

INTELLIGENCE BRIEF

Intellexa's Aladdin Ad Vector Is Unconfirmed as Spyware Vendors Lead Zero-days

Google ties more 2025 zero-day exploitation to commercial spyware vendors than to state hackers, while Intellexa's Aladdin ad vector is documented but unconfirmed in the wild. Patch phones fast and harden browsers.

EDITION

Fall/Winter 2026/2027 Edition

SP-02 · Spyware vendor

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

Recorded Future still sees Predator customers in Saudi Arabia, Kazakhstan, Angola and Mongolia and Google counts commercial vendors ahead of state hackers in 2025 zero-day use, but no source confirms Aladdin ad delivery by name in the wild. [1]

HEADLINE NUMBERS

15 of about 70

zero-days Google's Threat Analysis Group discovered and documented since 2021 that it attributes to Intellexa [3]

90

zero-days exploited in 2025, with commercial vendors ahead of state groups for the first time [4]

27

states that have signed the Pall Mall Code of Practice, per the UK NCSC [27]

561

spyware-market entities in 46 countries, per the Atlantic Council [29]

KEY FACTS

ALADDIN DESIGN

Forces a targeted ad onto a phone, aimed by public IP address or ad identifier; Amnesty says viewing the ad is enough to infect [2]

EVIDENCE OF USE

Recorded Future knew of no in-the-wild Aladdin use on December 3, 2025; Google saw malicious ads redirect targets for a few Predator customers since early 2025 [1]

MAIN DELIVERY ROUTE

One-time links sent over encrypted messaging apps; ad-based delivery appeared with only a few customers [3]

ZERO-DAY SHARE

Google counted 90 zero-days exploited in 2025, 15 on mobile, and for the first time tied more to commercial surveillance vendors than to state espionage groups [4]

ACTIVE CUSTOMERS

Saudi Arabia, Kazakhstan, Angola and Mongolia still observed in late 2025, with new evidence for Iraq; Egypt, Trinidad and Tobago and Botswana went quiet between March and June 2025 [1]

US CONTROLS

Four Intellexa Entity List entries and ten Intellexa SDN listings (four individuals, six entities) remain; NSO Group and Candiru stay on the Entity List [14]

02 What Happened

Part 1 of this series covers Intellexa's sanctions, the Greek convictions and the December 2025 leaks. This part asks what the evidence shows about the ad-based Aladdin vector and how the wider spyware market and the policy response have moved since the original edition. The short answer is that Aladdin is well documented as a design but thinly confirmed as an attack, while the vendors' lead in zero-day use and the policy gaps are both measurable.

- Amnesty Security Lab's analysis of the leaked files describes Aladdin as forcing a malicious ad onto a target's phone on any ad-serving site, with simply viewing the ad enough to infect, aimed by public IP address and possibly with help from a domestic mobile operator; Amnesty believes it supported active deployments in 2024.
- Recorded Future, publishing the day before, says Haaretz first reported Aladdin in April 2024 from 2022 documents as a proof of concept, and that it knows of no reporting that Aladdin has been used in the wild. It also says no confirmed Predator case matches the fully remote zero-click exploits seen with Pegasus.
- Google's December 3, 2025 analysis says one-time links over encrypted messengers remain Predator's primary delivery route, but for a few customers it saw malicious ads on third-party platforms fingerprint users and redirect targets to Intellexa exploit servers, with Intellexa increasingly involved since early 2025. Google does not use the name Aladdin or name the companies whose accounts partners shut down.
- Google's March 5, 2026 review counted 90 zero-days exploited in 2025, 15 of them on mobile operating systems against 9 in 2024, and attributed more of them to commercial surveillance vendors than to state-sponsored espionage groups for the first time. It calls Intellexa a prolific procurer that adapted its operations.
- Policy moved unevenly: Treasury delisted three Intellexa enablers in December 2025 (covered in Part 1), ICE's Paragon contract was reactivated in 2025 and closed out in January, and the Pall Mall Process industry guidelines are expected in November 2026.

- The Atlantic Council's September 2025 mapping counts 561 spyware-market entities in 46 countries, 43 of them founded in 2024, with US-based investors up from 11 to 31.

03 How It Works

01 Pick the target by IP or ad ID

Leaked Aladdin documentation says the system was designed around the target's public IP address, with other selectors such as an advertising ID, and that an operator can ask a domestic mobile operator for the IP. The ad is then bought to reach that device.

02 Buy the ad through ad-tech fronts

Recorded Future found two ad-sector companies, Pulse Advertise and MorningStar TEC, hosted on one IP address and linked to the Czech cluster, that it assesses may be involved in Aladdin. Google says partners shut down accounts of companies Intellexa created but names none.

03 Fingerprint and redirect on render

Google saw malicious ads on third-party platforms used to fingerprint users and redirect targeted ones to Intellexa's exploit delivery servers. Amnesty says viewing the ad is enough to trigger the infection, while Recorded Future's account of the 2022 proof of concept has bait ads that the target interacts with.

04 Run a browser exploit chain

A browser remote code execution bug is paired with a sandbox escape and privilege escalation. Google's 2025 examples are CVE-2025-6554 in Chrome's V8 engine and CVE-2025-48543 in the Android Runtime.

05 Install an implant that hides itself

Jamf's analysis of a Predator iOS sample found a SpringBoard hook that suppresses the green camera and orange microphone indicators. Jamf says this is post-compromise behavior, not a new iOS vulnerability.

06 Hide the customer behind tiers

Recorded Future describes servers that relay through up to five tiers, a push to hide behind Cloudflare and domain names harder to tie to a region. It saw less Predator infrastructure in 2025 than in 2024.

04 Who Is at Risk

Recorded Future says Predator's costly licensing makes operators likely to reserve it for high-value targets, and that executives and other high-profile people are increasingly targeted. The Treasury said Predator was used to target Americans, including US government officials, journalists and policy experts.

- Executives, counsel and deal teams who travel to or negotiate with parties in countries where Recorded Future assesses active customers: Saudi Arabia, Kazakhstan, Angola and Mongolia, with new evidence for Iraq.
- Journalists, human rights defenders and opposition figures in confirmed-use cases such as Angola, where the victim's iPhone ran iOS 16.2, and people in or connected to Pakistan's Balochistan region.
- Anyone whose phone renders web ads, if Aladdin works as designed, because the exposed group is set by the ad path rather than by a lure; the design is documented but its use is unconfirmed.
- Organizations with telecom, hosting or technology suppliers in Predator-active countries, since Amnesty says Mars and Jupiter injection needs operator cooperation and Aladdin targeting can draw on operator-supplied IP data.
- Compliance teams that screen only for the name Predator, since Amnesty confirms the product is also marketed as Helios, Nova, Green Arrow and Red Arrow.

Sectors in scope: Journalists and press freedom organizations, Opposition politicians and parliamentarians, Human rights defenders and lawyers, Government officials, Business leaders and other high-value private-sector targets.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 Google's March 5, 2026 zero-day review attributed more 2025 exploitation to commercial surveillance vendors than to state-sponsored espionage groups for the first time, counted 90 zero-days overall and 15 on mobile operating systems, and singled out Intellexa as a prolific procurer that adapted its operations.

SOURCE 4

02 Correction: the original edition presented Aladdin as an operational zero-click vector that became operational in 2024. Amnesty believes it supported active deployments in 2024, Google saw ad-based redirection with a few customers, and Recorded Future knew of no in-the-wild Aladdin use as of December 3, 2025; the 2026 items checked (Google's March review, Amnesty's Security Lab listing) do not address Aladdin.

SOURCE 1

03 Recorded Future's report, updated February 20, 2026, ties Pulse Advertise and MorningStar TEC, both hosted on IP address 173[.]236[.]243[.]198, to the Czech cluster and says they may be connected to Aladdin. It cites a July 28, 2022 invoice for 'project POC Aladin' to a Czech-cluster company, reported by Vsquare in August 2025, and finds less Predator infrastructure in 2025 than in 2024.

SOURCE 1

04 NPR reported on May 22, 2026 that ICE reactivated its Paragon Solutions contract in August 2025 and that a procurement notice shows it closed out on January 20; DHS said ICE has no relationship with Paragon or its acquirer and would not say whether ICE keeps access through a third party. The acting ICE director's April 1, 2026 letter acknowledged approving a commercial spyware tool without naming it.

SOURCE 23

05 WhatsApp's parent announced a contempt motion against NSO Group on June 8, 2026, alleging test accounts and fresh one-click lures after the permanent injunction; NSO's appeal is pending at the Ninth Circuit. Rep. Summer Lee asked Commerce on May 7, 2026 for its records on the US purchase of NSO.

SOURCE 19

06 Paragon's CEO told WIRED in October 2026 that the company has no way to know whether customers misuse its software and has no kill switch to disable them.

SOURCE 24

07 Amnesty and civil society partners said on July 6, 2026, after Citizen Lab found Pegasus on a former member of the European Parliament who sat on its spyware committee, that nearly three years after the PEGA report the EU has not delivered a meaningful EU-wide response, and asked the Commission for a public roadmap.

SOURCE 25

08 The Pall Mall Process industry guidelines for commercial cyber intrusion capabilities are expected to be finalized in November 2026, according to a September 17, 2026 joint civil society submission, with the UK NCSC counting 27 states that have signed the Code of Practice for States.

SOURCE 28

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Enforce current iOS, Android and browser updates through MDM within days of release, and deny corporate access from devices below the current version.**

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

02 **Turn on Lockdown Mode on iPhones, and the equivalent hardened mode on Android where offered, for executives, counsel, board members and frequent travelers.**

Recorded Future lists Lockdown Mode among its mitigations against Predator.

03 **Block ads and third-party trackers in managed mobile browsers and restrict ad-tracking identifiers on corporate devices.**

Google saw malicious ads redirect targets to exploit servers and Recorded Future recommends ad blocking and limiting ad identifiers, so the ad path is a plausible infection path that link training does not cover.

04 **Add mobile telemetry for camera or microphone use without an on-screen indicator, unexpected memory mappings in SpringBoard or mediaserverd, and processes impersonating system names under /private/var/containers/Bundle/.**

These are the behaviors Jamf and Amnesty documented in Predator samples.

05 **Write a mobile compromise playbook: isolate the device, capture an iOS backup or Android bug report before any reboot, notify counsel, and treat an Apple or Google threat notification as an incident.**

The Angolan infection ended when the phone restarted, which removed most of the evidence.

06 **Extend third-party risk reviews to telecom, hosting and technology suppliers in countries where Recorded Future assesses active Predator customers, and ask about lawful-intercept and operator cooperation duties.**

Amnesty says Mars and Jupiter injection depends on operator cooperation and Aladdin targeting can use operator-supplied IP data.

07 **Screen counterparties against the SDN and Entity lists for Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings, Thalestris, Aliada Group and the names Helios, Nova, Green Arrow and Red Arrow, and track delistings as closely as designations.**

Three enablers were delisted on December 30, 2025 while the entities stayed listed, so a stale list is wrong in both directions.

08 **Put commercial spyware on the board risk register with a named owner; Z7's 24/7 SOC and Microsoft 365 posture review can supply the identity and mobile telemetry behind it.**

Google now counts commercial vendors ahead of state espionage groups in 2025 zero-day use, so the risk is no longer niche.

07 Indicators

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

DOMAIN	pulseadvertise[.]com (ad-sector company Recorded Future assesses as potentially involved in Aladdin; treat as a hunting lead, not proof) [1]
DOMAIN	morningstartec[.]com (ad-sector company Recorded Future assesses as possibly involved in Aladdin; treat as a hunting lead, not proof) [1]
IP	173[.]236[.]243[.]198 (hosted both domains above, per Recorded Future) [1]
DOMAIN	badinigroup[.]com (Recorded Future, Predator customer assessed in Iraq) [1]
DOMAIN	birura[.]com (Recorded Future, Predator customer assessed in Iraq) [1]
DOMAIN	gardalul[.]com (Recorded Future, Predator customer assessed in Iraq) [1]
DOMAIN	keep-badinigroups[.]com (Recorded Future, Predator customer assessed in Iraq) [1]
IP	5[.]253[.]43[.]92 (Recorded Future Appendix A) [1]
IP	38[.]180[.]54[.]77 (Recorded Future Appendix A) [1]
IP	45[.]86[.]231[.]8 (Recorded Future Appendix A) [1]
IP	89[.]150[.]57[.]85 (Recorded Future Appendix A) [1]
BEHAVIOR	SpringBoard receiving sensor activity notifications without updating the UI, and unexpected memory mappings in SpringBoard or mediaserverd [6]

08 Sources

[1] **Intellexa's Global Corporate Web (CTA-2025-1203)** Recorded Future Insikt Group · December 3, 2025 (updated February 20, 2026 with a minor correction). https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-1203.pdf

[2] **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/

[3] **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

[4] **2025 zero-day exploitation review (Look What You Made Us Patch)** Google Threat Intelligence Group · March 5, 2026. https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review/

[5] **State-backed attackers and commercial surveillance vendors repeatedly use the same exploits** Google Threat Analysis Group · August 2024. https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

[6] **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/

[7] **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/

[8] **Predator still active, new links identified** Recorded Future Insikt Group · 2025 (report cta-2025-0612; page shows no date). https://www.recordedfuture.com/research/predator-still-active-new-links-identified

[9] **Tracking Candiru's DevilsTongue Spyware in Multiple Countries** Recorded Future Insikt Group · 2025 (analysis cutoff June 26, 2025). https://www.recordedfuture.com/research/tracking-candirus-devilstongue-spyware

[10] **Risky Biz News: Intellexa pulls new Predator spyware infra after thorough undressing** Risky Business News · March 4, 2024. https://news.risky.biz/risky-biz-news-intellexa-pulls-new-predator-spyware-infra-after-thorough-undressing/

[11] **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

[12] **Cyber-related Designations (Intellexa enablers)** US Treasury, Office of Foreign Assets Control · September 16, 2024. https://ofac.treasury.gov/recent-actions/20240916

[13] **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

[14] **Consolidated Screening List (CSV download, checked for Intellexa, Cytrox, NSO and Candiru entries)** US International Trade Administration · retrieved October 13, 2026. https://data.trade.gov/downloadable_consolidated_screening_list/v1/consolidated.csv

[15] **US imposes visa restrictions on 13 individuals tied to commercial spyware (headline paraphrased)** The Hacker News, reporting a State Department announcement · April 23, 2024. https://thehackernews.com/2024/04/us-imposes-visa-restrictions-on-13.html

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

[17] **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

[18] **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/

[19] **WhatsApp seeks contempt action against NSO Group** MediaNama · June 9, 2026. https://www.medianama.com/2026/06/223-whatsapp-seeks-contempt-action-against-nso-group/

[20] **Rep. Summer Lee Demands Answers from Dept. of Commerce on Trump Admin Ties to Sanctioned Spyware Firm** Office of Rep. Summer Lee · May 7, 2026. https://summerlee.house.gov/newsroom/press-releases/rep-summer-lee-demands-answers-from-dept-of-commerce-on-trump-admin-ties-to-sanctioned-spyware-firm

[21] **Spyware maker NSO Group confirms acquisition by US investors** TechCrunch · October 10, 2025. https://techcrunch.com/2025/10/10/spyware-maker-nso-group-confirms-acquisition-by-us-investors/

[22] **Former Trump official named NSO Group executive chairman** The Record · November 10, 2025. https://therecord.media/former-trump-official-named-nso-group-chairman

[23] **DHS says ICE has 'no relationship' with spyware maker Paragon Solutions** NPR (via KUNC) · May 22, 2026. https://www.kunc.org/npr-news/2026-05-22/dhs-says-ice-has-no-relationship-with-spyware-maker-paragon-solutions

[24] **The Secrets of a US Spyware King** Citizen Lab, reporting WIRED · October 8, 2026. https://citizenlab.ca/the-secrets-of-a-us-spyware-king/

[25] **Joint Statement: Pegasus in the parliament, the EU must act now** Amnesty International Security Lab · July 6, 2026. https://securitylab.amnesty.org/latest/2026/07/joint-statement-pegasus-in-the-parliament-the-eu-must-act-now/

[26] **Pall Mall Process Code of Practice for States** UK Government (Foreign, Commonwealth and Development Office) · April 4, 2025 (updated October 23, 2025). https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states

[27] **What makes a responsible cyber actor: introducing the Pall Mall industry consultation on good practice** UK NCSC · December 2, 2025 (page modified June 24, 2026). https://www.ncsc.gov.uk/blog-post/what-makes-a-responsible-cyber-actor

[28] **Essential Elements for Ensuring the Industry Guidelines for Commercial Cyber Intrusion Capabilities Deliver on their Potential** Joint civil society submission hosted by Freedom House · September 17, 2026. https://freedomhouse.org/sites/default/files/2026-09/Essential_Elements_for_the_Industry_Guidelines_on_CCICs.pdf

[29] **Mythical Beasts: Diving into the depths of the global spyware market (2025 edition)** Atlantic Council · September 10, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/

[30] **LANDFALL: new commercial-grade Android spyware in exploit chain targeting Samsung devices (headline paraphrased)** Palo Alto Networks Unit 42 · November 7, 2025. https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/

[31] **Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security (Executive Order 14093)** Federal Register · March 30, 2023 (record checked October 13, 2026). https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security

[32] **Order Granting Plaintiffs' Motion for Permanent Injunction (Dkt. 809), WhatsApp LLC v. NSO Group Technologies Ltd., No. 4:19-cv-07123** US District Court, Northern District of California · November 12, 2025. https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.809.0.pdf

NEXT STEP

What does this mean for your security?

Bring your questions about Intellexa's Aladdin ad vector and the commercial spyware market, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

Predator persists as Greece convicts four
Start with part 1 of 2 · z7solutions.com/z7-cyber/intellexa/

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 SECURITY CONVERSATION Book a Security Conversation ↗

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