BITSIGHT

LIVREBLANC

Sept stratégies pour enquêter sur le Deep et le Dark Web

Table des matières

01
Introduction

01 Introduction

Le deep et le dark web sont une véritable mine d'or d'informations sur l'activité des acteurs malveillants. Toutefois, exploiter cette ressource pour protéger votre organisation peut s'avérer difficile, surtout pour les non-initiés. Dans ce guide, nous présentons les 7 stratégies utilisées par les analystes de Bitsight pour enquêter sur le deep et le dark web, dans le but de renforcer votre programme de cyberveille.

02
Premiers pas

02 Premiers pas

Élaborer une vision complète du paysage des menaces pour votre entreprise ou organisation est une tâche complexe et exigeante. Il faut commencer par poser une question. Les questions de renseignement basées sur le deep et le dark web entrent généralement dans les catégories suivantes :

- Quelles sont les cibles des acteurs malveillants ?
- Comment ces acteurs comptent-ils frapper / quelles TTP (tactiques, techniques et procédures) utilisent-ils ?
- Dans quelle mesure cette menace se matérialise-t-elle ?

Une fois la ou les questions formulées, l'analyste doit définir une méthodologie et un cadre d'analyse pour y répondre. Chaque situation étant différente, certaines approches restent globalement efficaces pour confirmer ou infirmer une hypothèse.

Selon la nature de votre enquête sur les menaces, la meilleure approche peut consister à combiner plusieurs stratégies afin d'élargir vos recherches. Vous trouverez ci-dessous les sept stratégies que nous, chez Bitsight, jugeons particulièrement utiles.

Les 7 stratégies pour enquêter sur le deep et le dark web

01 Agréger les mentions pour identifier une tendance

02 Suivre les événements majeurs et les corréler à l'activité du dark web

03 Suivez les services

04 Rechercher les outils utilisés dans la chaîne d'attaque

05 Rechercher les produits issus des attaques

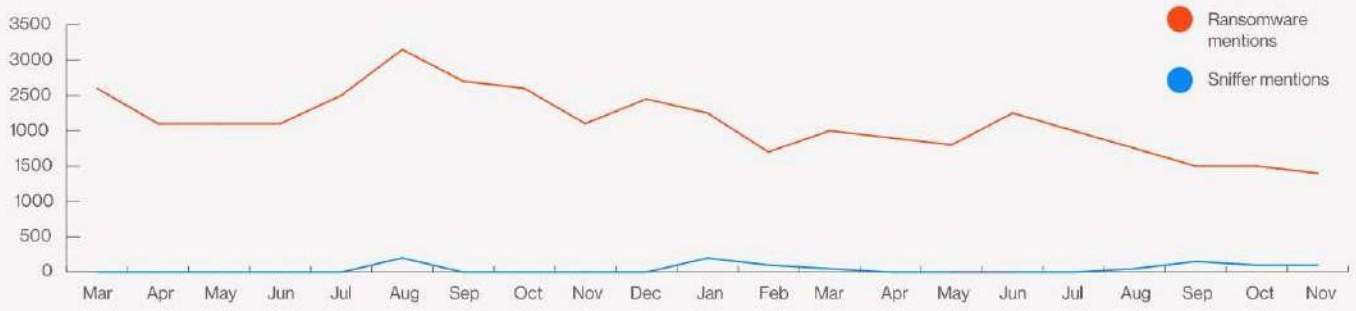
06 Rechercher des indices indirects

07 Extrapoler ce que les acteurs malveillants ne disent pas

Stratégie 1 : Agréger les mentions pour identifier une tendance

En suivant le nombre de requêtes sur le portail de renseignement sur les menaces de votre fournisseur au fil du temps, vous pouvez comprendre comment un sujet évolue dans les cercles souterrains. Cette approche peut fournir des informations précieuses sur le moment et la manière dont un phénomène particulier se renforce ou s'affaiblit.

Ce type d'analyse permet également de comparer deux tendances. Par exemple, les ransomwares et les sniffers de cartes bancaires (comme ceux utilisés par le groupe Magecart) ont été à l'origine d'attaques très médiatisées entre 2019 et 2020. Cependant, en comparant les mentions de chacun (voir graphique ci-dessous), on constate que les ransomwares sont nettement plus populaires que les sniffers de cartes bancaires parmi les acteurs du dark web. Cela peut suggérer, entre autres, que les attaques par sniffing sont plus difficiles à exécuter ou à monétiser, et attirent donc moins d'attention dans les milieux clandestins.



Nombre de mentions mensuelles de sniffers et de ransomwares identifiées sur le deep et le dark web en 2019 et 2020

Dans le portail d'investigation de Bitsight, vous pouvez créer une requête pour enquêter sur tout ce qui se trouve sur le Web profond et sombre, comme un type de menace, un acteur spécifique, un site ou un sujet général.

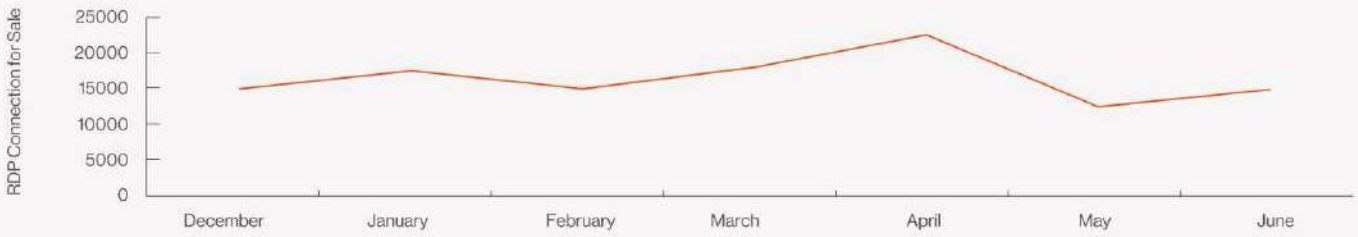
Une version plus avancée de cette approche consiste à examiner le nombre d'acteurs ou de sites uniques impliqués dans une requête particulière. Cela permet de mesurer l'ampleur et la diffusion d'un phénomène..

Par exemple, le graphique ci-dessous montre que lorsque les « meme stocks » (comme GameStop) ont explosé en janvier 2021, le nombre d'acteurs uniques participant aux canaux de messagerie sur le thème du trading a également fortement augmenté. Cela indique que de nombreux nouveaux acteurs ont rejoint les discussions.

Nombre d'utilisateurs uniques quotidiens actifs sur les canaux de messagerie dédiés au trading à la fin de 2019 et au début de 2020

Stratégie 2 : Suivre les événements majeurs et les corréler à l'activité du dark web

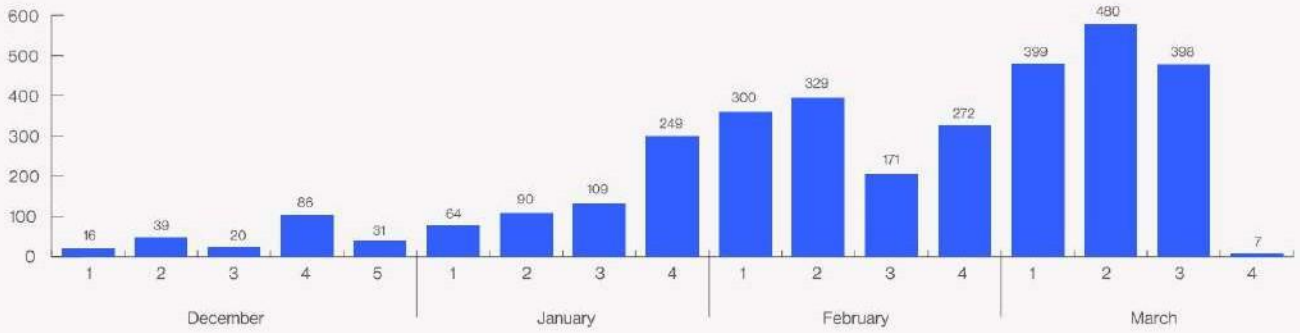
Les grandes actualités, en particulier celles liées à la cybersécurité et à la fraude, sont souvent discutées sur les forums clandestins. Les acteurs du dark web cherchent à tirer parti de ces événements pour créer de nouvelles opportunités. Par exemple, lorsque la pandémie de COVID-19 a entraîné une hausse sans précédent du télétravail, nous nous sommes demandé si cela allait provoquer une augmentation des serveurs RDP mis en vente sur le dark web. En effectuant une recherche dans le portail d'investigation de Bitsight sur les mentions de serveurs RDP en vente durant cette période, nos résultats ont confirmé notre hypothèse : davantage de télétravail signifiait davantage de serveurs RDP compromis.



Nombre de serveurs RDP compromis identifiés comme étant proposés à la vente sur le dark web à la fin de 2019 et au début de 2020

Grâce au portail d'investigation de Bitsight, les analystes peuvent accéder à des informations sur l'activité des acteurs malveillants, y compris sur des événements en temps réel.

De même, avec le déploiement des vaccins contre la COVID-19, nous avons constaté une augmentation du nombre de vaccins proposés à la vente chaque semaine sur les marchés clandestins.



Stratégie 3 : Suivre les services

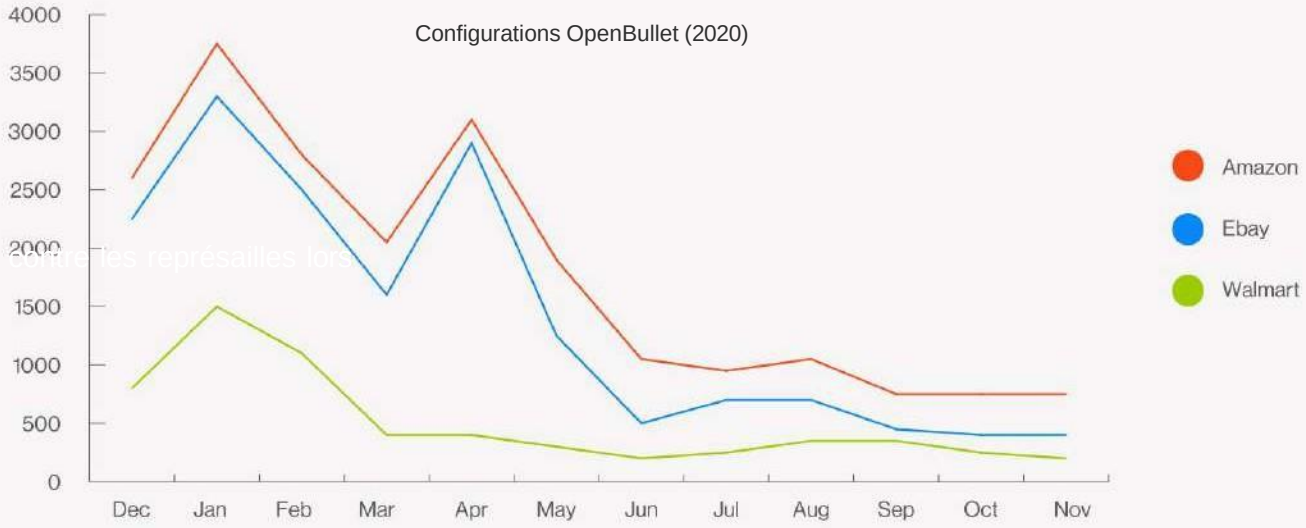
De nombreux acteurs du dark web se spécialisent dans un domaine particulier. Certains sont des auteurs de malwares, d'autres des ingénieurs sociaux, et d'autres encore savent blanchir de l'argent sans se faire détecter. Dans l'underground, ces acteurs proposent leurs attaques « en tant que service », permettant à n'importe quel cybercriminel en herbe d'assembler les éléments nécessaires pour lancer une attaque sophistiquée.

Un analyste peut étudier ces services pour comprendre l'ampleur des attaques. Les services plus rares et coûteux indiquent qu'ils sont à la fois très demandés et difficiles à exécuter. Par exemple, cet acteur propose l'interception de signaux mobiles pour des tarifs allant de 1 000 à 30 000 $.

De même, un autre acteur qui propose des « transferts » PayPal (c'est-à-dire du blanchiment d'argent) applique une commission de 25 %, ce qui montre que ces services sont considérés comme premium. À l'inverse, certains services sont très bon marché. Par exemple, l'accès shell à un site compromis, qui peut être utilisé dans le cadre d'une attaque plus vaste, ne coûte que 5,30 $. Cela indique que la compromission de sites web est plus simple, plus répandue, ou les deux

Stratégie 4 : Rechercher les outils utilisés dans la chaîne d'attaque

Dans une enquête axée sur les TTP (tactiques, techniques et procédures), il est pertinent de rechercher des outils spécifiques pouvant être utilisés dans un type d'attaque donné. Par exemple, OpenBullet est un outil populaire utilisé pour les attaques par credential stuffing (bourrage d'identifiants). En suivant l'évolution de ce logiciel, les défenseurs peuvent en comprendre les capacités et développer des protections adaptées. En analysant les services les plus ciblés par les configurations OpenBullet, les analystes peuvent identifier les services les plus exposés à ce type d'attaque.



Instances mensuelles de sites e-commerce majeurs ciblés par des configurations OpenBullet en 2020

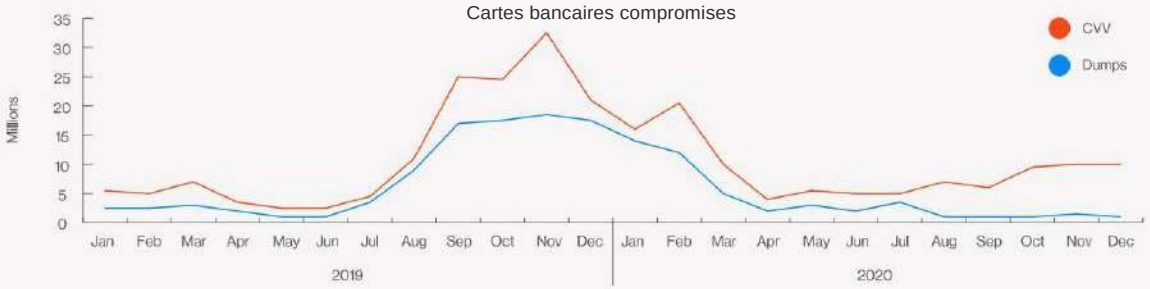
L'utilisation du portail d'investigation de Bitsight permet aux utilisateurs d'accéder discrètement à l'ensemble complet de nos renseignements sur les menaces, les protégeant ainsi contre d'éventuelles représailles au cours d'une enquête.

Stratégie 5 : Rechercher les produits issus des attaques

Les acteurs malveillants ne révèlent que rarement qui ils vont attaquer ou comment. En revanche, une fois l'attaque réussie, ils doivent en tirer profit. C'est pourquoi, sur les marchés et forums du dark web, les attaquants vendent des données compromises, des identifiants et des cartes bancaires. Parfois, des produits de moindre valeur sont même distribués gratuitement. Suivre ces produits issus des attaques peut fournir des indices sur ce qui a été compromis. Par exemple, une augmentation du nombre de journaux de plateformes de paiement vendus, comprenant des noms d'utilisateur et mots de passe valides, indique une forte hausse des attaques de type phishing.

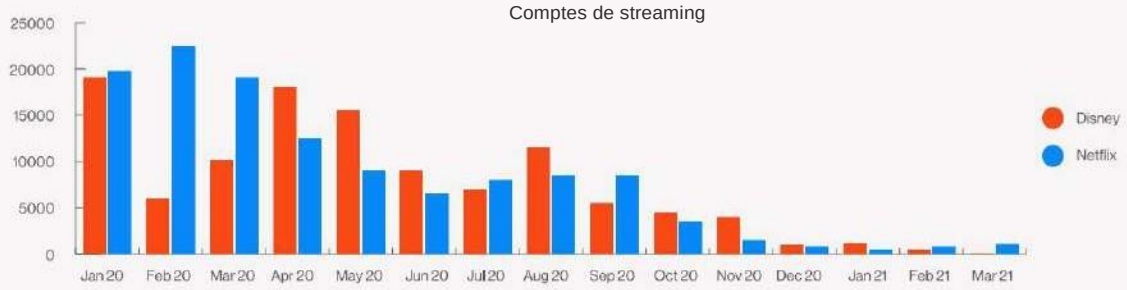
De la même manière, suivre les tendances en matière de quantités et de prix des produits vendus peut révéler des évolutions dans ce type d'attaque..

Par exemple, le graphique ci-dessous montre la quantité de cartes bancaires compromises (en CVV et dumps) vendues sur les marchés en 2019 et 2020.



Nombre mensuel de cartes bancaires compromises vendues sur les marchés clandestins en 2019 et 2020

Enfin, une forte baisse du nombre d'identifiants Netflix et Disney+ partagés peut indiquer que les mesures de défense sont devenues plus efficaces pour prévenir les attaques par credential stuffing.



Nombre mensuel d'identifiants compromis pour des services de streaming vendus sur les marchés clandestins en 2020 et au début de 2021

Stratégie 6 : Rechercher des indices indirects

Lorsqu'un analyste ne parvient pas à trouver de preuve formelle confirmant ou infirmant une hypothèse, il peut être utile de rechercher des preuves indirectes. Si l'hypothèse était vraie, que devrait-on également observer (et inversement) ?

Par exemple, nous avons voulu savoir s'il existait des signes indiquant une hausse de la cybercriminalité pendant les confinements liés à la COVID-19. Nous avons constaté une augmentation massive du nombre de mentions de services de transfert d'argent (blanchiment) proposés via PayPal et Cash App. Bien que cela ne prouve pas directement une montée de la cybercriminalité, nous avons estimé que cela reflétait la disponibilité générale de fonds acquis de manière frauduleuse.

Observer ces chiffres revient à compter les vautours autour d'un lion après la chasse : plus il y a de proies, plus les charognards sont nombreux.

Certains forums et places de marché sont fermés à la majorité des utilisateurs, ce qui les rend difficiles d'accès et encore plus difficiles à surveiller sur le long terme. La technologie de collecte automatisée de Bitsight est indétectable sur ces forums à accès restreint, offrant ainsi aux utilisateurs une visibilité unique sur l'activité souterraine.

Stratégie 7 : Extrapoler ce que les acteurs malveillants ne disent pas

Même si les acteurs du dark web ne partagent généralement pas leurs plans, il leur arrive parfois d'en dire un peu trop.
Peut-être ignorent-ils les bonnes pratiques en matière de sécurité opérationnelle, ou bien s'en moquent-ils. Ou encore, ils cherchent à démontrer leurs capacités pour attirer de nouveaux « clients », ou à se vanter afin de gagner en crédibilité.

Quelle que soit la raison, si un analyste parvient à trouver une « pépite », il est fort probable que d'autres acteurs soient impliqués dans le même type d'activité, mais de manière plus discrète.

Par exemple, un acteur a publié qu'il recherchait un partenaire pour intercepter des signaux de communication mobile afin de capturer des SMS, puis a indiqué plus tard qu'il avait « trouvé la solution et en avait une qui fonctionnait ». Bien qu'un seul message ne permette pas de mesurer l'ampleur du phénomène, on peut raisonnablement supposer que de nombreux autres acteurs utilisent également cette technique.

03
Résumé

03 Résumé

Les analystes en renseignement évoluent constamment dans un environnement où l'incertitude est grande, les données sont abondantes, et les ressources pour tout traiter sont limitées. Après avoir lu ce guide, nous espérons que vous comprenez mieux l'environnement que vous explorez, que vous êtes en mesure de définir les questions clés en matière de cyberveille, et que vous avez une méthode pour y répondre. En vous aidant à identifier les contenus les plus pertinents du deep et du dark web, ces stratégies vous permettront d'enquêter sur les cybermenaces potentielles de manière complète, précise et efficace.

Il est essentiel de se rappeler que la qualité d'une enquête dépend directement des outils utilisés. Une approche manuelle du renseignement sur le deep et le dark web ne vous mènera pas bien loin. Vous ne pourrez pas accéder aux bons sites, effectuer des recherches par mots-clés à grande échelle ni extraire des données quantitatives utiles.

Seul le portail d'investigation de Bitsight vous permet de découvrir efficacement les renseignements critiques et précieux nécessaires pour garder votre organisation informée et sécurisée.

À propos de Bitsight

Bitsight est le principal fournisseur mondial de renseignements sur les risques cyber, transformant la manière dont les responsables de la sécurité gèrent et atténuent les risques. En s'appuyant sur les données externes et les analyses les plus complètes du marché, Bitsight permet aux organisations de prendre des décisions éclairées et fondées sur les données, et fournit aux équipes de sécurité et de conformité de plus de 3 200 organisations dans plus de 70 pays les outils nécessaires pour détecter de manière proactive les expositions et agir immédiatement pour protéger leur entreprise et leur chaîne d'approvisionnement.

Grâce à sa plateforme innovante BitsightIQ, l'entreprise fournit des informations en temps réel sur les menaces, spécifiquement adaptées à la surface d'attaque externe et à l'écosystème tiers de chaque organisation

Pour en savoir plus, visitez Bitsight.com, consultez le blog Bitsight ou suivez-nous sur LinkedIn.

sales@bitsight.com

BOSTON (QG)
RALEIGH
NEW YORK
LISBONNE
SINGAPOUR

Bitsight est un leader de la gestion des risques cyber, transformant la manière dont les entreprises gèrent leur exposition, leur performance et leurs risques, pour elles-mêmes comme pour leurs tiers. Les entreprises font confiance à Bitsight pour prioriser leurs investissements en cybersécurité, renforcer la confiance au sein de leur écosystème et réduire leur risque de pertes financières. S'appuyant sur plus de dix ans d'innovation technologique, ses solutions intégrées apportent de la valeur sur l'ensemble des domaines liés à la performance de la sécurité des entreprises, aux chaînes d'approvisionnement numériques, à la cyberassurance et à l'analyse de données.

BITSIGHT