Bitdefender® Global Leader In Cybersecurity

Exploration LE DARKNET

La sous-culture des cybercriminels

Table des matières

Introduction

Le darknet est une partie distincte et cachée d'Internet, intentionnellement
Le darknet est traditionnellement inaccessible par les navigateurs standards et invisible pour les moteurs de recherche classiques, contrairement au deep web, qui comprend toutes les parties d'internet non indexées par les moteurs de recherche mais néanmoins accessibles avec une autorisation appropriée. Le darknet nécessite des logiciels, des configurations ou des autorisations spécifiques pour y accéder, ce qui le distingue du web de surface, qui est ouvert au grand public.

complexités et comprendre les sous-cultures qui fleurissent dans cet environnement protégé par l'anonymat. Ces sous-

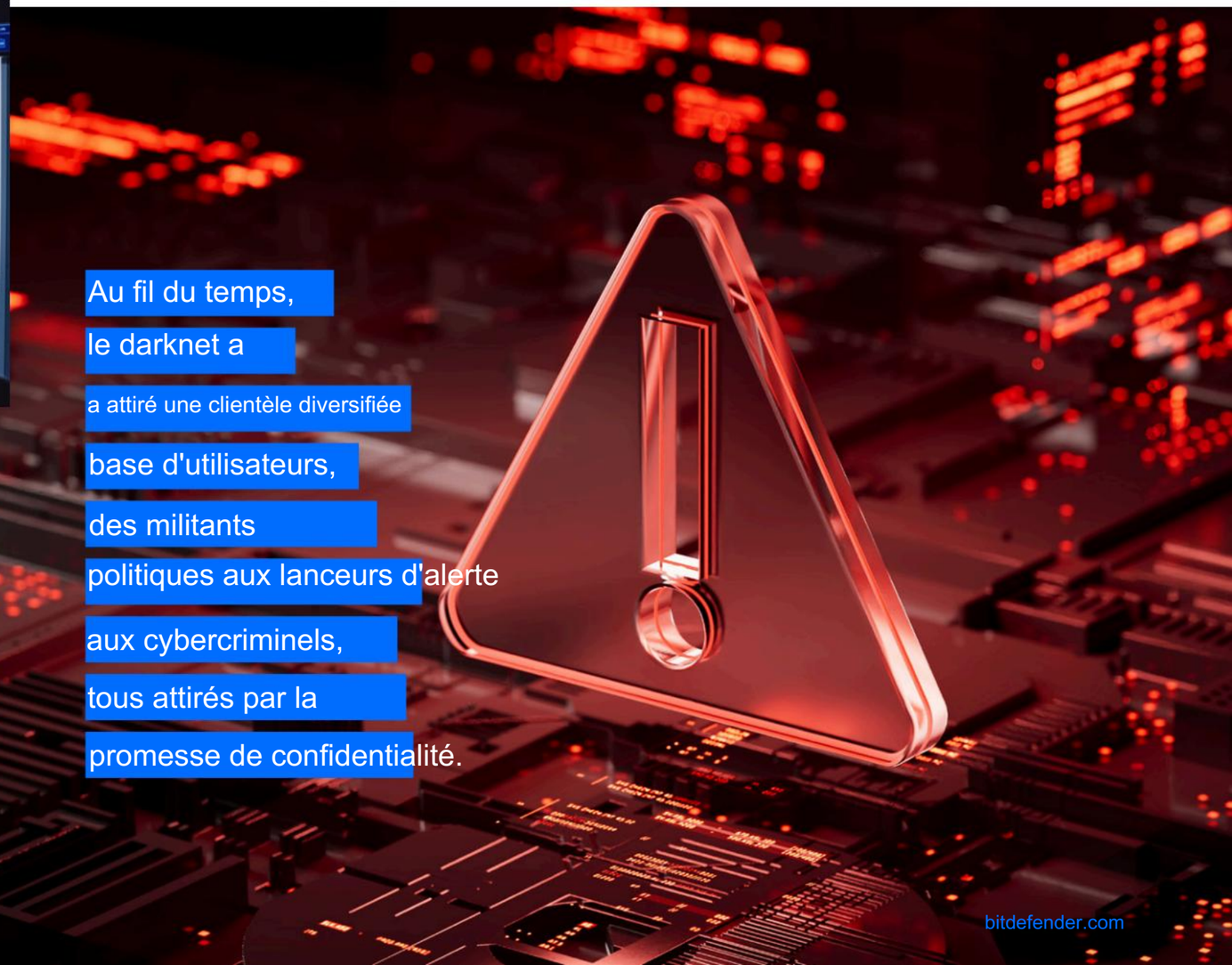
Comprendre le darknet est essentiel pour naviguer dans son réseau. Les cultures, qui vont des centres de cybercriminalité aux forums de dissidents politiques, influencent l'évolution des mesures de confidentialité sur Internet et le paysage des cybermenaces auxquelles les entreprises doivent faire face dans le cadre de leurs opérations.

Historique Contexte

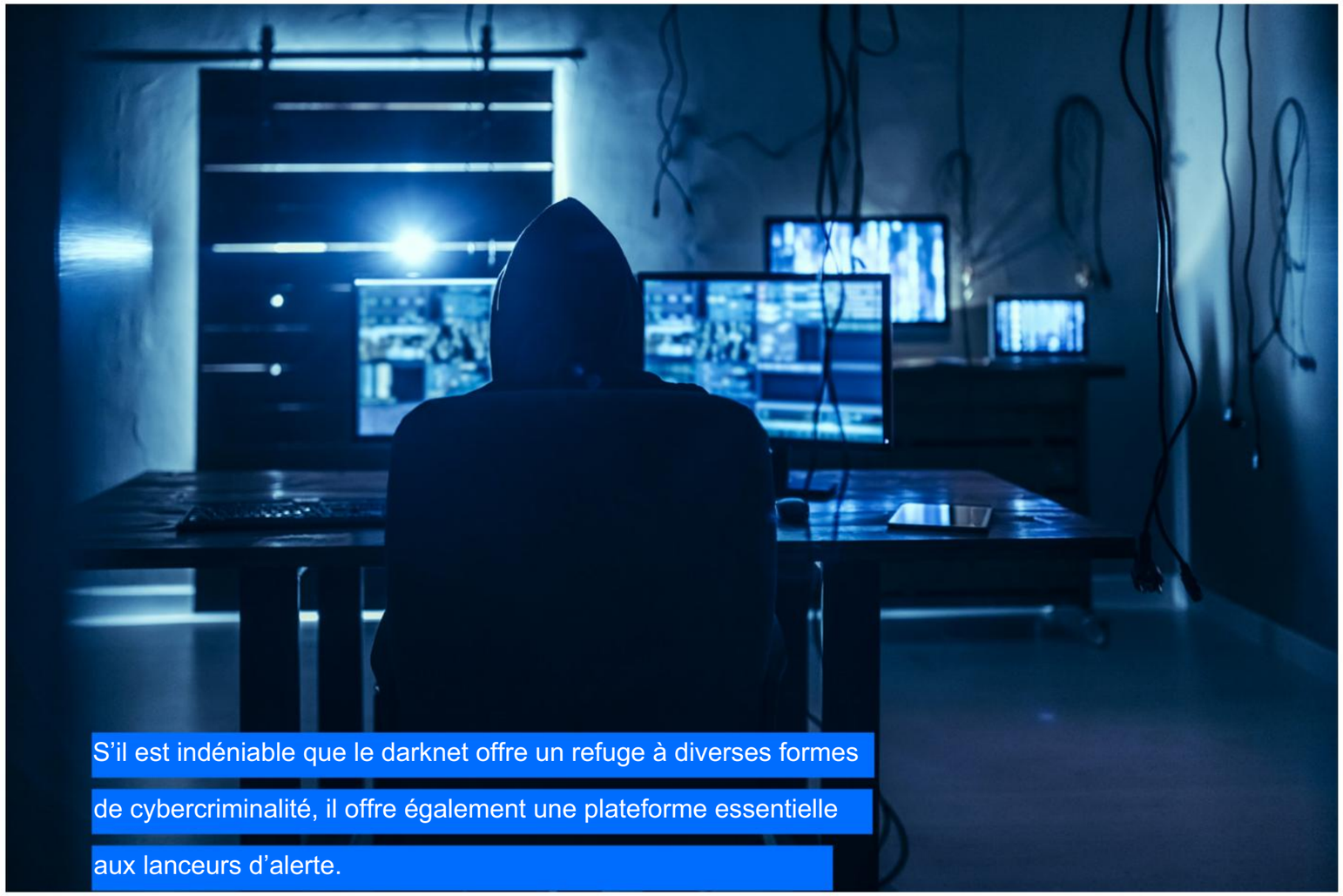
Le Darknet a commencé comme un outil de communication militaire conçu signé pour des échanges sécurisés et anonymes pendant le Froid Guerre, utilisant un cryptage avancé pour protéger les messages- Le cryptage a ouvert la voie à de nouvelles avancées technologiques Des avancées qui ont élargi les capacités et l'accessibilité du darknet . Le développement du réseau TOR (The Onion Router) L'anonymat des utilisateurs a été considérablement amélioré grâce au cryptage et au réacheminement du trafic Internet via un réseau mondial de relais, protégeant ainsi l'identité et la localisation des individus. Cette évolution a été complétée par l' essor des crypto-monnaies comme le Bitcoin, qui a facilité les transactions anonymes , faisant du darknet une plateforme attrayante pour diverses activités au-delà de ses objectifs gouvernementaux et militaires initiaux.

Au fil du temps, le darknet a attiré une base d'utilisateurs diversifiée, allant des activistes politiques et des lanceurs d'alerte aux cybercriminels, tous attirés par la promesse de la confidentialité. Ce changement démographique a donné naissance à une sous-culture complexe, riche de normes et de valeurs uniques. Associé aux évolutions technologiques, il a donné naissance à divers marchés, tels que la tristement célèbre Silk Road, qui a utilisé l'anonymat offert par TOR et l'obscurité financière des cryptomonnaies pour échanger des biens et des services illicites.

Ces marchés ont longtemps été considérés comme intouchables en raison de leur anonymat. Cependant, 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.



Commun Idées fausses



S’il est indéniable que le darknet offre un refuge à diverses formes de cybercriminalité, il offre également une plateforme essentielle aux lanceurs d’alerte.

pour partager des informations sensibles de manière anonyme, soutenir les individus dans des régimes oppressifs qui cherchent des moyens de liberté d'expression et faciliter la tâche des journalistes et des chercheurs qui ont besoin d'accéder ou de partager des données censurées en tout

Bitdefender Global Leader In Cybersecurity

Le darknet est souvent interprété à tort comme un monde souterrain obscur utilisé exclusivement pour des activités illicites, mais cette perspective néglige sa nature multiforme et ses utilisations légitimes.

Il est indéniable que le darknet est un refuge pour diverses formes de cybercriminalité. Il offre également une plateforme essentielle aux lanceurs d'alerte pour partager des informations sensibles de manière anonyme, soutient les individus dans les régimes oppressifs en quête de liberté d'expression et facilite la tâche des journalistes et des chercheurs qui ont besoin d'accéder ou de partager des données censurées en toute sécurité. Ces fonctions s'avèrent indispensables dans les pays où les médias conventionnels sont fortement contrôlés ou où le maintien de l'anonymat est crucial pour la sécurité et la liberté personnelles, comme en Russie.

Le Darknet n’est pas aussi facilement accessible que le suggèrent les mythes populaires. Il nécessite des connaissances techniques et des outils spécifiques pour naviguer, de sorte que l’ internaute moyen ne peut pas simplement se connecter et accéder à des contenus illicites . Ceux qui le font découvriront que le Darknet n’est pas aussi vaste que les médias le décrivent. Il est bien plus petit que la vaste étendue du Web de surface, ne représentant que 5 % du volume. Bien qu'il héberge une gamme de contenus illégaux, une part importante est consacrée à des activités légitimes.

S’il est vrai que l’anonymat offert par le darknet rend plus difficile l’action des forces de l’ordre, il s’agit d’un compromis en faveur de la capacité à protéger positivement la vie privée et à permettre la libre expression dans des environnements restrictifs.

La sous-culture des cybercriminels

Le darknet héberge diverses communautés allant des hackers aux militants politiques, chacun lié par des normes et des valeurs communes qui maintiennent l'ordre dans ce royaume caché.

La sécurité des informations est assurée par des applications de messagerie cryptées et des forums spécialisés, essentiels pour préserver l'anonymat et faciliter le libre échange d'idées. Ces plateformes soutiennent non seulement des activités illicites, mais servent également de lieux de discussion légitimes sur des 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 surveillance traditionnelle des forces de l'ordre, en s'appuyant plutôt sur des systèmes fondés sur la réputation pour régler les différends. Ce cadre favorise une culture où la confiance est primordiale et où les membres collaborent souvent pour atteindre des objectifs communs ou résoudre des menaces.

Structures sociales

Différentes structures sociales, allant des formats hiérarchiques aux formats décentralisés, contribuent à organiser le darknet. Dans certains forums et marchés du darknet, une hiérarchie distincte prévaut, où les modérateurs et les dirigeants jouent un rôle essentiel dans le maintien de l'ordre, l'établissement de règles et l'orchestration des activités. Ces dirigeants sont souvent des membres chevronnés jouissant d'une grande confiance et d'une grande autorité au sein de la communauté.

En revanche, d’autres parties du darknet fonctionnent de manière plus décente. base centralisée, où le pouvoir et la prise de décision sont répartis entre de nombreux membres. Cela réduit la dépendance à un seul dirigeant et augmente potentiellement la résilience de la communauté face aux perturbations telles que les actions des forces de l'ordre.

Devenir membre de ces communautés soudées est généralement une démarche rigoureuse, qui implique des procédures de sélection pour garantir la fiabilité et la loyauté. Les membres potentiels peuvent avoir besoin d'être cautionnés par des membres existants ou de prouver leurs compétences et leurs intentions au moyen de divers tests.

Une fois admis, les nouveaux membres apprennent progressivement les ficelles culturelles, y compris le jargon et les symboles spécifiques du groupe. Le langage spécialisé et l'utilisation de symboles renforcent l'identité du groupe et servent de barrière à l'entrée, en tenant à distance les non-initiés et en renforçant la sécurité. Ces éléments culturels signifient l'appartenance et le statut au sein du groupe, distinguent les initiés des étrangers et déterminent souvent l'accès à des couches plus profondes de la communauté ou à des informations plus sensibles.

Bâtir la confiance

La confiance est une denrée aussi précieuse que les biens et services échangés dans ses limites. Compte tenu de l'anonymat et des risques juridiques, la cybercriminalité...

Les banques ont développé des systèmes sophistiqués pour établir et maintenir la confiance. Au cœur de ces systèmes se trouvent des mécanismes de réputation, des services d'entiercement et des processus de vérification cryptographique qui garantissent la transmission intégrité et authenticité de l'action.

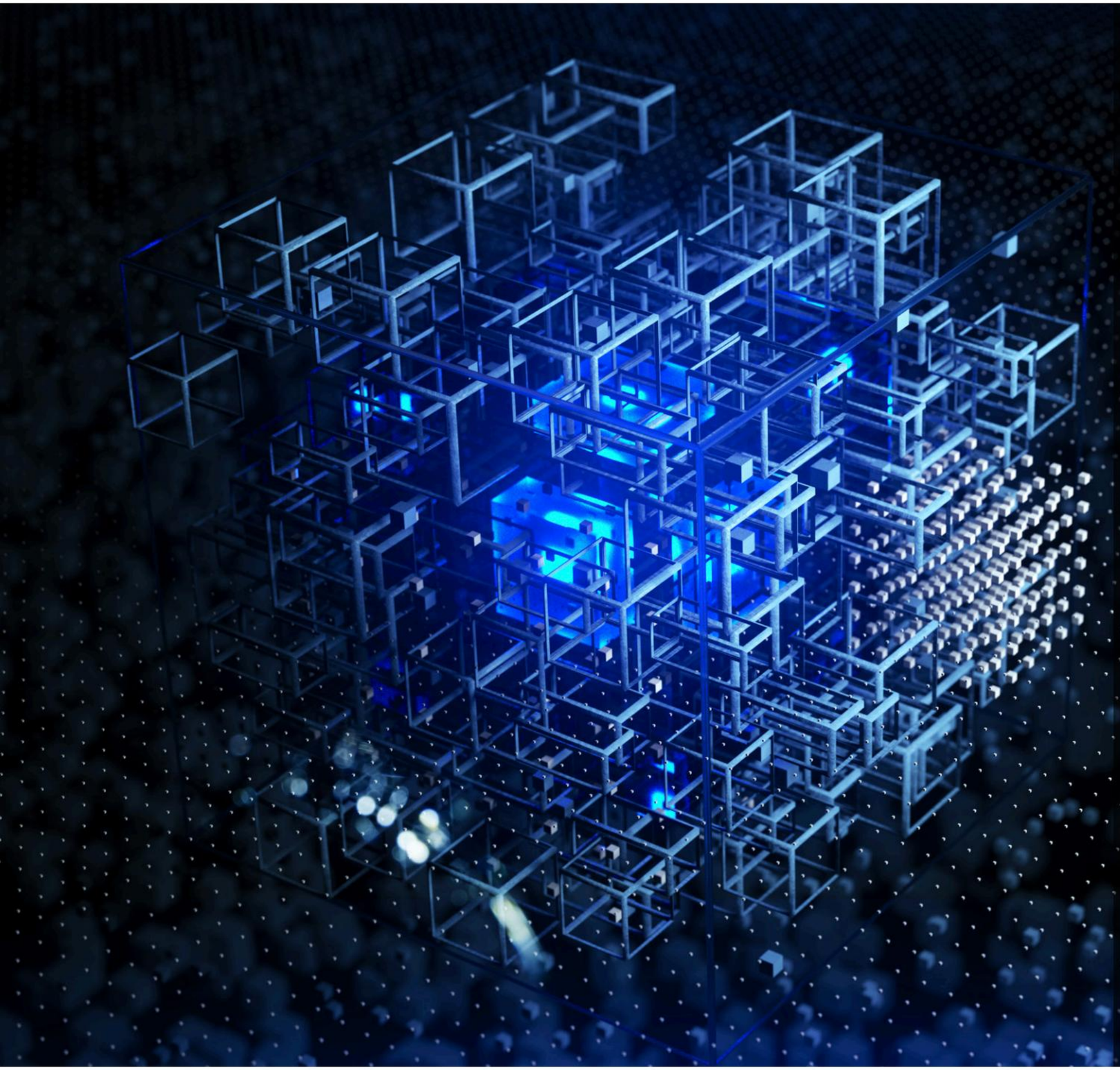
La vérification des biens et des services sur le darknet commence par des systèmes de séquestre, qui conservent les fonds sur un compte sécurisé jusqu'à ce que toutes les parties soient satisfaites de la transaction. Ce système protège les acheteurs des vendeurs frauduleux en ne libérant le paiement qu'une fois les marchandises reçues et vérifiées.

La cryptographie telle que Pretty Good Privacy (PGP) s'appuie sur l'entiercement en vérifiant de manière sécurisée les identités et en cryptant les communications. Cela garantit que les messages, les transactions et les identités restent confidentiels.

essentiels et authentiques, les protégeant des menaces externes et internes.

Les systèmes de réputation renforcent encore davantage la confiance au sein de la communauté. Tout comme les systèmes de feedback sur les plateformes de commerce électronique bien connues, les marchés du darknet utilisent des mécanismes de feedback générés par les utilisateurs pour évaluer les vendeurs. Ces évaluations donnent aux acheteurs potentiels un historique de confiance. fichier pour chaque vendeur, influençant les décisions et le comportement des acheteurs. Les liens avec les fournisseurs intensifient ce cadre de confiance, les marchés éliminant les vendeurs peu sérieux ou frauduleux en exigeant des vendeurs qu'ils déposent une signature.

Une quantité importante de cryptomonnaies est disponible sous forme d'obligations. Seuls ceux qui s'engagent dans des opérations à long terme sont prêts à souscrire de telles obligations.



Evolution de la cybercriminalité sur le Darknet

L'évolution de la cybercriminalité sur le darknet est continue course aux armements technologiques, où les progrès en matière de sécurité et les technologies numériques incitent les cybercriminels à développer davantage à des méthodes sophistiquées pour contourner ces mesures. Les événements mondiaux tels que les crises économiques influencent encore davantage ce cycle d'innovation, qui peut accroître les activités cybercriminelles, les individus cherchant à obtenir des gains financiers illicites. Cette dynamique est résumée dans l'essor de la cybercriminalité en tant que service (CaaS), qui a transformé la cybercriminalité en une profession plus organisée et plus accessible. Le CaaS propose des outils et des services de cybercriminalité prêts à l'emploi , un savoir-faire technique minimal

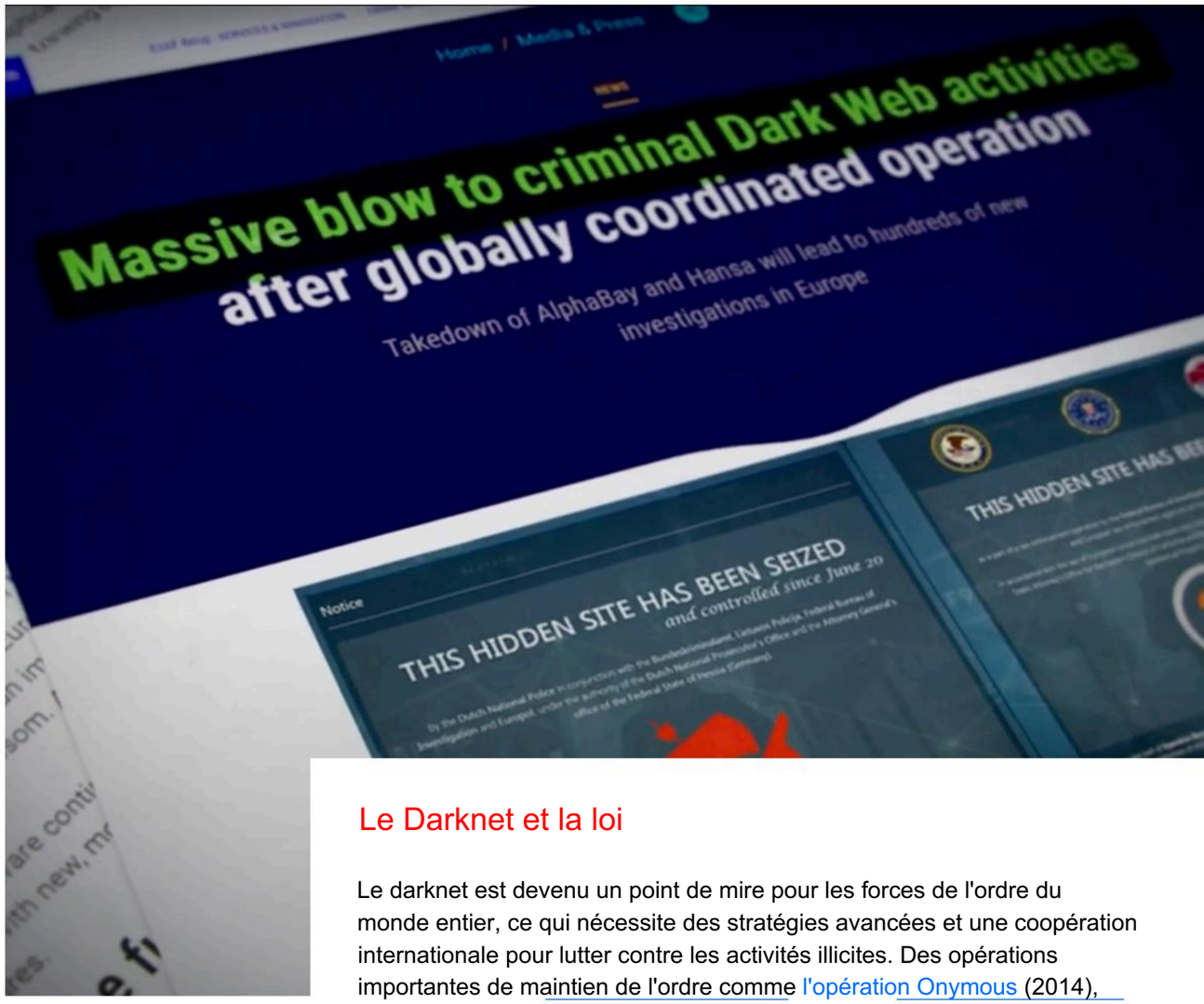
Alors que les forces de l'ordre et les organismes de réglementation intensifient leurs techniques de lutte contre la criminalité en ligne, les cybercriminels du darknet s'adaptent continuellement, en utilisant un cryptage avancé et un routage de trafic sophistiqué. et des techniques complexes de blanchiment d'argent pour échapper à la détection. Cette adaptation en cours complique les efforts des forces de l'ordre et met en évidence la professionnalisation et la résilience des réseaux de cybercriminalité. La prévalence croissante du CaaS accélère encore ce problème, transformant la cybercriminalité, la rendant plus systémique et plus difficile à maîtriser, et impactant considérablement le paysage de la cybercriminalité mondiale sur le darknet.

Activités illégales

Le darknet a considérablement évolué en tant que plaque tournante des activités illégales, avec des changements notables dans les types et les méthodes d'opérations. Le trafic de drogue sur le darknet s'est étendu au-delà des drogues récréatives traditionnelles pour inclure un éventail plus large de produits pharmaceutiques et de substances synthétiques, reflétant les progrès des techniques d'évasion et de distribution. Cette expansion se reflète dans le domaine des ventes d'armes illégales, qui sont également devenues plus sophistiquées et discrètes. Les trafiquants d'armes du darknet utilisent désormais des méthodes d'expédition et de dissimulation avancées, leur permettant de contourner des mesures de sécurité plus strictes et d'étendre leur portée au-delà des frontières internationales.

La fraude financière est également devenue plus complexe, les cybercriminels développant de nouveaux stratagèmes tels que des attaques de phishing élaborées, des ransomwares et des opérations complexes de blanchiment d'argent qui exploitent le 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 retracer. Cette utilisation des monnaies numériques a simplifié le financement des transactions illégales et posé des défis considérables aux efforts des forces de l'ordre, compliquant la détection et l'interception des transactions et contribuant à la course aux armements en cours entre les cybercriminels et les autorités.



Le Darknet et la loi

Le darknet est devenu un point de mire pour les forces de l'ordre du monde entier, ce qui nécessite des stratégies avancées et une coopération internationale pour lutter contre les activités illicites. Des opérations importantes de maintien de l'ordre comme l'opération Onymous (2014), Opération Baïonnette (2017), Opération DisrupTor (2020) et Opération Dark Hun (2021) ont perturbé les principaux marchés illicites, renforçant ainsi la lutte contre la criminalité sur le darknet. La cybercriminalité étant un problème mondial, ces opérations n'ont réussi que grâce aux efforts collaboratifs de plusieurs pays.

L'anonymat du darknet complique les efforts des forces de l'ordre, car le suivi des utilisateurs et de leurs activités devient redoutable.

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

Malgré l'efficacité de certaines opérations, la surveillance du darknet reste un véritable défi. L'anonymat du darknet complique les efforts des forces de l'ordre, car il devient difficile de suivre les utilisateurs et leurs activités . Les questions de juridiction compliquent encore davantage ces efforts, car les cybercriminels opèrent souvent dans plusieurs pays, exploitant les divergences juridiques entre les différentes juridictions.

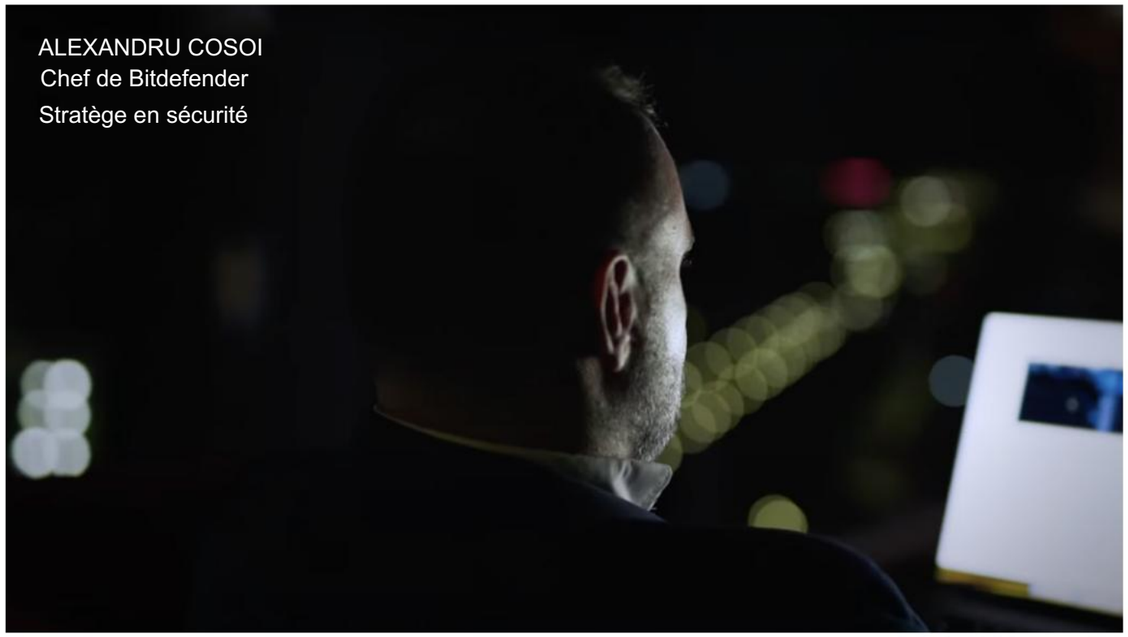
Les forces de l'ordre sont également confrontées à des obstacles opérationnels, comme le manque de formation spécialisée, les difficultés à maintenir la chaîne de traçabilité des preuves numériques et à contourner les failles juridiques exploitées par les cybercriminels. Par exemple, les services axés sur la confidentialité et les juridictions aux lois laxistes en matière de cybercriminalité peuvent par inadvertance fournir des refuges aux opérations du darknet.

Les forces de l'ordre finlandaises mérite une mention spéciale pour leur réponse rapide et efficace à ces efforts internationaux en Opération DisrupTor, qui a établi des normes élevées de rapidité et d'efficacité opérationnelle.

La communauté internationale doit travailler ensemble pour trouver une solution à la lutte contre la cybercriminalité. Les pays qui adoptent des cadres juridiques transfrontaliers peuvent rationaliser les opérations de maintien de l'ordre. De même, des protocoles de partage améliorés faciliteraient la réponse rapide et efficace aux cybermenaces émergentes et coordonneraient les efforts contre les réseaux complexes et transnationaux de cybercriminalité. 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, ce qui obligerait les cybercriminels à travai

En première ligne

EXPERTISE Cosoi constate que malgré les nouvelles stratégies innovantes de cybersécurité,



expérimenté dans la lutte contre la cybercriminalité. Il voit

Le paysage des menaces du Darknet devient de plus en plus complexe en raison des avancées technologiques et des tactiques de

Alexandru Cosoi, stratège en chef de la sécurité de Bitdefender, est cybercriminalité plus sophistiquées basées sur des analyses avancées et l'apprentissage automatique. Malgré ce défi imminent, Cosoi prédit que malgré l'évolution de leurs tactiques, les défenseurs feront de même en développant leurs contre-mesures.

Il note que le succès récent dans le démantèlement des principaux marchés du darknet tels que Hansa et AlphaBay montre que les forces de l'ordre peuvent s'adapter et devenir plus efficaces face à ces menaces. Cosoi souligne que ces victoires ne se sont pas produites dans une bulle mais ont nécessité une coopération internationale, permettant aux agences mondiales chargées de l'application de la loi d'exploiter efficacement leurs capacités croissantes pour lutter contre la cybercriminalité.

La charge ne repose pas uniquement sur les forces de l'ordre. Les partenariats public-privé seront essentiels pour aider à relever les défis croissants que le darknet apportera à la bataille.

Bitdefender a été et continuera d'être un partenaire solide, jouant un rôle proactif dans ces efforts. Cela comprend une collaboration avec les forces de l'ordre pour fournir une expertise cruciale en matière de cybersécurité, qui a joué un rôle déterminant dans plusieurs opérations clés. En analysant le trafic réseau, en décryptant les communications et en exposant les vulnérabilités des réseaux criminels, Bitdefender a considérablement influencé les capacités opérationnelles des marchés du darknet.

Bitdefender a été et continuera d'être un partenaire solide, jouant un rôle proactif dans ces efforts. Cela comprend la collaboration avec les services juridiques les forces de l'ordre ont fourni une expertise cruciale en matière de cybersécurité, qui a joué un rôle déterminant dans plusieurs opérations clés

Construire un Plus fort Avenir

Alors que nous cherchons à bâtir un avenir plus solide en matière de cybersécurité, la vision est claire : en éliminant les murs entre les agences, en renforçant les partenariats public-privé et

En assumant la responsabilité collective de lutter contre la cybercriminalité , nous pouvons ouvrir la voie à un monde numérique plus sûr. Cette approche collaborative non seulement améliore notre capacité à faire face aux complexités du darknet, mais préserve également le rôle de bastion de sécurité pour ceux qui ont véritablement besoin d'anonymat – comme les lanceurs d'alerte et les personnes sous régime oppressif – sans qu'il ne serve de refuge aux criminels.

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

Bitdefender Global Leader In Cybersecurity

Siège social de la Roumanie
Tours d'Orhideea
15A, route Orhideelor,
6e arrondissement,
Bucarest 060071
Tél. : +40 21 4412452
Télécopieur : +40 21 4412453

QG des États-Unis
3945 Cercle de la Liberté,
Suite 500, Santa Clara,
Californie, 95054

bitdefender.com

De confiance. Toujours.

Bitdefender est un leader de la cybersécurité qui propose les meilleures solutions de prévention, de détection et de réponse aux menaces dans le monde entier. Gardien de millions d'environnements grand public, commerciaux et gouvernementaux, Bitdefender est l'un des experts les plus fiables du secteur pour éliminer les menaces, protéger la confidentialité et les données et permettre la cyber-résilience. Grâce à des investissements importants dans la recherche et le développement, Bitdefender Labs détecte plus de 400 nouvelles menaces chaque minute et valide environ 40 milliards de requêtes quotidiennes sur les menaces. L'entreprise est à l'origine d'innovations révolutionnaires dans les domaines de la lutte contre les logiciels malveillants, de la sécurité IoT, de l'analyse comportementale et de l'intelligence artificielle. Sa technologie est sous licence auprès de plus de 150 des marques technologiques les plus reconnues au monde. Lancé en 2001, Bitdefender compte des clients dans plus de 170 pays et dispose de bureaux dans le monde entier.