

**24 September, 2025**

**Re: *Deniability by Design: DNS-Driven Insights into a Malicious Ad Network (Vane Viper: Russia-Cyprus AdTech Nexus Delivering Malware)* - a hatchet piece by Infoblox, Inc.**

The acronym “FUD” stands for Fear, Uncertainty, and Doubt. It describes an unethical tactic where exaggerated, false, negative or misleading information is disseminated, in order to influence market sentiment for the personal gain of the publisher. The article “*Deniability by Design: DNS-Driven Insights into a Malicious Ad Network (Vane Viper: Russia-Cyprus AdTech Nexus Delivering Malware)*”, irresponsibly authored and published by Infoblox Inc. on 16 September 2025 (hereinafter - the “Defamatory Article”) is a textbook example of FUD. Indeed, by authoring and publishing this Defamatory Article, Infoblox has crossed the line, subjecting itself and the Defamatory Article’s authors to personal liability for defamation.

Propeller Ads and AdTech Holdings respond to the Defamatory Article as follows:

## **1. Overview**

The Defamatory Article contains numerous inaccurate, unfounded, and outright false allegations about us and our business. These allegations were either fabricated or derived from unverified sources and were intentionally authored and published with the sole intent of disparaging our reputation and creating unfounded fear, uncertainty and doubt in our organization, products and services.

Even though we have always remained open to engagement, Infoblox and the authors of the Defamatory Article made no effort to contact us for clarification, comment, or rebuttal prior to publication - ostensibly because Infoblox wanted to omit from the Defamatory Article critical information regarding our robust compliance framework and established anti-abuse mechanisms. Indeed, if Infoblox actually believed its own rhetoric, it would have abstained from making public statements designed to bring alleged network vulnerability to the attention of potential abusers.

Moreover, the highly unprofessional Defamatory Article contains multiple glaring errors, relies on the authors’ subjective assessments, as well as unchecked sources and outdated and inaccurate research.

Incredibly, in the Defamatory Article Infoblox disseminates and tries to give life to a term of its own invention - “Vane Viper.” The Defamatory Article is intentionally drafted so that the reader is left a false impression that the article reports on some sort of a long established recognized evil conspiracy. Nothing can be further from the truth, and the wording of the Defamatory Article suggests that Infoblox knows this.

In short, the Defamatory Article is intentionally authored so as to lead readers to form a false impression that we are engaged in unlawful activities - which could not be further from the truth.

One is left to wonder whether the more logical explanation for Infoblox's publication of the Defamatory Article is analogous to an anti-virus vendor spreading rumors about a non-existent virus in order to drive its own sales.

## **2. Who We Are, How We Operate, and Our Commitment to Quality**

We operate a technological platform that facilitates automated interactions between independent third-party advertisers and publishers. Each party independently establishes its own parameters for campaign execution or monetization, and we do not exercise control over, nor we maintain any form of affiliation with, either party in this commercial exchange. The role of the platform is strictly limited to automate the interaction, it does not create, direct, or influence the content, conditions, or commercial relationships entered into by users of the platform.

Our operations are conducted in strict accordance with internationally recognized standards. Our group proudly holds **ISO certification for Information Security Management Systems (ISMS), ISAE 3000**, and is a member of **IAB**. We have also passed **independent audits**, including the **ABC brand safety audit**, which specifically confirmed the strength of our advertising moderation standards.

Transparency is not an afterthought but a cornerstone of our business model. Across all our projects, the terms and conditions clearly set out the operating company's name, registration data, address, and contact details - all openly available resources. Our companies undergo annual IT audits by internationally respected and accredited auditors, and our operations are fully transparent to the international financial institutions we work with. Thousands of clients, including global brands, rely on our services and trust our integrity.

To support transparency and maintain platform integrity, we operate a publicly accessible abuse reporting mechanism (available at: <https://abuse.propellerads.com>), which allows any third party to submit complaints concerning prohibited content or tactics. All such submissions are subject to prompt review, and campaigns found to be in violation of applicable policies are swiftly blocked. This system reflects an industry-standard approach to accountability, quality assurance, and user protection.

In addition, we have developed and deployed advanced proprietary technologies, such as the platform available at [adex.com](https://adex.com), specifically designed to detect and prevent fraudulent activity, including bot traffic and invalid ad impressions. These measures reflect a strong and ongoing commitment to maintaining the integrity and security of the digital advertising ecosystem. You may read about various successful fraud prevention cases on the company's blog at <https://adex.com/blog/>

It must also be emphasized that the threat landscape in digital advertising evolves continuously. Malicious cloaking techniques and fraudulent tactics are increasingly sophisticated, and even the largest and most well-resourced platforms - including Google and Meta - have acknowledged the impossibility of achieving absolute fraud prevention. Nonetheless, we devote substantial resources each year to content moderation, abuse detection, and fraud prevention measures, demonstrating a sustained and proactive commitment to platform security.

Our technologies and practices in combating fraud and cloaking are on par with the world's most prominent industry players. We continuously invest substantial resources into moderation and fraud prevention, ensuring that our clients benefit from the same level of safety and quality expected from the global leaders of digital advertising (<https://propellerads.com/blog/adv-banned-ad-campaigns-2024/>).

### **3. Fake Claims and Misrepresentation of Our Work, Our Products and Our Services**

**False Narrative Built on Circumstantial Details.** The Defamatory Article intentionally constructs a false narrative based on superficial elements such as shared contractors, registrars, or public records in order to mislead. As Infoblox surely knows, it is common for multiple companies to use the same vendors or infrastructure providers. Such coincidences do not prove ownership, control, or affiliation and certainly do not prove or even suggest improper business practices.

**Reliance on Outdated and Discredited Sources.** The Defamatory Article also employs obsolete references and alleged corporate links that simply do not exist. The structures depicted are fabrications that do not reflect our group's reality and are based on contrived associations rather than facts. Resurrecting such false narratives undermines trust and indicates an intent to sensationalize rather than to inform. It is even likely that much of this narrative was assembled in a manner resembling AI-generated content, recycling outdated claims without factual progression.

**Misrepresentation of Our Technology.** The Defamatory Article also misrepresents our technology. Our platform's logic is public and transparent: advertisers and publishers define campaign conditions, while our technology ensures automation, quality, and safety. All technologies we use, including push notifications, landing pages, traffic distribution systems (TDS), and other industry-standard tools, are legitimate, widely recognized, and openly applied across the global advertising ecosystem. Suggesting otherwise not only misinterprets our work, but also shows a lack of understanding of how modern digital advertising actually operates.

**Mischaracterization of Infrastructure.** The Defamatory Article further misrepresents the technical aspects of our infrastructure. All our domains are lawfully acquired from official ICANN-accredited registrars at prevailing market rates. DNS queries directed to our servers occur as part of the normal and lawful operation of our advertising technology, and are essential to ensuring service reliability and performance for publishers and advertisers. Such activity cannot be reasonably construed as indicative of malicious conduct.

Moreover, we do not conceal any aspect of our infrastructure. The subnets we lease and the domains we operate are fully transparent and publicly verifiable. These facts, readily available through standard public tools and registries, further confirm the openness and legitimacy of our technological framework.

Finally, it must be made absolutely clear that we do not and have never sought to obscure our operations. For years, we have remained open and available for direct engagement, and any party - researchers, media outlets, or other stakeholders - can and do contact us regarding our technology or operational practices.

The infrastructure we employ is fully transparent. IP ranges, domain associations, and other relevant technical data are publicly accessible and verifiable. Any attempt to characterize such openly available and routinely disclosed information as indicative of concealed or covert relationships is both misleading and inaccurate.

For the avoidance of doubt, we are not a hosting provider and do not engage in mass content hosting or distribution. We are a technology platform, and like any comparable operator in the sector, relies on multiple third-party service providers to ensure operational resilience and service quality. To suggest that such necessary and commonplace arrangements evidence control or affiliation is a mischaracterization of fact and reflects a fundamental misunderstanding of how modern technology infrastructure is structured and deployed.

**Industry Associations Misrepresented.** The Defamatory Article also portrays our membership in industry associations as proof of ownership or control. This is intentionally misleading. These associations are non-profit organizations, similar to IAB, that unite a wide range of technology companies. Our membership is public and does not create corporate links, shared ownership, or operational control. Presenting such participation as “evidence” of affiliation distorts reality and reflects a lack of understanding of how associations function.

**CSR Activities Mischaracterized.** The Defamatory Article even misrepresents our corporate social responsibility initiatives. We actively invest in community projects - from building public spaces to supporting environmental programs and sports organizations. These initiatives are aimed at improving quality of life where we live and work. Suggesting that such contributions are suspicious or part of a “hidden agenda” not only misleads readers but also undermines the broader value of CSR and the positive role companies can play in society.

#### **4. “THE VAULT IS UNLOCKED” Said Infoblox to Everyone But the Bank...**

Infoblox would have its readers believe that it conducted research which unearthed vulnerability associated with our products and services and published the Defamatory Article to warn and protect the public from the risks its “research” uncovered. It is telling, however, that rather than bringing this alleged vulnerability to our attention so as to help us identify and eliminate it - which

would *actually* protect the public - Infoblox chose to publicly expose this alleged vulnerability, which has the exact opposite effect. Indeed, if such a vulnerability actually existed, bringing it to the attention of potential wrongdoers would be utterly irresponsible, put the public at risk, and expose Infoblox to further liability.

Based on the foregoing, one can conclude that (a) Infoblox does not actually believe its own rhetoric and (b) Infoblox's publication of the Defamatory Article is analogous to an anti-virus vendor spreading rumors about a non-existent virus in order to drive its own sales.

## 5. Questionable Motives and Commercial Interests of Infoblox

**The text and tactics employed in the Defamatory Article suggest that Infoblox authored and published it in order to prop up its own commercial value by inventing a problem that actually does not exist.** Indeed, it appears that Infoblox has a history of such business tactics. Infoblox Inc., was publicly traded until 2016 (see <https://www.infoblox.com/company/news-events/press-releases/infoblox-announces-agreement-to-be-acquired-by-vista-equity-partners/>).

Since that time, transparency has decreased: ownership structure and ultimate control are no longer disclosed with the same rigor required of public companies. This naturally raises the question of who currently influences the direction and content of such publications, and how much weight can reasonably be placed on the conclusions of a company whose own transparency is limited.

Infoblox has also been involved in legal disputes, including shareholder lawsuits and patent litigation, such as ThreatSTOP, Inc. v. Infoblox, Inc. (<https://news.bloomberglaw.com/ip-law/threatstop-says-infoblox-used-pact-to-land-cyber-security-patent>). While we take no position on the merits of those cases, their existence could give the impression of a company prepared to act irresponsibly in pursuit of its interests.

The style and framing of Infoblox's blog publications strongly resemble well-documented **FUD** (Fear, Uncertainty, and Doubt) tactics - a communication method in which fear and uncertainty are emphasized to influence perception and decision-making. Such techniques have been described historically in the IT industry (see Social-Engineer, *Free Yourself from FUD*, July 2018) (<https://www.social-engineer.com/free-yourself-from-fud>). Instead of balanced research, the Defamatory Article is designed to unnecessarily alarm readers and create pressure to adopt Infoblox's own products and services.

For example, the Defamatory Article introduces the term "Vane Viper" (a term invented by Infoblox itself) as if this is a long-standing term recognized by the industry without providing a clear definition or presenting any substantiated evidence of unlawful conduct allegedly associated with this designation. Infoblox intentionally keeps the meaning, scope, and factual basis of this term ambiguous, leaving readers with an impression that we are involved in something malicious despite the fact that Infoblox goes out of its way not to explain its relevance or applicability to us. Should Infoblox possess specific, credible evidence of unlawful activity allegedly linked to this

term, we would be prepared to engage in a professional and constructive dialogue with their technical and legal representatives to examine and address any legitimate concerns.

The Defamatory Article also exhibits characteristics of sensationalism, not investigative journalism, namely, recycle of the same insinuations, often verbatim, without any logical progression from premise to conclusion and repetition of inflammatory claims without logical progression or evidentiary support. It is a textbook example of misleading "news" that aims to generate outrage rather than to uncover verifiable facts.

Ultimately, the Defamatory Article reads less like an investigation and more like an attempt to inflate the perceived value of Infoblox's own services in the eyes of perspective clients. Such publications are based solely on instilling fear in users, misrepresenting and exaggerating facts, and are nothing more than a form of "fear-based marketing" which, unfortunately, forensic service providers too often resort to, with one single purpose to inflate the value of their own services.

To the extent that Infoblox claims to have discovered and investigated such a vulnerability over an extended period of time, it is a matter of serious concern that no attempt was made to notify us or any other potentially affected parties prior to the publication of the Defamatory Article. The failure to follow established and widely accepted coordinated vulnerability disclosure protocols represents a significant departure from responsible cybersecurity practice.

By publicly disclosing procedural descriptions and method-level technical details in an open-access blog, Infoblox has increased the risk that malicious actors may exploit the alleged vulnerability. This approach is not only irresponsible but also undermines collective efforts within the cybersecurity community to manage and mitigate potential threats through responsible and constructive engagements and it may equip malicious actors with information to exploit, thereby putting users at risk.

Taken together, it may reasonably appear that such publications serve not only informational purposes but also potential commercial objectives - inflate the perceived value of your own services in the eyes of its clients. Such texts are based solely on instilling fear in users, misrepresenting and exaggerating facts, and are nothing more than a form of "fear-based marketing" which, unfortunately, forensic service providers too often resort to, with one single purpose to inflate the value of their own services.

## **6. Conclusion**

**It is demonstrably evident that Infoblox's publication of the Defamatory Article is a marketing scheme and not genuine research.** The Defamatory Article misleads the reader and its content bears no relation to our actual operations, demonstrates no fundamental understanding of our technology.

The Defamatory Article misrepresents who we are and what we do. Nevertheless, we remain committed to constructive cooperation to strengthen the safety and integrity of the digital advertising ecosystem. If anyone has an actual concern about our products and services, all they have to do is reach out - and it is unfortunate that Infoblox chose FUD and pretense of journalism instead of responsible business practices.

Notwithstanding the unfounded and disparaging statements that Infoblox circulated, Propeller Ads and Adtech Holding affirm their continued commitment to maintaining constructive and professional relationships with all partners, including Infoblox. We remain open to direct communication and collaboration with all stakeholders, as our priority is to foster transparency, strengthen cooperation, and contribute meaningfully to the improvement and sustainability of the broader ecosystem.