

Proofpoint Digital Risk Protection: Darknet-Daten

Unsere Darknet-Daten umfassen eine breit aufgestellte und ständig erweiterte Datenbank mit mehr als 1 Milliarde aktuellen und älteren Einträgen. Dazu gehören Darknet-Netzwerkdaten sowie Informationen zu hochriskanten Inhalten aus dem Deep Web und Surface Web. Wir indizieren und klassifizieren diese Daten kontinuierlich. Sie werden bei Risiken für Ihr Unternehmen (z. B. kompromittierten Anmeldedaten, Datenverlust, Markenbetrug) zuverlässig gewarnt, ohne dass Sie direkt auf das Darknet zugreifen müssen.

Datenquellen

- Anonyme Darknet-Netzwerke wie Tor, I2P und Zeronet
- Chat-Anwendungen und -Protokolle wie Telegram und IRC
- Anonyme Filesharing-Webseiten wie Mega
- Foren wie Raidforums, Bitshacking und Free Hacks
- Carding-Websites wie Carderbase, CrdClub und Chknet
- Dox-Websites wie Doxbin und Ghostbin
- Schwarzmärkte wie Silk Road 3.0 und Dream Market
- Dateiablage-Websites wie Pastebin, Opaste und Dpaste
- Alternative DNS-Server
- FTP- und Torrent-Dateiserver

Wichtigste Fakten

- Mehr als 1 Milliarden Einträge
- 95.000 individuelle Domänen (232.000 einschließlich gespiegelter Domänen)
- 450 Chat-Kanäle und Gruppen
- Mehr als 13,5 Millionen Ablagen und Dateien
- Mehr als 3 Millionen Dokumente aus Datenschutzverletzungen
- 40.000 Seiten aus geschlossenen Zugriffsseiten
- 10–15 Millionen Einträge pro Tag erfasst
- Closed-Source- und Open-Source-Inhalte

Kriminelle Inhalte und Bedrohungen

Folgende Bedrohungen können gefunden werden:

- Gefälschte und andere illegale Elemente, die auf Schwarzmärkten zum Verkauf angeboten werden
- Kompromittierte Anmeldedaten, darunter solche mit Klartext-Kennwörtern
- Vertrauliche Steuerbescheide, Ausweisnummern und Gesundheitsdaten
- Zum Verkauf angebotene Kreditkartennummern
- Vorstellung von Malware, Ransomware, Exploit-Kits und neuen Angriffstechniken
- Über Datenschutzverletzungen oder Insider-Lecks kompromittierte Daten
- Doxing* von Führungskräften oder wichtigen Mitarbeitern
- Tools und Vorlagen zum Starten von Phishing-Angriffen und anderen Betrugsversuchen

Zusammenfassung

Unsere Daten können in mehr als 47 Sprachen durchsucht werden; sie werden erfasst, ohne Sicherheitskontrollen zu unterlaufen oder für Daten zu bezahlen.

Proofpoint Digital Risk Protection findet Bedrohungen für Ihr Unternehmen in verschiedensten Darknet-Quellen. Unsere umfangreiche und aktuelle Datenbank gewährleistet, dass Sie über alle schwerwiegenden und relevanten Risiken für Ihr Unternehmen Bescheid wissen.

* Laut Wikipedia versteht man unter Doxing das internetbasierte Zusammentragen und anschließende Veröffentlichung personenbezogener Daten, zumeist mit bössartigen Absichten gegenüber den Betroffenen.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.com/de.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.