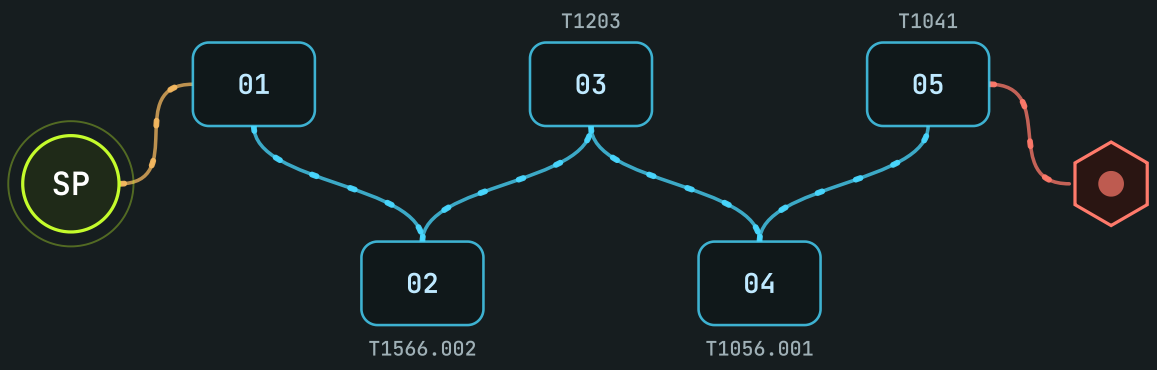


INTELLIGENCE BRIEF

Commercial spyware keeps selling through sanctions, verdicts and buyouts

Sanctions, court orders and a US buyout have not ended mercenary spyware. Google tied more 2025 zero-days to spyware vendors than to traditional state espionage groups. Patch fast; treat Apple alerts as incidents.

EDITION
Fall/Winter 2026/2027 Edition
SP-03 · Spyware vendor

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ONGOING RISK

Vendors keep operating despite sanctions, court orders and ownership changes, and Google attributed more 2025 zero-days to commercial surveillance vendors than to traditional state-sponsored espionage groups. [12]

HEADLINE NUMBERS

90
zero-days exploited in the wild in 2025 [12]

110
countries in Apple's August 2026 spyware alert wave [28]

561
spyware entities in 46 countries, 1992 to 2024 [20]

$475.7M
Cellebrite 2025 revenue, up 19 percent [19]

KEY FACTS

MARKET
561 entities in 46 countries (1992 to 2024); US investors now the largest group [20]

EXPLOITS
90 zero-days exploited in 2025; commercial vendors ahead of traditional state espionage groups for the first time [12]

DELIVERY
One-time links in encrypted messaging apps; Intellexa also redirects some targets through malicious ads [10]

LEGAL PRESSURE
NSO enjoined, Ninth Circuit appeal pending; Meta moved for contempt on June 8, 2026 [4]

SANCTIONS
Three of seven sanctioned Intellexa individuals delisted Dec 30, 2025; NSO and Candiru remain on the Entity List [34]

TARGETS
Apple sent threat notifications to users in 110 countries in a wave reported Aug 13, 2026 [27]

02 What happened

The original edition described an industry under legal pressure yet still growing. Ten months on, both trends held. NSO Group is under US investor control and bound by a permanent WhatsApp injunction, three Intellexa-linked individuals were delisted weeks after Google and Amnesty documented Predator operations continuing, and ICE's Paragon contract closed out while Paragon's chief executive said the company has no way to know whether customers misuse its software.

- Google Threat Intelligence Group counted 90 zero-days exploited in the wild in 2025 and, for the first time since it began tracking, attributed more zero-days to commercial surveillance vendors than to traditional state-sponsored espionage groups.
- A federal court entered the WhatsApp permanent injunction against NSO Group on November 12, 2025, with a final judgment of $4,447,190 after cutting the $167,254,000 punitive award to $4,002,471. The district court and the Ninth Circuit both denied stays, NSO's appeal is pending, and Meta moved for contempt on June 8, 2026.
- Treasury removed three Intellexa-linked individuals from the SDN list on December 30, 2025. Five senators wrote on February 13, 2026 that three of the seven designated individuals were delisted without the bipartisan briefing that committee staff had requested.
- NPR reported in May 2026 that DHS said ICE has no relationship with Paragon or its acquirer. A procurement notice shows the contract closed out on January 20 (NPR gives no year), and ICE's acting director wrote in an April 1 letter that use of the tool complied with the 2023 executive order.
- Apple told TechCrunch it sent a new batch of mercenary spyware threat notifications to users targeted in 110 countries, and says it has now notified users in over 150 countries in total. Apple notifies by lock screen push as well as by email.
- The FCC voted in November 2025 to rescind the January 2025 CALEA declaratory ruling and withdrew the rulemaking that accompanied it, with Commissioner Gomez dissenting.

03 How it works

01 A government buys access

A government customer buys the platform, and Intellexa keeps supplying exploits. Google found Intellexa increasingly buying steps of its exploit chains from external entities.

02 Delivery by link or by ad

MITRE ATT&CK T1566.002

Google says the primary route is one-time links sent over end-to-end encrypted messaging apps. Since early 2025 it has also seen Intellexa use malicious ads on third-party platforms to fingerprint users and redirect targets to exploit servers for a few customers. Leaked documents describe a separate ad-only system called Aladdin; Amnesty believes it supported active deployments in 2024, but Recorded Future knew of no in-the-wild use as of December 3, 2025.

03 Browser and kernel exploit chain

MITRE ATT&CK T1203

A captured iOS chain combined a Safari remote code execution bug with two kernel bugs to break out of the browser sandbox and run the payload with system privileges. Of roughly 70 zero-days that Google's Threat Analysis Group discovered and documented since 2021, 15 are Intellexa's.

04 Implant checks its surroundings

MITRE ATT&CK T1056.001

Google's analysis of the PREYHUNTER payload found modules that record calls, log keystrokes, capture camera images and hide notifications. A watcher module ends the infection if it finds developer mode, certain mobile security apps or a US or Israeli (IL) locale.

05 Data flows to the customer system

MITRE ATT&CK T1041

Collected data is viewed and stored in a Predator dashboard. A leaked mid-2023 training video shows Intellexa staff connecting to deployed customer systems over TeamViewer, which Amnesty says raises questions about customer oversight and how well live surveillance data is compartmentalized.

04 Who is at risk

Mercenary spyware is bought by governments and aimed at specific people. The cost lands on the organizations those people work for, because one infected phone exposes mail, messages and credentials for everyone around it.

- Government officials, journalists and policy experts: Treasury's March 5, 2024 release says Predator was used to target Americans, including U.S. government officials, journalists, and policy experts. Five US senators later wrote that foreign actors deployed it against officials including members of Congress, citing NBC News.
- Journalists and civil society activists: Italy's parliamentary oversight committee acknowledged in June 2025 that Italian intelligence services used Graphite against civil society activists, and Amnesty documented a Predator attempt against a Balochistan human rights lawyer in summer 2025.
- Staff who travel to or deal with countries where Google sent government-backed attack warnings tied to Intellexa customers, including Pakistan, Kazakhstan, Angola, Egypt, Uzbekistan, Saudi Arabia and Tajikistan.
- Telecommunications carriers and their customers, after the FCC rescinded its January 2025 CALEA security ruling in November 2025.
- Public agencies evaluating surveillance or forensic vendors, which carry sanctions, procurement and reputational exposure.

Sectors in scope: government officials and legislators, journalists and civil society, lawyers and human rights defenders, telecommunications carriers, policy and research organizations, executives in regulated industries.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 The WhatsApp injunction against NSO Group was entered on November 12, 2025, after Judge Hamilton cut the $167,254,000 punitive award to $4,002,471 on October 17. It covers only the WhatsApp platform: it bars NSO and anyone acting with it from building or using technology that interacts with WhatsApp, collecting its data, reverse engineering its code or creating accounts, orders deletion of related code and data, and excludes foreign sovereign customers and outside counsel. The district court denied a stay on December 19, 2025, the Ninth Circuit denied one on January 28, 2026, and NSO's appeal is pending.

SOURCE 33

02 NSO is now controlled by a US investor group, with former ambassador David Friedman as executive chairman after CEO Yaron Shohat and co-founder Omri Lavie left. TechCrunch reported in January 2026 that NSO is campaigning for removal from the Commerce Entity List, where the Consolidated Screening List still showed it on October 14, 2026, and that critics faulted its transparency report for omitting how many customers were rejected, investigated, suspended or terminated.

SOURCE 2

03 Treasury delisted Sara Hamou, Andrea Gambazzi and Merom Harpaz on December 30, 2025 under the CYBER2 program. A US official told CyberScoop each had demonstrated measures to separate from Intellexa and that the removal followed a petition for reconsideration. Senators Warren, Shaheen, Kim, Schiff and Bennet wrote on February 13, 2026 that Treasury gave committee staff no briefing, citing Google's December 3, 2025 finding that Intellexa adapted and continues selling and Amnesty's December 4, 2025 leak analysis.

SOURCE 9

04 ICE's Paragon contract was reactivated in August 2025 and a federal procurement notice says it closed out on January 20 (NPR gives no year). DHS told NPR in May 2026 that ICE has no relationship with Paragon or its acquirer and declined to say whether ICE keeps access through a third party. In an interview summarized by Citizen Lab on October 8, 2026, Paragon's CEO told WIRED the company has no way to know whether customers misuse its software and has no kill switch.

SOURCE 13

05 Google's March 5, 2026 review counted 90 exploited zero-days in 2025 (2024 now counted at 78), an all-time high of 43 or 48 percent against enterprise technologies, 15 on mobile operating systems versus 9 in 2024, and for the first time more zero-days attributed to commercial surveillance vendors than to traditional state-sponsored espionage groups.

SOURCE 12

06 Apple sent a new batch of threat notifications to users targeted in 110 countries, reported August 13, 2026, and now also pushes the alert to the iPhone lock screen. Citizen Lab said on August 20, 2026 that the scale and geographic diversity of public posts about the alerts was unprecedented and that there is a huge notification iceberg the public will never learn about.

SOURCE 27

07 The FCC voted in November 2025 to rescind the January 2025 CALEA declaratory ruling and withdraw the proposed rulemaking that accompanied it, calling the ruling unlawful and ineffective and saying carriers had taken important steps to strengthen cybersecurity. Commissioner Gomez was the only vote against.

SOURCE 21

08 Accountability came through courts rather than treaties: a Greek court convicted four people tied to Intellexa on February 26, 2026, which OCCRP called the first convictions in the Greek commercial spyware investigation, and the UK Supreme Court held in August 2026 that Bahrain is not immune from claims by two dissidents who allege it hacked them with FinSpy (Citizen Lab, September 2, 2026).

SOURCE 41

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch phones, browsers and messaging apps within days of release and enforce minimum OS versions through MDM.**

Google's 2025 zero-day review advises applying patches as soon as they become available; a patched device breaks the exploit chains already documented.

02 **Enable Lockdown Mode on iPhones and advanced protection on Android for executives, counsel, journalists and anyone who deals with high-risk countries.**

Apple told TechCrunch it has yet to see a case where a device was hacked while Lockdown Mode was enabled.

03 **Treat an Apple or Google threat notification as a security incident: isolate the device, reset credentials and sessions, and get a forensic review.**

A notification may not mean the device was hacked, but it means Apple suspects the person was targeted; Apple sent a new batch to users in 110 countries in August 2026.

04 **Run sanctions and ownership checks on any surveillance, forensic or intrusion vendor before purchase, and re-check annually.**

Delistings, ownership changes and restructurings affected NSO, Intellexa, Candiru and Paragon within the past two years.

05 **Do not assume carrier networks meet the January 2025 CALEA security requirements; keep sensitive calls and messages on end-to-end encrypted apps with disappearing messages.**

The FCC rescinded that ruling in November 2025, so the obligations it created no longer apply.

06 **Give staff a reporting path and a stand-in device plan for suspected targeting, and brief executives before travel to higher-risk jurisdictions.**

Targeting follows people and their contacts; the organizations around them absorb the damage.

07 **Monitor mail and identity logs for sign-ins from a newly compromised phone, and require phishing-resistant MFA on executive accounts.**

Google documented a keylogger in Intellexa's payload, so passwords and codes can be exposed; identity controls limit what the attacker can do next. Z7's 24/7 SOC and Microsoft 365 posture review cover this layer.

07 Sources

[1] **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/

[2] **Critics pan spyware maker NSO's transparency claims amid its push to enter US market** TechCrunch · January 8, 2026. https://techcrunch.com/?p=3080919

[4] **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/

[7] **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

[8] **Treasury removes Intellexa spyware-linked trio from sanctions list** CyberScoop · January 2, 2026. https://cyberscoop.com/treasury-removes-intellexa-spyware-linked-trio-from-sanctions-list/

[9] **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

[10] **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

[11] **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/

[12] **2025 zero-day exploitation review** Google Threat Intelligence Group · March 5, 2026. https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review/

[13] **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

[14] **A year on, Paragon has told Italian magistrates nothing about the Graphite spyware attacks** Wanted in Rome (reporting Wired Italia) · April 28, 2026. https://www.wantedinrome.com/news/paragons-spyware-infected-phones-in-italy-a-year-later-israel-has-said-nothing.html

[15] **The Secrets of a US Spyware King (summary of a WIRED interview with Paragon's CEO)** Citizen Lab (reporting WIRED) · October 8, 2026. https://citizenlab.ca/the-secrets-of-a-us-spyware-king/

[16] **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

[17] **Memento Labs, formerly Hacking Team, linked to Dante spyware used in Russia** The Record · October 27, 2025. https://therecord.media/memento-labs-formerly-hacking-team-dante-spyware-russia-kaspersky

[18] **Italian spyware vendor linked to Chrome zero-day attacks** BleepingComputer · October 27, 2025. https://www.bleepingcomputer.com/news/security/italian-spyware-vendor-linked-to-chrome-zero-day-attacks

[19] **Cellebrite Announces Record Fourth-Quarter and Full-Year 2025 Results** Cellebrite (PR Newswire) · February 11, 2026. https://tools.prnewswire.com/en-us/live/20823/release/20260211EN85170

[20] **Mythical Beasts: Diving into the depths of the global spyware market** 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/

[21] **FCC rolls back cybersecurity rules for telcos despite state hacking risks** BleepingComputer · November 21, 2025. https://www.bleepingcomputer.com/news/security/fcc-rolls-back-cybersecurity-rules-for-telcos-despite-state-hacking-risks/

[22] **Ransomware payments fell in 2025 as fewer victims paid, Chainalysis reports** The Record · February 26, 2026. https://therecord.media/ransomware-payments-chainalysis-cybercrime

[23] **North Korea stole a record amount of crypto in 2025** Fortune (reporting Chainalysis) · December 18, 2025. https://fortune.com/2025/12/18/north-korea-stole-a-record-amount-of-crypto/

[24] **Operation Endgame continues: international coalition takes malware offline** Eurojust · June 24, 2026. https://www.eurojust.europa.eu/news/operation-endgame-continues-international-coalition-takes-malware-offline

[25] **The Pall Mall Process Code of Practice for States** UK Government · updated October 23, 2025. https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states

[26] **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

[27] **If Apple sends you a push notification alerting you to a spyware attack, take it seriously** TechCrunch · August 13, 2026. https://techcrunch.com/2026/08/13/if-apple-sends-you-a-push-notification-alerting-you-to-a-spyware-attack-take-it-seriously/

[28] **Unprecedented number of Apple users received recent spyware alert** Citizen Lab · August 20, 2026. https://citizenlab.ca/unprecedented-number-of-apple-users-received-recent-spyware-alert/

[29] **U.K. Supreme Court opens door for spyware victims to sue foreign states** Citizen Lab · September 2, 2026. https://citizenlab.ca/uk-supreme-court-opens-door-for-spyware-victims-to-sue-foreign-states/

[31] **WhatsApp Inc. v. NSO Group Technologies Ltd., docket 4:19-cv-07123-PJH (entries 812, 813, 824, 834, 854, 877)** US District Court, N.D. Cal., via CourtListener · entries through September 10, 2026. https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/

[32] **Final Judgment (Dkt. 810)** US District Court, N.D. Cal. · November 12, 2025. https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.810.0.pdf

[33] **Order Granting Plaintiffs' Motion for Permanent Injunction (Dkt. 809)** US District Court, N.D. Cal. · November 12, 2025. https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.809.0.pdf

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

[35] **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

[36] **Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium** US Department of the Treasury · September 16, 2024. https://home.treasury.gov/news/press-releases/jy2581

[37] **Spyware maker cuts ties with Italy after government refused audit into hack of journalist's phone** The Record · June 9, 2025. https://therecord.media/paragon-spyware-maker-cuts-ties-italy-government

[38] **Defense cyber intelligence company RedLattice to go public in $1.25B SPAC deal** SiliconANGLE · September 28, 2026. https://siliconangle.com/?p=848558

[39] **REDLattice to Go Public Through Bold Eagle SPAC Merger** GovConWire · September 29, 2026. https://www.govconwire.com/?p=345910

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

[41] **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

[42] **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. 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

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

- Predator persists as Greece convicts four
  More from the edition · z7solutions.com/z7-cyber/intellexa/
- Spyware vendors lead zero-days; Aladdin unconfirmed
  More from the edition · z7solutions.com/z7-cyber/intellexa-part-2/
- 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.