FLASHPOINT

Brand Monitoring Capabilities

Flashpoint provides organizations the insight into how their brand is being impersonated for malicious purposes, the appropriate context around the threat in order to protect the enterprise, and a path to remediate risk rapidly. As malicious sites, social media accounts, and mobile apps continue to impact customers and employees, organizations require the ability to take immediate action to remove phishing assets in order to avoid further damage to the business and protect the brand.

Available Monitoring Offerings

DOMAIN

Provides teams the ability, resources, and insight into observed domain phishing activity related to the organizatio in order to eliminate threats such as typosquatting, phishing attacks, and brand impersonation through logo detection.

MOBILE APPS

Provides the ability to monitor official mobile app stores, third parties, and directory sites for fraudulent apps that are targeting or impersonating a brand.

SOCIAL MEDIA

Enables users to identify fake or duplicate accounts targeting the brand, enterprise, or employees from social media sites.

With the Flashpoint Takedown Management capability, users are able to request identified domains, social media accounts, and mobile apps to be removed.

Domain

KEY BENEFITS

- **Actionable Alerts with Context:** Receive notification of malicious URLs targeting an organization and its affiliated brands with the necessary context to know whether to action a takedown
- **Investigation of URL Incidents:** Analysts investigate and review potentially malicious URLs on your behalf in order to minimize false positives
- **Seamless Brand Management:** Centrally manage all your brands and logos within the Flashpoint Intelligence Platform
- **Track Insights Related to the Enterprise:** Analyze attacks on your organization's brands to determine which are at highest risk

PROTECT AGAINST PHISHING ATTACKS; IDENTIFY AND STOP BRAND IMPERSONATION

Cybercriminals continue to seek creative ways of manufacturing phishing pages to appear legitimate, including stealing company logos and other trademarked information in order to prompt unsuspecting users to enter sensitive information such as passwords or credit card numbers.

Flashpoint's ability to detect stolen logos or visuals provides brands the ability to uncover actors and infrastructure impersonating brands for malicious gain, enabling internal teams to swiftly identify pages and take action.

Mobile Apps

KEY BENEFITS

- **Investigate Identified Fraudulent Mobile Apps:** Review potential phishing apps across major app stores, as well as third-party marketplaces
- **Protect Customer Personally Identifiable Information (PII):** Proactively identify mobile apps targeting customers or employees in order to mitigate the risk of compromising sensitive assets, such as credentials, credit card information, and other information

MONITOR FOR MALICIOUS MOBILE APPS; PROTECT CUSTOMERS FROM THREAT ACTOR CAMPAIGNS

With the increasing importance and dependence on mobile apps for everyday life, threat actors have taken advantage and have increased targeting enterprise applications. Threat actors have shifted their attention to uploading fraudulent mobile apps on major app stores or third-party sites, which direct unsuspecting customers to download malware or share login credentials.

Flashpoint enables organizations to identify risks and threats targeting an enterprise's mobile app presence by detecting phishing apps before more harm can be done. Flashpoint's ability to cover and monitor major app stores, as well as third parties, provides users the full landscape of where threat actors are uploading malicious apps.

Social Media

KEY BENEFITS

- **Identify Fraudulent Social Media Profiles:** Protect your brand against reputational damage, credential stealing, and financial losses
- **Protect the Organization's Executive Team:** Receive alerts and immediate notification of social media accounts impersonating high-level executives and members of the enterprise
- **Review and Triage Identified Accounts:** Access the potential phishing content on the social media account via the Flashpoint Intelligence Platform and review the additional context

IDENTIFY PHISHING ACCOUNTS; PROTECT AGAINST REPUTATIONAL DAMAGE

Fraudulent social media accounts impersonating the brand can direct unsuspecting customers to malicious links, prompting them to enter their login credentials into phishing sites.

Flashpoint proactively alerts users to identified phishing accounts across major social media platforms, enabling teams to take action against threats such as phishing, misinformation, malware sites, and more.

DETECT FRAUDULENT SOCIAL MEDIA ACCOUNTS; MITIGATE RISK OF EXECUTIVE IMPERSONATION

High-profile executives today have a large social media presence and following across major platforms. Cybercriminals continue to exploit organization executives by creating accounts impersonating organization members, causing reputational damage through proliferating scams, or financial damage via employee or customer phishing schemes.

Flashpoint provides enterprises seamless access and notification to identified malicious social media accounts that are impersonating executives via the Flashpoint Intelligence Platform, highlighting how threat actors are leveraging executive personal brands for malicious gain.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**