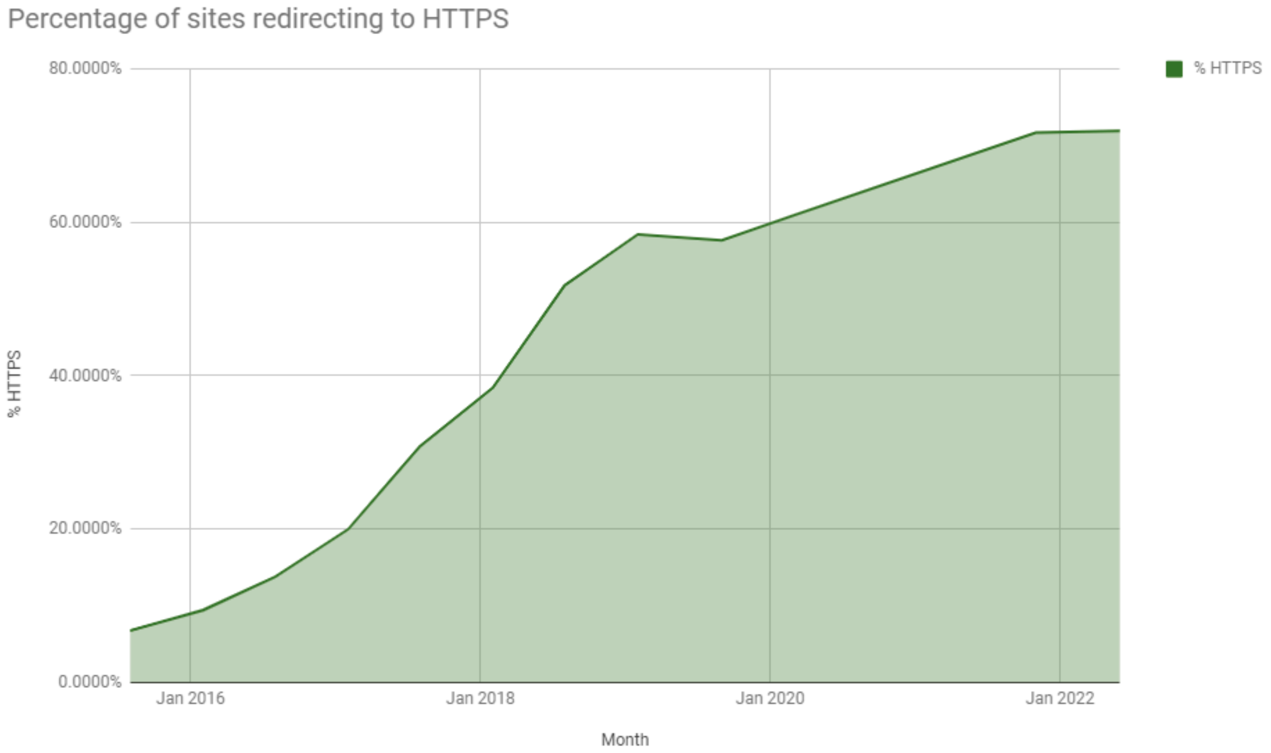


Figure 20: HTTPS usage by top 1 million websites – June 2022 (Scott Helme)

As a result, traditional bulk and mass surveillance products have become less effective as the content of communications suddenly became unavailable. The increased adoption of encryption is one likely driver for the increased demand for endpoint monitoring solutions, such as spyware. While network encryption protects from wiretapping of data in transit, attackers who can successfully compromise target device can still access content, including end-to-end encrypted communications in cleartext.

Deanonymizing WhatsApp and Signal

As internet traffic was increasingly encrypted, companies such as Nexa group started to offer new product lines such as JASMINE, which focused on analysing the metadata of encrypted traffic apps with a particular focus on messaging applications.

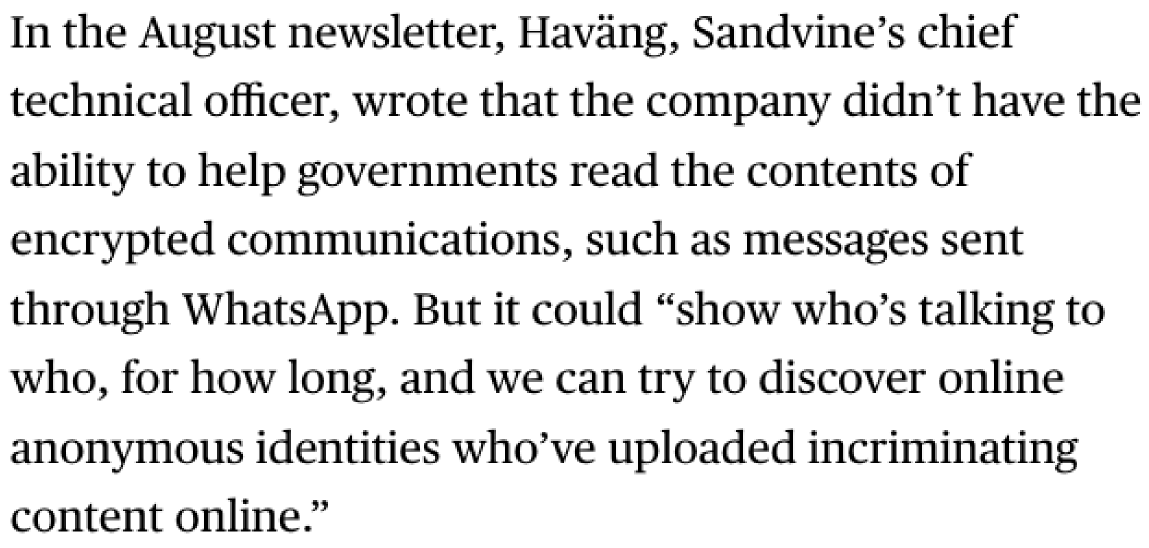
In its targeted interception mode – which starts from a single target – JASMINE has claimed it is able to identify communicating parties in encrypted but peer-to-peer applications such as Skype, which create direct network connections between participants. Additionally the JASMINE documentation explicitly claims support for identifying the IP addresses of participants in encrypted apps such as WhatsApp and Signal during voice and video calls where peer-to-peer connections are also used for calling by default.

The JASMINE documentation also explains that by analysing encrypted traffic "events" for a whole country – in mass interception mode – JASMINE has the ability to correlate and identify the participants in encrypted group chats on messaging apps, with specific support analysing WhatsApp chat conversations.

Such a metadata analysis system can record the distinctive network traffic pattern each time a phone receives a new encrypted message or notification from a chat application such as WhatsApp or Telegram. Over time, with dozens or hundreds of messages received, the correlation between these notification events for multiple individuals will get stronger.

Eventually these systems can, with a high degree of confidence, determine which phones in the country are consistently receiving a notification at the same time, therefore indicating the phones and individuals which are likely members of the same encrypted messenger chat group. Recent **reporting from the New York Times** revealed how states, for example Russia, are developing and deploying similar internet traffic analysis systems to track the users of encrypted messaging applications in the country.

This is not an abstract risk; other commercial surveillance vendors such as Sandvine have **reportedly developed and advertised** similar surveillance capabilities to government customers such as Algeria and Belarus.



In the August newsletter, Haväng, Sandvine's chief technical officer, wrote that the company didn't have the ability to help governments read the contents of encrypted communications, such as messages sent through WhatsApp. But it could "show who's talking to who, for how long, and we can try to discover online anonymous identities who've uploaded incriminating content online."

Figure 21: Sandvine offering similar encrypted traffic analysis systems (source: Bloomberg)

Figure 21: Sandvine offering similar encrypted traffic analysis systems (source: Bloomberg)

The possibility of revealing the protester who uploaded an incriminating Instagram video

Such encrypted traffic analysis systems can also be used to identify anonymous users who upload content on social media in a country. We can imagine a scenario where a protester uses Instagram to post videos of police violence or other rights violations on a pseudoanonymous Instagram channel. The upload will be encrypted with HTTPS, however, the file size of the uploaded video file and upload time is still visible to an observer recording network traffic metadata via surveillance systems deployed at their mobile operator.

The authorities could use a traffic correlation tool, similar to JASMINE, to search network logs for all mobile users who uploaded a large file to Instagram's servers shortly before the video appeared on the Instagram channel. While this search may be noisy, and provide a large pool of possible targets, each new uploaded video would provide more data points, which let the operator narrow down the list of suspects.

Unfortunately, technical attacks such as the traffic correlation approaches described here tend to become more effective as this technology develops. This is an area where advances in machine learning and AI could make such statistical correlation attacks more reliable and practical for governments to deploy indiscriminately, in order to monitor mass internet traffic and ultimately infer information about human social networks and connections at a nation-wide scale.

Recommendations

The aspiration is that the information shared in this report is actionable by civil society technologists and device vendors to make informed decisions about threat models and to prioritise possible security defences and mitigations. Unfortunately, technical fixes cannot solve this problem alone. Our private devices and digital public spaces will remain threatened until we have a global regulatory system in place with robust regulation of the cyber-surveillance industry, and which provides justice and accountability to those harmed by these products.

To Technology Vendors:

Major technology vendors and device manufacturers should urgently continue efforts to **harden** their products and services against the advanced exploits and attacks described in this report. This includes making 1-click browser attacks more difficult to develop and more brittle to maintain. It is valuable for technology vendors to continue to detect and fix such 1-click exploits being used in the wild. Remote zero-click attack surfaces, basebands, and other radio interfaces which can be exploited in close-access tactical attacks, should also be considered as an actively exploited attack surface. The following recommendations are possible mitigations:

- Provide an enhanced protection options for individuals who are at high risk from sophisticated attacks such as those described, in particular human rights defenders. While the number of people targeted from these tools may be a small percentage of the overall user pool, the harms resulting from these threats can be severe.
- To defend against network injection attacks, browser vendors should offer a HTTPS-only mode, as a user configurable option, or built in to enhanced protection mode like Apple’s Lockdown Mode. The user impact of such a feature may be higher in some regions with lower HTTPS penetration.
- Vendors should consider disabling legacy network protocols such as 2G, or providing some mechanisms to make downgrade attacks more difficult or visible.
- To defend against roaming-based attacks on 3G or 4G, vendors should consider providing a user visible prompt or approval process before the device connects to a new or previously unknown roaming network. Such a feature may be easier to deploy as an optional feature in an enhanced protection mode. It may also be possible to perform some on-device validation of the new roaming network location, notifying the user if the new moibile country code (MCC) is too geographically distant from the current network location to be implausible for a legitimate roaming handover.
- To defend against traffic correlation attacks, messaging apps and push notification services should consider traffic correlation attacks as practical real-world attacks which are deployed against their users and include this in their threat models. Some simple mitigations such as small timing delays in notifications, adding cover traffic or sending fixed size messages may help to significantly weaken the accuracy of these types of attacks. More open research is needed to analyse possible mitigations against these correlation attacks.

To At-Risk Individuals

The sophisticated spyware and digital attacks outlined in this report are used to target individuals who are of particular interest to government spyware operators because of their professional background, civil society work or information they possess. If you believe that you are at heightened risk of such attacks, there are practical steps you can take to make these kinds of advanced digital attacks more difficult:

- Always update your web browser and mobile operating system software as soon as any security updates are made available for your devices.
- Enable the enhanced security “Lockdown Mode” if you use an Apple device. This can make a successful compromise of your device significantly more challenging for an attacker.
- Using a reputable VPN provider can provide more privacy against surveillance from your ISP or government and prevent network injection attacks from those entities. A VPN will also make traffic correlation attacks – especially those targeting messaging apps – more difficult to perform and less effective.
- Features such as Signal’s optional ‘Relay Call’ mode can help hide revealing metadata, such as the IP address and location of the person you are calling from your ISP or government. In some situations, making or receiving calls from certain countries can expose the individual to heighten risks. A reputable VPN can also help mitigate these risks.
- Those with particular concerns about their devices being compromised can take actions to mitigate the extent of exposure including using “disappearing messages” where available and restarting their devices regularly which can remove non-persistent spyware infections.
- If you receive a state-sponsored attacker warning you should seek expert help to understand any ongoing risks for your accounts or devices.

If you are a human rights defender, journalist, or member of civil society and believe you have been targeted by this campaign or have received similar attack links through social media, please get in touch with the Security Lab at securitylab.amnesty.org.

Intellexa Product Glossary

This glossary is a non-exhaustive list of products and marketing names which have been used by Intellexa or Intellexa alliance entities. This has been compiled based on previously published research, as cited above, plus analysis of Intellexa alliance brochures as part of the Predator Files. We are not able to confirm if the actual performance of the products matches the descriptions in promotional materials.

Product Name	Product Type	Notes
Predator	Spyware	The Intellexa spyware agent which is installed on the infected mobile device. We use this term to describe the core mobile spyware products offered by Intellexa under and evolving set of brand names.
Helios	Spyware	Rebrand of Intellexa's Predator spyware agent.
Green Arrow	Spyware	Earlier brand name used to market the Intellexa alliance's Android spyware agent.
Red Arrow	Spyware	Earlier brand name used to market the Intellexa alliance's iOS spyware agent.
CyOP	Predator component	"Cyber Operations Platform" – Backend system to manage spyware targets and other

		components of the spyware system.
AAA	Avatar/Bot system	Automated Active Avatars (AAA) – Platform to manage ‘avatars’ aka fake social media and messenger accounts which can be used to social engineer a target into opening a 1-click link. Related to the RogueEye system originally deployed by Intellexa alliance member Senpai.
SpearHead	Tactical surveillance and infection	Wi-Fi interception system which can be used to geo-locate WiFi devices and to perform active attacks on connected devices. Appears to be originally developed by WS WiSpear. Can be installed in a vehicle, portably in a backpack or on a drone.
Alpha-Max	Tactical surveillance and infection	Cellular/4G/3G tactical interception hardware which can be used to monitor, and intercept traffic and calls connected handsets. Product originally of-

		fered by the Nexa group of companies.
Epsilon	Network injection add-on for Alpha-Max	Man-on-the-side system for injecting traffic into mobile traffic intercepted using the Alpha-Max interception systems. Can be used to inject HTTP redirects into target traffic to redirect phone to a spyware infection server.
PDS	Predator component	Predator Delivery System – Predator and the vectors and back-end use to deliver it.
Nebula	Interception analysis	Nebula is marketed as an “Insights platform” to analyse data collected and intercepted from other systems such as the Predator spyware tools and mass surveillance systems.
IS	Predator component	IS stands for “infection server”, the last server redirect stage at which a payload is being served to compromise a device.

NOVA	Spyware	A brand name for Intellexa spyware with an analysis component. It appears in a leaked 2022 commercial proposal.
Triton	Tactical infection	Tactical zero-click system using to target and infect Samsung devices. The attack uses a base-station to downgrade the device to 2G before infecting the device with spyware.
Mars	Strategic infection	Strategic infection vector using network injection system deployed at ISPs in a country.
Jupiter	Strategic infection	Jupiter is an extension for the Mars network injection system to enable interception of domestic HTTPS website.
Orion	Cyber-defence system	Cyber defensive system marketed by Intellexa for protection against cyber-attacks. The exact functionality is unclear.

Cerebro	Mass IP/internet traffic monitoring	Mass surveillance product developed by Nexa group which can ingest data from various probes, including telephony data, internet, GSM and satellite data. It replaced the earlier Eagle product.
Jasmine	Mass IP/internet traffic monitoring	Jasmine is a Nexa group product designed to analyse encrypted traffic and protocols. The product can be used to perform traffic correlation attacks and deanonymisation of users of social media platforms and messaging apps.
IOTA	Mass IP/internet traffic monitoring	Internet and network metadata analysis system which is integrated with Cerebro.
Eagle	Mass IP/internet traffic monitoring	Eagle was a deep packet inspection system developed by Amesys.
GLINT	Mass IP/internet traffic monitoring	GLINT was a strategic nationwide interception system developed by Amesys. Advertised

		capabilities include scalability to analyse multiple 10 gigabit/s full duplex links and to aggregate interception data IP networks, microwave links, GSM networks and satellite networks. GLINT was integrated with the Eagle analysis system.
SMINT	Internet traffic monitoring	SMINT was an older tactical system used for collecting network and GSM traffic from targeted networks. It also integrated the Eagle analysis system.

The Intellexa alliance

The Intellexa alliance, its subsidiaries and partnerships have evolved over time since its inception into a complex worldwide company structure. For readability purposes, both EIC and Amnesty International use the following breakdown:

Nexa group – **Nexa Technologies (France)**, Nexa Technologies CZ s.r.o (Czech Republic), Advanced Middle East Systems (United Arab Emirates), **Trovicor fz (United Arab Emirates)**.

Intellexa group – **Wispear/Passitora (Cyprus)**, **Cytrox (North Macedonia)**, Cytrox Holdings Zrt (Hungary), **Intellexa S.A (Greece)**, **Intellexa Ltd (Ireland)**, **Thalestris Ltd (Ireland)**.

Intellexa alliance – is a technological and commercial alliance concluded in 2019 between the Intellexa group and the Nexa group. The two groups of companies maintained a separate shareholding. In the **press release announcing**

the birth of the alliance, the member companies were Nexa Technologies, Advanced Middle East Systems, Cytrox, WiSpear and Senpai Technologies.9 It is unclear whether the alliance between the Nexa group and the Intellexa group is still active today.

The Intellexa group of companies was founded in 2018 by the former Israeli army officer Tal Dilian and several of his associates, which sells the Predator spyware. Since 2020, it has been controlled by the holding company Thalestris, which is based in Ireland. The Intellexa group's main companies are Cytrox (North Macedonia), which develops the Predator spyware system, WiSpear (Cyprus), specialist in Wi-Fi interception, and Senpai Technologies (Israel), a specialist in open-source intelligence and the creation of virtual avatars.

The Nexa group of companies, which mainly operated from France, specialized in traffic interception and mass surveillance systems (IP, voice, satellite, IMSI catchers, big data analysis). The group was created in 2012 to take over the surveillance business of the French company Amesys. It included from the start, Nexa Technologies (France) and Advanced Middle East Systems (Dubai), a sister company used by Nexa as a sales office. Between 2019 and 2022, the companies of the Nexa group were **controlled by the holding company Boss Industries (France)**. In 2019, Boss Industries purchased the company Trovicor (Dubai), which specializes in "lawful interception" (telephone monitoring systems). In 2020, the **Nexa group decided to abandon Nexa Technologies** as a brand and began to operate under the commercial name Trovicor Intelligence. In 2022 Nexa Technologies **sold its assets to the French company ChapsVision**, and in 2023 changed its name to RB 42 and announced that it had **ceased its activities in the surveillance business**. Boss Industries is still the owner of Trovicor, according to public documents.

Cytrox, is a North Macedonian company **established in 2017** which was the original creator of the Predator spyware and was **acquired by WiSpear** in 2018.

Amesys, based in France, was a telecom and defence company, which created a mass-monitoring system called Eagle, capable of performing mass surveillance of internet (IP) traffic at the scale of a whole country. Amesys ceased its activities in the cybersurveillance business in 2012, after the transfer of its assets to Nexa Technologies, which renamed Eagle as Cerebro.

RESEARCH

PREDATOR SPYWARE