Bitdefender® Global Leader In Cybersecurity

Explorer LE DARKNET

La sous-culture des cybercriminels

Table des matières

Bitdefender Global Leader In Cybersecurity

03 Introduction

04 Contexte historique

05 Principales idées reçues

06 La sous-culture des cybercriminels

07 Structures sociales

07 Instaurer la confiance

08 Évolution de la cyber-criminalité sur le darknet

09 Activités illégales

09 Le darknet et la loi

11 Une expertise de première ligne

12 Bâtir un avenir plus fort

Introduction

Le darknet est une segment distinct et caché de l'Internet, rendu volontairement inaccessible par le biais des navigateurs standard et invisible pour les moteurs de recherche conventionnels, au contraire du Deep Web, qui inclut toutes les parties de l'Internet non indexées par les moteurs de recherche mais néanmoins accessibles si l'on dispose des autorisations nécessaires. L'accès au darknet nécessite des logiciels, des configurations ou des autorisations spécifiques, ce qui le différencie du Web surfacique, ouvert au grand public.

Il est essentiel de comprendre le darknet dans toute sa complexité pour appréhender les sous-cultures qui prospèrent dans cet environnement protégé par l'anonymat. Ces sous-cultures, qui vont des plateformes cybercriminelles aux forums pour dissidents politiques, influencent l'évolution des mesures de confidentialité sur Internet et du paysage des cybermenaces, dont les entreprises doivent tenir compte dans leurs opérations.

Contexte historique

Conçu pour sécuriser et anonymiser les échanges durant la guerre froide, le darknet a d'abord été un outil de communication militaire utilisant un chiffrement avancé pour protéger les messages. Le chiffrement a ouvert la voie à d'autres avancées technologiques, qui ont étendu les capacités et l'accessibilité du darknet. Le développement du réseau Tor (The Onion Router) a considérablement amélioré l'anonymat en chiffrant et en réacheminant le trafic Internet via un réseau de relais mondial, protégeant ainsi l'identité et l'emplacement géographique des individus. Cette évolution a été complétée par l'essor des cryptomonnaies, telles que le Bitcoin, qui facilitent les transactions anonymes, faisant du darknet une plateforme attrayante pour diverses activités, au-delà de ses finalités gouvernementales et militaires initiales.

Au fil du temps, le darknet a attiré une base diversifiée d'utilisateurs, allant des activistes politiques aux lanceurs d'alerte en passant par les cybercriminels, tous séduits par la promesse de la confidentialité. Cette évolution démographique est à l'origine d'une sous-culture complexe, riche de normes et de valeurs uniques. Combinée aux avancées technologiques, elle a donné naissance à plusieurs places de marché, telles que la tristement célèbre Silk Road, qui utilisait l'anonymat offert par TOR et l'obscurité financière des cryptomonnaies pour faire le commerce de biens et de services illicites.

Ces places de marché ont longtemps été considérées comme intouchables, en raison de leur anonymat. Toutefois, le démantèlement de Silk Road par le FBI a marqué un tournant dans l'histoire du darknet, montrant que même le darknet est vulnérable aux forces de l'ordre.

Au fil du temps, le darknet a attiré une base diversifiée d'utilisateurs, allant des activistes politiques aux lanceurs d'alerte en passant par les cybercriminels, tous séduits par la promesse de la confidentialité.

Principales idées reçues

Le darknet sert de refuge à la cybercriminalité et offre aussi une plateforme aux **lanceurs d'alerte** qui peuvent y partager anonymement des informations sensibles ; soutient les personnes soumises à des régimes oppressifs, qui cherchent à s'exprimer librement ; et facilite le travail des journalistes et des chercheurs, qui ont besoin d'accéder à des données censurées, ou de les partager, en toute sécurité.

Le darknet est souvent considéré à tort comme un monde clandestin obscur, utilisé uniquement à des fins illicites, mais cela ne tient pas compte de sa nature plurielle ni de ses utilisations légitimes. Même s'il est indéniable que le darknet sert de refuge à la cybercriminalité, il offre également une plateforme essentielle aux lanceurs d'alerte, qui peuvent y partager anonymement des informations sensibles ; soutient les personnes soumises à des régimes oppressifs, qui cherchent à s'exprimer librement ; et facilite le travail des journalistes et des chercheurs, qui ont besoin d'accéder à des données censurées, ou de les partager, en toute sécurité. Ces fonctions s'avèrent indispensables dans les pays dans lesquels les médias conventionnels sont fortement contrôlés par l'État, où dans lesquels le maintien de l'anonymat est essentiel pour la sécurité et la liberté des personnes, comme c'est le cas en Russie.

Contrairement aux croyances populaires, il n'est pas si facile d'accéder au darknet. La navigation y requiert des connaissances et des outils techniques spécifiques, de sorte qu'il n'est pas simple pour l'utilisateur lambda de s'y connecter pour accéder à des contenus illicites. Les personnes qui y parviennent découvrent que le darknet est loin d'être aussi vaste que ce que les médias laissent entendre. Bien plus restreint que le vaste Web surfacique, il ne représente que 5 % du volume de ce dernier. Bien qu'il héberge tout un éventail de contenus illégaux, une part importante du darknet est consacrée à des activités légitimes.

Même s'il est vrai que l'anonymat offert par le darknet complique les opérations des forces de l'ordre, il s'agit d'un compromis nécessaire qui permet de protéger favorablement la confidentialité et la liberté d'expression dans les environnements répressifs.

La **sous-culture** des cybercriminels

Le darknet héberge diverses communautés allant des pirates informatiques aux activistes politiques, toutes liées par des normes et des valeurs communes, qui maintiennent l'ordre au sein de ce royaume caché. Les communications y sont protégées par des applications de messagerie et des forums spécialisés chiffrés, qui sont essentiels pour préserver l'anonymat et faciliter le libre échange des idées. Ces plateformes ne soutiennent pas uniquement les activités illicites ; elles sont également le lieu de discussions légitimes sur divers sujets, tels que la technologie et la politique, reflétant la dynamique sociale complexe du darknet.

La résolution des conflits et la coopération au sein de ces communautés s'adaptent au manque de supervision classique par les forces de l'ordre, en recourant plutôt à des systèmes basés sur la réputation pour régler les différends. Ce cadre favorise une culture où la confiance est primordiale, et les membres collaborent souvent pour atteindre des objectifs communs ou répondre à des menaces.

En revanche, d'autres parties du darknet fonctionnent sur une base plus décentralisée, où le pouvoir et la prise de décisions sont répartis entre de nombreux membres.

Structures sociales

Diverses structures, qu'elles soient hiérarchiques ou décentralisées, contribuent à l'organisation du darknet. Dans certains forums et places de marché du darknet, une hiérarchie distincte prévaut, dans laquelle les modérateurs et les dirigeants jouent un rôle critique dans le maintien de l'ordre, la définition des règles et l'orchestration des activités. Ces leaders sont souvent des membres aguerris qui jouissent d'une grande confiance et d'une grande autorité au sein de la communauté.

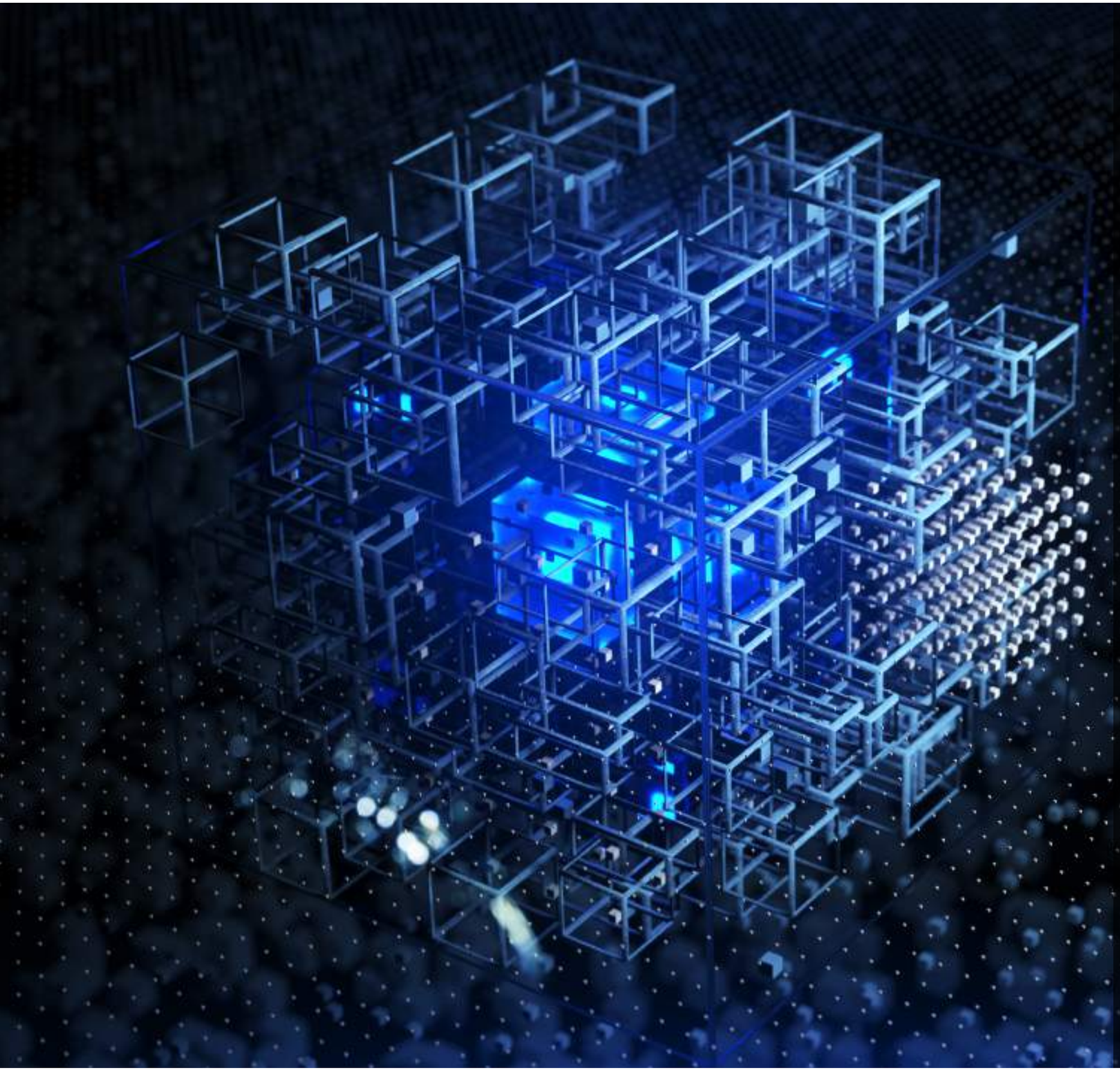
En revanche, d'autres parties du darknet fonctionnent sur une base plus décentralisée, où le pouvoir et la prise de décisions sont répartis entre de nombreux membres. Cela réduit la dépendance à un leader unique, et augmente potentiellement la résistance de la communauté aux perturbations, telles que les actions des forces de l'ordre.

Devenir membre de ces communautés très soudées implique de se soumettre à des procédures d'évaluation généralement rigoureuses, qui visent à s'assurer de la fiabilité et de la loyauté des individus. Dans certains cas, les futurs membres devront être cautionnés par des membres actuels, ou devront apporter la preuve de leurs compétences et de leurs intentions en se soumettant à divers tests.
Une fois admis, les nouveaux membres apprennent progressivement les ficelles du métier, y compris le jargon et les symboles spécifiques au groupe. Ce langage spécialisé et l'utilisation de symboles renforcent l'identité du groupe et servent de barrières à l'entrée, en tenant les profanes à distance et en améliorant la sécurité. Ces éléments culturels dénotent l'appartenance au groupe et le statut au sein du groupe, distinguant les initiés des non initiés et déterminant souvent l'accès à des couches plus profondes de la communauté ou à des informations plus sensibles.

Instaurer la confiance

La confiance est une valeur précieuse : elle est indispensable pour que l'échange de biens et de services puisse avoir lieu. Compte tenu de l'anonymat et des risques juridiques qu'impliquent leurs opérations, les cybercriminels ont développé des systèmes sophistiqués permettant d'instaurer et d'entretenir la confiance. Au cœur de ces systèmes se trouvent des mécanismes de réputation, des services de séquestre et des processus de vérification cryptographique qui garantissent l'intégrité et l'authenticité des transactions.
La vérification des biens et des services sur le darknet commence par des systèmes de séquestre, qui conservent les fonds sur des comptes sécurisés jusqu'à ce que toutes les parties soient satisfaites de la transaction. Ce système protège les acheteurs contre les vendeurs malhonnêtes, en ne libérant les paiements qu'une fois les marchandises reçues et vérifiées.
La cryptographie, à l'instar de la technologie Pretty Good Privacy (PGP), s'appuie sur le séquestre en vérifiant les identités de manière sécurisée et en chiffrant les communications. Les messages, transactions et identités restent ainsi confidentiels et authentiques, ce qui les protège des menaces externes et internes.

Les systèmes de réputation renforcent eux aussi la confiance au sein de la communauté. Tout comme les plateformes de commerce électronique recourent à des systèmes de commentaires, les places de marché du darknet font appel à des mécanismes de commentaires générés par les utilisateurs pour évaluer les vendeurs. Ces évaluations fournissent aux acheteurs potentiels un profil de confiance historique pour chaque vendeur, qui influence leurs décisions et leur comportement. Les cautions des vendeurs renforcent encore un peu plus ce cadre de confiance : les places de marché éliminent en effet les vendeurs peu sérieux ou malhonnêtes en demandant aux vendeurs de verser une caution importante en cryptomonnaie. Seuls les vendeurs engagés dans des opérations à long terme sont disposés à se plier à cette contrainte.



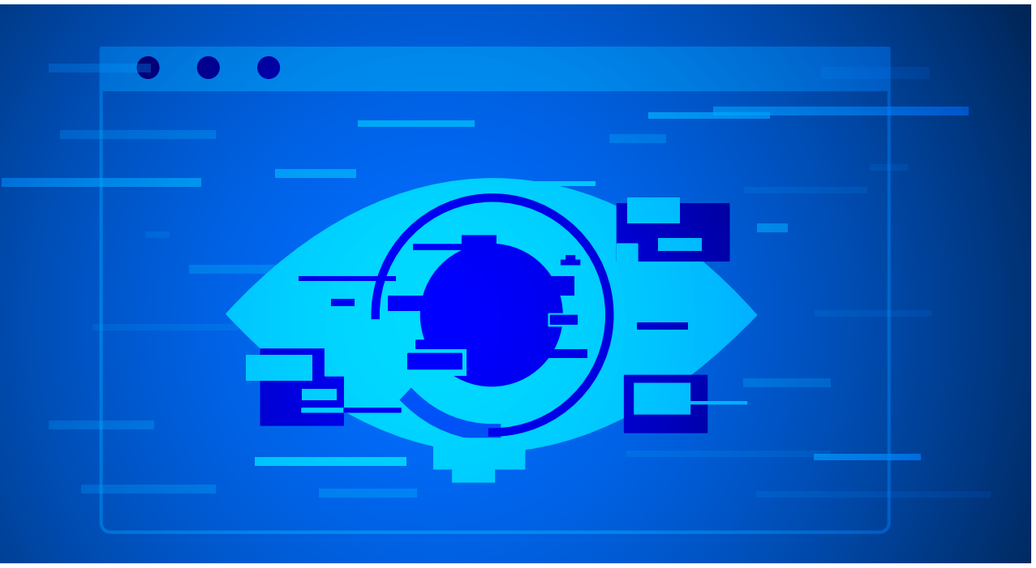
Évolution de la **cybercriminalité** sur le darknet

L'évolution de la cybercriminalité sur le darknet est comparable à une course aux armements technologiques permanente : les progrès technologiques réalisés dans les domaines de la sécurité et du numérique incitent en effet les cybercriminels à développer des méthodes toujours plus sophistiquées pour contourner les nouvelles mesures mises en œuvre. Les évènements mondiaux, tels que les récessions économiques, influencent encore davantage ce cycle d'innovation, ce qui peut entraîner une intensification des activités des cybercriminels qui cherchent à réaliser des profits illicites. Ces dynamiques se traduisent par un essor de la cybercriminalité en tant que service (CaaS), qui a transformé la cybercriminalité en une profession plus organisée et plus accessible. La CaaS offre des outils et des services de cybercriminalité prêts à l'emploi, permettant même à ceux ayant un minimum de savoir-faire technique de mener des attaques complexes, ce qui élargit la portée et l'ampleur des opérations cybercriminelles.

Alors que les forces de l'ordre et les organismes de réglementation renforcent leurs techniques de lutte contre la criminalité en ligne, les cybercriminels qui sévissent sur le darknet s'adaptent en permanence, recourant à des techniques de chiffrement avancées, à un routage sophistiqué du trafic et à des techniques complexes de blanchiment d'argent pour échapper à la détection. Cette adaptation continue complique la tâche des forces de l'ordre et met en évidence la professionnalisation et la résilience des réseaux cybercriminels. La prévalence croissante de la CaaS intensifie encore ce problème en transformant la cybercriminalité, qui devient plus systémique et plus difficile à enrayer, et en modifiant significativement le paysage mondial de la cybercriminalité sur le darknet.

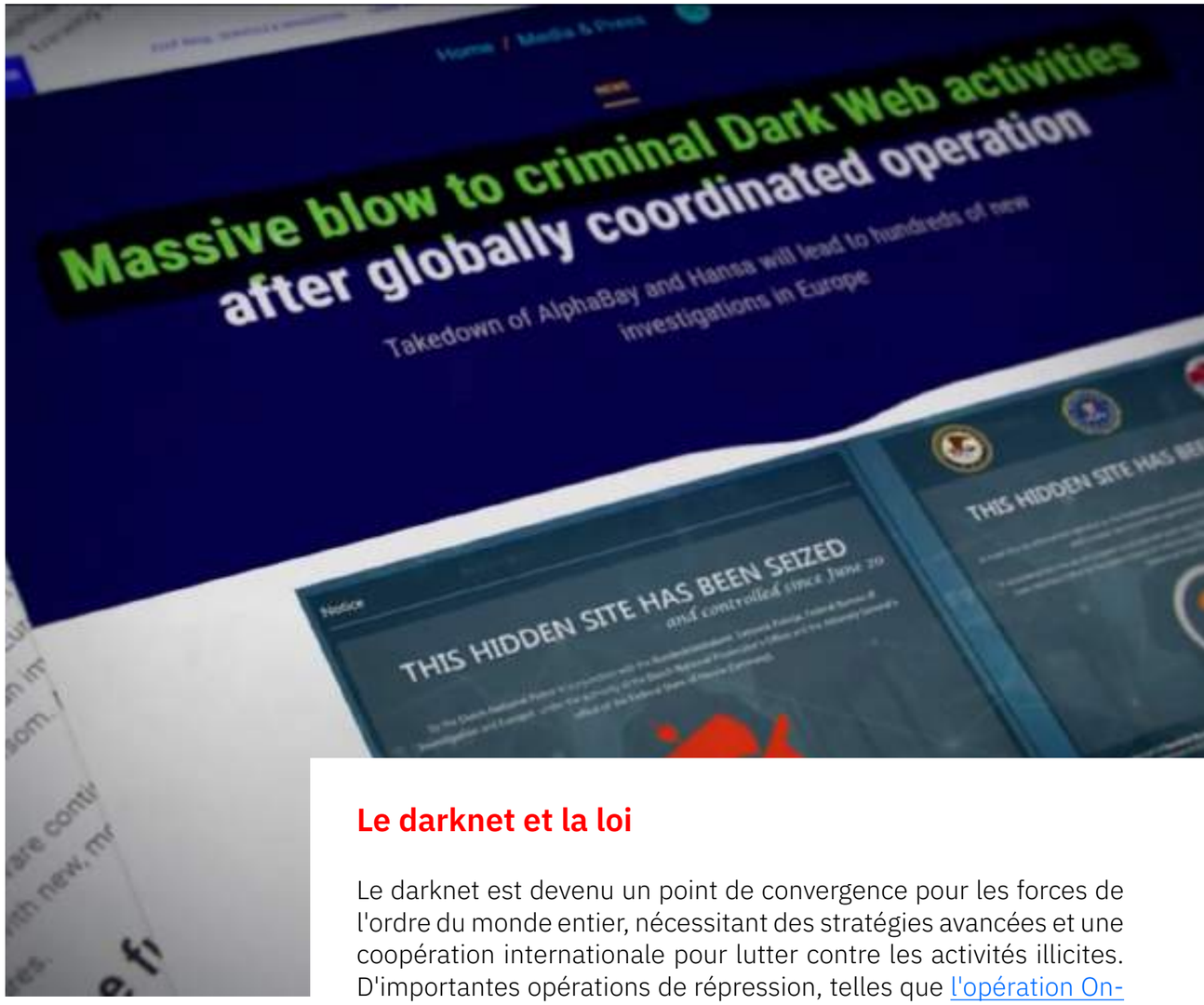
Activités illégales

Le darknet a considérablement évolué en tant que plaque tournante des activités illégales, enregistrant des changements notables dans les types d'opérations et les méthodes employées. Le trafic de drogue sur le darknet s'est étendu au-delà des drogues récréatives traditionnelles pour englober une gamme plus large de produits pharmaceutiques et de substances de synthèse, reflétant les progrès des techniques d'évasion et de distribution. Cette expansion est également perceptible dans le milieu des ventes illégales d'armes, qui a lui aussi gagné en sophistication et en discrétion. Les vendeurs d'armes du darknet recourent désormais à des méthodes d'expédition et de dissimulation avancées, qui leur permettent de contourner des mesures de sécurité plus strictes et d'étendre leur rayon d'action au-delà de leurs frontières nationales.



La fraude financière est elle aussi devenue plus complexe, avec des cybercriminels qui mettent au point de nouveaux stratagèmes (attaques de phishing, ransomwares, opérations complexes de blanchiment d'argent, etc.) qui tirent parti du système financier mondial.

La prolifération des cryptomonnaies a encore facilité ces activités illégales, en offrant un moyen de réaliser des transactions sécurisées et anonymes, difficiles à tracer. Cette utilisation des monnaies numériques a simplifié le financement des transactions illégales et posé d'importants problèmes aux forces de l'ordre, en compliquant la détection et l'interception des transactions et en contribuant à la course aux armements entre les cybercriminels et les autorités.



Le darknet et la loi

Le darknet est devenu un point de convergence pour les forces de l'ordre du monde entier, nécessitant des stratégies avancées et une coopération internationale pour lutter contre les activités illicites. D'importantes opérations de répression, telles que l'opération Onymous (2014), l'opération Bayonet (2017), l'opération DisrupTor (2020) et l'opération Dark HunTor (2021), ont perturbé de grands marchés illicites, renforçant la lutte contre la criminalité basée sur le darknet. La cybercriminalité étant un problème mondial, ces opérations n'ont pu être menées à bien que grâce à la collaboration de plusieurs pays.

L'anonymat du darknet complique les efforts des forces de l'ordre, car il devient très difficile de suivre les utilisateurs et leurs activités.

Les forces de l'ordre finlandaises méritent une mention spéciale pour leur participation rapide et efficace à ces efforts internationaux dans le cadre de l'opération DisrupTor, qui a établi des normes élevées en matière de rapidité et d'efficacité opérationnelles.

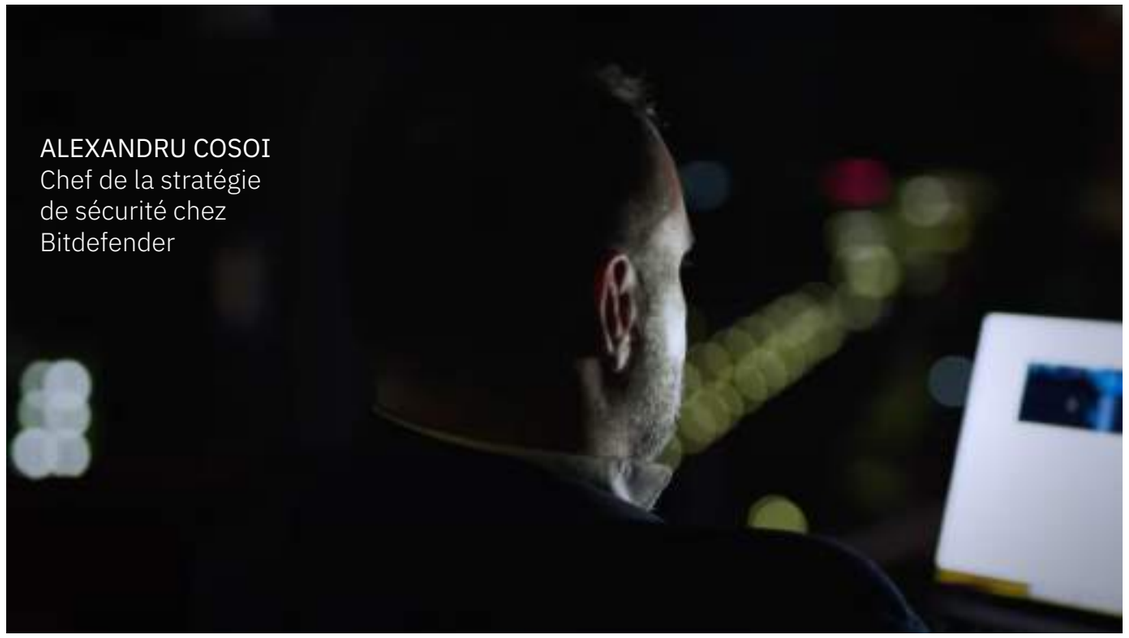
Quelle que soit l'efficacité de certaines opérations, la surveillance du darknet reste difficile. L'anonymat du darknet complique les efforts des forces de l'ordre, car il devient très difficile de suivre les utilisateurs et leurs activités. Des questions juridiques complexifient encore ces efforts, dans la mesure où les cybercriminels opèrent souvent dans plusieurs pays, exploitant les divergences juridiques entre les différentes juridictions.

Les forces de l'ordre sont également confrontées à des obstacles opérationnels, tels que le manque de formations spécialisées, la difficulté à maintenir la chaîne de possession des preuves numériques et la difficulté à combler les lacunes juridiques exploitées par les cybercriminels. Par exemple, les services axés sur la protection de la vie privée et les juridictions dotées d'une législation laxiste en matière de cybercriminalité peuvent, par inadvertance, offrir un refuge aux opérations du darknet.

La promotion de normes et de pratiques mondiales en matière de cybersécurité dans les secteurs privé et public peut améliorer la protection des données, la réponse aux incidents et la sécurité des infrastructures critiques dans le monde entier.

La communauté internationale doit collaborer au développement d'une solution pour lutter contre la cybercriminalité. Les pays qui adoptent des cadres juridiques transfrontaliers peuvent rationaliser les opérations des forces de l'ordre. De la même façon, des protocoles de partage améliorés faciliteraient des réponses rapides et efficaces aux cybermenaces émergentes et permettraient de coordonner les efforts entrepris contre des réseaux cybercriminels complexes et transnationaux. La promotion de normes et de pratiques mondiales en matière de cybersécurité dans les secteurs privé et public peut améliorer la protection des données, la réponse aux incidents et la sécurité des infrastructures critiques du monde entier, rendant la tâche plus difficile aux cybercriminels.

Une expertise
DE PREMIÈRE LIGNE



Alexandru Cosoi, chef de la stratégie de sécurité chez Bitdefender, a une grande expérience de la lutte contre la cybercriminalité. Selon lui, le paysage des menaces du darknet est de plus en plus complexe, en raison des avancées technologiques et de la sophistication des tactiques cybercriminelles, alimentées par des technologies d'analyse avancée et de Machine Learning. Dans le contexte de ce défi imminent, Cosoi estime qu'en dépit de l'évolution des tactiques cybercriminelles, les défenseurs ne seront pas en reste, développant leurs propres contre-mesures.

Il note que les récents succès rencontrés dans le démantèlement d'importantes places de marché du darknet, telles que Hansa et AlphaBay, montrent que les forces de l'ordre sont capables de s'adapter et de devenir plus efficaces dans la lutte contre ces menaces. Cosoi souligne également que ces victoires ne se sont pas le fruit d'un microcosme, mais ont nécessité une coopération internationale, permettant aux forces de l'ordre mondiales de tirer efficacement parti de leurs capacités croissantes en matière de lutte contre la cybercriminalité.

Cosoi note enfin qu'en dépit de nouvelles stratégies de cybersécurité innovantes, la charge ne repose pas uniquement sur les forces de l'ordre. Le renforcement des partenariats public-privé sera déterminant pour aider à relever les défis croissants posés par le darknet.

Bitdefender est, et continuera d'être, un partenaire solide, jouant un rôle proactif dans ces efforts. Ce rôle consiste notamment à collaborer avec les forces de l'ordre, en leur fournissant une expertise cruciale qui a été déterminante dans le cadre de plusieurs opérations clés. En analysant le trafic réseau, en déchiffrant les communications et en exposant les vulnérabilités présentes dans les réseaux criminels, Bitdefender a eu un impact significatif sur les capacités opérationnelles des marchés du darknet.

Bitdefender est, et continuera d'être, un partenaire solide, jouant un rôle proactif dans ces efforts. Ce rôle consiste notamment à collaborer avec les forces de l'ordre, en leur fournissant une expertise cruciale qui a été déterminante dans le cadre de plusieurs opérations clés.

Bâtir **un avenir** plus fort

Alors que nous cherchons à bâtir un avenir cybersécuritaire plus fort, notre vision est claire :en éliminant les barrières entre les agences internationales, en renforçant les partenariats public-privé et en assumant la responsabilité collective de la lutte contre la cybercriminalité, nous pouvons ouvrir la voie d'un monde numérique plus sûr. Cette approche collaborative améliore non seulement notre capacité à aborder les complexités du darknet, mais elle permet également de le préserver en tant que bastion de sécurité pour ceux qui ont réellement besoin d'anonymat, tels que les lanceurs d'alerte et les personnes soumises à des régimes oppressifs, sans qu'il serve de refuge aux cybercriminels.

La lutte contre la cybercriminalité est un défi partagé qui transcende les frontières et les secteurs. En favorisant une meilleure compréhension entre les gouvernements, les entreprises et les individus du monde entier, nous pouvons faire en sorte que le darknet ne devienne pas un terrain de jeu pour des activités illicites, mais reste un outil critique pour la sécurité personnelle et la liberté d'expression. Grâce à ces efforts concertés, l'avenir de la cybersécurité s'annonce radieux : assurer la sécurisation du paysage numérique tout en préservant les valeurs fondamentales de la confidentialité et de la liberté.

Bitdefender® Global Leader In Cybersecurity

Siège en Roumanie
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T : +40 21 4412452
F : +40 21 4412453

Siège aux États-Unis
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com/fr-fr/

Trusted.Always.

Bitdefender est un leader mondial de cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender compte parmi les experts les plus fiables de l'industrie pour l'élimination des menaces, la protection de la vie privée et des données, et la cyber résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent plus de 400 nouvelles menaces chaque minute et répondent à environ 40 milliards de requêtes de menaces par jour. La société a été la première à innover dans le domaine des malwares, de la sécurité de l'IoT, de l'analyse comportementale et de l'intelligence artificielle. Sa technologie est utilisée sous licence par plus de 150 éditeurs parmi les plus reconnus au monde. Fondée en 2001, Bitdefender a des clients dans 170 pays et possède des bureaux dans le monde entier.