



# FROM PROMPT TO PLATFORM:

//AI and the New Era of Executive Targeting

# // EXECUTIVE SUMMARY

In May 2025, 360 Privacy identified two mirror websites, [luigiwasright.com](https://luigiwasright.com) and [theceodatabase.com](https://theceodatabase.com), that published detailed personal and professional information on **23,273 executives across 1,083 companies**. The sites claimed to “hold executives accountable” for perceived corporate harms. 360’s Threat Team detected clear AI fingerprints: emoji-laden code comments, precise Unicode-to-header pairings, and a stripped-down template codebase that indicated a low-skill, machine-generated build. Through a methodical investigation combining metadata forensics, open-source tracing of a PayPal support link resolving to an active LLC in North Carolina, and high-fidelity behavioral footprint correlation, the team established a credible and direct attribution to a single actor. After activating its response playbook and coordinating with government channels, 360 Privacy aided in securing the takedown of both domains within 24 hours. This incident reflects a broader shift in threat dynamics: generative AI has already expanded the global pool of potential site builders from roughly **12.5 million to 75 million**, multiplying the threat landscape six-fold. In response, 360 Privacy has strengthened its monitoring framework to detect derivative infrastructure that reuses the same technical patterns or attribution markers. This helps establish a forward-looking industry precedent for detecting and neutralizing AI-enabled threat infrastructure at scale.

---

## STRATEGIC CONTEXT

Online dissent has evolved into operationalized exposure, where data publication is the primary weapon rather than protest rhetoric. AI toolchains and low-cost hosting now allow adversaries to turn a grievance into a fully indexed search platform within minutes. Social-media narratives cast senior executives as the human face of systemic failure, making them attractive pressure points. By blending open-source profiles with brokered B2B datasets, the operator behind [luigiwasright.com](https://luigiwasright.com) and [theceodatabase.com](https://theceodatabase.com) collapsed the barrier between corporate identity and private life. Search queries that once yielded news headlines now surface direct phone numbers and personal addresses. The pair of mirror sites therefore represents a scalable blueprint for future copycat campaigns.

---

## DATA EXPOSED ON THE SITES

- Executive names
- Mobile and work numbers
- LinkedIn URLs
- Job titles
- Company names and valuations

The collection displays a high-confidence enrichment footprint: phone headers, personal LinkedIn URLs, seniority tiers, and revenue bands match a documented export schema from a leading B2B contact database with 97% likelihood, indicating the data was copied wholesale rather than assembled manually.

By fusing professional identifiers with direct-contact vectors, the architecture collapsed the wall between corporate role and private life. What began as sentiment became infrastructure, and exposure became the mechanism for pressure and disruption. The pair of mirror sites therefore represent a scalable blueprint for future copy-cat campaigns.

---

## OPERATIONAL RISK FRAMING

**Visibility is vulnerability.** Publishing executive PII was the primary goal, not an accident.

**AI has tilted the threat equation.** Escalating hostility now meets a collapsing skill barrier, allowing minimally skilled adversaries to deploy capabilities once reserved for advanced threat actors.

**Narratives drive targeting.** Online escalation can migrate to the physical world when exposure is used as a tool of disruption.

---

## TECHNICAL ATTRIBUTION AND OBSERVATIONS

### 1. DOMAIN INFRASTRUCTURE


INDICATOR	EVIDENCE
Shared Hosting Environment	Both domains, registered on 6 April 2025 (luigiwasright.com) and 8 May 2025 (theceodatabase.com), were purchased through Namecheap and resolved to the same DigitalOcean IPv4 address. WHOIS entries were privacy-redacted, but the registrar-hosting congruence provided the initial linkage.
Structural Site Mirroring	The sites shared an identical navigation bar (Home, Search, About, Donate) and matched visual scaffolding. Content was mirrored verbatim, including a welcome message with an unusually high number of long dashes, a stylistic hallmark often seen in AI-generated prose, and an index of exactly 23,273 executives across 1,083 companies.
Embedded Contact Trail	The About Page listed luigiwasright.notifications@gmail.com as the administrator and routed financial donations to a PayPal page for No App Bans LLC. The Gmail address appeared in mailto link parameters on both domains, while the LLC's existence was confirmed through the North Carolina business registry.
Behavioral Attribution	Boolean Google queries surfaced two Facebook posts (1 May and 2 May 2025) from a user promoting luigiwasright.com. The personal Facebook account for the person of interest showed posts that referenced living near a hospital in North Carolina, membership and frequent posting in a Facebook group dedicated to a specific city in North Carolina, and educational history at a technical college.

INDICATOR	EVIDENCE
<b>Corporate Registration</b>	A Bizapedia search for “No App Bans LLC” yielded a record naming the same individual from the Facebook posts promoting luigiwasright.com in early May. North Carolina Secretary of State filings confirmed the formation of the LLC in February 2025 at a physical address located roughly half a mile from the referenced hospital on Facebook and the registered agent name matched the Facebook user promoting the website.
<b>Trust and Deed Cross-Match</b>	County deed archives linked the registered physical address to an irrevocable trust bearing the same individual’s name which also matched the name of the individual that posted luigiwasright.com on Facebook in early May. Multiple data-broker reports corroborated the match across name, address, and phone fields.
<b>Phone and Non-Profit Linkage</b>	Open-source research revealed the individual pled guilty to an assault on a police officer in 2015, appeared in the minutes for several municipal meetings in North Carolina spanning several years, and also served as an Executive Director for a local non-profit sharing the same registered physical address from the LLC filing. The associated Verizon mobile number observed with the Non-Profit record and various data brokers was a western North Carolina number with an area code of 828 and ending in 19 was verified as active via broker datasets and confirmed associated to the identified individual.
<b>Email Recovery Profiling</b>	Google account-recovery prompts for luigiwasright.notifications@gmail.com revealed recovery options tied to a ProtonMail alias beginning with the individual’s first 3 letters of her first name and the same phone number ending in 19, conclusively binding the email to the person of interest.

## ATTRIBUTION SUMMARY

This attribution sequence reflects layered digital tradecraft: infrastructure pivots (shared IP and registrar), contact-vector overlap (Gmail ↔ PayPal ↔ LLC), behavioral breadcrumbs (Facebook activity), registry artifacts (Bizapedia and North Carolina filings), and final confirmation through email-recovery telemetry and data-broker overlays. Each breadcrumb reinforced the chain of evidence, yielding a legally defensible, high-confidence identity match and enabling rapid escalation and takedown.

## 2. AI-BASED CONSTRUCTION

INDICATOR	EVIDENCE
Unnatural Code Comments	<!--  Moved empowerment line here --> embeds a Unicode icon inside an HTML comment, behavior typical of AI-generated code rather than human authorship.
Unicode-Icon Fingerprinting	Five interface labels (Browse A-Z, Advanced Search, Optional Fields, Contact Me, Contact Admin) use emojis that exactly match ChatGPT-4o's preferred tokens, creating a high-confidence 4o match.
Public Availability of GPT-4o	Since 30 April 2025, GPT-4o has been accessible on ChatGPT without authentication, allowing non-technical users to generate full site code at no cost; reliance on 4o rather than a paid model suggests a free account.
Ai-Style Code Layout and Comments	Folder structure, file names, and explanatory comments mirror ChatGPT's default scaffolding, progressing from high-level outline to specifics.
Choice of Infrastructure	Sites were hosted on Ubuntu with Nginx in a DigitalOcean droplet with public SSH, precisely the configuration GPT-4o returns when prompted for the simplest hosting path.

### ATTRIBUTION SUMMARY

All indicators confirm a start-to-finish generative-AI build that required little beyond basic hosting knowledge. Combining data from Evans Data, the Stack Overflow Developer Survey, and DigitalOcean suggests that about 12.5 million developers worldwide could have built such a site unaided; with low-barrier AI tools, that pool rises to roughly 75 million, widening the aperture for copy-cat platforms.

## 3. BUSINESS-TO-BUSINESS DATA DRIFT

The dataset behind the two sites was lifted almost verbatim from commercial B2B lead-generation feeds. The list turns a marketing asset into a doxxing kit by binding an executive's corporate identity to private contact channels. By combining firmographic attributes (job title, LinkedIn URL, company valuation) with direct personal identifiers, adversaries bypass traditional gatekeepers and deliver hostile content straight to executives' personal devices. Boards should treat the B2B data supply chain with the same rigor applied to consumer-data brokers, enforcing contractual redaction of personal fields and monitoring downstream resale.

---

## 4. REPORTING AND PLATFORM TAKEDOWN

360 Privacy filed high-fidelity reports with the registrar (Namecheap), the hosting provider (DigitalOcean), and U.S. government channels (CISA, FBI). Both sites were removed within 24 hours of escalation.

---

## 5. ONGOING MONITORING

360 Privacy continuously scans for clones or syntactically similar deployments by combining infrastructure matching, icon-mapping replication, and attribution-pattern recognition. The stance remains: identify, trace, report, and reduce exposure.

---

## KEY TAKEAWAYS FOR THE INDUSTRY

**The technical curve has flattened.** Anyone with intent and basic AI access can now spin up targeting platforms, expanding the pool of capable threat actors six-fold.

**Unicode-to-content mapping is a new fingerprint.** Token-to-icon models give defenders a fresh attribution method for AI-generated threat surfaces.

**Infrastructure fingerprints form a single signature.** Overlapping IP blocks, contact handles, payment rails, data-broker profiles, social-media breadcrumbs, and business filings interlock to puncture the veil of adversary anonymity.

**B2B datasets are becoming personal-exposure tools.** As commercial datasets embed personal email and mobile numbers, their value for targeting rises sharply.

**Digital exposure is a precursor, not a side effect.** These sites are engineered stages that amplify outrage, facilitate doxxing, and lower the threshold for real-world harm.

**Organizational security must include exposure intelligence.** Modern protection demands digital-footprint reduction, anticipation of adversarial AI use, and early detection of symbolic-targeting platforms.

---

## CONCLUSION

Our analysis shows a straightforward chain: a full export from a commercial B2B data broker was imported into a generative-AI code template and published almost unchanged. That one-step workflow: broker dump → AI-built site, removes the cost, skill, and time that once constrained this kind of exposure. The practical effect is clear: the number of people who can stand up a searchable doxxing platform has grown by roughly an order of magnitude. Executive-protection programs now need to treat broker datasets and AI-driven site generation as linked risk factors and adjust monitoring, takedown, and data-broker governance accordingly.



**// CONTACT US TODAY**  [info@360privacy.io](mailto:info@360privacy.io) | **STAY CONNECTED** |  **VISIT US** [360privacy.io](https://360privacy.io) |  **360 Privacy**