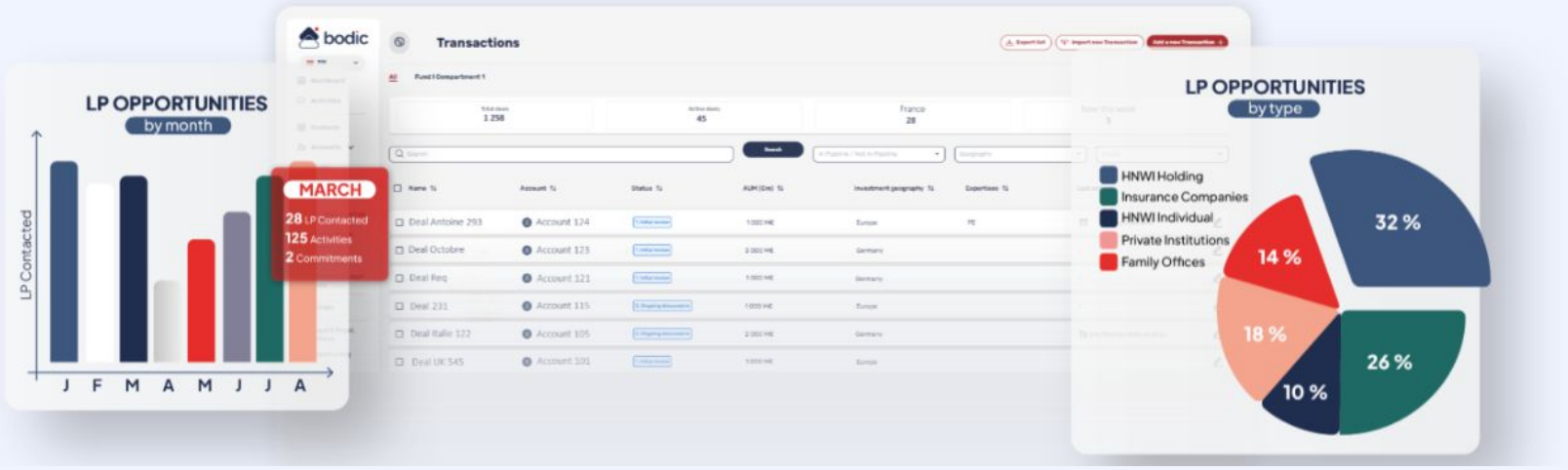
bodic

Votre partenaire DATA pour optimiser les performances de votre société de gestion



Les Fiches Pratiques IA DATA

5 minutes pour comprendre un concept technique

F#12 : Darknet – Menace silencieuse pour le monde du Private Equity ?

Juillet 2025

www.bodic.eu

Introduction

Le **darknet**, souvent fantasmé ou caricaturé, constitue une **zone grise d'internet** où se développent des usages aussi légitimes que criminels. Pour les fonds, il représente un **risque croissant** mais **invisible**, encore **peu intégré** dans les grilles de due diligence.

Comprendre le darknet en 3 couches

Pour bien situer le darknet, il faut distinguer trois niveaux d'Internet :

Surface web : ce que tout le monde utilise au quotidien.
Ex : sites indexés par Google, accessibles via un navigateur classique) ;

Deep web : contenu non indexé, mais légal et accessible avec les bons accès. Ex : intranet d'entreprise, bases de données en ligne, messageries privées, interface d'admin, API privées ou protégées) ;

Darknet : espace intentionnellement caché, accessible uniquement via des outils spécifiques comme le réseau TOR, souvent utilisé pour préserver l'anonymat des utilisateurs.

Darknet : de quoi parle-t-on ?

- Né à l'origine pour des **besoins militaires**, puis popularisé via **TOR** et les **cryptomonnaies**
- **Accès restreint**, usage de messageries chiffrées, forums fermés
- **Usages légitimes** (journalisme, dissidence) vs **usages illicites** (CaaS, ventes illégales, blanchiment)

Pourquoi le Private Equity est concerné ?

- ❖ **Risque réputationnel** : données sensibles d'un portefeuille exposées ou vendues
- ❖ **Risque opérationnel** : vulnérabilités IT découvertes ou commercialisées sur le darknet (ex : accès VPN à vendre)
- ❖ **Risque juridique** : non-conformité RGPD ou négligence dans la gestion des fuites
- ❖ **Risque stratégique** : concurrents ou attaquants accédant à des documents confidentiels

Exemples de signaux faibles à surveiller

Signal faible détecté	Ce que cela peut indiquer	Action recommandée
Nom de domaine d'une participation mentionné sur un forum TOR	Tentative de ciblage, fuite d'info ou préparation d'attaque	Lancer une recherche approfondie + notifier le RSSI / DSI de la cible
Identifiants de collaborateurs exposés dans des bases piratées	Risque d'usurpation d'identité ou d'accès frauduleux au SI	Forcer une rotation des mots de passe, activer MFA, sensibiliser les utilisateurs
Accès RDP, VPN ou base de données à vendre (ex : « accès admin ERP X »)	Compromission active des systèmes ou faille critique exposée	Isoler le système concerné, analyser la compromission (forensic), notifier la direction
Données financières ou documents confidentiels en vente (pitchs, rapports,...)	Fuite interne ou compromission d'une boîte mail / portail	Auditer l'origine de la fuite, renforcer les droits d'accès, notifier les LP si nécessaire
Adresse email générique de type IR@fonds.com utilisée en phishing	Tentative d'attaque ciblée contre le fonds ou ses investisseurs	Ajouter un filtre anti-phishing, surveiller les noms de domaine similaires, sensibiliser les LP
Mentions ou rumeurs sur une opération en cours sur des canaux privés	Fuite d'info pré-deal ou manipulation de marché	Identifier l'origine, contenir l'info en interne, vérifier les processus de cloisonnement

Comment les fonds peuvent réagir ?

- **Mettre en place une veille darknet structurée**, avec des outils ou partenaires capables de détecter les fuites, identifiants compromis ou tentatives de revente de données critiques (dashboards, accès VPN, ...) ;

- **Auditer la surface d'attaque numérique des participations**, en identifiant les points d'exposition : emails professionnels présents dans des leaks, ports RDP ouverts, interfaces non protégées, VPN mal configurés.

- **Sensibiliser les équipes internes** (deal, portefeuille, relations investisseurs) aux signaux faibles issus du darknet : usurpation d'identité, phishing ciblé, fuites sur des opérations sensibles en cours.

- **Intégrer le risque darknet dans les grilles de due diligence IT & cyber**, avec un score d'exposition et alertes en cas de compromission avérée.

- **Prévoir un plan de réponse** en cas de détection : com maîtrisée, traçabilité juridique, notification LP, mesures de remédiation, ...

Mise en pratique (exercice)

Vous êtes en **phase d'audit** sur une cible tech (SaaS B2B, 120 personnes, forte croissance). Un partenaire cybersécurité vous signale que :

- des identifiants avec domaines @starttarget.com apparaissent sur un forum darknet ;
- un accès VPN admin à distance semble en vente (port RDP exposé) ;
- un document marketing confidentiel est listé dans un bundle à vendre.

Que faites-vous ?

1

Analyser l'alerte

Vérifier la **source** (fuite récente ? Brute ou re-traitée ?)
puis Identifier la **gravité** : simple fuite d'email ou accès critique ?

2

Échanger avec le CTO de la cible

A-t-il connaissance de cette exposition ? Quels correctifs ont été faits ?
Quel niveau de maturité cyber de l'équipe ? Un RSSI est-il en place ?

3

Évaluer l'impact sur la valorisation

Risque juridique (RGPD, contrats clients), opérationnel / réputationnel ?
Ajustement du **multiple** ? Clause spécifique dans le SPA ?

4

Proposer un plan de remédiation

Rotation des identifiants exposés, renforcement **MFA**, cloisonnement **VPN**. Accompagnement post-deal dans le **Value Creation Plan**

À retenir

- L'essor du **Cybercrime-as-a-Service (CaaS)** démocratise l'accès aux outils d'attaque ;
- Le darknet n'est pas "immense" mais **stratégiquement dense ;**
- L'anonymat est **relatif** : le FBI et Europol ont déjà démantelé plusieurs réseaux ;
- Certains fonds plus avancés incluent déjà le **dark web monitoring** dans leur stratégie cyber.

Vous souhaitez aller plus loin sur ces sujets Data Cyber Protection ? **Bodic** et son partenaire **TechItSimple** vous accompagnent pour mieux vous protéger et pour aider vos équipes à monter en compétences : **contact@bodic.eu**

bodic

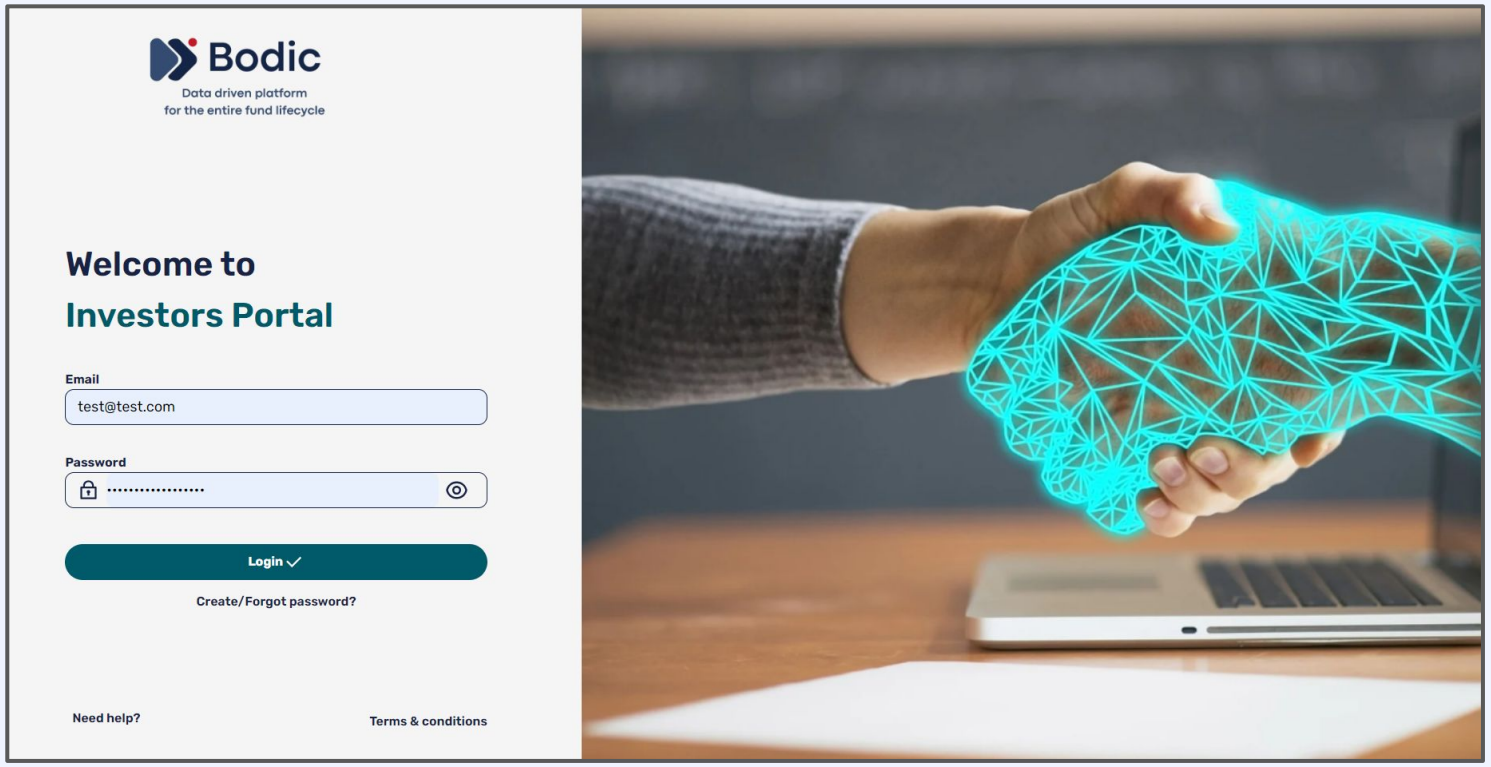
Votre partenaire DATA pour optimiser les performances de votre société de gestion

Cette fiche vous a plu ? N'hésitez pas à partager ce post !

Envie d'aller plus loin ?

Découvrez nos solutions sur www.bodic.eu

contact@bodic.eu



Les 10 points
d'une digitalisation réussie
pour une société de gestion

- LIVRE BLANC 2025 -

Télécharger notre livre blanc

www.bodic.eu