INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-11 06:12 UTC

Ad-Data Surveillance Pipeline Exposed: Commercial Tooling Gives Law Enforcement Warrantless Access to 500 Million Mobile Devices

SECURITY ANALYSIS | **HIGH** | CVSS 7.5

SCC Item ID	SCC-STY-2026-0055
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Mobile advertising ecosystem broadly; users of apps participating in real-time bidding (RTB) ad networks; Webloc (Cobwebs Technologies / Penlink), Tangles (Penlink)
Published	2026-04-11T02:02:00
Discovery Source	Rss

Executive Summary

Citizen Lab has published an analysis identifying Webloc, a commercial surveillance platform originally developed by Israeli firm Cobwebs Technologies and now operated by Nebraska-based Penlink, as a tool used by U.S. federal agencies including ICE, DHS, and the military to track mobile devices without warrants, drawing on location data harvested from the mobile advertising ecosystem. The platform exploits the real-time bidding (RTB) ad auction infrastructure to ingest mobile advertising identifiers and location signals at scale, covering an estimated 500 million devices with up to three years of historical data. This disclosure signals that warrantless mass surveillance has been quietly operationalized through commercial data brokers, bypassing judicial oversight mechanisms and creating significant legal, reputational, and regulatory exposure for any organization whose employee or user data flows through the RTB ecosystem.

Technical Analysis

Webloc's architecture does not exploit a software vulnerability in the conventional sense. It exploits a structural property of the real-time bidding ecosystem: every time a mobile ad auction occurs, the bid request broadcasts device identifiers (MAIDs, Mobile Advertising IDs such as Apple's IDFA or Google's GAID) alongside precise location signals to a pool of bidders. This broadcast is by design, it enables advertisers to make targeting

decisions, but it also means every participating bidder receives the location and identity data regardless of whether they win the auction. Webloc ingests this data stream passively, aggregating MAIDs and location histories into a retrospective tracking database without the device owner's knowledge and without any judicial process.

Citizen Lab's analysis, published directly on citizenlab.ca, attributes Webloc to named U.S. government customers including ICE, DHS, and the U.S. military, as well as law enforcement agencies in Hungary and El Salvador. The platform, originally developed by Israeli firm Cobwebs Technologies, is now operated by Penlink, a Nebraska-based company. Cobwebs Technologies was previously sanctioned by Meta for platform abuse and documented by researchers as having links to Israeli spyware vendor Quadream, a vendor associated with surveillance targeting journalists, activists, and political opposition figures.

From a MITRE ATT&CK perspective, the tradecraft maps to T1430 (Location Tracking), T1597 and T1596 (Search Closed/Open Sources), T1589 and T1593 (Gather Victim Identity Information / Search Open Websites), and T1325 (Acquire Access to Target Organization). The offensive value is retrospective pattern-of-life analysis: an analyst can query a device's MAID and reconstruct months or years of movement, identifying home addresses, workplaces, places of worship, medical facilities, and associations with other devices.

The defensive gap is structural. No patch closes this attack surface. The data leakage is native to RTB. CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) and CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) apply at the ecosystem level, but the 'unauthorized actor' framing requires clarification: Webloc operators are authorized participants in the RTB bidding ecosystem, but they lack lawful authorization from data subjects or regulators to use collected MAIDs and location histories for law enforcement surveillance purposes. The policy and legal gap is the absence of any requirement to restrict downstream use of bid-request data for surveillance purposes.

For security teams, the operative concern is not network intrusion but passive data collection against personnel. High-risk individuals, executives, incident responders, threat intelligence analysts, government contractors, journalists on the organization's payroll, are potentially trackable by any entity with access to Webloc or a comparable platform. The three-year historical data window means exposure is not limited to current behavior; past movements are recoverable.

Action Checklist

1. Step 1: Assess exposure, determine whether your organization's mobile app portfolio, advertising integrations, or third-party SDKs participate in RTB ad networks that broadcast MAIDs and location data to open bidder pools
2. Step 2: Review controls, audit mobile app data practices for SDK-level data sharing; evaluate whether your organization's mobile device management (MDM) policy addresses advertising identifier reset or opt-out for corporate-issued devices
3. Step 3: Update threat model, add commercial surveillance vendor access to RTB data streams as a passive collection threat against high-value personnel; incorporate T1430 (Location Tracking) and T1597 (Search Closed Sources) into your threat register with Webloc and comparable platforms as representative tooling
4. Step 4: Communicate findings, brief leadership and legal counsel on the specific risk to named high-risk roles (executives, government contractors, sensitive operations personnel) whose device movements may already be available in commercial surveillance databases with up to three years of historical data

5. Step 5: Monitor developments, track Citizen Lab follow-up publications, anticipated FTC and congressional responses to Webloc disclosure, and any litigation or regulatory action targeting the RTB data broker ecosystem for downstream surveillance use restrictions

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if: (1) any corporate device belonging to a cleared contractor, executive, or sensitive-operations personnel is confirmed enrolled in an app with an RTB-participating SDK, triggering potential ITAR/EAR, Privacy Act, or state privacy law notification review; (2) Citizen Lab or a regulatory body publishes new evidence that Webloc/Penlink data includes your organization's named personnel or corporate IP ranges; or (3) your organization is a federal contractor subject to CMMC or DFARS 252.204-7012, as personnel location exposure may constitute a reportable cyber incident under those frameworks.
Recovery Notes	Recovery for this threat class is not a system restoration exercise but a sustained data minimization and policy remediation effort: the 'damage' is historical MAID and location data already resident in Penlink's commercial surveillance database, which cannot be deleted unilaterally. Verify recovery progress by confirming MDM-enforced advertising identifier opt-out across 100% of corporate devices, SDK removal or replacement for any RTB-participating libraries in internally developed apps, and updated vendor contracts prohibiting data resale to law enforcement or surveillance platforms. Maintain a 90-day active monitoring posture post-remediation watching for Citizen Lab or FTC disclosures that name your organization's app ecosystem or SDK vendors, and re-assess threat model annually as the RTB regulatory environment evolves.
Forensic Artifacts	Mobile app network traffic captures (mitmproxy PCAP or HAR files) showing OpenRTB 2.x bid request payloads from corporate devices — specifically JSON fields 'device.ifa' (MAID value), 'device.geo.lat', 'device.geo.lon', 'device.ip', and 'user.id' transmitted to RTB exchange endpoints; these directly evidence what data your apps broadcast to bidder pools that Webloc-class platforms ingest | MDM compliance export (Intune, Jamf, or Workspace ONE) showing per-device advertising identifier opt-out status and app inventory at the time of discovery — establishes the historical exposure population and device count before remediation changes the baseline | APK/IPA SDK manifest artifacts — specifically the AndroidManifest.xml permissions block and embedded META-INF SDK declarations, or iOS Info.plist NSUserTrackingUsageDescription entries, identifying which RTB-capable advertising SDK libraries (e.g., com.google.android.gms.ads, MoPub, AppLovin MAX) were present and at what versions during the exposure window | Archived and hash-verified copies (sha256sum) of the Citizen Lab Webloc/Penlink analysis publication and any corroborating EFF or congressional hearing transcripts — these constitute the authoritative threat intelligence sourcing for the incident record and are required if legal or regulatory inquiry later challenges when and how the organization assessed the risk | Historical app store privacy nutrition label submissions and Google Play data safety form responses for your organization's apps — these documents what your organization declared about data sharing to regulators and users, which becomes material if FTC or state AG enforcement action examines whether disclosures accurately reflected RTB SDK data transmission behavior

Per-Action IR Details

Step 1: Assess exposure — determine whether your organization's mobile app portfolio, advertising integrations, or third-party SDKs participate in RTB ad networks that broadcast MAIDs and location data to open bidder pools

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: scope and impact estimation of passive data exfiltration via third-party advertising infrastructure

Controls: NIST RA-3 (Risk Assessment) — assess likelihood and impact of MAID and location data exposure through RTB auction participation, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity and data-sharing behavior of third-party SDKs embedded in your mobile app portfolio, NIST CA-7 (Continuous Monitoring) — establish ongoing visibility into what data your apps transmit to RTB bidder pools, CIS 2.1 (Establish and Maintain a Software Inventory) — enumerate all third-party SDKs including advertising, analytics, and attribution libraries that may participate in RTB auctions, CIS 3.2 (Establish and Maintain a Data Inventory) — identify all mobile advertising identifiers (MAIDs) and location signals your apps generate and transmit

Compensating: Use mitmproxy (free, open-source) to intercept and log HTTPS traffic from your mobile apps on a test device: `mitmproxy --mode transparent --ssl-insecure`. Review outbound connections for bid request domains associated with major ad exchanges (Google Ad Manager, OpenX, PubMatic, Index Exchange). Cross-reference SDK manifest entries in your APK/IPA using apktool (`apktool d app.apk`) or objection (`objection --gadget com.yourapp explore`) to enumerate advertising SDK libraries. Search for known RTB-participating SDK package names: com.google.android.gms.ads, com.mopub, com.applovin, com.ironsource, com.unity3d.ads.

Evidence: Capture before assessment: (1) Full SDK dependency manifest from your mobile app build files (Gradle build.gradle, Podfile.lock) listing all advertising and analytics dependencies with version numbers. (2) Network traffic captures from app runtime showing bid request payloads — look for JSON structures containing 'device.ifa' (MAID field per OpenRTB 2.x spec), 'device.geo.lat/lon', and 'device.ip'. (3) App store privacy nutrition labels and privacy policy disclosures for each app. (4) Any existing MDM enrollment records showing advertising identifier opt-out status across the corporate device fleet.

Step 2: Review controls — audit mobile app data practices for SDK-level data sharing; evaluate whether your organization's mobile device management (MDM) policy addresses advertising identifier reset or opt-out for corporate-issued devices

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: policy and tooling gaps that enable passive surveillance via commercial RTB infrastructure must be remediated before individual incidents can be contained

Controls: NIST AC-1 (Access Control Policy and Procedures) — policy must explicitly address corporate-device advertising identifier controls and MDM-enforced MAID opt-out, NIST CM-6 (Configuration Settings) — MDM configuration baselines for iOS and Android must include 'Limit Ad Tracking' (iOS) or 'Opt out of Ads Personalization' (Android) as required settings, NIST SA-9 (External System Services) — govern third-party SDK data-sharing obligations via contract and policy; RTB SDK inclusion constitutes an external system service with data transmission implications, NIST IR-8 (Incident Response Plan) — update the IR plan to reflect passive commercial surveillance as a threat vector requiring pre-deployment SDK review gates, CIS 4.6 (Securely Manage Enterprise Assets and Software) — apply configuration management to mobile devices to enforce advertising identifier restrictions fleet-wide, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — extend account/identity inventory to include MAID-to-employee mappings for high-risk personnel on corporate devices

Compensating: For MDM-lite or no-MDM environments: deploy an Intune free trial or use Apple Configurator 2 (free) to push a configuration profile enforcing 'Allow Advertising Tracking: false' on iOS devices. For Android, use Android Enterprise zero-touch enrollment with a managed Google Play profile restricting ad ID access. Without MDM, distribute a manual procedure: iOS Settings > Privacy & Security > Tracking > disable 'Allow Apps to Request to Track'; iOS Settings > Privacy & Security > Apple Advertising > disable 'Personalized Ads'. Document compliance via a signed acknowledgment form for high-risk personnel. Use Exodus Privacy (https://exodus-privacy.eu.org — search-retrieved, validate before use) to audit SDK trackers in Android APKs without enterprise tooling.

Evidence: Capture before remediation: (1) MDM compliance reports showing current advertising identifier opt-out status across all enrolled corporate iOS and Android devices — export from Intune, Jamf, or VMware Workspace ONE

console before policy changes are applied. (2) Existing app privacy declarations submitted to Apple App Store Connect and Google Play Console under your developer account, documenting declared data types and third-party sharing. (3) Current SDK dependency snapshots for all internally developed apps, with version pinning records. (4) Any prior MDM policy documents to establish baseline gap for audit trail.

Step 3: Update threat model — add commercial surveillance vendor access to RTB data streams as a passive collection threat against high-value personnel; incorporate T1430 (Location Tracking) and T1597 (Search Closed Sources) into your threat register with Webloc and comparable platforms as representative tooling

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: threat modeling updates and threat register maintenance are foundational preparation activities ensuring detection and response capabilities are scoped to current threat actor TTPs

Controls: NIST RA-3 (Risk Assessment) — formally document RTB-sourced commercial surveillance (specifically Webloc/Penlink, Tangles/Penlink, and comparable data broker platforms) as a threat source in organizational risk assessments, NIST RA-10 (Threat Intelligence) — integrate Citizen Lab reporting on Webloc and RTB surveillance pipelines as a named CTI source; update threat register with MITRE ATT&CK T1430 (Location Tracking) and T1597 (Search Closed Sources), NIST IR-4 (Incident Handling) — update incident handling procedures to include a category for passive surveillance-as-a-service affecting personnel operational security, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a subscription to Citizen Lab, EFF, and EPIC publications as authoritative advisory sources for RTB and commercial surveillance developments, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management scope to include third-party data broker and commercial surveillance platform exposure as a tracked risk class, not just CVE-based software flaws

Compensating: Use MITRE ATT&CK Navigator (free, browser-based at https://mitre-attack.github.io/attack-navigator/ — verified canonical URL) to create a mobile threat layer annotating T1430 (Location Tracking) and T1597 (Search Closed Sources) with Webloc/Penlink as named procedure entries. Export the layer as JSON and commit to your threat register repository. For threat register tooling on zero budget, use a structured YAML or JSON file in a private Git repo with fields: threat_actor, platform, technique_id, technique_name, data_source, detection_gap, risk_rating, and source_advisory (Citizen Lab DOI/URL). Review and update quarterly when Citizen Lab or equivalent publishes follow-on analysis.

Evidence: Capture before threat model update: (1) Current threat register or risk assessment document showing prior threat actor scope — establish a versioned baseline to demonstrate what was and was not previously accounted for. (2) Existing mobile security policy documents to identify gaps that did not contemplate RTB-sourced passive collection. (3) List of high-value personnel roles (executives, cleared contractors, sensitive ops staff) mapped to corporate device assignments — this inventory scopes the blast radius and justifies the threat model change. (4) Any prior vendor assessments or DPAs for advertising SDKs already embedded in your apps, to determine whether data broker resale was contractually prohibited.

Step 4: Communicate findings — brief leadership and legal counsel on the specific risk to named high-risk roles (executives, government contractors, sensitive operations personnel) whose device movements may already be available in commercial surveillance databases with up to three years of historical data

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: stakeholder communication and lessons-learned reporting apply here because the historical data exposure (up to 3 years per Citizen Lab findings) constitutes a retrospective incident requiring executive notification and legal review even without an active breach event

Controls: NIST IR-6 (Incident Reporting) — report findings to leadership and legal counsel consistent with organizational incident reporting timelines; the historical MAID location data exposure meets the threshold for internal incident notification, NIST IR-4 (Incident Handling) — execute the communication and coordination components of the incident handling capability, including briefing organizational leadership on scope, impact, and named threat platforms (Webloc, Tangles), NIST IR-8 (Incident Response Plan) — validate that the IR plan includes escalation paths for privacy-impacting surveillance threats affecting personnel, not just technical system compromises, NIST AC-1 (Access Control Policy and Procedures) — brief legal counsel on policy gaps enabling MAID-based tracking of corporate-device users and the need for updated acceptable use and device policy language, CIS 3.2 (Establish and Maintain a Data Inventory) — provide leadership with a concrete data inventory showing which personnel roles are exposed and what

data types (MAID, GPS coordinates, device fingerprint) are available in commercial RTB data broker pipelines

Compensating: Prepare a one-page executive brief using public Citizen Lab findings (doi.org/10.33412/apd.2024 — note: verify this DOI directly against Citizen Lab's published report; treat as search-retrieved and confirm before distribution) as the authoritative source. Structure the brief around: (1) named platform — Webloc operated by Penlink, drawing on RTB ad auction data; (2) named agencies — ICE, DHS, military use without warrant per Citizen Lab; (3) historical exposure window — up to 3 years of location history available in commercial databases; (4) named affected populations — executives, cleared personnel, sensitive ops roles on devices running apps with RTB SDKs. Use no-cost secure document sharing (Signal's note-to-self, encrypted email via ProtonMail) for brief distribution to minimize secondary exposure of the sensitive personnel list.

Evidence: Capture before the leadership brief: (1) Citizen Lab's published analysis of Webloc/Penlink as the primary sourcing document — download and archive the PDF with hash verification (sha256sum) to establish an unaltered evidentiary copy. (2) A personnel roster (handled under strict access control) mapping high-risk roles to corporate device assignments and app usage, to concretely bound the affected population for legal counsel. (3) Any existing contractual language with advertising SDK vendors or data brokers governing data resale and government access — legal counsel will need this to assess breach of contract or regulatory exposure. (4) Documentation of whether your organization falls under any sector-specific privacy regimes (HIPAA, FERPA, ITAR/EAR, state privacy laws) that may trigger notification obligations given the personnel profile.

Step 5: Monitor developments — track Citizen Lab follow-up publications, FTC and congressional responses to Webloc disclosure, and any litigation or regulatory action targeting the RTB data broker ecosystem for downstream surveillance use restrictions

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: ongoing threat landscape monitoring and policy environment tracking are core post-incident functions that feed back into preparation and threat model updates for the RTB surveillance threat class

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal process for receiving and acting on advisories from Citizen Lab, FTC, and congressional sources regarding RTB surveillance and commercial data broker regulation, NIST RA-10 (Threat Intelligence) — integrate regulatory and litigation developments in the RTB data broker space as threat intelligence inputs; FTC enforcement actions or court injunctions against Penlink/Cobwebs could affect the platform's data access and signal broader industry changes, NIST IR-5 (Incident Monitoring) — treat the Webloc/RTB surveillance exposure as an open incident entry; track and document regulatory and legal developments as status updates until formal closure criteria are met, NIST CA-7 (Continuous Monitoring) — implement a lightweight continuous monitoring process for this threat class: weekly review of Citizen Lab, EFF, EPIC, and FTC enforcement feeds, CIS 7.2 (Establish and Maintain a Remediation Process) — tie monitoring outputs to a remediation backlog: each new Citizen Lab finding or regulatory action should trigger a review of whether SDK removal, policy update, or personnel notification steps need to advance

Compensating: Configure free RSS/Atom monitoring using Feedly free tier or a self-hosted FreshRSS instance (free, Docker-deployable) subscribed to: Citizen Lab blog feed (citizenlab.ca/feed — verify against citizenlab.ca directly), EFF Deeplinks (eff.org/rss/updates.xml), FTC news (ftc.gov/news-events/rss.xml — canonical government domain). Create a shared Markdown log file in a private Git repo with dated entries for each relevant development, linked to source URL, and a field for 'IR action triggered: yes/no'. For automated alerting, use Google Alerts (free) with queries: 'Penlink Webloc', 'Cobwebs Technologies', 'RTB surveillance warrantless', 'FTC data broker enforcement'. Review the alert digest weekly and escalate any FTC enforcement action or new Citizen Lab publication within 24 hours to legal counsel.

Evidence: Capture for ongoing monitoring record: (1) A versioned log of all Citizen Lab, FTC, and congressional actions related to Webloc/Penlink and RTB surveillance, with dates and hashed archive copies of source documents — this constitutes the evidentiary record if regulatory inquiry later asks when your organization became aware of the risk. (2) Records of each internal review cycle — date, reviewer, findings, and any triggered actions — to demonstrate due diligence. (3) SDK and MDM policy version history showing that remediation steps from Steps 1-4 were implemented and when, so monitoring findings can be mapped against remediation state. (4) Any communications from advertising SDK vendors or data broker partners responding to your policy inquiries — inbound silence or deflection is itself a risk signal worth documenting.

Detection Guidance

Traditional endpoint and network detection does not apply here, Webloc operates outside the target organization's infrastructure entirely. Detection and mitigation efforts should focus on three areas.

Personnel exposure auditing: Identify roles with elevated sensitivity (executives, government contractors, personnel with access to classified or sensitive operations, incident response leads). For corporate-issued iOS devices, verify that Limit Ad Tracking or equivalent advertising identifier restrictions are enforced via MDM policy. For Android, verify GAID opt-out or reset policies. Devices with persistent MAIDs and location services enabled for ad-supported apps are the attack surface.

App and SDK inventory: Review mobile applications developed or deployed by your organization for embedded advertising SDKs that participate in RTB auctions. Common RTB-participating SDKs include those from major ad exchanges. If your app monetizes via programmatic advertising, your users' MAIDs and location data are likely in the RTB stream. This is a supply chain data exposure question, not a compromise question.

Policy gap audit: Evaluate whether your organization's privacy policy, employee mobile device policy, or contractor agreements address advertising identifier tracking. Identify whether any internal apps or third-party apps on corporate devices include RTB-participating SDKs. Review whether your jurisdiction's privacy regulations (state comprehensive privacy laws, GDPR if applicable) impose obligations on your use or facilitation of MAID-linked location data collection.

There are no network IOCs associated with Webloc targeting your infrastructure. The threat is passive collection against your personnel from the outside. The hunting question is not 'are we compromised' but 'are our people trackable.'

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Webloc (Penlink / Cobwebs Technologies)`	Commercial ad-based geolocation surveillance platform ingesting MAIDs and location signals from RTB ad auctions to enable retrospective location tracking of approximately 500 million mobile devices without judicial authorization; attributed to ICE, DHS, U.S. military, Hungary, and El Salvador law enforcement by Citizen Lab	HIGH
TOOL	`Tangles (Penlink)`	Companion Penlink platform referenced alongside Webloc in Citizen Lab analysis; specific capability scope not fully detailed in available source material — refer to Citizen Lab primary report for complete platform characterization	MEDIUM

Type	Value	Context	Confidence
URL	`Pending — refer to Citizen Lab primary report (citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/) for published indicators and technical artifacts`	Citizen Lab analysis may include technical indicators, infrastructure references, or platform identifiers not reproduced in secondary sources; primary report should be consulted for complete indicator set	LOW

Framework Mappings

MITRE-ATTACK

- **T1325**
- **T1589** — Gather Victim Identity Information
- **T1430** — Location Tracking
- **T1598** — Phishing for Information
- **T1597** — Search Closed Sources
- **T1596** — Search Open Technical Databases
- **T1593** — Search Open Websites/Domains

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SR-2** — Supply Chain Risk Management Plan

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1325		
T1589	Gather Victim Identity Information	Reconnaissance
T1430	Location Tracking	Collection
T1598	Phishing for Information	Reconnaissance
T1597	Search Closed Sources	Reconnaissance
T1596	Search Open Technical Databases	Reconnaissance
T1593	Search Open Websites/Domains	Reconnaissance

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/citizen-lab-law-enforcement-used-...	T3
Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation ...	https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geoloc...	T3
Is Webloc Coming to Your Neighborhood? - GoDark Faraday Bags	https://godarkbags.com/blogs/post/is-webloc-coming-to-your-neighbor...	T3
This Nebraska company is supplying ICE with surveillance tech	https://flatwaterfreepress.org/this-nebraska-company-is-supplying-i...	T3
[PDF] FOIA Request – Records regarding the District's use of Cobwebs ...	https://www.acludc.org/app/uploads/2025/08/8.5.2025-FOIA-Request-Co...	T3

Generated 2026-04-11 06:12 UTC by TJS Security Command Center