OMNI

DNS Monitoring from Detection to Takedown

Monitoring: Remove the DNS Blindspot

Comprehensive protection for clients from domain abuse and malicious activities that rely on the DNS as a cybersecurity blindspot

We provide early identification and context-driven reports of DNS-based threats (phishing, ransomware, misinformation) to help our clients avoid the legal consequences and damages of a breach scenario

Ignoring this blindspot can cost hundreds of thousands in breach and legal fees; addressing the DNS threat vector eliminates those costs and enhances an organization's information security posture

Detection: We mean it when we say "Comprehensive"

With unique data sets, analyses, and methodologies, we scour the planet, 24x7x365 to identify threats, infringement, counterfeits, misinformation -- if it's malicious, it will be on our radar

We leave no stone unturned -- we identify string matches, permutations, double permutations, IDNs, subdomains, and track, in near real time, APT campaigns that target or could target our clients

We engineer around data blackholes from ccTLDs that simple brand protection systems do not acknowledge, scouring the entire planet for registrations that do not exist in any data sets

Prioritization: Human analysis for actionable, timely, and relevant intel

We believe in and utilize human expertise and analyses: there is no AI, no machine learning, and no substitute for the decades of investigative and information security expertise that go into our reports

Driven by context and data points that matter to information security professionals and legal teams, our reports provide actionable and understandable intelligence designed to facilitate swift action

Preventing alert fatigue, we do not barrage clients with automated reports of inconsequential activities

Takedowns: Tailored, targeted, effective

We have the legal skills and technical foresight to terminate the intentions of threat actors

Every situation is unique: never automated and always specifically tailored to the threat at hand, we analyze all ToS, AUP, Privacy Policies, etc., to create takedown requests that get results, quickly

Our services and reports are protected by attorney-client privilege and as attorney work product, affording our clients an additional level of security and assurance without increasing headcount

OMNI in the News


MOTHERBOARD VICE

Evidence Suggests the GOP Bought at Least 17 Anti-James Comey Domains

The Republican party has apparently created a series of domains to discredit and attack former FBI director James Comey. Meanwhile, Democratic party sympathizers appear to have created similar domains to counter the Republicans' anti-Comey campaign.

"Using the tool, which Urbelis and his colleagues call Open-Source Multidisciplinary Network Intelligence or OMNI, he found 36 domains that contain the name Comey and were registered in 2018." – Lorenzo Franceschi-Bicchierai, MOTHERBOARD (19 April 2018)

"... Alexander Urbelis, a partner at the New York-based Blackstone Law Group who detected the new registrations." – Tami Abdollah, ASSOCIATED PRESS (23 July 2018)

BLACKSTONE LAW GROUP

1201 Broadway, 9th Floor
New York, New York 10001
(212) 779 3070
info@blackstone-law.com