FORTRA™

DATASHEET (PHISHLABS)

Dark Web Monitoring

Illuminate Dark Web Threats

The dark web is a vital part of the cybercrime underground, home to fraud and cyber threats that can go unnoticed by security teams. Threat actors leverage the anonymous nature of the dark web to cause financial and reputational damage to enterprises through compromised credentials, the exploitation of stolen data, threats of physical harm to executives, and covert planning of future attacks.

Fortra's PhishLabs proactively monitors the dark web and provides enterprises with expert-curated intelligence to protect against brand threats and compromised credentials.

Uncover Brand Threats and Compromised Credentials Across the Dark Web

Transactions conducted on dark web forums and marketplaces provide threat actors the discreet cover they need to plan and execute attacks. Like-minded criminals plan attacks, buy, sell, and solicit resources like stolen credentials, combo lists of logins and banking details. These actions allow them to gain insider access to the systems of targeted organizations as well as steal critical data. Lack of visibility into exchanges and fully unredacted lists of compromised credentials that are not anonymized behind paywalls, make it difficult for security teams to proactively defend against an attack. PhishLabs comprehensive protection against dark web threats protects brands and their employees and customers.

Dark Web Brand Monitoring

PhishLabs Dark Web Brand Monitoring observes dark sites, marketplaces, discussion groups, and forums. It detects a broad set of brand and executive mentions and threats such as stolen PII, card data, emails, phishing kits, and fraud tools targeting organizations, as well as Initial Access Brokers marketing illegal means of entry into corporate networks. Through this monitoring, PhishLabs provides expert-curated intelligence and risk awareness to protect corporate and executive brands, and valued assets.

PRODUCT SUMMARY

Fortra's Dark Web Monitoring investigates dark web marketplaces, chat rooms, and forums to provide expert-curated intelligence and risk awareness to protect corporate and executive brands as well as valued assets. This is supported by Fortra's proprietary sources, feeds, and methods that enhance visibility into brand mentions, threats, stolen corporate email addresses, and employee and customer credentials obtained by threat actors. In addition, the intelligence collected is curated by Fortra's expert dark web analysts, saving organizations time and effort when classifying search results.

KEY FEATURES

- **Dark Web Brand Monitoring**
  Proactively monitors the dark web and provides enterprises with expert-curated intelligence to protect corporate and executive brands, and valued assets.

- **Compromised Credentials Monitoring**
  Provides broad visibility into actionable employee and customer stolen credentials uncovered from dark web sites and harvested through malware, to proactively guard against future attacks.

Compromised Credentials Monitoring

Through Compromised Credentials Monitoring, PhishLabs provides visibility into credentials that have been leaked or stolen by infostealers, botnets, and other malware. Complete and unredacted visibility into compromised logins, emails, and passwords enables customers to implement proactive countermeasures like forced password resets and account lockouts to guard against potential account takeovers, breaches, and malware attacks.

Dark Web Brand Monitoring
Dark sites, marketplaces and forums

Compromised Credentials Monitoring
Infostealers, botnets and other malware

Brand and Executive mentions, Stolen PII, card data, BINs, emails Phishing kits, Fraud tools Initial access brokers

Actionable compromised logins
Emails, passwords, secret codes
Not parked behind paywalls

Continuous targeted surveillance
Monitor for changes in activity

Implement proactive countermeasures
Forced password resets/account lockouts
Stop exfiltration of outbound transfers

With focused, direct monitoring of marketplaces and other dark web sites to identify references to stolen data and criminal activity associated with enterprises, PhishLabs Dark Web Monitoring delivers high-value intelligence and links key points of data to threat actor personas to continue surveillance and monitor for changes in activity. Whether working to stop the sale of personally identifiable information (PII), stolen credentials, the exploitation of source code, monitoring threatening chatter, or the distribution of malware exploit kits, PhishLabs' dark web surveillance helps mitigate future attacks.

Maintain Vigilance with Dark Web Monitoring

Undetected dark web exchanges, compromised credentials, and attack planning can quickly become serious threats to targeted enterprises and executives. Left ignored, threat actors can use dark web resources to cause irreversible brand damage, physical harm, and execute crippling account takeovers. To protect against attacks, enterprises must be properly equipped to track down and monitor threatening activity. The intelligence to take proper action internally to force password resets, account lockouts, and even stop the exfiltration of outbound transfers in flight is also needed to protect valuable brands and employees.

PhishLabs delivers holistic visibility into dark web threats through targeted intelligence collection. Dark Web Monitoring surveillance combines automated detection and expert human analysis that empowers enterprises to proactively identify and defend against future attacks that originate in the dark web.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.