STRATEGIC INTELLIGENCE DOSSIER

INTELLEXA
CYTROX
PREDATOR

A public-source technical and corporate history of the mercenary spyware consortium, 2017–2026

Classification: UNCLASSIFIED // PUBLIC OSINT SYNTHESIS
Cut-off date: 6 October 2026
Prepared for: Crygma / Encrygma research file
Scope: company structure, product architecture as published, customer attribution, sanctions, litigation, and defensive implications
Excluded: exploit reproduction, payloads, deployment procedures

Primary anchors: U.S. Treasury OFAC, Google GTIG, Amnesty Security Lab, Citizen Lab, Cisco Talos, Recorded Future Insikt, ICIJ, Reuters, OCCRP

0. Control note, methodology, and limits

This dossier is a synthesis of public primary sources on the Intellexa consortium, the Cytrox developer entities, and the Predator mercenary spyware product line, current to 6 October 2026. It is written as an intelligence and defensive-security reference, not as a product manual. It does not contain exploit code, gadget sequences, payload structure sufficient for reconstruction, configuration recipes, or deployment procedure.

Source hierarchy used throughout: (1) official government instruments — U.S. Department of the Treasury OFAC press releases of 5 March 2024 and 16 September 2024, Commerce Entity List actions of 18 July 2023, and the 30 December 2025 delisting notice as reported by CyberScoop citing a U.S. official; (2) peer technical publications — Google Threat Intelligence Group (3 December 2025), Amnesty International Security Lab (Predator Files, 6 October 2023; Intellexa Leaks, 4 December 2025), Citizen Lab (16 December 2021 and later), Cisco Talos (25 May 2023 and 21 December 2023), Jamf Threat Labs (February and April 2026); (3) investigative journalism with document access — European Investigative Collaborations Predator Files (October 2023), ICIJ Cyprus Confidential, Haaretz, Inside Story, Recorded Future Insikt Group (December 2025, updated 20 February 2026); (4) court reporting — Athens Misdemeanour Court, 26 February 2026, as reported by Reuters, OCCRP, ICIJ, and TechCrunch.

Attribution of a customer country is graded. **Confirmed** means a forensic infection tied to a named victim plus infrastructure, a court finding, or an official government statement. **Assessed** means scanning, shipment records, or infrastructure clustering by a named research group, typically at medium confidence. **Claimed in sales material or leaks** means a vendor document or investigative reconstruction not independently forensically confirmed in this dossier. Customer lists from different projects do not fully overlap; absence from a later scan does not prove a contract ended.

No single document can be the entire source of information in existence. Corporate registries, sealed Greek investigative files, Israeli export-control files, and unpublished victim forensics remain outside the public record. What follows is the fullest open-source reconstruction available on the cut-off date.

1. Executive assessment

Predator is a full-device mercenary implant for iOS and Android, originally built by Cytrox (North Macedonia / Hungary, founded 2017) and commercialized from 2019 through the Intellexa alliance assembled by Tal Jonathan Dilian, a former commander in Israeli military intelligence. The product is not a single binary. Public analyses describe a delivery studio, a licensing and anonymization back end, a loader (publicly analyzed on Android as ALIEN), and a surveillance implant (PREDATOR / Helios) with modular collection against messaging, microphone, camera, location, and files.

Delivery, as documented, is predominantly one-click: a social-engineered link, opened in Safari or Chrome, loads a browser exploit and then the implant. Strategic vectors documented in internal material and later confirmed in the wild include network injection (Mars, Jupiter; observed with a Sandvine PacketLogic device in the 2023 Egypt case against politician Ahmed Eltantawy) and an advertising-ecosystem vector branded Aladdin, designed to force a malicious advertisement onto a device identified by public IP or advertising identifier. Tactical vectors in sales material include a Samsung Exynos baseband path branded Triton. Google's Threat Intelligence Group assessed in December 2025 that Intellexa accounted for 15 of roughly 70 mobile-browser zero-days it had documented since 2021, and that the vendor both develops and buys exploit-chain stages.

The political and legal position of the consortium changed sharply between 2023 and 2026, without a clean operational shutdown. The U.S. Commerce Department listed Intellexa S.A., Intellexa Limited, Cytrox AD, and Cytrox Holdings ZRT on 18 July 2023. Treasury designated Dilian, Sara Aleksandra Fayssal Hamou, and five entities on 5 March 2024, then five further individuals and Aliada Group Inc. on 16 September 2024, citing use against U.S. officials, journalists, and policy experts. On 30 December 2025 Treasury removed Hamou, Merom Harpaz, and Andrea Nicola Constantino Hermes Gambazzi, an official telling CyberScoop each had separated from the consortium. On 26 February 2026 an Athens misdemeanour court convicted Dilian, Hamou, Felix Bitzios, and Greek supplier Yiannis Lavranos of breaching communications confidentiality and illegal system access in the Predatorgate affair, imposing cumulative sentences of 126 years and eight months, capped at eight years, suspended pending appeal. The court referred the matter back for investigation of possible espionage and state-secret offences. In July 2026 eight named victims sued Intellexa S.A. and 13 individuals for one million euros each.

Operationally, Recorded Future Insikt and Amnesty assessed in December 2025 that Predator customer infrastructure remained active in Saudi Arabia, Kazakhstan, Angola, and Mongolia, with a Mozambique-linked cluster through at least late June 2025, suspected Iraq activity, and a summer 2025 one-click attempt against a human-rights lawyer in Pakistan's Balochistan. The December 2025 leak is the most important structural finding since the sanctions: Intellexa support staff retained TeamViewer reach into on-premises customer environments and, in training material, into the Predator Delivery Studio, including logs and

surveillance data. That finding undercuts the vendor's recurring claim that it only sells a tool and never sees operations.

2. Subject identification

2.1 What the names actually denote

Cytrox is the developer lineage. Public corporate records and Treasury's March 2024 designation describe Cytrox Holdings ZRT (Hungary) as the earlier developer of Predator, with production later at Cytrox AD in North Macedonia. Wikipedia's corporate summary, consistent with Citizen Lab 2021, lists a 2017 founding and names Ivo Malinkovski as CEO of the North Macedonian entity. Israeli-registered vehicles historically associated with the Cytrox name include Balinese Ltd (formerly Cytrox AD Software Ltd) and Peterbald Ltd (formerly Cytrox AD EMEA Ltd). Those Israeli vehicles were not in the March 2024 OFAC set.

Intellexa is not one company. Treasury's own language, which should be preferred over marketing copy, calls it "a complex international web of decentralized companies" and, separately, "a marketing label for a variety of offensive cyber companies." Dilian began organizing the group in 2018. The 2019 alliance layer, as described by Citizen Lab and Cisco Talos, brought together WiSpear (later Passitora Ltd; Wi-Fi interception), Cytrox, Senpai Technologies (OSINT and persona tooling), and the Nexa Technologies family (France; formerly Amesys, later reported as RB 42). Intellexa S.A. in Greece is the entity Treasury described in 2024 as a principal sales channel. Thalestris Limited (Ireland) holds distribution rights and has functioned as a holding and payments vehicle. Intellexa Limited (Ireland, and a separate British Virgin Islands vehicle of the same style has been reported) resells and holds assets.

Predator is the flagship implant brand. Internal and marketing synonyms documented by Amnesty include Helios, Nova, Green Arrow (Android agent), and Red Arrow (iOS agent). The operator console has been marketed as the Cyber Operations Platform (CyOP) and appears in leak material as the Predator Delivery Studio (PDS) or Helios Delivery Studio (HDS). Related alliance products that are not the implant itself include WiSpear Wi-Fi interception, Senpai persona tooling, and network-injection appliances marketed as Mars and Jupiter.

2.2 Tal Jonathan Dilian

Dilian is a former commander of an elite Israeli intelligence unit, publicly described across ICIJ, Haaretz, and Treasury material as the founder and architect of the consortium. He has resided between Cyprus and Switzerland. In 2019 Cypriot authorities investigated a surveillance van linked to his WiSpear operation; that inquiry was later closed, and in September 2026 Dilian publicly treated a fresh decision by Cyprus's Independent Authority Against Corruption not to reopen it as vindication. He was designated by OFAC on 5 March 2024. He did not enter a formal plea in Athens; he was convicted on 26 February 2026 and has said he will appeal. Through counsel in December 2025 he denied committing any crime or operating any cyber system in Greece or elsewhere. In March and June 2026 statements, and in a July 2026 Israeli libel filing reported by Greek outlets, he said the company sells only to authorized governments and that Greece was a customer — a formulation that, if accurate, places the Greek state inside the procurement chain the Athens government has denied.

3. Chronology, 2017–2026

Date	Event	Confidence
2017	Cytrox founded in North Macedonia; early Android implant work. Ivo Malinkovski later identified as CEO.	Public corporate / research
2018	WiSpear acquires Cytrox. Dilian organizes what becomes Intellexa Group.	Citizen Lab; Atlantic Council reconstruction
2019	Alliance layer: WiSpear, Cytrox, Senpai, Nexa. Predator activity assessed from at least this year.	Talos; Recorded Future
2019	Cyprus "spy van" investigation involving Dilian / WiSpear. Later closed.	Contemporary reporting; 2026 Cyprus closure
2020	Internal OPSEC document for the implant (filenames, encrypted store, guard module). Athens office space associated with Hamou.	Amnesty leak; Treasury
2020–21	Greek targeting window later charged. Journalist Thanasis Koukakis infected.	Athens court; forensic reporting
Jun 2021	Ayman Nour's iPhone concurrently infected with Predator and NSO Pegasus. One-click WhatsApp links; iOS 14.6.	Citizen Lab, high confidence
Dec 2021	Citizen Lab publishes Pegasus vs Predator. Scanning suggests customers in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, Serbia.	Citizen Lab

Date	Event	Confidence
2021	Google TAG reports a five-bug Android chain used to deliver ALIEN/PREDATOR (four Chrome, one Linux/Android).	Google TAG
2022	Predatorgate becomes public in Greece. EYP chief and the prime minister's general secretary resign. Documento publishes a target list.	Greek press; PEGA
28 Jul 2022	Invoice line "Payment for project POC, Aladin" tied by later reporting to the ad-vector proof of concept.	VSquare / Haaretz
18 Jul 2023	Commerce Entity List: Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings ZRT.	U.S. Commerce
Sep 2023	Egypt: Ahmed Eltantawy targeted by network injection (Sandvine PacketLogic) plus an iOS chain Apple patched as CVE-2023-41993/41992/41991. Android chain used CVE-2023-4762.	Citizen Lab; Google TAG
Oct 2023	Predator Files (EIC / Amnesty). Sales reconstructed to at least 25 countries. Vietnamese targeting of U.S. lawmakers reported.	EIC; Amnesty; congressional reporting
5 Mar 2024	OFAC designates Dilian, Hamou, Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings ZRT, Thalestris Limited.	Treasury
May 2024	Angolan journalist Teixeira Cândido's phone compromised after the March sanctions.	ICIJ
16 Sep 2024	OFAC designates Bitzios, Gambazzi, Harpaz, Karaoli, Artemiou, and Aliada Group Inc. (BVI).	Treasury
2024–25	Infrastructure increasingly behind Cloudflare; domain-naming changes reduce scanner visibility.	Insikt
Jun 2025	CVE-2025-6554 (Chrome V8 type confusion) observed in a Saudi-linked context; fixed in Chrome 138.	Google GTIG
Summer 2025	Balochistan human-rights lawyer receives a malicious WhatsApp link consistent with Predator one-click.	Amnesty
30 Dec 2025	OFAC removes Hamou, Harpaz, and Gambazzi. Official: separation from the consortium.	CyberScoop
3–4 Dec 2025	Google GTIG zero-day monograph and Amnesty Intellexa Leaks publish together.	Google; Amnesty
26 Feb 2026	Athens court convicts Dilian, Hamou, Bitzios, Lavranos. Sentences capped at eight years, pending appeal. Referral for possible espionage.	Reuters; OCCRP; ICIJ
Jul 2026	Eight victims sue for €1 million each. Dilian filing in Israel reported to admit a sale to Greek authorities.	Reuters; Greek press
Sep 2026	Cyprus anti-corruption body closes the van inquiry. Dilian claims vindication.	tovima / Alpha Cyprus

Table 1. Consolidated chronology. Customer attributions in later sections are graded separately.

4. Corporate architecture

4.1 The designated core

Treasury's March 2024 action is the cleanest official map of the core. Dilian is described as founder and architect, with control exercised directly and through Hamou. Hamou is described as a corporate offshoring specialist who rented Greek office space for Intellexa S.A. and held leadership roles at Intellexa S.A., Intellexa Limited, and Thalestris Limited. Intellexa S.A. (Greece) develops and exports. Intellexa Limited (Ireland) resells and holds assets. Cytrox AD (North Macedonia) develops Predator. Cytrox Holdings ZRT (Hungary) previously developed it. Thalestris Limited (Ireland) holds distribution rights and acts as a financial holding company.

The September 2024 action maps the enabling layer. Felix Bitzios, a Greek national, is described as beneficial owner of a consortium company used to supply Predator to a foreign-government client and as manager of Intellexa S.A. Andrea Gambazzi is described as beneficial owner of Thalestris and Intellexa Limited. Merom Harpaz is described as a top executive and manager of Intellexa S.A. Panagiota Karaoli directs multiple Thalestris-controlled entities. Artemis Artemiou is general manager and board member of Cytrox Holdings and an employee of Intellexa S.A. Aliada Group Inc., British Virgin Islands, directed by Dilian, "enabled tens of millions of dollars of transactions" and held shares in Cytrox Holdings.

4.2 Alliance and peripheral vehicles

Outside the OFAC core, researchers have consistently named WiSpear / Passitora (Wi-Fi interception; the 2018 acquirer of Cytrox), Senpai Technologies (Israel; OSINT and synthetic personas), and Nexa Technologies / Amesys lineage (France). The Atlantic Council's 2024 market study noted that Balinese, Peterbald, Passitora, and Senpai were not in the 2024 Treasury set. Recorded Future's 2025–26 corporate-web study added a Czech-linked cluster around Dvir Horef Hazan: PULSE FZCO (UAE consultancy used in shipments), Zelus Analytics, and two advertising-sector firms, Pulse Advertise and MorningStar TEC, assessed as possibly supporting Aladdin. Greek intermediaries named in that study include IANUS Consulting, Remote Greece,

and ADDAPP Technologies, the last sharing address services with Apollo Technologies and Hermes Technologies.

A separate commercial residue surfaced in 2025 reporting by ICIJ: Medovie, a skincare brand previously linked to Hamou, resumed through a Portuguese company, MDV Skin Care, owned by Sylwia Jastrzebska, previously listed as a director of a Cytrox affiliate. That is not evidence of continued spyware activity; it is evidence that the personal and corporate network did not dissolve when the spyware entities were designated.

4.3 Why the structure is the product

The consortium form is operational, not cosmetic. It separates exploit development (Cytrox), sales (Intellexa S.A.), distribution rights (Thalestris), payments (Aliada, Thalestris), and alliance specialties (Wi-Fi, OSINT, lawful-intercept heritage) across North Macedonia, Hungary, Greece, Ireland, Israel, Cyprus, France, and the British Virgin Islands. Export-control and sanctions screening then has to hit every node. The December 2025 delisting of three individuals, on a representation that they had separated, shows the inverse: personal designations can be walked back without the product disappearing. Greece functioned as a sales, training, and — in the Krikel relationship — a domestic procurement hub, which is why the Athens case is the first criminal conviction of mercenary-spyware executives.

5. Product architecture, as published

The following is a functional description assembled from Amnesty's 2023 Predator Files technical annex, Amnesty's December 2025 leak analysis, Citizen Lab 2021, Cisco Talos 2023, and Google GTIG 2025. It is intentionally non-reconstructive.

5.1 Operator stack

The operator-facing system is the Cyber Operations Platform, also appearing as Predator Delivery Studio / Helios Delivery Studio. Leak imagery shows a web console on an internal host (the training video used a PDS login at an internal admin port, username "cyop"). From published brochures and the leak, the console manages targets, infection links, and collected data. A storage design described in the July 2020 OPSEC note encrypts an AES content key to a per-customer RSA public key, and keeps a SQLite store (fs.db) encrypted with SQLCipher under a per-customer passphrase (FS_KEY). Exfiltration is prioritized: high-priority items immediately, medium on demand, low (bulk files) subject to battery, charger, and network state, with storage caps so the implant does not exhaust the device. A guard module is described as self-destructing on detection attempts and reporting a reason code.

Backend roles named in the training material include infection servers, command-and-control servers, a URL shortener, a file server, an API server, and a config server. C2 is fronted by a multi-hop anonymization chain. TeamViewer, with licenses purchased from at least June 2021, was the remote-support path into customer environments. That choice is forensically useful: it is a commodity remote-desktop tool, and its use into on-premises government deployments is itself an accountability fact.

5.2 Implant components

On Android, Talos analyzed two components obtained via Citizen Lab from the 2021 Egypt activity. ALIEN is not a dumb loader. It establishes the low-level foothold, including SELinux manipulation in the sample set, and then loads PREDATOR. PREDATOR's main logic was assessed to sit in a component Talos called tcore, with a privilege mechanic called kmem; Talos did not obtain those modules. Published capability from tcore's described surface includes audio recording, collection from Signal, WhatsApp, and Telegram, hiding applications, and blocking execution of selected applications across reboot. The Android payload has been described as a shared object named pred.so under a local temporary path.

On iOS, Citizen Lab obtained a 64-bit Mach-O loader that expects a kernel task port and a pid, initializes through a routine named kmem_init, and loads a Python 2.7 runtime. Persistence observed in 2021 used the Shortcuts automation feature: a downloaded automation fired on launch of apps such as Safari or WhatsApp, checked battery level, pulled further JavaScript, and suppressed automation notifications with a configuration profile. Crash logs were wiped. Additional downloaded binaries included a photo module and a hooker. Amnesty later matched the 2020 OPSEC filename and configuration strings to these in-the-wild samples, which is the strongest public link between the internal document set and the implant Citizen Lab and Talos analyzed.

Jamf Threat Labs, publishing in February and April 2026 on samples targeting pre-iOS 17 and devices through the A16 generation, described a post-exploitation engine that forges pointer-authentication codes by searching Apple's own JavaScriptCore for a signing gadget, caches signed pointers, moves kernel read/write between processes, and suppresses the camera and microphone recording indicators with a single hook on a SpringBoard sensor-activity provider by abusing Objective-C's tolerance of a nil receiver. Jamf noted that the VoIP recording module did not itself suppress indicators and

depended on a separate stealth module being enabled. Apple's Secure Page Table Monitor, which moves page-table management to a higher exception level on later devices, is assessed by Jamf as a structural mitigation against the kernel-patching approach in those samples. Those papers are the right place for defenders who need indicator logic; this dossier does not reproduce the instruction sequences.

5.3 Collection, as claimed and as observed

Treasury's public description, which matches vendor brochures analyzed by Amnesty, lists extraction of contacts, call logs, and messages; microphone recording; media; geolocation; and access to applications and personal information. Amnesty's brochure analysis adds the marketing claim of total access to data stored on or transmitted from the device, and design intent to leave no audit trail. Wikipedia's summary of the technical reporting includes interception and falsification of messages; falsification should be treated as a reported capability, not as a capability demonstrated in every forensic case. Google's description of the PREYHUNTER helper stage — the last stage of the 2023 iOS chain, distinct from the full implant — includes VoIP recording to a predictable path under /private/var/tmp, a keylogger, camera capture, and SpringBoard hooks to hide notifications. That is post-exploitation scaffolding, not the whole product.

6. Infection vectors

Predator's public record is mostly one-click, unlike NSO's best-known zero-click messaging exploits. Amnesty's December 2025 assessment said the implant "relies, almost exclusively, on so-called 1-click attacks." The strategic and tactical vectors below are how the vendor tried to make that one click unnecessary, or to deliver the link without a message the target could screenshot.

6.1 One-click links

The baseline: a message in WhatsApp, SMS, or a similar channel contains a link. Opening it in Safari (iOS) or Chrome (Android) runs a browser exploit and downloads the implant. Citizen Lab's 2021 Egyptian cases were single-click WhatsApp links against iOS 14.6. The summer 2025 Pakistan case described by Amnesty was a WhatsApp link to a Balochistan lawyer. Links have used lookalike news domains (Egyptian and Kazakh themes appear in the public set). The operational weakness is social: the link can be forwarded to a researcher. That is exactly how several public cases began.

6.2 Network injection — Mars and Jupiter

Sales material analyzed by Amnesty describes Mars and Jupiter as systems that inject a response when the target's traffic passes a cooperating network point, so that a browser fetch receives exploit content without a clicked link. The 2023 Eltantawy case is the public proof. When the target used Vodafone Egypt mobile data, visits to ordinary sites were redirected to a Predator delivery site. Citizen Lab attributed the injection device, with high confidence, to a Sandvine PacketLogic deployment. This requires access to a telecom or ISP path. It degrades as traffic moves to TLS, unless the operator also has a decryption position. Google noted an Android chain in the same Egyptian activity delivered both by injection and by SMS/WhatsApp links, using at least CVE-2023-4762 for renderer code execution.

6.3 Aladdin — advertising-ecosystem delivery

Aladdin is the vector that most changes the threat model. Internal material promoted it as a remote zero-click: a malicious advertisement forced onto a device identified by public IP, advertising ID, email, or location, rendered inside an ordinary site or app. The leaked design used the target's public IP as the selector, with the assumption that a domestic customer could obtain that IP from a mobile operator. Amnesty assessed that Aladdin was supported in active deployments in 2024 alongside Mars and Jupiter, and that development continued into 2025 through advertising-sector companies. Google GTIG independently reported that from early 2025 Intellexa used malicious ads to fingerprint and redirect, and that partners had shut related ad accounts. A July 2022 invoice line for an "Aladin" proof of concept, reported by VSquare and Haaretz, places the concept two years before the sanctions. Recorded Future's Czech-cluster advertising firms are the current public lead on the corporate side of this vector. No public forensic case has yet shown a fully confirmed Aladdin infection of a named victim end to end; the evidence is internal documentation plus infrastructure and ad-ecosystem reporting.

6.4 Tactical radio vectors

Leak material describes proximity vectors branded Triton, Thor, and Oberon. Triton is identified as a Samsung Exynos baseband exploit reached by downgrading the target to 2G. Thor and Oberon are described only as similar radio or physical-access paths. These require proximity or a radio position. They matter for close-access operations and for travel corridors; they are not the mass remote case.

6.5 Exploit supply

GTIG's December 2025 paper is the authority on the zero-day side. Intellexa is assessed as both a developer and a buyer. The 2023 iOS chain captured against Egyptian targets was internally named "smack." Stage one was a Safari remote-code-execution zero-day, CVE-2023-41993, built on a framework called JSKit that Google assesses was acquired from an outside party and has been seen with other surveillance vendors and, in a different bug, in a Russian campaign. Stage two used CVE-2023-41991 and CVE-2023-41992 to leave the Safari sandbox and gain kernel read/write. Stage three, PREYHUNTER, is a helper/watcher pair: the watcher aborts on developer mode, a console, U.S. or Israeli locale, Cydia, Frida, tcpdump, sshd, common security products, a custom proxy, or a custom root CA. That watcher is a fingerprint of the vendor's operational caution, and a detection opportunity if the abort itself leaves a trace.

7. Public vulnerability record

All vulnerabilities below were patched by the relevant vendor before or at disclosure. Listing a CVE is not an invitation to develop against it. The table is Google GTIG's December 2025 association of zero-days with Intellexa since 2021, reproduced for defensive inventory.

CVE	Role	Product	Public description
CVE-2025-48543	Sandbox escape + LPE	Android	Use-after-free in Android Runtime
CVE-2025-6554	RCE	Chrome	V8 type confusion; seen June 2025, Saudi context; fixed in 138
CVE-2023-41993	RCE	iOS WebKit	JIT remote code execution; stage one of smack
CVE-2023-41992	Sandbox + LPE	iOS	Kernel IPC use-after-free
CVE-2023-41991	LPE	iOS	Code-signing bypass
CVE-2024-4610	LPE	ARM Mali	Improper GPU memory operations
CVE-2023-4762	RCE	Chrome	V8 type confusion; Egypt Android chain
CVE-2023-3079	RCE	Chrome	V8 type confusion
CVE-2023-2136	Sandbox	Skia	Integer overflow in SKSL
CVE-2023-2033	RCE	Chrome	V8 use-after-free
CVE-2021-38003	RCE	Chrome	V8; part of the 2021 five-bug chain
CVE-2021-38000	RCE	Chrome	Intent validation flaw
CVE-2021-37976	Sandbox	Chrome	Information leak
CVE-2021-37973	Sandbox	Chrome	Use-after-free in Portals
CVE-2021-1048	Sandbox + LPE	Android	Use-after-free in ep_loop_check_proc

Table 2. Zero-days publicly associated with Intellexa by Google GTIG, December 2025. All patched.

Two implications follow. First, a defender who only tracks NSO will miss a vendor that Google ranks as the most prolific mobile-browser zero-day exploiter in its 2021–2025 set. Second, patch latency is the exposure window. The Chrome configuration mitigation that Google pushed for CVE-2025-6554 before the full fix is the model: vendor telemetry plus a forced config change closes the window faster than a version upgrade alone.

8. Customers, deployments, and named abuses

8.1 How to read the map

Three lists circulate and should not be collapsed. Citizen Lab's 2021 scan named likely customers from endpoint placement. The 2023 Predator Files reconstructed sales or pitches, a wider and softer set. Recorded Future's 2024–25 infrastructure tracking is the best public view of who was still operating after the sanctions. A country can appear in one list and not another because a contract ended, infrastructure moved behind Cloudflare, or the earlier claim was a pitch rather than a deployment.

8.2 Assessed operators

Country / actor	Basis	Grade
Egypt	2021 double infection of Ayman Nour; 2023 Eltantawy network injection; Citizen Lab customer scan.	Confirmed activity

Country / actor	Basis	Grade
Greece	Court finding of use against at least 87 people, 2020–21; Krikel procurement; Dilian's later statement that the customer was the state.	Confirmed deployment; operator identity politically contested
Saudi Arabia	2021 scan; Insikt activity into 2025; June 2025 Chrome zero-day context.	Assessed, repeated
Kazakhstan	Leak logs and lookalike domains; Insikt shipment to OOO Seven Hills, Oct 2023, activity into Aug 2025.	Assessed
Angola	Insikt; May 2024 infection of journalist Teixeira Cândido after sanctions.	Confirmed victim; operator assessed
Vietnam	Predator Files; reported 2023 attempts against U.S. members of Congress.	Reported; high policy salience
Iraq	Insikt 2025, Badini-dialect domains, medium confidence.	Assessed, medium
Pakistan	Amnesty summer 2025 WhatsApp link to a Balochistan lawyer; Insikt suspected cluster.	Confirmed attempt
Mozambique	Insikt cluster through at least late June 2025.	Assessed
Armenia, Indonesia, Madagascar, Oman, Serbia	Citizen Lab 2021 scan.	Assessed at the time
Botswana	Insikt shipment to Directorate of Intelligence and Security, Oct 2023; activity to about June 2025.	Assessed, possibly ended
Philippines	Shipment to ComWorks, Sep 2023; earlier customer reporting.	Assessed
Sudan RSF	Lighthouse Reports / Predator Files reconstruction of a sale.	Reported sale
Mongolia, DRC, Trinidad and Tobago	Insikt infrastructure. Trinidad assessed ceased mid-2025.	Assessed
UAE, Qatar, Jordan, Kenya, Singapore, Pakistan, Austria, Germany, Switzerland	Predator Files sales or pitch reconstruction, Oct 2023. Not the same as a confirmed abuse.	Claimed / reconstructed

Table 3. Customer and deployment picture, graded. Not a finding that every listed state abused the tool.

8.3 Named public victims and targets

Ayman Nour, exiled Egyptian politician, June 2021, Predator and Pegasus on the same device, different operators (Citizen Lab, high confidence). An anonymous exiled Egyptian journalist, same period. Ahmed Eltantawy, Egyptian opposition politician, 2023, network injection on Vodafone Egypt. Thanasis Koukakis, Greek financial journalist, 2020–21, forensic traces later matched by Amnesty to Predator paths under /private/var/tmp. Nikos Androulakis, then a member of the European Parliament and later PASOK leader, was a public complainant in the Greek scandal; the Athens court found use against politicians, ministers, intelligence staff, military personnel, and businesspeople, with 87 people the figure used in the February 2026 judgment. Teixeira Cândido, Angolan journalist, May 2024. A Balochistan human-rights lawyer, summer 2025. U.S. officials, journalists, and policy experts, as a class, in Treasury's designation basis; congressional reporting named an attempted Vietnamese use against Representative Michael McCaul and Senators John Hoeven, Chris Murphy, and Gary Peters in 2023. Google has sent government-backed attack warnings tied to this activity in Pakistan, Kazakhstan, Angola, Egypt, Uzbekistan, Saudi Arabia, and Tajikistan.

8.4 Vendor access to customer systems

The December 2025 Amnesty finding should be treated as a standing fact about the product's governance. A mid-2023 training video shows support staff using TeamViewer into live customer environments code-named Dragon, Eagle, Falcon, Flamingo, Fox, Glen, Lion, Loco, Phoenix, and Rhino, plus a demo master. On at least one system the instructor identified a live customer environment and opened an Elasticsearch view of infection and C2 logs, then a PDS session. Amnesty did not find evidence that each connection was approved per session. Dilian's counsel, responding on 3 December 2025, did not answer the access questions and repeated the denial of criminal conduct. For any state customer, the implication is that a foreign vendor retained a path to operational data after delivery. For any victim, it means the circle of people who could see extracted photos and messages was not limited to the customer agency.

9. Greece: Predatorgate

Greece is the canonical abuse case because it combined a European Union member-state customer, a domestic press, a parliamentary inquiry, a data-protection fine, and, in 2026, the first criminal convictions of mercenary-spyware executives.

The public scandal broke in 2022. Koukakis and Androulakis reported surveillance. Forensic work found Predator on phones that had also, in some cases, been under lawful or quasi-lawful intercept by the National Intelligence Service (EYP). The head of EYP and the prime minister's general secretary resigned. The government denied operating Predator. A 2024 Supreme Court prosecutor decision shelved the case against EYP and sent four private-sector defendants to trial on misdemeanour charges. The European Parliament's PEGA committee treated Greece as one of the principal EU spyware cases, alongside Spain, Poland, and Hungary.

On 26 February 2026 the Athens Misdemeanour Court convicted Tal Dilian, Sara Hamou, Felix Bitzios, and Yiannis Lavranos, owner of the Greek security firm Krikel that purchased the system. The offences were breach of communications confidentiality and illegal access to information systems. Each received a cumulative sentence of 126 years and eight months, calculated across victims, with time to be served capped at eight years under misdemeanour rules, suspended pending appeal. An appeal hearing was reported as set for December 2026. The court referred the file back for investigation of possible espionage, violation of state secrets, spyware trafficking, and the role of third parties including people on the EYP payroll. That referral is the legally important part: the misdemeanour conviction does not close the question of state involvement.

Dilian's post-trial statements sharpened that question. He told Greek media the company sells only to authorized governments, and Greek reporting on a July 2026 Israeli filing said he stated Predator had been sold to Greek government bodies. Opposition parties treated this as an admission that EYP, or a cut-out serving it, was the customer. The government has not accepted that account. In July 2026 eight victims, represented by Zacharias Kesses, sued Intellexa S.A. and 13 individuals for one million euros each in moral damages; more suits were flagged. Separately, reporting in 2026 described a serving intelligence officer whose own phone was infected suing Dilian and three others, framing the affair as a national-security offence.

Krikel's role deserves its own line. Recorded Future reported covert training inside Krikel's offices, consistent with the earlier Predator Files claim that Athens hosted a training centre originally planned for Skopje. Police raids on Intellexa and Krikel offices followed the scandal. Training-in-place plus a local reseller is the pattern other jurisdictions should look for: the foreign vendor rarely appears as the contracting party on the face of the file.

10. Sanctions, export controls, and litigation

10.1 United States

Three instruments, with different legal effects. The Commerce Entity List (18 July 2023) imposes a license requirement on export, re-export, and transfer of specified U.S.-origin items to the listed companies. It does not freeze assets. OFAC designation under E.O. 13694, as amended by E.O. 13757, blocks property and prohibits U.S. persons from dealing with the designee. Visa restrictions were also used against Intellexa-linked persons, as noted in later policy summaries.

March 2024 designees: Dilian; Hamou; Intellexa S.A.; Intellexa Limited; Cytrox AD; Cytrox Holdings ZRT; Thalestris Limited. September 2024 designees: Bitzios; Gambazzi; Harpaz; Karaoli; Artemiou; Aliada Group Inc. The stated basis was development, operation, and distribution of commercial spyware used to target Americans, including U.S. officials, journalists, and policy experts, and proliferation to authoritarian regimes. Treasury explicitly described zero-click infection in the March release; the forensic record is mostly one-click plus injection, so the official wording is broader than the dominant observed mode.

On 30 December 2025 OFAC removed Hamou, Harpaz, and Gambazzi. A U.S. official told CyberScoop the removals followed petitions for reconsideration, that each person had separated from the consortium, and that the circumstances of designation no longer applied. Dilian, Bitzios, the companies, Karaoli, Artemiou, and Aliada were not reported removed in that action. The delisting is lawful administrative process; it is also evidence that personal designations are reversible on a separation representation, which a future compliance team should not treat as a finding that the product line stopped.

10.2 European and multilateral

The European Parliament's PEGA committee (2022–23) documented spyware abuse in several member states and recommended an EU moratorium-style tightening; it did not produce a ban. Greece's data-protection authority fined Intellexa in 2023. The UK- and France-led Pall Mall Process, launched February 2024, is a political commitment on commercial cyber-intrusion capabilities, not a treaty with an inspection regime. None of these instruments has the blocking effect of OFAC. The February 2026 Athens judgment is, so far, the only criminal conviction of senior mercenary-spyware executives. Its practical force depends on the appeal and on whether the referred espionage investigation is actually pursued.

10.3 What sanctions did and did not do

They raised the cost of banking, cloud, exploit purchase, and travel, and they marked the consortium for every compliance programme that screens SDN and Entity List names. They did not seize the installed base. Insikt and Amnesty both assess continued customer operations through 2025. ICIJ's August 2025 look at associated persons found commercial activity resuming around figures who had been slowed, not a wind-down. A sanctions strategy against a consortium works only if it is iterated against successor vehicles, advertising front companies, and payment nodes — Aliada was designated precisely because it was such a node.

11. Comparison with peer mercenary vendors

Dimension	Predator / Intellexa	Pegasus / NSO (public contrast)
Origin	Cytrox, North Macedonia 2017; Israeli leadership via Dilian; EU vehicles.	Israeli, Unit 8200 alumni; regulated, controversially, by Israeli export control.
Dominant delivery	One-click browser chains; network injection; ad vector in development.	Best known for zero-click messaging exploits (FORCEDENTRY and successors).
Exploit posture	15 mobile-browser zero-days in GTIG's 2021–25 set; buys stages (JSKit).	Historically the reference zero-click vendor; also multi-bug chains.
Concurrent infection	Nour phone carried both, different customers, June 2021.	Same case.
Corporate form	Alliance / consortium across 6+ jurisdictions.	Group structure, but more identifiable as one vendor.
U.S. status	Entity List 2023; OFAC 2024; partial personal delisting Dec 2025.	Entity List; no equivalent early personal OFAC set.
Criminal exposure	Four executives convicted in Greece, Feb 2026, under appeal.	No equivalent executive conviction as of this cut-off.
Vendor visibility into ops	TeamViewer into on-prem customer stacks, per 2025 leak.	NSO has denied operational access; public evidence differs by case.

Table 4. Contrast with NSO is illustrative, not a ranking of capability.

Other peers relevant to a defensive programme — Candiru, QuaDream, Paragon, RCS-style vendors — share the market but not this corporate file. The practical point is overlap: a high-value target can be in two vendors' customer sets at once, as Nour was. Detection engineering that assumes a single implant family will under-call.

12. Defensive and forensic implications

This section states publicly documented indicators and posture choices. It is not a hunting playbook and it does not include signatures sufficient to build a detector from scratch; those belong in the cited papers.

12.1 Device posture

Lockdown Mode on iOS, available since iOS 16, removes or constrains several surfaces Predator has used: just-in-time compilation paths in the browser, inbound link previews, and a range of attachment types. It is the single highest-leverage control for an at-risk iPhone user and is recommended by Apple, Citizen Lab, and Amnesty for people who may be targeted. Rapid installation of iOS and Chrome updates closes the specific CVEs in Table 2. A daily reboot disrupts implants that are not persistent across boot; Predator's 2021 iOS persistence used Shortcuts automations, so a reboot alone is not a guarantee, but it removes non-persistent stages and is cheap. On Android, a current patch level plus Google Play Protect and restriction of sideloading reduce, but do not eliminate, the Chrome-chain path. HTTP-first / HTTPS upgrade in Chrome reduces the network-injection window that does not have a TLS break.

12.2 Published forensic traces

Citizen Lab and Amnesty have published iOS traces including Predator processes invoked with a domain argument, an automation referencing the delivery domain, and paths under /private/var/tmp associated with UserEventAgent and WebKit networking in the Greek case. The PREYHUNTER helper writes VoIP audio under /private/var/tmp/l/ with a characteristic filename pattern, and opens a Unix socket at /tmp/helper.sock; those are scaffolding indicators from the 2023 chain, useful if a device is imaged before cleanup. Android public indicators include pred.so and an encrypted fs.db. Domains from the early public set — distedc[.]com, gosokm[.]com, youtubesyncapi[.]com, egyqaz[.]com, and later Kazakh lookalikes kz-news[.]cc and kz-ordas[.]com — are historical. Current infrastructure, per Insikt, sits behind Cloudflare with changed naming, so domain blocklists age in months.

12.3 Enterprise and government

Mobile threat-notification programmes (Apple threat notifications, Google government-backed attack warnings) have been the discovery path for multiple Predator victims. A government that issues high-risk devices should treat a notification as an incident, not a suggestion, and should image before the user reboots where lawful. Network-injection defence is a telecom problem: anomalous redirects on mobile DNS or HTTP, and PacketLogic-class appliances on a national network, are collection opportunities for a defender with lawful access to operator logs. Advertising-vector defence is newer. Ad-blocking, private DNS, and restriction of in-app WebViews reduce Aladdin-style exposure; they do not defeat a selector that rides a first-party app the user will not give up. Travel devices, kept clean and rebooted, remain the correct control for proximity baseband vectors.

12.4 What a buyer should assume

Any agency that bought Predator should assume, on the Amnesty evidence, that the vendor could reach the console and the logs. That is a counterintelligence fact independent of whether the original procurement was lawful. Contractual “no vendor access” clauses were not, in the leaked training environment, the operational reality.

13. Assessment and open questions

Predator is a mature, modular mercenary implant with a documented record against journalists, opposition politicians, and at least one EU member-state’s own political class, and with a vendor that kept a support path into customer deployments. The consortium form delayed but did not prevent accountability: Entity List in 2023, personal sanctions in 2024, criminal convictions in 2026. It also allowed partial personal delisting in December 2025 and continued customer infrastructure through 2025. The product is not dead. The corporate brand is damaged. Those are different statements.

Open questions a follow-on collection effort should prioritize. First, the December 2026 Athens appeal and the referred espionage file: whether Greek officials are drawn in, and whether Dilian’s “sold to the government” statement is tested under oath. Second, successor vehicles after the SDN designations — advertising firms in the Czech/UAE cluster, and any rebrand of the delivery studio. Third, whether Aladdin has produced a forensically confirmed named-victim infection, as opposed to a documented capability. Fourth, the status of Dilian’s own SDN listing and of Aliada after the 2025 delistings. Fifth, whether Apple SPTM and Lockdown Mode have forced a measurable shift from iOS zero-days toward Android and ad delivery, which GTIG’s 2025 Chrome and Android CVEs suggest but do not prove.

13.1 Confidence

High confidence: Cytrox developed Predator; Intellexa commercialized it; Dilian founded the consortium; the March and September 2024 designations occurred as published; the February 2026 Athens convictions occurred as reported by Reuters, OCCRP, and ICIJ; one-click and network-injection delivery are forensically shown; Google’s CVE associations are the vendor’s own published research. Medium confidence: the 2025 customer-country infrastructure list, Iraq included. Lower confidence: the full 25-country Predator Files sales list, which mixes contracts, pitches, and infrastructure. Contested: the identity of the Greek operational customer. Dilian says a government; the government has denied operating the system; the court convicted the vendors and suppliers and sent the state question back to prosecutors.

14. Primary source list

Official

U.S. Department of the Treasury, “Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium,” 5 March 2024, home.treasury.gov press release jy2155.

U.S. Department of the Treasury, “Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium,” 16 September 2024, press release jy2581.

U.S. Department of Commerce, Entity List additions, 18 July 2023 (Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings ZRT).

CyberScoop, “Treasury removes Intellexa spyware-linked trio from sanctions list,” 2 January 2026, citing a U.S. official on the 30 December 2025 action.

Technical

Google Threat Intelligence Group, “Intellexa’s Prolific Zero-Day Exploits Continue,” 3 December 2025.

Amnesty International Security Lab, “To Catch a Predator: Leak exposes the internal operations of Intellexa’s mercenary spyware,” 4 December 2025.

Amnesty International Security Lab, “Predator Files: Technical deep-dive into Intellexa Alliance’s surveillance products,” 6 October 2023.

Citizen Lab, “Pegasus vs. Predator,” 16 December 2021, and the 2023 Eltantawy network-injection report (with Google TAG).

Cisco Talos, “Mercenary mayhem: A technical analysis of Intellexa’s PREDATOR spyware,” 25 May 2023; “Intellexa and Cytrox,” 21 December 2023.

Jamf Threat Labs, recording-indicator analysis, 4 February 2026; iOS kernel-engine analysis, 10 April 2026.

Recorded Future Insikt Group, “Intellexa’s Global Corporate Web,” December 2025, updated 20 February 2026, and prior infrastructure tracking.

Legal and investigative

Reuters, 26 February 2026 (convictions) and 7 July 2026 (civil suits). OCCRP, 26 February 2026 and 13 March 2026. ICIJ, 26 February 2026 and 12 August 2025. TechCrunch, 16 September 2024, 4 December 2025, 26 February 2026. Haaretz, December 2025. European Investigative Collaborations, Predator Files, October 2023. Atlantic Council, “Markets matter,” April 2024.

End of dossier. Cut-off 6 October 2026. Prepared as a public-source synthesis for defensive and research use. Descriptions of capabilities are drawn from published vendor documents and published security research. Nothing in this document is an instruction for acquisition, development, or use of intrusion software.