

ZERODAYRAT

*Public-source record of a Telegram-sold
Android and iOS surveillance kit, 2026*

Classification: UNCLASSIFIED // PUBLIC OSINT SYNTHESIS

Cut-off date: 6 October 2026

Prepared for: Crygma / Encrygma research file

Primary anchor: iVerify, Daniel Kelley, 10 February 2026

Scope: identity, delivery model, claimed capabilities,
attribution limits, and defensive implications

Excluded: builder, panel deployment, lure craft,
overlay or clipboard procedures, purchase paths

Secondary: SecurityWeek, Dark Reading, The Hacker News,
Infosecurity Magazine, CSO Online, Forbes — all February 2026

0. Control note

This dossier is the public record on the mobile toolkit sold under the name ZeroDayRAT, as documented by iVerify on 10 February 2026 and repeated by the trade press that week. It is a defensive synthesis. It does not include a builder, panel installation, lure text, overlay technique, clipboard logic, or any purchase path. Almost every technical claim traces to one vendor blog and to screenshots of an operator panel. Where a claim is the seller's compatibility statement rather than a demonstrated exploit, it is marked as such.

The name is a marketing string. Nothing in the iVerify report, SecurityWeek, Dark Reading, or The Hacker News establishes a zero-day vulnerability, a zero-click chain, or a kernel exploit. Infection, as described, requires the victim to install a binary. SMS interception defeats SMS one-time codes only. It does not defeat hardware keys, passkeys, or an authenticator that never renders a code in a text message.

1. Executive assessment

ZeroDayRAT is a commercial mobile surveillance and theft kit, first observed by iVerify on 2 February 2026 and published on 10 February by Daniel Kelley. It is sold on Telegram, with separate channels for sales, support, and updates, in English, Spanish, Portuguese, Russian, and Chinese. Buyers receive a builder and a browser panel they host themselves. The Android component is an APK. The iOS component is described only as a payload. Delivery is smishing, phishing mail, fake app stores, and links in WhatsApp or Telegram.

The panel, as shown by iVerify, offers device profiling, GPS history on an embedded map, notification capture, an account census, full SMS search plus the ability to send SMS, live camera, screen recording, microphone, and a keylogger with a live screen preview. Two theft modules are described: a crypto stealer aimed at MetaMask, Trust Wallet, Binance, and Coinbase, including clipboard substitution of wallet addresses, and a banking stealer using overlays against banking apps, Indian UPI apps including PhonePe and Google Pay, Apple Pay, and PayPal. Secondary reporting cites a price of about 2,000 dollars, attributed to Kelley; that figure is not in the primary blog and should be treated as an approximate quote, not a tariff.

Kelley told SecurityWeek the operator posts in Chinese, uses a Russian domain, and has targeted victims in India, and that the mismatch looks deliberate. No named developer, no hash set, and no central server were published. Each buyer runs an instance, so takedown is per deployment. No later independent teardown, infection census, or arrest was in the open sources collected for this cut-off. The eight-month gap after February 2026 is itself a finding: the family is known from marketing and a panel demo, not from a measured victim population.

2. What the name does and does not mean

ZeroDayRAT is the seller's brand. iVerify adopted it. It is not evidence of a zero-day. The Hacker News, citing iVerify, says binaries are generated by a builder supplied to buyers and that the panel can be set up on the buyer's server. CSO Online and Infosecurity describe the same install requirement. A journalists' shorthand that the tool "takes over an iPhone via text" overstates the mechanism: the text is the lure, the install is the compromise. On Android the reported path is a sideloaded APK requesting the permissions stalkerware usually requests, including accessibility. On iOS the public record does not explain the signing model, the entitlement set, or whether the payload is a sideloaded enterprise app, a TestFlight abuse, or a claimed jailbreak-free implant. The iOS depth of compromise is therefore the weakest part of the file.

Advertised range is Android 5 through 16 and iOS up to 26, including iPhone 17 Pro. That is a compatibility claim. It is not a finding that every version in the range is equally compromised, or that an exploit exists for current, locked-down iOS. A defender should plan for a social-engineered install on Android, and should treat the iOS claim as unverified until a sample is published.

3. Chronology

Date	Event	Grade
2 Feb 2026	iVerify first observes sales activity on Telegram.	Researcher statement
10 Feb 2026	iVerify blog. Same-day coverage by Dark Reading, SecurityWeek, Infosecurity, CyberInsider.	Primary plus press
11–17 Feb 2026	Forbes, The Hacker News, CSO Online, TechSpot repeat the findings. No second lab publishes samples.	Secondary
Feb 2026	Kelley: Chinese-language posts, a Russian domain, Indian victims; five-language marketing.	Interview, SecurityWeek
Feb–Oct 2026	No public hash release, no measured infection count, no announced seizure in the sources reviewed.	Absence
6 Oct 2026	Cut-off. Family remains a panel-demonstrated MaaS, not a census-backed campaign.	This dossier

Table 1. Public chronology. Silence after February is not proof the kit disappeared.

4. Commercial model

The structure is malware-as-a-service with the server pushed to the customer. Telegram is the storefront and the support desk, not the command channel of the implant. That differs from Millenium RAT, whose implants call the Telegram Bot API. Here the operator panel is self-hosted, which removes a single C2 to seize and multiplies the number of endpoints a takedown must hit. iVerify and SecurityWeek both note that a Telegram channel ban is slow and replaceable. Languages of advertisement — English, Spanish, Portuguese, Russian, Chinese — are a distribution choice, not an attribution. The Russian domain plus Chinese posts plus Indian victim context is, on Kelley's own reading, noise intended to frustrate attribution. No corporate registry, sanctions listing, or court case is attached to the brand.

Price. Dark Reading and later summaries put the kit near 2,000 dollars, citing Kelley. The primary blog does not print a price. Relative to Millenium RAT at 50 to 90 dollars, that is a higher tier of commodity mobile spyware, still far below a mercenary license. Relative to Predator, it is a different market: no government end-user licence, no exploit subscription, no vendor remote-hands into the customer console of the Intellexa kind.

5. Capabilities, as shown

5.1 Panel surface

iVerify's screenshots and description break the panel into tabs. Overview: model, OS, battery, country, lock state, SIM and carrier, dual-SIM numbers, app-usage timing, a live activity timeline, a preview of recent SMS. Location: GPS coordinates and history on an embedded Google map. Notifications: app name, title, body, and time, with WhatsApp, Instagram, Telegram, and YouTube named. Accounts: enumerated registrations and emails for Google, WhatsApp, Instagram, Facebook, Telegram, Amazon, and Indian services including Flipkart, PhonePe, and Paytm. SMS: inbox search, incoming one-time codes, and the ability to send from the victim number. Surveillance: front or back camera, screen recording, microphone. Keylogger: inputs with app context and timestamps, beside a live screen preview. These are panel features demonstrated to the researcher. They are not each independently verified on a victim handset in a published forensic report.

5.2 Financial modules

The crypto module is described as scanning for MetaMask, Trust Wallet, Binance, and Coinbase, logging identifiers and balances, and replacing a copied address on the clipboard. The banking module is described as overlays on banking apps, PhonePe, Google Pay, Apple Pay, and PayPal. Clipboard substitution and overlays are well-known criminal techniques; naming them here is identification, not a procedure. No confirmed loss figure has been published.

5.3 What “MFA bypass” means

Dark Reading's headline follows from SMS control. If the implant can read and send SMS, SMS one-time passwords are visible to the operator, and the victim number can be used to request or forward codes. That is account-takeover support against SMS-based factors. It is not a break of FIDO2, passkeys, or an authenticator app whose codes never appear in the SMS store. Calling it an MFA bypass without that qualifier overstates the finding.

6. Delivery and platform reality

Reported lures are a text with a link, a phishing email, a fake store, or a link in WhatsApp or Telegram. The victim installs an APK or an iOS payload that looks like an ordinary app. No exploit chain, CVE, or zero-click has been named. Android accessibility abuse is the implied post-install privilege for overlays, keylogging, and notification read; iVerify does not publish the manifest. iOS remains unspecified. A claim of support through iOS 26 on a current iPhone, without a published sample, is the point a second lab would need to test before the family is treated as a peer of mercenary iOS implants.

7. Indicators and detection

iVerify published no hashes, package names, or domains in the blog. SecurityWeek said few or no indicators of compromise were available. The Russian domain mentioned by Kelley was not printed. Detection therefore cannot start from a blocklist. Useful signals, all indirect: an enterprise device sideloading an APK outside the managed store; an accessibility service granted to an app the user cannot name; sudden SMS sent from a handset the user did not use; clipboard addresses that do not match what was

copied, visible as unexpected crypto outflows; battery drain and camera or microphone indicators the user did not trigger. None of these is specific to this brand. Mobile threat defence that flags newly installed sideloaded apps and accessibility grants is the control that matches the described infection, not a signature for ZeroDayRAT.

For individuals, the matching posture is the ordinary one for stalkerware. Do not install apps from a text message. On Android, restrict sideloading and review accessibility services. Prefer passkeys or an authenticator over SMS codes for accounts that matter. On iOS, do not install profiles or enterprise apps from a link. A factory reset after removing the Apple ID or Google account from a shared device remains the blunt recovery when stalkerware is suspected; it is not a forensic preservation step.

8. Comparison

Dimension	ZeroDayRAT	Millenium RAT	Predator
Platform	Android APK; iOS payload claimed	Windows only	iOS and Android implants
Access	User installs a binary	User runs a file	One-click, injection, ad vector; zero-days
C2	Buyer-hosted panel	Telegram Bot API	Vendor anonymization chain
Price, public	About 2,000 dollars, secondary	50–90 dollars	Government licence, unpublished
Storefront	Telegram channels	Forums, git hosts, site	Direct sales
Financial theft	Clipboard and overlays	Wallets among stealer features	Not the product purpose
Public samples	None in the primary blog	Hashes published by Group-IB	Samples from Citizen Lab, Talos, Google
Measured scale	No census	62,289 endpoints, Group-IB	Country clusters, not a device count

Table 2. Peer contrast. ZeroDayRAT sits in commodity mobile stalkerware, not in the mercenary tier.

9. Assessment

High confidence: a kit by this name was marketed on Telegram in early February 2026; iVerify reviewed a panel and described install-based delivery; SMS, location, notification, and financial-theft features were shown as panel functions; the seller offered support in five languages. Medium confidence: the 2,000-dollar price; Indian targeting; a Russian domain. Low confidence: equal function on every claimed OS version, especially current iOS; any victim count; any link to a named person or state. Not supported: zero-day exploitation, zero-click infection, a single takedown-able server.

The open gap is a sample. Until a second lab publishes an APK hash, an iOS binary, and a network indicator, ZeroDayRAT remains a documented commercial offer and a demonstrated panel, not a fully characterized malware family. That is enough to brief a mobile-security team. It is not enough to write a detector.

10. Sources

Daniel Kelley, iVerify, “Breaking Down ZeroDayRAT — New Spyware Targeting Android and iOS,” 10 February 2026. SecurityWeek, 10 February 2026. Dark Reading, 10 February 2026. Infosecurity Magazine, 10 February 2026. The Hacker News, 16 February 2026. CSO Online, 17 February 2026. Forbes, 16 February 2026. No primary update with samples was located between those pieces and 6 October 2026.

End of dossier. Cut-off 6 October 2026. Public-source synthesis for defensive use. Nothing in this document is an instruction to build, buy, or operate intrusion software.