OMNI

DNS Monitoring, from Detection to Takedown

Monitoring: Remove the DNS Blindspot

- We identify early-stage indicators of cyberattacks and malicious activity in the DNS, providing targeted intel about APT activities and infrastructure, and many other DNS-based threats for preemptive and proactive blocking.
- Tracking and monitoring sophisticated actors is a significant part of what we do, and we have helped hundreds of companies successfully deflect APT activity before it even touched their networks.
- Providing comprehensive DNS intelligence, our services are akin to adding several FTE threat hunters to your SecOps Team.

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 black holes 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 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 sophisticated threat actors and APT groups.
- By reviewing data from the perspective of an attacker and connecting the dots within our data sets, we can issue powerful and efficient takedowns and provide advice about the best types of defensive practices to neutralize an attack.
- Of value to more than cybersecurity teams, legal departments also rely on our identification of misinformation, brand impersonation, counterfeit marketplaces, IP infringement, and other legal issues we can promptly address.

BLACKSTONE LAW GROUP

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

OMNI in the News

REUTERS

Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike

"The attempted break-in at the WHO was first flagged to Reuters by Alexander Urbelis, a cyber security expert and attorney with the New York-based Blackstone Law Group, which tracks suspicious internet domain registration activity."
– Raphael Satter,
REUTERS (23 March 2020)

Mystery: Who bought websites implying US senators 'for sale'

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

THE CORONAVIRUS CRISIS

Cybersecurity Lawyer Who Flagged The WHO Hack Warns Of 'Massive' Remote Work Risks

March 30, 2020 · 5:00 AM ET
Heard on Morning Edition

"The breach was discovered by Alexander Urbelis...[by] monitoring the Internet for indications that the group has reawakened or reactivated some of its infrastructure." - Emma Bowman, NPR (30 March 2020)