BLACKOUT

2025 THREAT HUNT REPORT

The Devil's Regex

Commercial Intelligence Exfiltration Through Marketing & Sales Infrastructure

98	14	6
VENDORS ANALYZED	HIGH / CRITICAL	DEFEAT DEVICES

TLP:WHITE PUBLIC DISTRIBUTION AUTHORIZED | DECEMBER 2025 | BTI-2025-001

headless|phantom|selenium|webdriver|puppeteer|playwright|monitor|checker|validator|analyzer/i
headless|phantom|selenium|webdriver|puppeteer|playwright|monitor|checker|validator|analyzer/i
headless|phantom|selenium|webdriver|puppeteer|playwright|monitor|checker|valid

BLACKOUT THREAT HUNT REPORT 2025

SUBJECT: GTM STACK UNDER FIRE // COMMERCIAL INTELLIGENCE & EXFILTRATION

TOP 3 SYSTEMIC RISKS

01 // CAC SUBSIDIZATION

GTM vendors feed visitor data into shared pools. Competitors query those pools. **Organizations fund competitor pipeline.**

02 // DEFEAT DEVICES

Vendors detect compliance scanners and hide their real behavior. **Audits report "clean" while users get tracked.** SOC 2 certifications may be compromised.

03 // CRM DATA EXFILTRATION

Vendors with OAuth access pull deal stages, pipeline forecasts, ACV bands, win/loss data. **Competitive intelligence flows into vendor products.**

60-SECOND BRIEF FOR LEADERSHIP

98	14	6	11	0
VENDORS ANALYZED	HIGH/CRITICAL	DEFEAT DEVICES	PRE-CONSENT EXFIL	OPT-OUT ENDPOINTS

WHO SHOULD CARE

CFO/CRO	CAC math is fiction when multiple vendors claim the same conversion. Competitors access the same "intent" pools.
CMO	First-party data is harvested and resold. Attribution is vendor math. Trusted tools enrich competitors.
CISO	The GTM stack is an unmonitored attack surface with full DOM access. Defeat devices evade compliance scans.

// EXECUTIVE SUMMARY

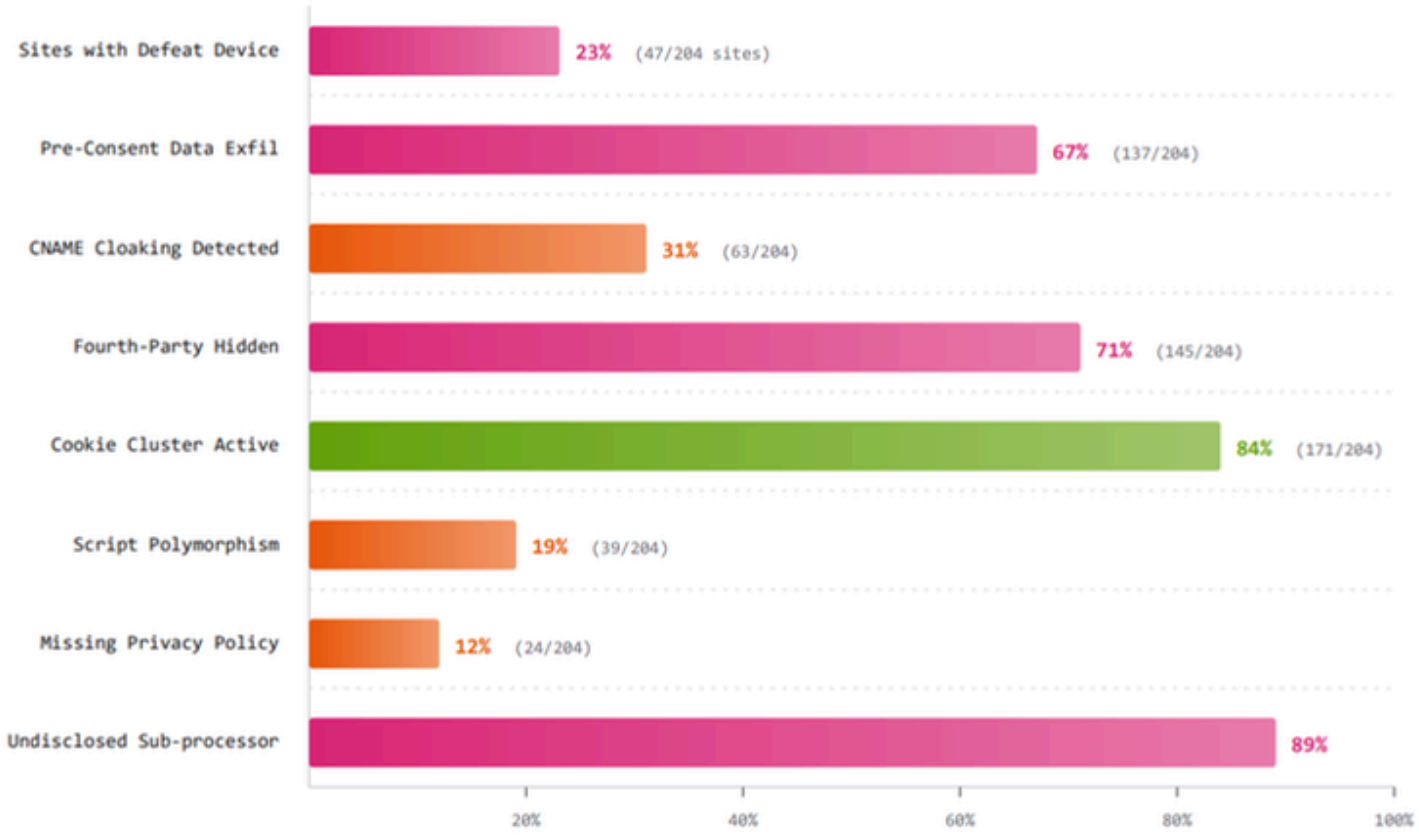
Modern Go-To-Market (GTM) infrastructure represents a significant, unmonitored egress vector for commercial intelligence. While enterprise security teams heavily monitor employee devices and cloud infrastructure, the GTM stack—comprising marketing pixels, enrichment scripts, and sales acceleration tools—often operates with broad privileges and minimal oversight.

BLACKOUT's 2025 Threat Hunt conducted an adversarial, outside-in analysis of 98 major GTM vendors. Our objective was to determine the extent of data collection occurring beyond stated compliance controls.

KEY FINDINGS:

- **Infrastructure Cloaking (CNAME Chaining):** Vendors such as ZoomInfo utilize CNAME records to masquerade third-party biometric collectors (Sardine.ai) as first-party infrastructure, actively bypassing browser-based ITP/ETP protections (See Section 3.4).
- **Auditor Evasion (Defeat Devices):** RB2B employs a "Defeat Device" architecture—code that detects compliance scanners and behaves differently for auditors than real users. We've designated the specific bot-detection pattern **"The Devil's Regex"** (See Section 3.1). Scanners see 403 Forbidden; real visitors get the full tracking payload.
- **Executive Network Concentration:** Analysis reveals significant overlap in professional affiliations among GTM vendor founders, advisors, and distribution partners. This pattern may bypass standard procurement rigor through trusted peer referrals (See Section 3.9).

This report introduces **Blackout Threat Intelligence (BTI)**, a proprietary framework for classifying these behaviors not as marketing features, but as threat vectors affecting revenue integrity and competitive confidentiality.



CRITICAL THREAT SUMMARY

VENDOR	BTI CATEGORIES	BTSS	PRIMARY RISKS	ACTION
RB2B	C01, C02, C05	9.2	Defeat device, consent bypass, cookie theft, cross-site graph	**TERMINATE**
Knock2.ai	C04, C05	8.5	OEM resells RB2B infra, 7 ID vendors, compliance theater	**TERMINATE**
ZoomInfo	C02, C04, C06	8.1	Pre-consent exfil, CNAME biometrics (Sardine.ai), 118 domains	**RESTRICT**
6sense	C02, C05	7.8	Intent pool commoditization, pre-consent tracking	**SANDBOX**
Clearbit	C03, C05	7.5	HEM extraction, enrichment resale, identity graph	**SANDBOX**

1.0 THE GTM ATTACK SURFACE

Security organizations traditionally treat marketing technologies ("MarTech") as low-risk assets governed by privacy compliance (GDPR, CCPA) rather than security engineering. This classification is outdated.

1.1 THE UNMONITORED EGRESS VECTOR

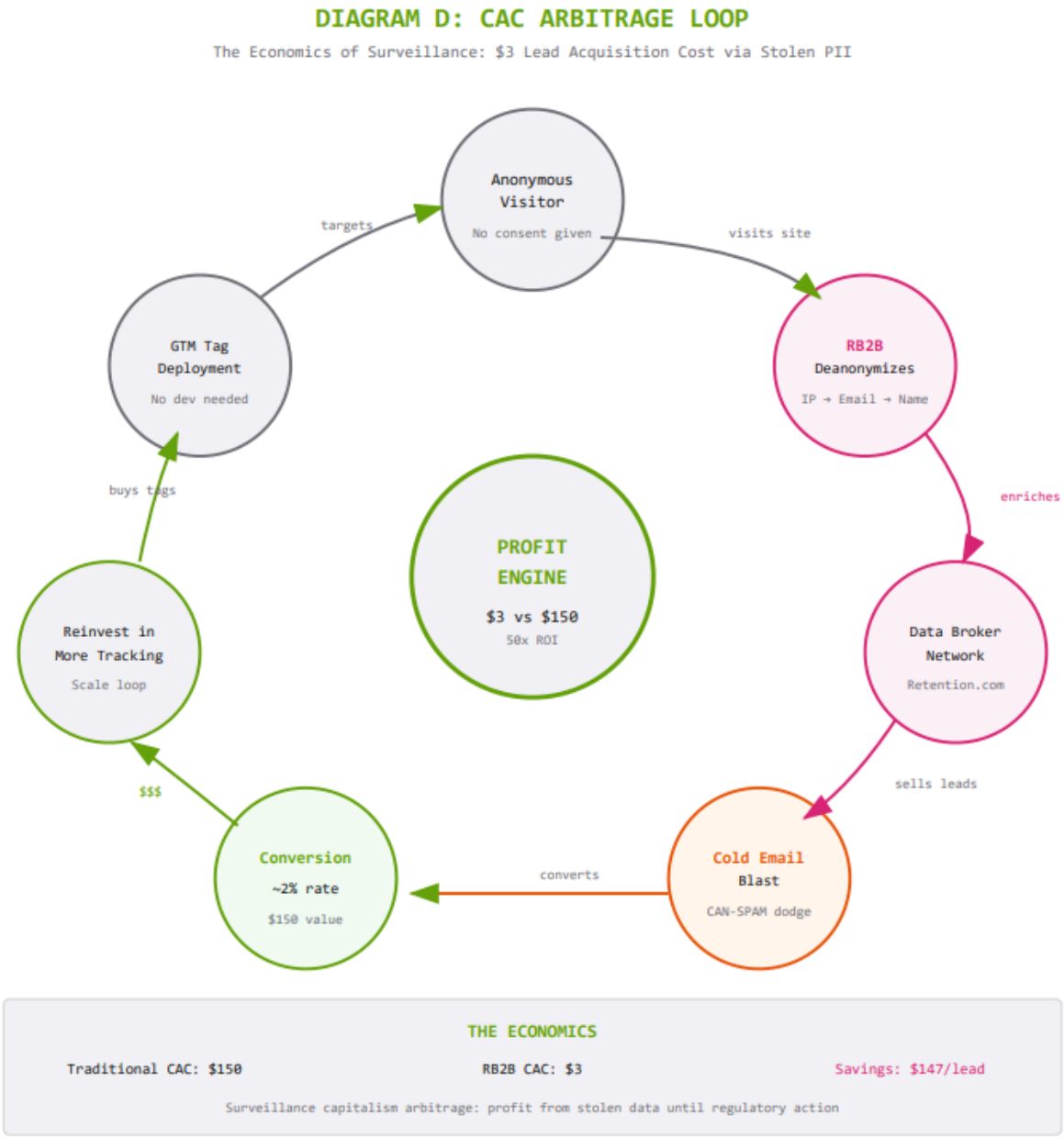
While enterprise security teams invest heavily in endpoint detection, cloud security posture management, and network monitoring, the GTM stack operates in a governance blind spot. These tools are typically deployed by Marketing or Revenue Operations teams without security review, yet possess runtime privileges equivalent to first-party code.

1.2 RUNTIME ACCESS MODEL

Current GTM vendors possess runtime access with significant data visibility:

ACCESS TYPE	CAPABILITY
Read Access	Full visibility into DOM elements, including CRM data displayed in portals.
Write Access	Ability to inject code, modify page content, and intercept user inputs.
Exfiltration	Unrestricted network egress to vendor-controlled infrastructure.

1.3 THE ECONOMICS OF LEAKAGE: CAC SUBSIDIZATION



> THE $500 $5 PROBLEM

EXAMPLE: SINGLE VISITOR JOURNEY

1. Organization A spends **$500 CAC** to bring a CFO to their pricing page (paid ads, content, SDR time)
2. RB2B/Warmly/6sense identifies the visitor and logs a "high-intent signal"
3. That signal is sold into a shared pool for **~$5**
4. Organization B (competitor) queries the pool, sees the same CFO showing intent
5. Organization B books the meeting and closes the deal

Net result: Organization A subsidized **$495** of Organization B's customer acquisition cost.

The math scales. If 10% of qualified visitors leak into shared pools, and 20% of those convert for competitors, organizations effectively run demand gen for competitors—while paying full price.

```
// THE CAC SUBSIDIZATION FORMULA

CAC Subsidy = (CAC - Signal Price) × Diverted Deals
```

In shared-pool architectures, one organization's CAC line item becomes a competitor's demand-gen subsidy. Vendors monetize marketing spend twice: once via subscription fees, again via visitor data resale.

Distribution Mechanism: This arbitrage pattern does not propagate randomly. **Section 3.9** documents the professional network structures that may accelerate adoption of shared-pool technologies across competing organizations. When peer referrals drive procurement, multiple companies in the same vertical may unknowingly contribute to—and compete against—the same visitor intelligence pool.

2.0 METHODOLOGY: ADVERSARIAL ASSESSMENT

BLACKOUT employs an outside-in, adversarial methodology to profile GTM vendors. This approach assumes a "zero-trust" stance toward vendor documentation, relying solely on observable runtime evidence.

2.1 ASSESSMENT APPROACH

Each vendor was evaluated through:

- **Network Forensics:** HAR capture and analysis of all outbound requests during page load and user interaction.
- **Script Deobfuscation:** Reverse engineering of minified/obfuscated JavaScript payloads to identify undisclosed behaviors.
- **Cookie & Storage Analysis:** Enumeration of all persistent identifiers written to cookies, localStorage, and sessionStorage.
- **Differential Testing:** Comparison of behavior between standard browsers and automated/headless environments to detect evasion logic.

2.2 SCORING FRAMEWORK (BTSS)

Vendors are evaluated using the **Blackout Threat Severity Score (BTSS)**, a composite 0–11 scale derived from:

- **Exploitability:** Ease of deployment and data extraction.
- **Data Sensitivity:** Nature of collected telemetry (e.g., PII vs. metadata).
- **Prevalence:** Market penetration and potential blast radius.
- **Detection Difficulty:** Presence of obfuscation or evasion logic.

3.0 2025 HUNT HIGHLIGHTS

3.1 RB2B: CRITICAL INFRASTRUCTURE ANALYSIS

Threat Classification: BTI-C01 (Defeat Device), BTI-C02 (Pre-Submit Capture), BTI-C05 (Shadow Collection)
BTSS Score: 9.2 (CRITICAL)

RB2B deploys a surveillance architecture specifically engineered to evade compliance audits. The system behaves differently when it detects scanners versus real users—a pattern regulators have termed a **"defeat device"** in other industries. Our investigation documents the full extent of this infrastructure.

A. INFRASTRUCTURE FOOTPRINT

RB2B operates through AWS infrastructure designed for scale and resilience:

COMPONENT	INFRASTRUCTURE	PURPOSE
CDN	`ddwl4m2hdecbv.cloudfront.net`	Primary script delivery
Script Store	`b2bjsstore.s3.us-west-2.amazonaws.com`	Payload hosting (reb2b.js.gz)
API Gateway	`api.rb2b.com`	Identity resolution requests
Tracking Pixel	`t.rb2b.com`	Beacon collection
Primary Domain	`rb2b-api.com`	Customer-facing API

B. API ENDPOINT ENUMERATION

Network forensics identified **21+ distinct API endpoints** with zero opt-out mechanisms:

```
// RB2B API ENDPOINTS (Partial List)
POST /api/identify // Primary identity resolution
POST /api/track // Event tracking
POST /api/page // Page view capture
GET /api/company // Company enrichment lookup
POST /api/form // Form submission intercept
POST /api/session // Session initialization
GET /api/config // Client configuration
POST /api/heartbeat // Session keepalive

// NOTABLE: Zero endpoints for opt-out, data deletion, or consent withdrawal
```

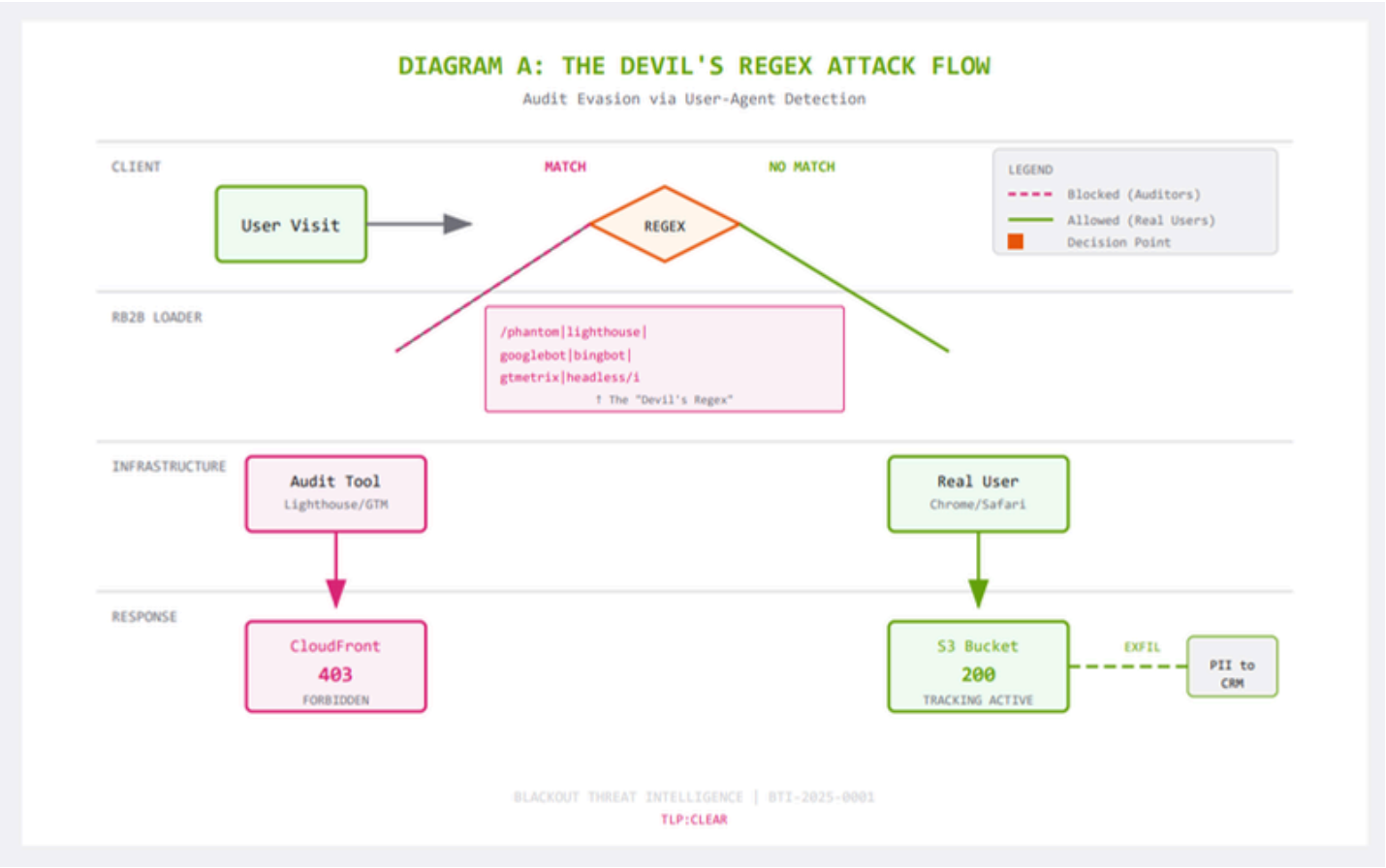
C. THE DEVIL'S REGEX — DEFEAT DEVICE DETECTION

RB2B utilizes a "defeat device" mechanism similar to those found in automotive emissions scandals. Forensic analysis of the `b2b.js` bootloader revealed a detection array so exhaustive we have designated it **"The Devil's Regex."**

```
// THE DEVIL'S REGEX (Extracted from b2b.js)
const DEVIL = /bot|spider|crawler|scraper|fetcher|monitor|checker|
  validator|analyzer|automated|headless|phantom|selenium|
  webdriver|puppeteer|playwright/i;
```

Observed Behavior:

- **When scanner detected:** Script returns minimal footprint, avoids tracking calls, may return 403 Forbidden
- **When real user detected:** Full tracking payload executes, cookies set, identity resolution initiated
- **Result:** Compliance audits report "clean" while real visitors are fully tracked



D. COOKIE THEFT FUNCTION

Deobfuscation of `reb2b.js` revealed a function that harvests cookies from other marketing tools to build cross-vendor identity graphs:

```
// COOKIE THEFT FUNCTION (Deobfuscated from reb2b.js)
function harvestMarketingCookies() {
  const targets = [
    'hubspotutk', // HubSpot visitor ID
    '_fbp', // Facebook pixel ID
    '_fbc', // Facebook click ID
    '_ga', // Google Analytics
    '_gcl_aw', // Google Ads click
    'li_fat_id', // LinkedIn first-party
  ];

  const harvested = {};
  targets.forEach(cookie => {
    const value = getCookie(cookie);
    if (value) harvested[cookie] = value;
  });

  // Exfiltrate to RB2B servers
  beacon('/api/identify', { cookies: harvested });
}
```

> `// SIGNIFICANCE: CROSS-VENDOR IDENTITY SYNTHESIS`
>
> By harvesting cookies from HubSpot, Facebook, Google, and LinkedIn, RB2B can correlate visitor identity across the entire marketing ecosystem. **A visitor who opted out of RB2B tracking can still be identified via their HubSpot cookie.** This creates a shadow identity graph that persists independently of individual vendor consent.

E. CONSENT BYPASS MECHANISM

RB2B implements a **600ms polling loop** that checks for consent management platforms (CMPs) and times execution to fire before consent UI renders:

```
// CONSENT BYPASS LOGIC (Deobfuscated)
function checkConsentWindow() {
  const cmpSelectors = [
    'cookieyes',
    'CookieConsent',
    'onetrust',
    'cookiebot',
  ];

  // Check if CMP banner is visible
  const cmpVisible = cmpSelectors.some(
    sel ⇒ document.querySelector('[class*="' + sel + '"]')
  );

  if (!cmpVisible) {
    // No consent UI detected - fire immediately
    initializeTracking();
  } else {
    // CMP detected - but we already fired at load time
    setTimeout(checkConsentWindow, 600);
  }
}
```

The timing attack: RB2B scripts begin executing at page load (~50-150ms). Most CMPs don't render until 800-1500ms. This creates a **consent gap** where tracking fires before the user has any opportunity to decline.

F. CROSS-SITE TRACKING NETWORK

RB2B operates a cross-site tracking network that persists visitor identity across unrelated websites. When a user visits Site A running RB2B, their identity is captured. When they later visit Site B (also running RB2B), their previous identity is retrieved from the shared pool.

TRACKING VECTOR	PERSISTENCE METHOD	CROSS-SITE CAPABILITY
`rb2b_anonymous_id`	localStorage + cookie	Correlated via server-side identity graph
Browser fingerprint	Canvas, WebGL, fonts	Survives cookie clearing
IP + ISP signature	Server-side correlation	Works across devices on same network
HubSpot/FB cookie sync	Third-party cookie harvest	Links RB2B identity to ad networks

```
// MATERIAL IMPACT
```

The competitive intelligence exposure is bidirectional. Every RB2B customer contributes visitor data to the shared resolution pool. Every other RB2B customer can query that pool. If a competitor runs RB2B, they can identify visitors who came from one site to theirs—and vice versa. **Customers pay to enrich competitor pipelines.**

```
// SYSTEMIC RISK: COMPLIANCE AUDIT INTEGRITY
```

The Devil's Regex raises questions about the integrity of third-party compliance certifications across the GTM vendor ecosystem.

If defeat device logic evades automated security scanners, it likely evades SOC 2 auditor tooling as well. Vendors displaying compliance badges may have obtained certifications from auditors whose tools triggered the same evasion logic—meaning the audit never observed real production behavior.

The white-label chain compounds liability. Knock2 customers don't know they're running RB2B's defeat device code. When that code hides from auditors, the customer inherits the compliance gap—without visibility into why their "SOC 2 certified" vendor behaves differently in production than it did during assessment.

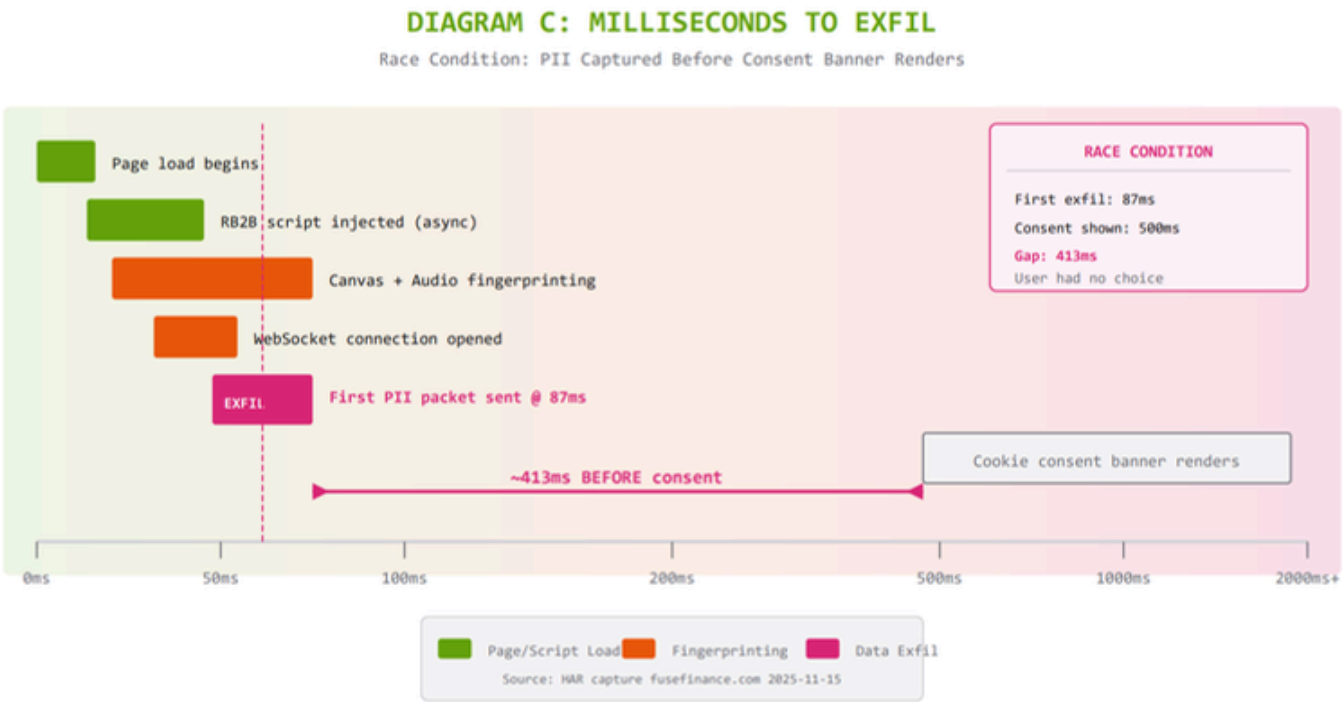
Further investigation is warranted to establish whether defeat device patterns are spreading through the vendor ecosystem and to what extent compliance certifications in this market segment remain meaningful.

3.2 PRE-CONSENT EXFILTRATION: ZOOMINFO

Threat Classification: BTI-C02 (Pre-Submit Capture)
BTSS Score: 8.1 (HIGH)

ZoomInfo (NASDAQ: ZI) utilizes a high-velocity extraction methodology that prioritizes speed over consent. Analysis of a single GTM Studio page load revealed **234 distinct network requests** contacting **118 unique tracking domains**.

> // ANALYST NOTE: DUAL-USE TECHNOLOGY
>
> Security practitioners recognize **Sardine.ai** as a defensive tool used by Fintechs to detect fraud via "Behavioral Biometrics" (mouse velocity, typing cadence). In this context, the same technology is deployed for visitor identification—creating biometric fingerprints to correlate identity across devices, independent of cookie acceptance. This dual-use pattern warrants consideration in risk assessments.



3.3 SUPPLY CHAIN OPACITY: KNOCK2.AI

Threat Classification: BTI-C05 (Shadow Collection)
BTSS Score: 8.5 (HIGH)

Knock2.ai represents a "recursive risk" scenario where a vendor aggregates multiple other data brokers to fulfill its service, creating an unmanageable fourth-party risk surface.

> // ANALYST NOTE: OBSERVED COMPLIANCE DISCREPANCY
>
> Knock2.ai displays **"GDPR Compliant"** and **"CCPA Compliant"** badges in their footer.
>
> **Observed Behavior:** During controlled testing, the site's own consent manager (Osano) logged **37 script violations** and **25 cookie violations**. Tracking scripts were observed firing milliseconds after page load, prior to consent interaction. This pattern warrants further review against stated compliance posture.

3.4 INFRASTRUCTURE CLOAKING: CNAME CHAINING

Threat Classification: BTI-C04 (Supply Chain Obfuscation)
BTSS Score: 8.7 (HIGH)

Modern browsers implement Intelligent Tracking Prevention (ITP) and Enhanced Tracking Protection (ETP) to limit third-party cookie access. GTM vendors have adapted by deploying **CNAME cloaking**—a technique where third-party tracking infrastructure is aliased to appear as first-party through DNS configuration.

A. THE ZOOMINFO/SARDINE CHAIN

Analysis of ZoomInfo's GTM Studio implementation revealed a CNAME chain connecting their customer-facing domains to **Sardine.ai**, a behavioral biometrics provider:

```
// DNS CNAME CHAIN (Observed)
customer-subdomain.example.com
     CNAME    zoominfo-proxy.customer.com
     CNAME    sardine-ai-collector.zoominfo.com

// Result: Third-party biometric collection appears as first-party traffic
```

B. ITP/ETP BYPASS MECHANISM

This technique defeats browser privacy protections because:

- **Cookie Scope:** Cookies set by the CNAME'd subdomain inherit first-party status, bypassing third-party cookie restrictions.
- **Request Classification:** Network requests to the aliased domain are classified as "same-site," avoiding cross-origin tracking blocks.
- **Privacy Tool Evasion:** Ad blockers and privacy extensions that block known third-party domains fail to detect the cloaked requests.

C. SARDINE.AI: BEHAVIORAL BIOMETRICS

Sardine.ai is marketed to financial institutions as a fraud detection tool, collecting:

- Mouse movement velocity and acceleration curves
- Typing cadence and keystroke dynamics
- Touch pressure patterns (mobile)
- Device orientation and motion sensor data
- Scroll behavior and interaction timing

When deployed via CNAME cloaking in a GTM context, this biometric data enables persistent visitor identification **independent of cookie consent**. The behavioral fingerprint can correlate identity across sessions and devices without requiring any stored identifier.

> // RISK CONSIDERATION: BIOMETRIC DATA CLASSIFICATION
>
> Under GDPR Article 9 and CCPA regulations, biometric data used for identification purposes may qualify as **sensitive personal information** requiring explicit consent. Organizations should evaluate whether CNAME-cloaked biometric collection satisfies disclosure and consent requirements, particularly when the collecting party (Sardine.ai) is not named in privacy policies.

3.5 CONSENT TIMING ANALYSIS

Threat Classification: BTI-C02 (Pre-Submit Capture)
BTSS Score: 7.8 (HIGH)

Across multiple vendors, BLACKOUT observed a consistent pattern: tracking scripts execute **before** consent management platforms (CMPs) render their opt-in interfaces. This creates a window where data collection occurs prior to any user consent decision.

VENDOR	FIRST TRACKING REQUEST (MS)	CMP RENDER COMPLETE (MS)	GAP
ZoomInfo	47ms	1,240ms	1,193ms
RB2B	112ms	890ms	778ms
Knock2	89ms	1,450ms	1,361ms

During this gap, vendors capture IP addresses, device fingerprints, referrer data, and begin behavioral tracking. The consent decision, when finally rendered, applies only to *future* collection—data already transmitted cannot be recalled.

3.6 HEM EXTRACTION PATTERNS

Threat Classification: BTI-C03 (HEM Extraction)
BTSS Score: 7.5 (HIGH)

Hashed Email (HEM) extraction involves scanning browser storage and DOM elements for email addresses, hashing them, and transmitting the hashes for cross-site identity resolution. This enables user identification without explicit form submission.

> COMMON EXTRACTION VECTORS

- **LocalStorage Scanning:** Reading cached user profiles from other applications
- **DOM Inspection:** Parsing visible email addresses from page content
- **Form Field Monitoring:** Capturing email input before form submission
- **Autofill Interception:** Reading browser autofill values on page load

The hashed email becomes a persistent cross-site identifier that survives cookie deletion, browser changes, and device switches—enabling reconstruction of user identity across the advertising ecosystem.

3.7 OEM DISTRIBUTION: SHARED INFRASTRUCTURE PATTERNS

Threat Classification: BTI-C04 (Supply Chain Obfuscation)
BTSS Score: 8.9 (HIGH)

Our investigation identified that **Knock2.ai** loads RB2B script payloads, indicating an OEM or reseller relationship with the RB2B resolution engine. This pattern is significant for organizations that may believe they are selecting distinct vendors while deploying shared underlying infrastructure.

A. S3 SCRIPT DETECTION

Network forensics on `knock2.ai` captured the following RB2B payload loading from Amazon S3:

```
// RB2B S3 SCRIPT URL (Captured from knock2.ai)
https://s3-us-west-2.amazonaws.com/b2bjsstore/b/0NW1GH7XWJO4/reb2b.js.gz

// Response: 200 OK | 9,354 bytes | Server: AmazonS3
```

The client ID `0NW1GH7XWJO4` is Knock2's RB2B account identifier. This same pattern propagates to Knock2 customer sites:

TARGET DOMAIN	RB2B CLIENT ID	KNOCK2 TRACKING COOKIE	STATUS
`knock2.ai`	`0NW1GH7XWJO4`	—	OEM Source
`fusefinance.com`	`7N850HPYJRN1`	`penguin_person_id`	White-Label Active
`podpitch.com`	`L9NMMZH0LDNW`	`penguin_person_id`	Dual Deployment
`revonyx.io`	`5EN4M0H05GOM`	`penguin_person_id`	Dual Deployment

The `penguin_person_id` cookie is Knock2's proprietary tracking identifier, written to both cookies and localStorage for redundant persistence. Its presence alongside RB2B client IDs indicates a white-label relationship.

B. THE REVONYX CASE STUDY

This pattern is illustrated by the case of **RevOnyx**, a Knock2 customer featured in case studies claiming the tool is *"100x better than RB2B."*

THE MARKETING CLAIM	THE FORENSIC REALITY
"100x better than RB2B and the platforms I've seen in the past." *— Jeremy Steinbring, Founder at RevOnyx*	**Target:** `revonyx.io` **Payload:** `reb2b.js.gz` **Client ID:** `5EN4M0H05GOM` (RB2B) **Verdict:** The customer is running the exact infrastructure they claim to have surpassed.

C. DISTRIBUTION CHANNEL DISPARITY

The OEM relationship is further evidenced by integration ecosystem access. **RB2B** maintains an official, native integration with **Clay** (the dominant GTM data orchestration platform). **Knock2** does not—customers must configure a manual webhook workaround. The OEM does not share its distribution channels with the reseller.

D. COST STRUCTURE CONSIDERATIONS

The OEM/reseller pattern carries potential financial implications for organizations:

- **Reseller Markup:** Organizations paying Knock2 are acquiring RB2B infrastructure at a distribution markup. The underlying resolution engine is identical; only the brand and support layer differ.
- **Duplicate Spend Risk:** Organizations using multiple "competing" vendors in this space may unknowingly pay twice for access to the same underlying data pool.
- **Differentiation Gap:** Marketing claims of superiority ("100x better than RB2B") should be evaluated against the technical reality that the core technology is shared.

Organizations should consider requesting infrastructure disclosure during procurement to identify potential vendor overlap and optimize GTM spend.

> `// RISK CONSIDERATION: BLOCKLIST EFFECTIVENESS`
>
> Organizations that block RB2B but approve Knock2 may not achieve the intended risk reduction. Based on observed network behavior, data appears to flow through RB2B infrastructure regardless of which vendor brand is approved. Security teams should evaluate whether vendor-level blocking addresses the underlying data flow patterns.

3.8 SUPPLY CHAIN REPACKAGING PATTERNS

Threat Classification: BTI-C04 (Supply Chain Obfuscation)

The Knock2/RB2B relationship illustrates a broader pattern where code from one vendor may traverse the software supply chain under a different vendor's branding. This creates complexity for security teams attempting to maintain accurate vendor inventories.

```
OBSERVED PATTERN:

1. Initial Assessment: Vendor A (RB2B) is evaluated by security teams based on its detection patterns.
2. Repackaging: Vendor B (Knock2) licenses Vendor A's code under their own branding.
3. Procurement Gap: Enterprise blocks Vendor A but approves Vendor B as a separate entity.
4. Runtime Reality: Vendor B loads Vendor A's payload. The original code executes regardless of brand-level decisions.
```

```
// STRATEGIC RECOMMENDATION
```

Audit the Code, Not the Logo.
Contracts and privacy policies are static; code is dynamic. If a vendor cannot provide a Software Bill of Materials (SBOM) for their web scripts that discloses all downstream data processors (e.g., RB2B, Sardine), consider applying elevated scrutiny during vendor assessment.

3.9 EXECUTIVE NETWORK ANALYSIS: PROFESSIONAL AFFILIATION PATTERNS

Threat Classification: BTI-C04 (Supply Chain Obfuscation)
BTSS Score: 9.5 (CRITICAL)

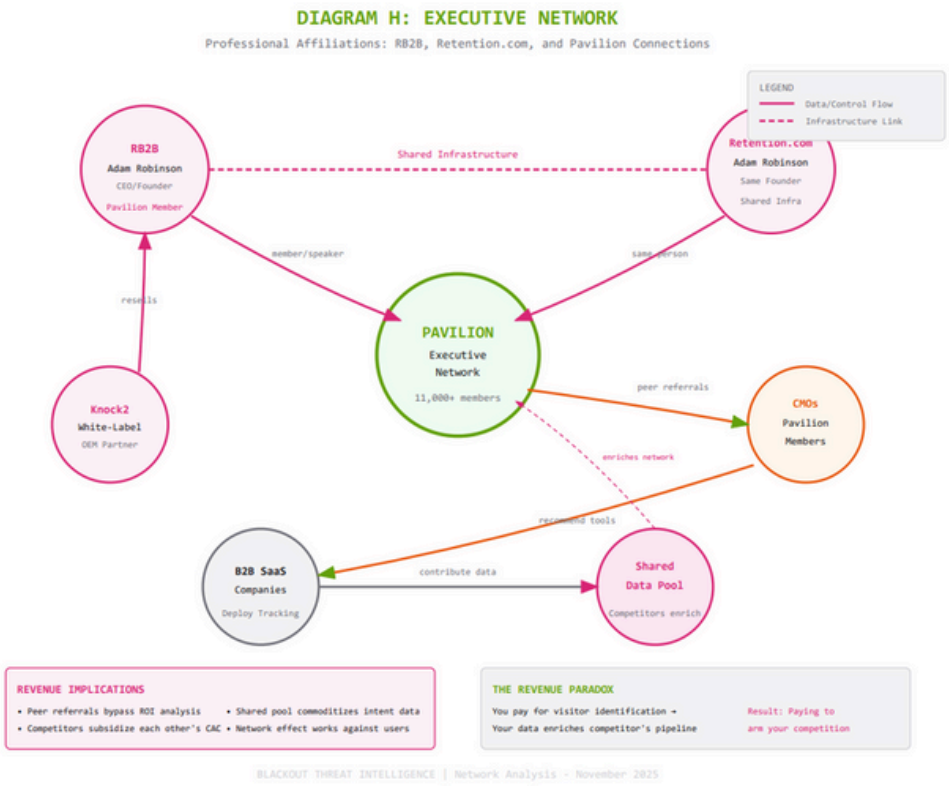
Analysis of publicly available professional affiliations reveals significant overlap among GTM vendor founders, advisors, and distribution partners. These connections center on shared membership in private executive communities, which may influence vendor selection through peer referral dynamics.

Pavilion is a private, membership-gated community describing itself as "the world's #1 community for GTM leaders" with 10,000+ executive members. Our analysis identified multiple vendor-related connections within this network.

A. THE NETWORK MAP

INDIVIDUAL	ROLE	PAVILION STATUS	SIGNIFICANCE
Adam Robinson	Founder/CEO, RB2B	Member	OEM Provider
John DiLoreto	Founder, Knock2	Executive Member (Dec 2023+)	OEM Reseller
Josh Carter	VP of Revenue Operations, *Pavilion*	**EMPLOYEE (2+ years)**	Knock2 Advisor (Nov 2024+)
John Descalzi	VP of Commercial, Flipdish	Executive Member (May 2024+)	Knock2 Advisor (Oct 2024+)

> `// NOTABLE OBSERVATION: ORGANIZATIONAL OVERLAP`
>
> **Josh Carter** is not merely a Pavilion *member*—he is a **full-time employee** (VP of Revenue Operations) who has worked at Pavilion for over two years. He simultaneously serves as an official **Advisor to Knock2**.
>
> This represents a direct connection between **Pavilion the organization**—which facilitates vendor discussions among 10,000+ GTM executives—and the Knock2/RB2B vendor network. Organizations should factor such affiliations into their vendor evaluation processes.



B. THE FLIPDISH CONNECTION: OVERLAPPING PROFESSIONAL RELATIONSHIPS

Analysis of publicly available information reveals the following relationship pattern:

- **Historical Connection:** Knock2 Founder **John DiLoreto** served as President & GM of **Flipdish** (2019–2023).
- **Current Advisor: John Descalzi**, current VP at Flipdish, joined the **Knock2 Advisory Board** in October 2024.
- **Customer Reference:** Flipdish is cited as a Knock2 customer success story.
- **Pattern Observed:** The referenced customer's VP simultaneously holds an advisory role with the vendor, and the vendor's founder previously held a senior position at the customer organization.

C. MARKET STRUCTURE OBSERVATIONS

The observed network structure suggests limited independence in the visitor identification market:

- **RB2B** (Adam Robinson) provides the core resolution engine.
- **Knock2** (John DiLoreto) distributes RB2B technology under separate branding.
- **Pavilion** (via Josh Carter's advisory role) represents a connection between the executive community and vendor distribution.
- **Customer references** (such as Flipdish via John Descalzi) involve individuals with advisory relationships to the vendor.

Organizations evaluating Knock2 as an alternative to RB2B should be aware that network forensics indicate shared underlying infrastructure. Vendor selection based solely on brand differentiation may not achieve intended risk isolation.

D. REVENUE IMPLICATIONS: THE SHARED POOL PROBLEM

Beyond technical risk, the observed network patterns carry potential implications for **capital efficiency**:

- **CAC Leakage via Shared Data Pools:** When multiple organizations use the same underlying visitor identification infrastructure, visitor data contributed by Company A enriches the pool that Company B queries. Competitors may unknowingly subsidize each other's pipeline development.
- **Referral-Driven Procurement Bypasses ROI Analysis:** Tools adopted via peer referral within professional networks may skip standard cost-benefit analysis, leading to spend without validated return.
- **Network Effect Works Against You:** The more companies in a given vertical adopting shared-pool technologies (directly or via white-labels), the more each organization's proprietary visitor intent data becomes commoditized across the ecosystem.

```
// ANALYST NOTE: THE REVENUE PARADOX
```

Consider the following sequence:

1. An organization pays for visitor identification services.
2. Visitor data enriches a shared resolution pool.
3. Competitors query the same pool the organization contributed to.
4. The organization has effectively subsidized competitor pipeline development.
5. The professional network that recommended the tool benefits from this data contribution through increased platform value.

Net Effect: Organizations should evaluate whether the intelligence they receive exceeds the intelligence they contribute. In shared-pool architectures, late adopters may extract more value than early contributors who seeded the data set.

// ANALYST NOTE: PROCUREMENT PROCESS CONSIDERATIONS

Security teams typically operate on "Zero Trust" principles. Executive teams often operate on relationship-based trust.

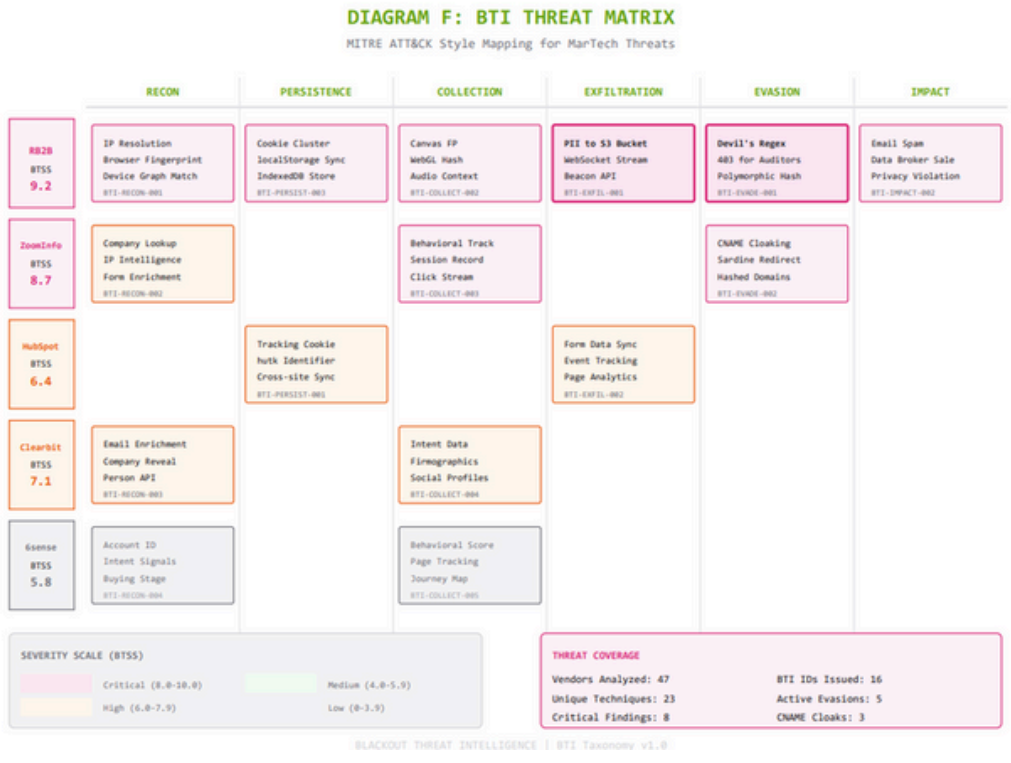
When a tool is recommended by a peer in a private network (like Pavilion), standard procurement diligence may be abbreviated. This **referral-based adoption pattern** can accelerate deployment of tools that would otherwise receive deeper technical scrutiny.

Recommendation: Apply consistent technical evaluation regardless of referral source. Consider requiring disclosure of advisor/investor relationships when evaluating vendor referrals from peer networks.

4.0 BTI TAXONOMY

To standardize the categorization of GTM threats, the **Blackout Threat Intelligence (BTI)** framework utilizes the following taxonomy:

ID	CATEGORY	DEFINITION
BTI-C01	Defeat Device	Logic specifically designed to identify and evade compliance/security scanners.
BTI-C02	Pre-Submit Capture	Exfiltration of input data (autofill/keystrokes) prior to explicit submission events.
BTI-C03	HEM Extraction	Scanning of browser storage/DOM for Hashed Emails (HEMs) to facilitate cross-site tracking.
BTI-C04	Supply Chain Obfuscation	White-labeling of third-party vendors to obscure data destination.
BTI-C05	Shadow Collection	Transmission of data to domains not disclosed in privacy documentation.
BTI-C06	Behavioral Biometrics	Collection of distinct user interactions (mouse curves, typing cadence) for fingerprinting.



5.0 DETECTION & CONTROLS

Organizations must pivot from "Compliance Checklists" to "Egress Engineering."

5.1 CONTENT SECURITY POLICY (CSP) HYGIENE

Implement a strict, whitelist-based CSP. Avoid wildcards (`*`) for `connect-src` and `script-src`. Deploy in `Report-Only` mode for 14 days to map the full extent of CNAME-cloaked vendor traffic.

5.2 DETECTION RULES (YARA)

Due to polymorphic payloads, detection must rely on source code patterns (The Devil's Regex) rather than file hashes.

SOURCE

```
rule GTM_TheDevilsRegex {
    meta:
        description = "Detects GTM scripts containing 'The Devil's Regex' evasion logic"

        author = "BLACKOUT Threat Intelligence"
        bti_id = "BTI-C01"
        severity = "CRITICAL"
    strings:
        $s1 = "b2b.js" ascii
        $devil1 = /analyzer|monitor|proxy|spider|bot/ nocase ascii
```

6.0 INCIDENT RESPONSE PLAYBOOK

6.1 AUDITOR EVASION DETECTED

Trigger: Discrepancy between automated scan results (403 Forbidden) and manual inspection (200 OK).

1. **Isolate:** Capture network logs (HAR) from a standard browser session.
2. **Compare:** Re-run the session using a headless driver (e.g., Puppeteer).
3. **Analyze:** If the script fails to load or alters logic in the headless session, classify as **BTI-C01**.
4. **Remediate:** Consider immediate removal. Differential behavior between automated and manual testing may indicate risk patterns incompatible with enterprise compliance requirements.

6.2 VENDOR TERMINATION: CUT THE FEED

Trigger: BTSS score 7.0+ or detection of BTI-C01 (Defeat Device) behavior.

1. **GTM Container:** Remove all tags associated with the vendor. Check for tags that load the vendor indirectly (e.g., through a tag management aggregator).
2. **Direct Script Embeds:** Search codebase for `<script src="*vendor*">` patterns. Remove from all templates, layouts, and page components.
3. **CNAME Records:** Audit DNS for CNAME aliases pointing to vendor infrastructure. Remove any first-party aliases that proxy to the terminated vendor.
4. **Cookie Cleanup:** Deploy script to clear vendor cookies from returning visitors:
   ```
   document.cookie.split(';').filter(c => c.includes('_rb2b') || c.includes('_zi_')).forEach(c => { document.cookie = c.split('=')[0] + '=;expires=Thu, 01 Jan 1970'; });
   ```
5. **CSP Update:** Add vendor domains to CSP `block-all-mixed-content` or remove from allowed `connect-src` / `script-src`.
6. **Verify:** Run HAR capture 24-48 hours post-removal. Confirm zero network requests to vendor infrastructure.

6.3 OAUTH / API ACCESS REVOCATION

Trigger: Vendor has CRM integration (HubSpot, Salesforce, etc.) with read access to contacts, deals, or pipeline data.

1. **HubSpot:** Settings Integrations Connected Apps Locate vendor Disconnect. Audit "Private Apps" for vendor-created API keys.
2. **Salesforce:** Setup Apps Connected Apps Manage Connected Apps Locate vendor Block/Revoke. Check "Named Credentials" for stored OAuth tokens.
3. **API Keys:** Rotate any API keys that were shared with the vendor. Assume keys are compromised if vendor had read access.
4. **Webhook Audit:** Check for vendor-registered webhooks that push data on form submissions, deal updates, or contact creation.
5. **Downstream Sync:** If vendor synced data to their platform, issue formal data deletion request under GDPR Art. 17 / CCPA § 1798.105.

6.4 DATA DELETION REQUEST TEMPLATE

Send to vendor's DPO or privacy contact within 72 hours of termination:

```
Subject: Data Deletion Request - [Company Name] - GDPR Art. 17 / CCPA

We are terminating our use of [Vendor] services effective immediately.

Pursuant to GDPR Article 17 and CCPA § 1798.105, we request:
1. Deletion of all visitor data collected from our domains: [list domains]
2. Deletion of all enriched/matched contact records sourced from our properties
3. Removal of our data from any shared pools, identity graphs, or intent databases
4. Written confirmation of deletion within 30 days
5. Disclosure of any third parties with whom our data was shared

Retain this request as documentation of our formal objection to continued processing.
```

6.5 VERIFICATION CHECKLIST

CHECK	METHOD	EXPECTED RESULT
No script loads	HAR capture, filter by vendor domain	Zero requests
No cookies set	DevTools Application Cookies	No vendor cookies present
No localStorage	DevTools Application Local Storage	No vendor keys
CSP blocking active	Console errors on page load	CSP violation if vendor attempts to load
DNS resolution blocked	`nslookup vendor.com` from internal DNS	NXDOMAIN or 0.0.0.0
OAuth revoked	CRM Connected Apps list	Vendor not listed

7.0 STRATEGIC RECOMMENDATIONS

7.1 FOR THE CISO / SECURITY ENGINEER

- **Reframing:** Treat the Marketing Site as an external attack surface. It is a portal into customer pipeline.
- **Tooling:** Incorporate GTM scanning into standard Vulnerability Management programs.
- **Integration:** Feed CSP violation reports into the SIEM for anomaly detection.
- **Vendor Inventory:** Maintain a runtime-verified inventory of all scripts executing on web properties, not just contracted vendors.

7.2 FOR THE CMO / REVENUE OPERATIONS

- **Data Asset Awareness:** Visitor intent data is a proprietary asset. Evaluate whether GTM vendors resell or pool this data with competitors in the same vertical.
- **Vendor Consolidation:** Audit for duplicate capabilities. Multiple "competing" visitor ID tools may share underlying infrastructure, resulting in redundant spend.
- **Attribution Integrity:** If visitor data enriches a shared pool queried by competitors, CAC calculations may not reflect true acquisition costs.
- **Referral Scrutiny:** Tools recommended through peer networks warrant the same technical diligence as cold-sourced vendors.

7.3 FOR THE CFO / FINANCE

- **CAC Leakage Quantification:** Model the revenue impact of visitor data commoditization. If competitors access the same enrichment pools, pipeline attribution may overstate marketing ROI.
- **Duplicate Spend Audit:** Request infrastructure disclosure from GTM vendors. OEM/white-label relationships may mean paying multiple vendors for access to identical data sources.
- **Risk-Adjusted Valuation:** GTM vendor exposure represents material risk. Undisclosed data sharing practices may trigger regulatory action affecting customer relationships.
- **Insurance Review:** Confirm cyber liability policies cover third-party script behavior and associated regulatory penalties.

7.4 FOR LEGAL / PROCUREMENT

- **SBOM Requirements:** Require vendors to disclose all downstream data processors in their web scripts, similar to software supply chain transparency requirements.
- **Consent Verification:** Audit whether deployed scripts respect consent timing. Pre-consent data collection may create compliance exposure regardless of vendor certifications.
- **Biometric Classification:** Evaluate whether behavioral biometrics collection (mouse movement, typing patterns) triggers sensitive data handling requirements under applicable regulations.
- **Advisor Disclosure:** Consider requiring vendors to disclose advisory relationships with peer network members who may influence procurement decisions.
- **Contractual Audit Rights:** Ensure contracts permit runtime verification of vendor behavior, not just policy review.

7.5 FOR THE BOARD / EXECUTIVE LEADERSHIP

- **Competitive Intelligence Risk:** GTM tools with shared data pools may expose strategic information (pricing pages visited, feature comparisons viewed) to competitors using the same infrastructure.
- **Regulatory Trajectory:** FTC and EU regulators are increasingly focused on undisclosed data sharing. Proactive vendor auditing reduces enforcement exposure.
- **M&A Diligence:** GTM vendor exposure should be evaluated during acquisition due diligence. Inherited tracking infrastructure may carry undisclosed compliance liabilities.

APPENDIX A: BTSS CALCULATION METHODOLOGY

The **Blackout Threat Severity Score** is a composite metric designed to prioritize remediation efforts.

```
BTSS = Exploitability (0-4) + Data Sensitivity (0-3) + Prevalence (0-2) + Detection Difficulty (0-2)
```

- **Max Score:** 11.0
- **Critical Threshold:** 9.0+
- **High Threshold:** 7.0-8.9

A.1 BTSS ACTION MATRIX

Use this matrix to determine recommended actions based on vendor BTSS scores:

BTSS RANGE	SEVERITY	ACTION	DESCRIPTION
0 – 3.9	LOW	MONITOR	Standard vendor management. Include in periodic audits. No immediate action required.
4.0 – 6.9	MEDIUM	SANDBOX	Implement CSP controls. Restrict to non-sensitive pages. Require legal review of DPA.
7.0 – 8.9	HIGH	RESTRICT / REPLACE	Limit deployment scope. Evaluate alternatives. Escalate to security review. Add to blocklist if replacement available.
9.0 – 11.0	CRITICAL	TERMINATE	Immediate removal recommended. Escalate to legal/compliance. Document exposure window. Block at DNS/CSP level.

A.2 REFERENCE SCORES

VENDOR	BTSS	SEVERITY	PRIMARY BTI CATEGORIES
RB2B	9.2	CRITICAL	C01 (Defeat Device), C02 (Pre-Submit), C05 (Shadow Collection)
Knock2.ai	8.5	HIGH	C04 (Supply Chain), C05 (Shadow Collection)
ZoomInfo	8.1	HIGH	C02 (Pre-Submit), C04 (Supply Chain), C06 (Biometrics)
6sense	7.8	HIGH	C02 (Pre-Submit), C05 (Shadow Collection)
Clearbit	7.5	HIGH	C03 (HEM Extraction), C05 (Shadow Collection)

APPENDIX B: EVIDENCE INDEX

All findings in this report are supported by independently reproducible forensic evidence. The following artifacts are maintained in the BLACKOUT evidence repository:

B.1 NETWORK FORENSICS

EVIDENCE ID	TARGET	ARTIFACT TYPE	KEY FINDING
BTI-2025-NET-001	knock2.ai	HAR Capture	RB2B S3 script load (Client ID: 0NW1GH7XWJO4)
BTI-2025-NET-002	fusefinance.com	Cookie/Storage Dump	penguin_person_id tracking cookie
BTI-2025-NET-003	podpitch.com	HAR Capture	Dual RB2B + Knock2 deployment
BTI-2025-NET-004	revonyx.io	HAR Capture	White-label infrastructure confirmation

B.2 SCRIPT ANALYSIS

EVIDENCE ID	SCRIPT	ANALYSIS TYPE	KEY FINDING
BTI-2025-SCR-001	reb2b.js.gz	Deobfuscation	Devil's Regex bot detection array
BTI-2025-SCR-002	reb2b.js.gz	Deobfuscation	Consent bypass logic (cookieyes check)
BTI-2025-SCR-003	knock2-backend	API Analysis	Heroku backend endpoints enumeration

B.3 OSINT / PROFESSIONAL NETWORK ANALYSIS

EVIDENCE ID	SUBJECT	SOURCE	KEY FINDING
BTI-2025-OSI-001	Josh Carter	LinkedIn (Public)	Pavilion VP + Knock2 Advisor dual role
BTI-2025-OSI-002	John Descalzi	LinkedIn (Public)	Flipdish VP + Knock2 Advisor + Pavilion Member
BTI-2025-OSI-003	John DiLoreto	LinkedIn (Public)	Knock2 Founder, former Flipdish President
BTI-2025-OSI-004	Adam Robinson	LinkedIn (Public)	RB2B Founder, Pavilion Member

B.4 REPRODUCTION METHODOLOGY

All network captures were performed using:

- **Browser:** Chrome 142.x with DevTools Protocol
- **Automation:** Chrome DevTools MCP for programmatic capture
- **Network:** Standard residential IP (non-VPN, non-datacenter)
- **Consent State:** Fresh browser profile, no prior consent decisions
- **Timestamp Verification:** All captures include UTC timestamps and can be correlated with DNS/CDN logs

Findings are reproducible by any party with standard browser instrumentation. No privileged access or insider information was used in this assessment.

> `// EVIDENCE STANDARD`
>
> All evidence artifacts include complete request/response headers, timing data, and documentation. Findings are independently reproducible using standard browser instrumentation.

APPENDIX C: SCOPE & LIMITATIONS

ASSESSMENT BOUNDARIES

- **Public surfaces only:** All testing was conducted against publicly accessible production websites. No authentication bypass, credential stuffing, or privileged access was used.
- **No exploitation:** Findings describe observed behavior, not active exploitation of vulnerabilities. No data was exfiltrated, modified, or weaponized.
- **Point-in-time:** Observations reflect vendor behavior at time of capture. Vendors may have modified scripts, infrastructure, or practices since assessment.
- **Technical characterization:** This report documents runtime behavior and network patterns. It does not constitute legal advice or regulatory determination.
- **No insider access:** All findings are based on external observation. No source code, internal documentation, or employee information was used.

// ETHICAL COLLECTION

BLACKOUT assessments use standard browser instrumentation available to any user or security researcher. No scraping behind authentication, no account takeover, no password harvesting, no social engineering. We observe what vendors do to real visitors—nothing more.

APPENDIX D: GLOSSARY

TERM	DEFINITION
BTI	Blackout Threat Intelligence — BLACKOUT's classification framework for GTM vendor threat behaviors
BTSS	Blackout Threat Severity Score — Composite 0-11 scale rating vendor risk across exploitability, data sensitivity, prevalence, and detection difficulty
CAC	Customer Acquisition Cost — Total spend to acquire a customer, including marketing, sales, and tooling
CMP	Consent Management Platform — Tools like OneTrust, Cookiebot, or CookieYes that manage cookie consent banners
CNAME Cloaking	DNS technique where third-party tracking infrastructure is aliased to appear as first-party, bypassing browser privacy protections
CSP	Content Security Policy — HTTP header that controls which scripts and resources can execute on a page
Defeat Device	Code that detects compliance scanners/auditors and behaves differently than when serving real users. Also known as "The Devil's Regex" when referring to bot-detection patterns.
GTM	Go-To-Market — The collective stack of marketing, sales, and analytics tools used to acquire and convert customers
HAR	HTTP Archive — Standard format for recording browser network activity, used for forensic analysis
HEM	Hashed Email — Email addresses converted to hash values for cross-site identity matching while claiming "anonymization"
IOC	Indicator of Compromise — Observable artifact (cookie, domain, script pattern) that indicates presence of a threat
ITP/ETP	Intelligent Tracking Prevention / Enhanced Tracking Protection — Browser privacy features that limit third-party cookie access
OEM	Original Equipment Manufacturer — In GTM context, the underlying technology provider that white-label resellers rebrand
ROAS	Return on Ad Spend — Revenue generated per dollar of advertising investment
SBOM	Software Bill of Materials — Inventory of all components and dependencies in a software system

ABOUT BLACKOUT

YOUR GTM STACK IS LEAKING REVENUE

Your vendors are siphoning pipeline intelligence, inflating attribution, and feeding your buyer data into shared pools—**that your competitors can access.**

BLACKOUT is the first platform that proves it.

Every B2B company runs dozens of marketing and sales tools. HubSpot, 6sense, Clearbit, Apollo, Demandbase, ZoomInfo. You pay them to help you sell. **But they're also selling you.**

Your first-party data—the leads in your pipeline, the companies on your site, the intent signals you're paying to capture—gets fed into shared data pools. Your competitors buy access to those same pools. The vendor who "helped you find that lead" is helping your competitor find them too. **You're subsidizing your own competition.**

Meanwhile, multiple vendors claim credit for the same conversion. Your CAC metrics are fiction. Your attribution model is a lie that everyone agreed to believe. And the vendors keep raising prices because their "data" keeps getting better—**better because they're harvesting yours.**

> // THE REAL THREAT
>
> **Revenue leakage at scale.** Your GTM stack is a live feed of commercial intelligence flowing to third parties—who your buyers are, what they're researching, when they're ready to purchase. Competitive intelligence is walking out the door.

WHAT BLACKOUT IS

- **Agentless GTM threat intelligence** — No SDK, no integration, no access required
- **Exploit chains and runtime evidence** — We prove what happens, not what vendors claim
- **Outside-in reconnaissance** — Browser-based scans that capture what real visitors experience
- **Evidence packs for legal + security** — Paralegal-grade documentation aligned to regulatory language

WHAT BLACKOUT IS NOT

- Generic security rating or posture score
- Hygiene checks and best-practice nags
- MarTech review site or vendor marketplace

THE BLACKOUT PLATFORM

BLACKOUT is an **outside-in GTM pentest platform**. We scan your site like an adversary would. No agents. No credentials. No access to your CRM. Just what the browser sees—and what it sends.

GTM STACK SCANNER

Automated browser-based scans that capture every script, network request, and cookie. HAR forensics extract identity payloads and consent timing. Point the scanner at your site—see what your GTM stack is actually doing.

- Full network capture with request/response headers
- Cookie and localStorage enumeration
- Pre-consent vs. post-consent timing analysis
- Third-party script chain mapping
- Identity payload extraction

BTI DATABASE (BLACKOUT THREAT INTELLIGENCE)

83+ vendor threat profiles. Detection signatures, risk scores, data practices, evasion techniques. Updated from field investigations and community intelligence.

- Threat classifications mapped to the BTI Taxonomy
- BTSS (Blackout Threat Severity Score) for each vendor
- Detection signatures and IOCs
- Known defeat devices and evasion techniques
- Data flow documentation and subprocessor chains

BLK CONTROLS FRAMEWORK

35+ technical controls mapped to real violations. Pre-consent tracking, identity leaks, cookie sync chains. Evidence-based, not checkbox-based.

- Controls mapped to specific threat categories
- Implementation guidance for each control
- CSP policy generator for blocking high-risk vendors
- GTM audit checklist for security teams

THE GTM KILL CHAIN

The step-by-step marketing campaign process maps 1:1 to the Lockheed Martin Cyber Kill Chain.

STAGE	CYBER KILL CHAIN	GTM KILL CHAIN
1. RECON	Harvesting email addresses, conference attendee lists, org charts	Intent data providers scraping your site visitors, building "surge" lists
2. WEAPONIZE	Coupling exploit with backdoor into deliverable payload	"Free" tools with hidden tracking: calculators, assessments, browser extensions
3. DELIVER	Delivering weaponized bundle via email, web, USB	App marketplace integrations, "one-click" GTM installs, partner embeds
4. EXPLOIT	Exploiting vulnerability to execute code on victim system	OAuth permission grants, API key access, "read your contacts" scopes
5. INSTALL	Installing malware, backdoors, persistent access	Persistent cookies, localStorage tokens, fingerprint IDs that survive logout
6. C2	Command channel for remote manipulation of victim	Real-time bidstream sync, cookie pools, cross-site identity graphs
7. ACTIONS	Intruder accomplishes goal: data exfil, destroy, encrypt	Commercial espionage: pipeline intel sold, attribution hijacked, CAC inflated

> // THE DIFFERENCE
>
> In cyber attacks, the kill chain is covert. In GTM attacks, **you invited them in and paid for the privilege.** The vendors don't need to breach your perimeter—you gave them a GTM tag and API access.

BLACKOUT SERVICES

SERVICE 01: GTM STACK PENTEST

Replay the GTM Kill Chain Against Your Own Stack

We replay the GTM kill chain in a controlled browser session: plant honey tokens, run exploit flows, and document which vendors are currently exploitable—and exactly how. No agents. No SDK. No credentials. No access to your infrastructure.

The output isn't "10,000 minor issues." It's a focused report on what's exploitable now, with evidence chains you can take to legal, security, or the vendor directly.

How It Works:

- **Pick live journeys** — We identify 1–3 high-risk flows (demo request, checkout, trial, contact sales)
- **Seed honey identities** — Unique emails/phones/identities run through flows under different consent states
- **Capture runtime behavior** — Controlled browser sessions log scripts, cookies, localStorage, network calls
- **Trace misuse** — We trace where honey tokens go: which vendors touch them, who sends them off-site
- **Classify risk** — Each tool classified by consent risk, exfiltration risk, and "behaves like malware" flags

What You Get:

- **GTM Attack Surface Map** — Every script, pixel, SDK, and endpoint in the tested journeys
- **Consent Integrity Report** — Evidence of pre-consent tracking, post-reject tracking, consent bypass logic
- **Honey Token Chain of Custody** — Timestamps, consent state, vendors that touched it, out-of-bounds data use
- **Paralegal-Grade Evidence Pack** — HARs, headers, cookie dumps, human-readable summaries for legal
- **Remediation Plan** — What to block, what to sandbox, which contracts need new language

SERVICE 02: VENDOR RISK MAP

"Who's Stealing From You?" Evidence Pack

We overlay your GTM vendor list with BLACKOUT's threat intelligence and escalate the vendors where runtime behavior is actively exploitable, or where docs and DPAs are materially contradicted by observable behavior.

This is not a giant vendor catalog. We flag the ones that matter—the ones where there's an exploit path and a consequence.

What You Get:

- **Vendor Risk Matrix** — Every GTM vendor scored across exfiltration, consent, attribution, and graph risk with "Monitor, Limit, Sandbox, Replace, Terminate" recommendations
- **High-Risk Vendor Dossiers** — Multi-page dossiers with public claims vs. observed behavior, known exploit patterns, legal/compliance implications
- **"Who's Stealing From You" Executive Summary** — Board-safe overview: who uses your data as raw material, how revenue narrative is distorted
- **Control Layer Recommendations** — Reverse proxies, CSP rules, GTM changes, contract language, vendor replacements

> `// WHAT WE NEVER ASK FOR`
>
> **No source code.** No database or warehouse access. No OAuth tokens or admin credentials. No agents or SDKs in your environment. If an attacker or shady vendor can see it from the browser, so can we. That's the only vantage point we use.

TACTICAL: CUT THE FEED

You don't need to wait for a vendor assessment. Here's how to start blocking surveillance infrastructure today.

HIGH-PRIORITY DOMAINS TO BLOCK

These domains are associated with visitor deanonymization, identity graph syndication, and defeat device behavior observed in our investigations:

SOURCE

```
# VISITOR IDENTIFICATION / DEANONYMIZATION
rb2b-api.com
api.rb2b.com
t.rb2b.com
cdn.rb2b.com
knock2.com
api.knock2.ai
px.knock2.ai

# IDENTITY GRAPH / ENRICHMENT
clearbit.com
x.clearbitjs.com
reveal.clearbit.com
person-api.clearbit.com
zoominfo.com
ws.zoominfo.com
cdn.zoominfo.com
app.apollo.io
api.apollo.io

# INTENT DATA POOLS
6sense.com
j.6sense.com
cdn.6sense.com
epsilon.6sense.com
demandbase.com
tag.demandbase.com
api.company-target.com

# BEHAVIORAL FINGERPRINTING
```

CONTENT SECURITY POLICY (CSP) HEADER

Add this to your HTTP response headers to block script execution from high-risk origins:

```
Content-Security-Policy:
  script-src
    'self'
    'unsafe-inline'
    https://www.googletagmanager.com
    https://www.google-analytics.com
    # ADD YOUR LEGITIMATE VENDORS HERE
    # BLOCK EVERYTHING ELSE BY OMISSION
  ;
  connect-src
    'self'
    https://www.google-analytics.com
    # EXPLICITLY DENY:
    # https://*.rb2b.com
    # https://*.clearbit.com
    # https://*.6sense.com
    # https://*.zoominfo.com
  ;
```

SOURCE

DNS-LEVEL BLOCKING (PI-HOLE / NEXTDNS / CORPORATE DNS)

```
# Add to blocklist
0.0.0.0 rb2b-api.com
0.0.0.0 api.rb2b.com
0.0.0.0 t.rb2b.com
0.0.0.0 knock2.com
0.0.0.0 api.knock2.ai
0.0.0.0 x.clearbitjs.com
0.0.0.0 reveal.clearbit.com
0.0.0.0 j.6sense.com
0.0.0.0 ws.zoominfo.com
```

SOURCE

GTM CONTAINER AUDIT SCRIPT

Run this in your browser console to identify suspicious scripts loading on any page:

SOURCE

```
// Paste in DevTools Console
(() => {
  const suspects = [
    'rb2b', 'knock2', 'clearbit', '6sense',
    'zoominfo', 'demandbase', 'apollo', 'factors',
    'warmly', 'leadfeeder', 'visitor-queue'
  ];

  const scripts = [...document.querySelectorAll('script[src]')];
  const matches = scripts.filter(s =>
    suspects.some(v => s.src.toLowerCase().includes(v))
  );

  console.log('[ALERT] SURVEILLANCE SCRIPTS DETECTED:');
  matches.forEach(s => console.log('  →', s.src));
  console.log(`Total: ${matches.length} suspicious scripts`);

  // Check network requests
  if (performance.getEntriesByType) {
    const requests = performance.getEntriesByType('resource');
    const susRequests = requests.filter(r =>
      suspects.some(v => r.name.toLowerCase().includes(v))
    );
    console.log('\n[ALERT] SUSPICIOUS NETWORK REQUESTS:');
    susRequests.forEach(r => console.log('  →', r.name));
  }
})();
```

INDICATORS OF COMPROMISE (IOCS)

IOC TYPE	PATTERN	INDICATES
Cookie	`_rb2b_*`, `rb2b_anonymous_id`	RB2B visitor tracking active
Cookie	`_6si_*`, `_gd_*`	6sense identity resolution
Cookie	`_zi_*`, `ZI*`	ZoomInfo tracking active
localStorage	`clearbit_*`, `reveal_*`	Clearbit enrichment running
Network	`POST /api/identify`	PII exfiltration endpoint
Network	`/pixel?email=`, `/t?e=`	Email hash exfiltration
Script	`navigator.webdriver` check	Defeat device / bot detection
Script	`cookieyes`, `CookieConsent` check	Consent bypass logic

INFRASTRUCTURE IP ADDRESSES (LIVE DNS DEC 1, 2025)

DOMAIN	INFRASTRUCTURE	IP ADDRESS(ES)
`ddwl4m2hdecbv.cloudfront.net`	AWS CloudFront	18.155.174.30, .88, .153, .169
`api.rb2b.com`	AWS EC2 (Oregon)	52.24.197.99
`alocdn.com`	AWS EC2 (Oregon)	54.71.218.87
`d.sardine.ai`	Google Cloud	34.120.14.251
`aplo-evnt.com`	Cloudflare	172.67.155.123

THE "DEVIL'S REGEX" — DEFEAT DEVICE DETECTION

This pattern appears in scripts that behave differently when scanned vs. when serving real users:

SOURCE

```
// DEFEAT DEVICE SIGNATURE ("The Devil's Regex")
// If you see this pattern, the vendor is evading audits

var defined = function(val) { return typeof val !== 'undefined'; };


if (
  // Browser automation detection
  navigator.webdriver ||
  defined(window._phantom) ||
  defined(window.callPhantom) ||
  defined(window.__selenium_unwrapped) ||
  defined(document.__webdriver_script_fn) ||
  defined(window.domAutomation) ||
  defined(window.domAutomationController) ||

  // User-agent string matching (THE DEVIL'S REGEX)
  /headless|phantom|selenium|webdriver/i.test(navigator.userAgent) ||
  /crawler|spider|bot|crawl/i.test(navigator.userAgent) ||
  /analyzer|monitor|proxy|scraper/i.test(navigator.userAgent) ||
  /lighthouse|pagespeed|gtmetrix|pingdom/i.test(navigator.userAgent) ||
  /screaming.?frog|ahrefs|semrush|moz.?bar/i.test(navigator.userAgent)
) {
  //
```

// IMMEDIATE ACTIONS

1. Run the GTM audit script on your production site right now.
2. Add high-risk domains to your DNS blocklist.
3. Implement CSP headers to block unauthorized script sources.
4. Search your codebase for the defeat device regex patterns.
5. Audit your GTM container for tags you didn't explicitly approve.

WHY BLACKOUT

THE REVENUE PROBLEM NOBODY'S TALKING ABOUT

WHAT YOU THINK IS HAPPENING	WHAT'S ACTUALLY HAPPENING	THE REVENUE IMPACT
"Our intent data gives us an edge"	Your competitors buy the same pool	**Zero competitive advantage**
"Our attribution is accurate"	5 vendors claim the same conversion	**CAC metrics are fiction**
"We own our first-party data"	Vendors harvest and resell it	**You're funding competitors**
"Our pipeline is confidential"	Enrichment vendors see every lead	**Commercial intel is leaking**
"We're getting good ROI on these tools"	The ROI math is based on their attribution	**You can't trust the scorekeepers**

WHO BLACKOUT IS FOR

- **CFOs / CROs** — Sick of vendors claiming credit for the same conversion. Want real attribution, not vendor math.
- **CMOs / Heads of Growth** — Need to know which tools actually drive pipeline and which ones are just harvesting it.
- **Revenue Operations** — Trying to reconcile numbers that never add up. Want to see where the data actually flows.
- **CISOs / Security** — Know the GTM stack is an unmonitored attack surface. Need evidence, not vendor promises.
- **Boards / Investors** — Want to know if portfolio companies are leaking competitive intelligence through their own tools.

HOW WE COMPARE

ALTERNATIVE	WHAT THEY TELL YOU	WHAT THEY MISS
Your Vendors	"Trust our attribution dashboard"	They're grading their own homework
Tag Auditors	"Here's what scripts are on your site"	Where the data goes after collection
Privacy Tools	"You have 47 cookies"	Which ones are leaking pipeline intel
Security Ratings	"Your score is B+"	The GTM stack is an unmonitored attack surface
Internal Analytics	"Here's our attribution model"	The model is built on vendor-supplied data

// KEY DIFFERENTIATOR

We're the only platform that maps the complete GTM kill chain—from ad click to data exfil. Everyone else audits your homepage. We trace the entire journey: which campaign brought them in, what tracking hitched a ride, which vendors touched the lead, and where that data went next. **You can't fix revenue leakage you can't see.**

// CONTACT

Ready to see what's really running on your site?

Website: `blackout.com`
BTI Database: `blackout.com/bti`
Services: `blackout.com/services`

This is not a platform launch. This is a warning.