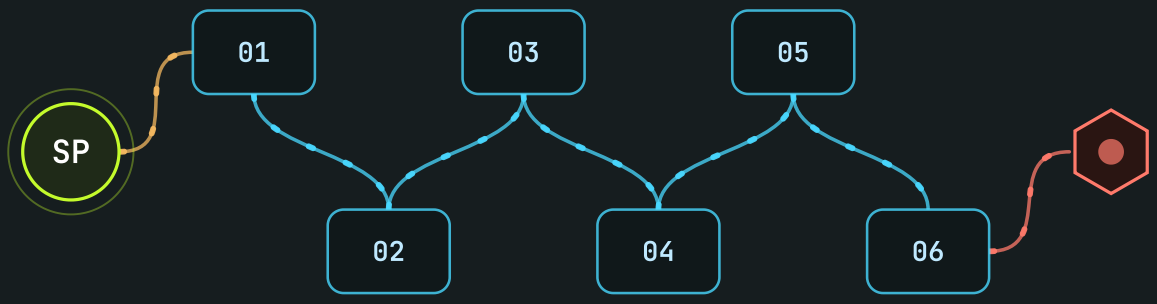


INTELLIGENCE BRIEF

Intellexa's Predator persisted under US sanctions as Greece convicted four

Google and Recorded Future found Intellexa's Predator still running in late 2025 despite US sanctions, and an Athens court convicted four people in 2026. Patch phones fast and use Lockdown Mode for high-risk staff.

EDITION
Fall/Winter 2026/2027 Edition
SP-01 · Spyware vendor

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ACTIVE

Recorded Future's December 2025 report found customers in Saudi Arabia, Kazakhstan, Angola and Mongolia still communicating with Predator infrastructure and concluded Intellexa remains active, though use appeared to slow in 2025; the latest operational evidence reviewed dates from December 2025. [33]

HEADLINE NUMBERS

15
zero-days attributed to Intellexa since 2021 [6]

4
convicted in Athens, sentences capped at 8 years, suspended pending appeal [13]

3 of 7
sanctioned individuals delisted by the Treasury on December 30, 2025 [17]

87+
victims verified by the Athens court, at least [12]

KEY FACTS

INITIAL ACCESS
One-click links over messaging apps such as WhatsApp; ISP-level network injection (Mars, Jupiter); Aladdin ad vector described in leaked documents, with in-the-wild use unconfirmed [8]

ZERO-DAYS ATTRIBUTED
15 of about 70 documented by Google's TAG since 2021, all patched [6]

US SANCTIONS
Dilian, Bitzios, Artemiou, Karaoli, five Intellexa entities and Aliada Group remain on the SDN list; Hamou, Harpaz and Gambazzi were removed December 30, 2025 [4]

PROSECUTION
Four convicted in Athens on February 26, 2026; sentences suspended pending appeal; a prosecutor asked for further investigation including possible espionage charges [13]

RECENT CONFIRMED CASE
Amnesty confirmed in February 2026 that Predator infected Angolan journalist Teixeira Cândido's iPhone on May 4, 2024 [10]

PLATFORMS
iOS and Android through mobile browser exploits; a Samsung Exynos baseband exploit (Triton) appears in leaked documents, recent use unclear [8]

02 What happened

Intellexa builds and sells the Predator spyware suite to government customers. The US Treasury sanctioned its founder Tal Dilian and core entities in 2024, the Commerce Department placed four entities on the Entity List in 2023, and leaked files published in December 2025 showed staff could reach live customer surveillance systems. After the sanctions, Google and Amnesty International still found Predator in use, and Google reported that Intellexa kept procuring or developing new zero-day exploits.

- Google's Threat Intelligence Group attributes 15 unique zero-days to Intellexa since 2021, including CVE-2025-6554 in Chrome (observed in Saudi Arabia in June 2025) and CVE-2025-48543 in the Android Runtime, and calls the vendor one of, if not the most, prolific spyware vendors exploiting zero-days against mobile browsers.
- The December 4, 2025 Intellexa Leaks (Inside Story, Haaretz and WAV Research Collective, with technical analysis by Amnesty International) include a mid-2023 training video in which an instructor connects through TeamViewer to a deployed customer system codenamed EAGLE_2, which Amnesty attributes to Kazakhstan; a control panel in the video lists at least ten potential customers.
- The same files describe Aladdin, a vector designed to infect a phone when a targeted advertisement is merely viewed, aimed by public IP address that an operator can request from a domestic mobile operator. Amnesty believes it was supported in active deployments in 2024; Recorded Future says it is not aware of any reporting that Aladdin has been used in the wild.
- On February 26, 2026 an Athens court convicted Dilian, Sara Hamou, Felix Bitzios and Yiannis Lavranos, owner of the Greek firm Krikel, of violating communications secrecy and data protection laws; each was sentenced to 126 years and eight months, which Greek law caps at eight years for misdemeanors, suspended pending appeal. The court found Predator was used to surveil at least 87 verified victims.
- On December 30, 2025 the Treasury removed Hamou, Merom Harpaz and Andrea Gambazzi from the SDN list; a US official said each had demonstrated measures to separate from the consortium, and five senators demanded a briefing by February 27, 2026.
- Amnesty International confirmed in February 2026 that Predator infected Angolan journalist Teixeira Cândido's iPhone on May 4, 2024, the first forensically confirmed Predator case targeting civil society in Angola, with possible Angola-linked infection domains first seen in March 2023.

03 How it works

01 Target selection and delivery

Operators send a one-click link over a messaging app such as WhatsApp, inject a link into unencrypted traffic with ISP cooperation (Mars) or into domestic HTTPS sites where the customer holds certificates (Jupiter), or, per leaked documents, buy a targeted advertisement keyed to the target's public IP address (Aladdin). Google saw malicious ads fingerprint users and redirect a few customers' targets to exploit servers.

02 Browser exploitation

A mobile browser zero-day chain gives remote code execution, then a sandbox escape and privilege escalation. Google's list includes V8 type confusion bugs for Chrome, a WebKit chain delivered through a framework called JSKit on iOS, and CVE-2025-48543, a use-after-free in the Android Runtime used for sandbox escape and privilege escalation.

03 Implant installation

Predator lands as a modular implant. On iOS, Jamf's February 2026 analysis shows a component that hooks SpringBoard so the camera and microphone indicators never appear once the device is fully compromised; Jamf says this is not a vulnerability disclosure.

04 Anti-analysis and kill switch

A watcher checks for developer mode, jailbreak artifacts, security tools and a US or Israeli locale. If a check fires, the implant reports an error code in the 301 to 311 range to its command server and exits, which gives the operator a diagnostic on why a deployment failed.

05 Command and control

Delivery and command infrastructure is multi-tiered. Recorded Future reported an additional tier that anonymizes customer operations after the sanctions and exposure, and in December 2025 found less infrastructure than in 2024, a push to hide infrastructure behind Cloudflare, and domain naming changes that make it harder to tie domains to customers.

06 Vendor-side visibility

Leaked training material shows Intellexa staff connecting to a customer system over TeamViewer and viewing logs of live infection attempts. Amnesty notes that mercenary spyware vendors typically say they have no access to customer systems once installed.

04 Who is at risk

Predator is sold to governments and used against the people those governments want to watch. Treasury said it was used to target Americans including US government officials, journalists and policy experts; the senators' February 13, 2026 letter says foreign actors used it to surveil officials including members of Congress, and ICIJ reports the Greek victims included government ministers, military officials, journalists and the leader of the main opposition party.

- Journalists, press freedom advocates and human rights lawyers in or connected to Predator-active countries (Amnesty cites cases in Angola, Egypt, Pakistan and Greece).
- Opposition politicians, as in the cases of Egyptian presidential hopeful Ahmed Eltantawy (Citizen Lab) and Greek opposition leader Nikos Androulakis (Amnesty).
- Executives, politicians and others in sensitive roles, whom Recorded Future says Predator's high cost points operators toward; it saw customers still active in late 2025 in Saudi Arabia, Kazakhstan, Angola and Mongolia, with new evidence for Iraq.
- Anyone on an unpatched phone: every Intellexa zero-day Google lists has a vendor patch, and the Angolan victim's iPhone was on iOS 16.2, which Amnesty calls outdated, though it says it is unclear whether that mattered.
- Organizations whose suppliers or counterparties touch the sanctioned entities, since the SDN and Entity List entries remain in force.

Sectors in scope: Journalists and press freedom organizations, Opposition politicians and parliamentarians, Human rights defenders and lawyers, Government officials, including US officials (Treasury) and members of Congress (senators' letter), Ministers, military officials and business figures (Greek victim set).

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 An Athens court convicted Tal Dilian, Sara Hamou, Felix Bitzios and Yiannis Lavranos on February 26, 2026 of breaching the confidentiality of telephone communications and illegally accessing information systems; the sentences were suspended pending appeal and a prosecutor asked for further investigation including possible espionage charges. Citizen Lab's John Scott-Railton called it the first time an executive at a mercenary spyware company had been convicted and sentenced to prison.

SOURCE 13

02 Dilian told Reuters on March 24, 2026 that he will appeal and take his case to national, regional and international institutions; the Greek government spokesman said on March 27, 2026, as reported by Dnews, that he has been convicted at first instance and is now a defendant in an appeal trial.

SOURCE 14

03 The Treasury removed Hamou, Harpaz and Gambazzi from the SDN list on December 30, 2025, 26 days after the leaks; a US official told The Record each had demonstrated measures to separate from the consortium. Senators Bennet, Warren, Shaheen, Kim and Schiff wrote on February 13, 2026 that three of the seven designated individuals were removed without the briefing committee staff requested on December 10, 2025, and asked for one by February 27, 2026. As of October 14, 2026 Dilian, Bitzios, Artemiou, Karaoli, the five consortium entities and Aliada Group remain on the SDN list, per the Consolidated Screening List.

SOURCE 17

04 Amnesty International's Security Lab forensically confirmed that Predator infected Angolan journalist Teixeira Cândido's iPhone on May 4, 2024, and determined with high confidence that the WhatsApp links he received were Predator infection attempts; its event timeline lists 11 messages with Predator links starting May 3, 2024, and it cannot conclusively identify the customer.

SOURCE 10

05 Jamf Threat Labs reverse engineered a Predator iOS sample on January 14, 2026 and documented its anti-analysis checks (developer mode, jailbreak artifacts, security tools, US or Israeli locale), an error code taxonomy (301 to 311) reported to the command server, and crash log suppression.

SOURCE 24

06 Google's March 5, 2026 zero-day review counted 90 exploited zero-days in 2025, with 15 on mobile operating systems versus 9 in 2024, and for the first time attributed more exploitation to commercial surveillance vendors than to state-sponsored espionage groups; it describes Intellexa as a prolific procurer and user of zero-days that adapted its operations.

SOURCE 7

07 Recorded Future's December 3, 2025 report found less Predator infrastructure in 2025 than in 2024, customers in Saudi Arabia, Kazakhstan, Angola and Mongolia still communicating, customers in Egypt, Trinidad and Tobago and Botswana ceasing communication between March and June 2025, and, with medium confidence, a customer in Iraq likely operational in 2025.

SOURCE 33

08 In July 2026 eight Greek victims reportedly filed a civil damages claim of about 8 million euros in Athens against Intellexa and 13 people including Dilian; Reclaim The Net, citing Heise, reports a hearing in April 2027. This rests on one advocacy outlet's secondary reporting and is unconfirmed by a court record or wire report.

SOURCE 16

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Turn on Lockdown Mode on the iPhones of executives, counsel, board members and anyone who travels to a Predator-active country.**

Citizen Lab reported that Apple's security engineering team confirmed Lockdown Mode blocks the Predator attack used against Ahmed Eltantawy in 2023, and Recorded Future also recommends it against advanced spyware.

02 **Enforce mobile OS and browser updates within days, not weeks, and block access from devices below the current release.**

Every zero-day Google attributes to Intellexa has a vendor patch, and the Angolan victim's phone was on iOS 16.2 when it was infected.

03 **Deploy ad and script blocking in managed mobile browsers and treat it as a security control.**

Leaked documents describe Aladdin infecting a phone when a targeted ad is merely viewed, Google saw malicious ads redirect Predator targets to exploit servers, and Recorded Future recommends ad blocking.

04 **Require MDM enrollment with minimum OS versions for any device that reaches corporate email or data, and deny unenrolled BYOD.**

Every Intellexa zero-day Google lists was patched and Google urges quick patching; MDM minimum versions are how an organization enforces that on devices it does not physically control.

05 **Add mobile telemetry for camera or microphone use without an on-screen indicator, unexpected memory mappings in SpringBoard or mediaserverd, and processes such as iconservicesagent running from /private/var/containers/Bundle/.**

These are behaviors Jamf documented in an analyzed Predator sample and Amnesty documented on a confirmed infection.

06 **Screen vendors, resellers and counterparties against the OFAC SDN list and the BIS Entity List, including the rebrands Helios, Nova, Green Arrow and Red Arrow.**

Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings, Thalestris and Aliada Group remain on the SDN list (the first four also on the Entity List), and Predator has been marketed under other names.

07 **Brief high-risk staff that unsolicited WhatsApp links, even from a plausible journalist or student, are hostile, and give them a reporting path.**

The Angola and Pakistan cases both involved a one-click link sent over WhatsApp, in Pakistan from an unknown number.

08 **Fold commercial spyware into the incident response plan, including forensic capture of iOS backups and Android bug reports before a reboot.**

Cândido's infection ended when his phone restarted, which is good for the victim and bad for the evidence; a Z7 24/7 SOC engagement can add mobile telemetry and a tested response path.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

DOMAIN	`exclusivo24h[.]com` [10]
BEHAVIOR	Process named iconservicesagent running from /private/var/containers/Bundle/ on iOS [10]
BEHAVIOR	Camera or microphone in use with no indicator shown; SpringBoard receives sensor notifications without updating the UI [25]

08 Sources

[1] **Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium** US Department of the Treasury · March 5, 2024. https://home.treasury.gov/news/press-releases/jy2155

[2] **Cyber-related Designations; Global Magnitsky Designations** US Treasury, Office of Foreign Assets Control · September 16, 2024. https://ofac.treasury.gov/recent-actions/20240916

[3] **Non-Proliferation and Iran-related Designations; Cyber-related and Russia-related Designations Removals** US Treasury, Office of Foreign Assets Control · December 30, 2025. https://ofac.treasury.gov/recent-actions/20251230

[4] **Consolidated Screening List (CSV download, checked for Intellexa-related entries)** US International Trade Administration · retrieved October 14, 2026. https://data.trade.gov/downloadable_consolidated_screening_list/v1/consolidated.csv

[5] **Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits** US Bureau of Industry and Security · July 18, 2023. https://www.bis.gov/press-release/commerce-adds-four-entities-entity-list-trafficking-cyber-exploits

[6] **Sanctioned but Still Spying: Intellexa's Prolific Zero-Day Exploits Continue** Google Threat Intelligence Group · December 3, 2025. https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue

[7] **Look What You Made Us Patch: 2025 Zero-Days in Review** Google Threat Intelligence Group · March 5, 2026. https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review/

[8] **To Catch a Predator: Leak exposes the internal operations of Intellexa's mercenary spyware** Amnesty International Security Lab · December 4, 2025. https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/

[9] **Global: 'Intellexa Leaks' investigation provides further evidence of spyware threats to human rights** Amnesty International · December 4, 2025. https://www.amnesty.org/en/latest/news/2025/12/intellexa-spyware/

[10] **Journalism under attack: Predator spyware in Angola** Amnesty International Security Lab · February 18, 2026. https://securitylab.amnesty.org/latest/2026/02/journalism-under-attack-predator-spyware-in-angola/

[11] **Greece: Convictions in 'Predatorgate' scandal offer rare accountability in abuse of surveillance technology** Amnesty International · February 26, 2026. https://www.amnesty.org/en/latest/news/2026/02/greece-spyware-scandal/

[12] **Greek Court Hands Down Maximum Sentences in 'Predator' Spyware Case, Orders More Prosecutions** OCCRP · February 26, 2026. https://www.occrp.org/en/news/greek-court-hands-down-maximum-sentences-in-predator-spyware-case-orders-more-prosecutions

[13] **Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal** ICIJ · February 26, 2026 (updated February 27, 2026). https://www.icij.org/news/2026/02/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/

[14] **Intellexa founder says he plans to appeal Greek court ruling over wiretapping scandal** Reuters (republished by Internazionale) · March 24, 2026. https://www.internazionale.it/ultime-notizie-reuters/2026/03/24/intellexa-founder-says-he-plans-to-appeal-greek-court-ruling-over-wiretapping-scandal

[15] **Greek government rejects Intellexa founder's claims as Predator scandal reignites** Dnews (News in English) · March 27, 2026. https://www.dnews.gr/eidhseis/news-in-english/579747/greek-government-rejects-intellexa-founder-s-claims-as-predator-scandal-reignites

[16] **Predator Spyware Victims File 8 Million Euro Damages Suit in Athens** Reclaim The Net · July 13, 2026. https://reclaimthenet.org/predator-spyware-victims-file-e8-million-damages-suit-in-athens

[17] **Letter to Secretaries Bessent and Rubio regarding commercial spyware sanctions delistings** US Senators Bennet, Warren, Shaheen, Kim and Schiff · February 13, 2026. https://www.bennet.senate.gov/wp-content/uploads/2026/02/letter_to_bessent_and_rubio_re_commercial_spyware_sanctions_delistings.pdf

[18] **Treasury removes sanctions for three executives tied to spyware maker Intellexa** The Record · December 30, 2025. https://therecord.media/treasury-sanctions-intellexa-removed

[23] **Predator Spyware Infrastructure Returns Following Exposure and Sanctions** Recorded Future Insikt Group · 2024 (report cta-2024-0905; page shows no date). https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions

[24] **Predator's kill switch: undocumented anti-analysis techniques in iOS spyware** Jamf Threat Labs · January 14, 2026. https://www.jamf.com/blog/predator-spyware-anti-analysis-techniques-ios-error-codes-detection/

[25] **How Predator spyware defeats iOS recording indicators** Jamf Threat Labs · February 19, 2026. https://www.jamf.com/blog/predator-spyware-ios-recording-indicator-bypass-analysis/

[26] **PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions** Citizen Lab · September 22, 2023. https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

[27] **Apple Warns Users in 110 Countries They May Be Targets of Mercenary Spyware** The Hacker News · August 14, 2026 (updated August 18, 2026). https://thehackernews.com/2026/08/apple-warns-users-in-110-countries-they.html

[29] **How Democratizing Threat Hunting is Changing Mobile Security** iVerify · February 19, 2025. https://iverify.com/blog/how-democratizing-threat-hunting-is-changing-mobile-security

[31] **EU Civil-Liberties Groups Demand Action on Pegasus Hit on PEGA MEP** State of Surveillance · July 7, 2026. https://stateofsurveillance.org/news/eu-amnesty-cdt-pegasus-kouloglou-pega-action-call-2026/

[32] **Bennet, Warren, Colleagues Press Treasury and State to Explain Lifting of Sanctions on Three Enablers of Commercial Spyware Used Against Americans, Journalists, and Dissidents** Office of Senator Michael Bennet · February 18, 2026. https://www.bennet.senate.gov/2026/02/18/bennet-warren-colleagues-press-treasury-and-state-to-explain-lifting-of-sanctions-on-three-enablers-of-commercial-spyware-used-against-americans-journalists-and-dissidents/

[33] **Intellexa's Global Corporate Web** Recorded Future Insikt Group · December 3, 2025 (page updated February 20, 2026). https://www.recordedfuture.com/research/intellexas-global-corporate-web

[34] **Apple sends new round of cyber threat notifications to users in 84 countries (headline paraphrased from the URL; quotes Apple's statement that the warnings went out December 2, 2025)** MacTech · December 5, 2025. https://www.mactech.com/2025/12/05/apple-sends-new-round-of-cyber-threat-notifications-to-uses-in-84-countries/amp/

[35] **Spyware company Intellexa fined 50,000 euros for holding up Greek inquiry (headline paraphrased from the URL)** The Record · January 18, 2023. https://therecord.media/spyware-company-intellexa-fined-e50000-for-holding-up-greek-inquiry/

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions™ SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

Spyware vendors lead zero-days; Aladdin unconfirmed
Continue with part 2 of 2 · z7solutions.com/z7-cyber/intellexa-part-2/

Spyware vendors outlast sanctions and verdicts
More from the edition · z7solutions.com/z7-cyber/commercial-spyware-landscape-2025/

Qilin still tops most ransomware counts
More from the edition · z7solutions.com/z7-cyber/qilin/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A CALL z7solutions.com/book/

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.