BlueVoyant

DIGITAL BRAND PROTECTION

OVERVIEW

Every day, cybercriminals stand up thousands of phishing campaigns that are designed to deceive their targets, harvest personal information and credentials, and take over online accounts. Attackers use a variety of methods to steal information, from setting up fake websites to large-scale malicious email campaigns.

According to industry research, one in every three consumers would hold the victimized organization responsible by closing their online account following a breach, or by ending their business relationship with the organization entirely.

As organizations expand their digital presence, threat actors increase their use of applications and social media as attack vectors, taking advantage of the gaps in organizations' visibility of their mobile assets and social media networks to attack their brand and customers. Successful phishing campaigns negatively impact customers' trust and your brand reputation, and they divert revenue away from your business.

With BlueVoyant's Brand Protection you can proactively detect and disrupt phishing attacks, fake social media accounts and rogue applications targeting your customers, partners and employees. Minimize organizational risk and manifest real business impact by utilizing our high-fidelity alerts, continuous monitoring, and effective take-down.

Unfortunately, these defenses are often focused either on events inside the perimeter, or are passive in nature, which can mean that emerging threats, such as large scale malware campaigns and attacks targeting a specific organization, its leadership and employees, or its vendor ecosystem can go undetected.

BlueVoyant can help. Using an unparalleled combination of data, analytics and skilled staff, BlueVoyant is capable of identifying both general and specific external threats, providing organizations with the type of early warnings that can help dramatically improve cybersecurity.

HIGH FIDELITY ALERTS

Our solution combines machine learning with cybersecurity expertise to uncover websites, social media accounts and applications impersonating your brand while continuously adjusting detection parameters as the threat landscape evolves. Our services include:

- **Web Impersonation**
- **Social Media Impersonation**
- **App Impersonation**

WEB IMPERSONATION

Anti-Phishing Detection

BlueVoyant discovers domains that impersonate organization, logo, products, and trademarks. More than 100M potential phishing domains are analyzed daily utilizing a wide range of open and proprietary data sources including active and passive DNS records, domain registration data, and advanced web-crawling capabilities. Key features:

- Detection of domains involved in large scale phishing email campaigns.
- Advanced detection of look-alike domains and subdomains.
- Monitoring of new domain registrations to quickly identify new phishing campaigns as they are set up.

SOCIAL MEDIA IMPERSONATION

Fake Social Media Accounts Detection

BlueVoyant identifies fraudulent social media accounts that mimic your brand and key-personnel across Facebook, Twitter, Instagram and LinkedIn.

APP IMPERSONATION

Rogue Application Detection

BlueVoyant actively detects third-party modifications of legitimate apps, unauthorized brand affiliations, and rogue applications, both for mobile devices and desktop. On a daily basis our solution dynamically scans Google Play, Apple App Store, and more than 170 different unofficial app-stores to uncover the existence of illegitimate applications.

DIGITAL BRAND PROTECTION

PROACTIVE DETECTION AND REMOVAL OF PHISHING THREATS, FAKE SOCIAL MEDIA ACCOUNTS, AND ROGUE APPLICATION

CONTINUOUS MONITORING

Tracking each inactive domain and website over time is costly and requires a secured infrastructure with probing capabilities at scale. BlueVoyant provides ongoing monitoring of suspicious domains and real-time alerting when phishing campaigns go live. With BlueVoyant's continuous monitoring, you will be alerted of any active phishing campaign and recurring risk.

EFFECTIVE TAKE-DOWN

BlueVoyant offers a take-down service that leverages our 24/7 Security Operation Centers (SOC) to commence immediate action on your behalf and to remove threats quickly. Our fast-lane procedures and ability to automatically generate supporting evidence help expedite take-downs and shorten the time to remediation.

ABOUT BLUEVOYANT

BlueVoyant is an analytics-driven cybersecurity company whose mission is to protect organizations of all sizes against agile and well-financed cyber attackers. Founded and led by experts in the cyber security and government security sectors, BlueVoyant's offerings are built with real-world insight and applicability, plus an eye on the threat horizon.

Through our Advanced Threat Intelligence, Managed Security Services, and Incident Response Services, we excel in intelligence gathering, cybersecurity defense, detection of attacks, and response coupled with remediation. Our SOCs around the world keep us on top of developing and established threat actors and the well-financed tools they are developing to out-smart traditional security measures. Our 24/7 SOCs, offices around the world, and our security analytics platform positions us to best help our customers defend against emerging cyber threats.