Livre blanc CrowdStrike

CROWDSTRIKE

WEB PUBLIC, WEB INVISIBLE, DARK WEB ET AUTRES EN LIGNE DE MIRE

Identification des menaces externes, protection de votre marque et réduction des risques

RÉSUMÉ

La cybercriminalité gagne du terrain. Internet regorge de communautés, de places de marché et de forums malfamés, où se réunissent les cybercriminels et où prospère l'économie numérique clandestine. Les cyberadversaires font tout pour mettre la main sur vos données, exploiter votre marque et escroquer vos clients. Vous devez braquer les projecteurs sur ces coins sombres du Web pour identifier les menaces, résoudre les incidents potentiels et minimiser les risques pour vos ressources essentielles. Cependant, la Toile a de nombreuses ramifications, que la plupart des entreprises ne peuvent appréhender, faute de temps, de moyens financiers ou de connaissances.

Ce livre blanc plonge dans les méandres du Web souterrain. Il décrit certaines des tactiques déployées par les cyberadversaires pour dérober des données et commettre des fraudes. Il explique en quoi CrowdStrike Falcon X Recon™ peut vous aider à identifier à la source les activités potentiellement malveillantes et criminelles, de manière rapide, simple et rentable, grâce à l'adoption d'une approche proactive de la gestion des menaces.

Le coût total moyen d'une compromission de données est de 3,86 millions de dollars.

IBM Security
Cost of a Data Breach Report 2020[1]

LES CYBERCRIMINELS ENGRANGENT DES SOMMES FOLLES

La cybercriminalité est une affaire en or. Des identifiants compromis aux numéros de cartes bancaires, en passant par les données confidentielles des clients et la propriété intellectuelle : tout se vend sous le manteau sur Internet. Les cyberadversaires modernes profitent d'une économie souterraine florissante et ont à leur disposition un vaste écosystème.

Les cybercriminels peuvent tirer parti de kits d'outils à code source libre, ainsi que de kits de ransomware, de malware et de phishing à la demande pour sévir et déployer facilement des campagnes d'attaque. L'achat et la vente de données se déroulent sur d'innombrables places de marché clandestines. Avec un peu de perspicacité, les cyberadversaires peuvent même mettre la main sur des informations confidentielles, notamment des identifiants, sur des sites ouverts et des référentiels de code publics tels que GitHub[2].

La cybercriminalité peut perturber vos activités et hypothéquer les résultats financiers de votre entreprise. Elle peut ternir votre réputation et donner lieu à de lourdes amendes réglementaires et de coûteux règlements judiciaires. D'après les analystes du secteur de la sécurité, les pertes mondiales occasionnées par la cybercriminalité devraient atteindre 6 billions de dollars US en 2021[3]. Selon des rapports sectoriels, le coût total moyen d'une compromission de données s'élève à 3,86 millions de dollars US, en tenant compte à la fois des coûts directs (p. ex., investigations informatiques) et des coûts indirects (p. ex., perte de revenus due à l'atteinte à la réputation)[4].

1 **IBM Security Cost of a Data Breach Report 2020**

2 Les développeurs codent souvent en dur les clés et les clés secrètes API dans les applications.

3 **Cybersecurity Ventures**, novembre 2020

4 **IBM Security Cost of a Data Breach Report 2020**

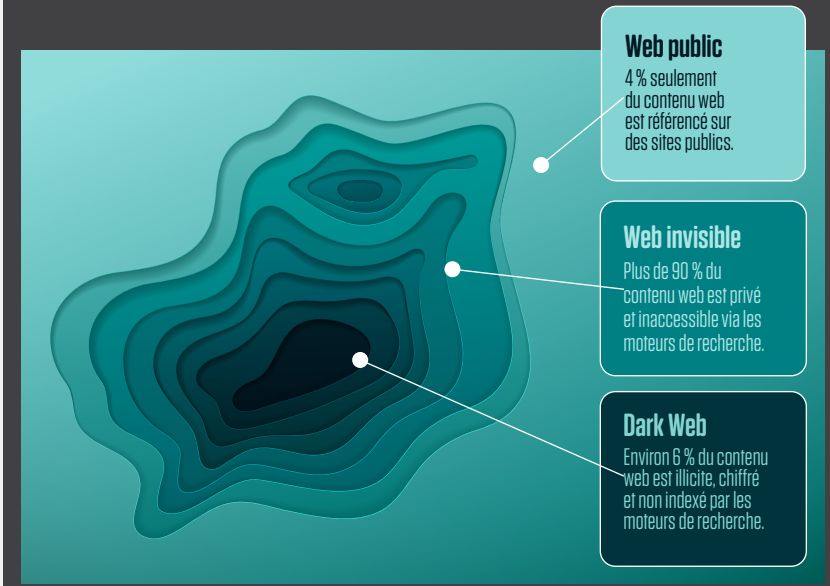
DES MENACES EXTERNES OMNIPRÉSENTES

Il y a une armada de cybercriminels tapie dans l'ombre sur le Web invisible et le Dark Web. Ces acteurs malveillants rôdent également au nez et à la barbe de tous sur le Web public, dans les blogs et sur les réseaux sociaux. Et pour encore aggraver les choses, ils opèrent en marge de la Toile et utilisent les plateformes de messagerie, des applications mobiles malveillantes et d'autres outils pour se livrer à leurs activités illicites. Les cybercriminels organisés, les pirates à la solde d'États et les cyberactivistes redoublent d'inventivité pour passer sous les radars et faire des ravages. À chaque minute qui passe, votre entreprise est exposée à des milliers de cyberadversaires prêts à exploiter votre marque, à dérober vos données et à escroquer vos clients. Le tableau 1 présente quelques tactiques très prisées des cybercriminels.

Tactique	Exemples
Usurpation de l'identité de votre marque dans les e-mails et les SMS, dans les applications mobiles, sur les réseaux sociaux et sur les sites web	■ Attaques de phishing qui font main basse sur des identifiants ou d'autres données confidentielles auprès de consommateurs peu méfiants ■ Contrefaçons de produits vendues sous votre marque ■ Arnaques de la supply chain conduisant les fournisseurs à commettre des fraudes ou des vols à leur insu
Vol et recel d'informations et de données confidentielles de l'entreprise	■ Identifiants (noms d'utilisateur, mots de passe, clés API, etc.) d'accès à des systèmes informatiques et des applications stratégiques ■ Documents internes, propriété intellectuelle, données confidentielles des employés et communications confidentielles ■ Données des clients, notamment les données personnelles et les renseignements médicaux personnels ■ Cartes de crédit professionnelles, numéros SWIFT et numéros de passeport
Arnaques et pratiques commerciales trompeuses	■ Faux codes de réduction, bons-cadeaux et points de fidélité
Achat et vente de logiciels malveillants, ainsi que d'outils et de services de piratage	■ Enregistreurs de frappe, voleurs de mots de passe et outils de piratage des réseaux sociaux ■ Kits d'exploit, générateurs de malwares et chevaux de Troie ■ Services de chiffrement, de courrier indésirable et de deepfake (falsification de vidéos)

Tableau 1. Exemples de tactiques couramment employées par les cyberadversaires

WEB PUBLIC vs WEB INVISIBLE vs DARK WEB — QUELLE EST LA DIFFÉRENCE ?



Le Web public comprend tout contenu indexé par les moteurs de recherche qui s'affiche dans les résultats de recherche de Google, Bing, etc.

Le Web invisible est constitué d'une multitude de contenus privés qui ne sont ni indexés ni accessibles via un moteur de recherche. Ce contenu exige des identifiants de connexion et bloque explicitement les robots d'indexation.

Le Dark Web est uniquement accessible à l'aide d'un navigateur spécial, tel que Tor (The Onion Router) ou I2P. C'est un repère d'informations volées, de marchandises illégales et d'une myriade de forums criminels et d'activités clandestines.

L'APPROCHE PROACTIVE : VOTRE MEILLEURE LIGNE DE DÉFENSE CONTRE LES MENACES EXTÉRIEURES

Les cyberescrocs peuvent nuire à la réputation de votre entreprise et occasionner de lourdes pertes financières. En matière d'identification et d'atténuation des menaces venues de l'extérieur, mieux vaut prévenir que guérir. Néanmoins, la radioscopie régulière du Web clandestin, territoire vaste et dynamique s'il en est, est une tâche titanesque, hors de portée de la majorité des entreprises.

Rares sont les entreprises qui disposent du budget et des équipes compétentes pour concevoir, déployer et gérer un moteur de collecte de données évolutif au plus haut point. Et peu savent naviguer dans les abîmes de l'Internet.

Surveiller les recoins du Web n'est pas une sinécure.

- **Suivre les changements mobilise beaucoup d'énergie.** L'écosystème criminel est en constante évolution. Il y a sans cesse de nouveaux sites et forums à surveiller et de nouveaux cybercriminels à traquer.
- **Les accès aux sites illicites sont difficiles à obtenir.** Bien souvent, ils se font exclusivement sur invitation.
- **Vous devez en outre faire preuve d'intelligence et de discrétion.** Si les cybercriminels savent qu'ils sont pris en filature (ou espionnés par un robot), ils couperont les ponts.
- **Vous devez capturer et conserver en permanence des données de cyberveille brutes.** Les activités malveillantes sont de nature éphémère. Des sites disparaissent du jour au lendemain, voire après quelques heures, et les cybercriminels suppriment fréquemment les messages compromettants. Vous devez donc recueillir des données tant que c'est possible.

À l'instar de la majorité de ses pairs, votre entreprise n'a tout simplement ni le temps, ni les connaissances, ni les moyens de surveiller les recoins du Web pour y débusquer les activités malveillantes. CrowdStrike peut vous aider en mettant à votre disposition l'expérience, la technologie et des professionnels dédiés afin que vous gardiez une longueur d'avance sur les cyberadversaires.

CROWDSTRIKE FALCON X RECON : RECONNAISSANCE DES RISQUES NUMÉRIQUES SUR LE WEB PUBLIC, LE WEB INVISIBLE, LE DARK WEB ET AILLEURS

CrowdStrike Falcon X Recon expose les activités potentiellement malveillantes du Web public, du Web invisible, du Dark Web et autres, pour vous offrir une plus grande visibilité, protéger votre marque et réduire les risques. La solution recueille des données et surveille l'activité de millions de pages web à accès restreint, de forums et de places de marché illicites, de sites de plagiat, de sites de fuite de données et de plateformes de réseaux sociaux et de messagerie, de manière proactive. Elle livre ainsi de précieuses informations sur les comportements suspects associés à votre marque. Avec Falcon X Recon, vous pouvez exécuter des requêtes en temps réel pour déjouer les fraudes, les compromissions de données, les campagnes de phishing et autres cybermenaces. De plus, la solution traque constamment les activités malveillantes sur les sites clandestins et envoie des notifications automatiques en cas de risques.

Falcon X Recon s'appuie sur la plateforme CrowdStrike Falcon® native au cloud, gage d'une grande simplicité et d'une efficacité immédiate. Avec Falcon X Recon, il n'y a rien à implémenter ni à administrer. Vous pouvez donc recentrer votre temps et vos ressources sur l'identification des menaces et la protection de votre entreprise. La solution CrowdStrike® est prise en charge par une équipe d'experts qui a à cœur de vous aider à améliorer la connaissance situationnelle.

COLLECTE

Falcon X Recon collecte des données de cyberveille brutes à grande échelle. La solution extrait automatiquement les données de millions de pages web cachées et de milliers de sites à accès restreint où les criminels se rencontrent, achètent et vendent. La solution glane des données dans les forums, les places de marché, les boutiques d'application, les sites de plagiat, etc. à accès restreint.

Avec Falcon X Recon, vous pouvez recueillir des données de cyberveille en temps réel sur des sites illicites sans vous faire repérer. La solution capture les données et les conserve. De cette façon, les cybercriminels ne peuvent pas brouiller les pistes en supprimant des messages ou en fermant des sites. Falcon X Recon peut servir à identifier les menaces imminentes et barrer la route des cyberadversaires ou à avoir l'œil sur les malversations et les activités criminelles. La solution peut également suivre et analyser l'historique de données afin d'identifier des tendances et des profils de comportement.

INVESTIGATION

Grâce à Falcon X Recon, vous pouvez facilement découvrir les menaces externes qui pèsent sur votre entreprise et mener les investigations qui s'imposent. La solution fournit des assistants conviviaux assortis de critères de recherche prédéfinis (p. ex., noms de marque, dirigeants, domaines, vulnérabilités et adresses électroniques). Il est possible de lancer des requêtes *ad hoc* en temps réel ou de surveiller en permanence le Web souterrain en exécutant des règles personnalisées pour passer efficacement au crible les données de cyberveille brutes.

Falcon X Recon affiche les résultats des investigations sous la forme de fiches concises et faciles à comprendre. Vous pouvez consulter les publications originales des cybercriminels, de même que des informations contextuelles concernant l'escroc et le site. Les messages en langue étrangère, y compris ceux rédigés dans le jargon des hackers, sont automatiquement traduits en anglais. (Le moteur de traduction automatique prend en charge 18 langues étrangères.)

NOTIFICATION

Falcon X Recon envoie des notifications automatiques en cas d'activité suspecte. Vous pouvez définir des règles personnalisées pour signaler les comportements potentiellement malveillants ou criminels. Vous pouvez classer les alertes par catégorie et par priorité, de même que définir la fréquence à laquelle elles sont générées (immédiate, quotidienne ou hebdomadaire) et les personnes et les équipes qui les reçoivent. Vous avez la possibilité d'envoyer des alertes aux équipes chargées de la sécurité et des opérations informatiques, ainsi qu'à d'autres départements de l'entreprise qu'il convient d'informer des fuites de données confidentielles, des escroqueries et des abus, notamment les services marketing, juridique, des ressources humaines et de lutte contre la fraude.

PRINCIPAUX AVANTAGES

Visibilité accrue : extraction automatique des données de millions de sites clandestins ou à accès restreint, sans se faire repérer

Réduction des risques : envoi de notifications en temps réel concernant les menaces pour votre marque et votre entreprise

Investigations simplifiées : exécution rapide et aisée de requêtes ad hoc fournissant des résultats intuitifs et exploitables

Éclairage supplémentaire : surveillance de l'activité criminelle, des tendances historiques et des menaces émergentes

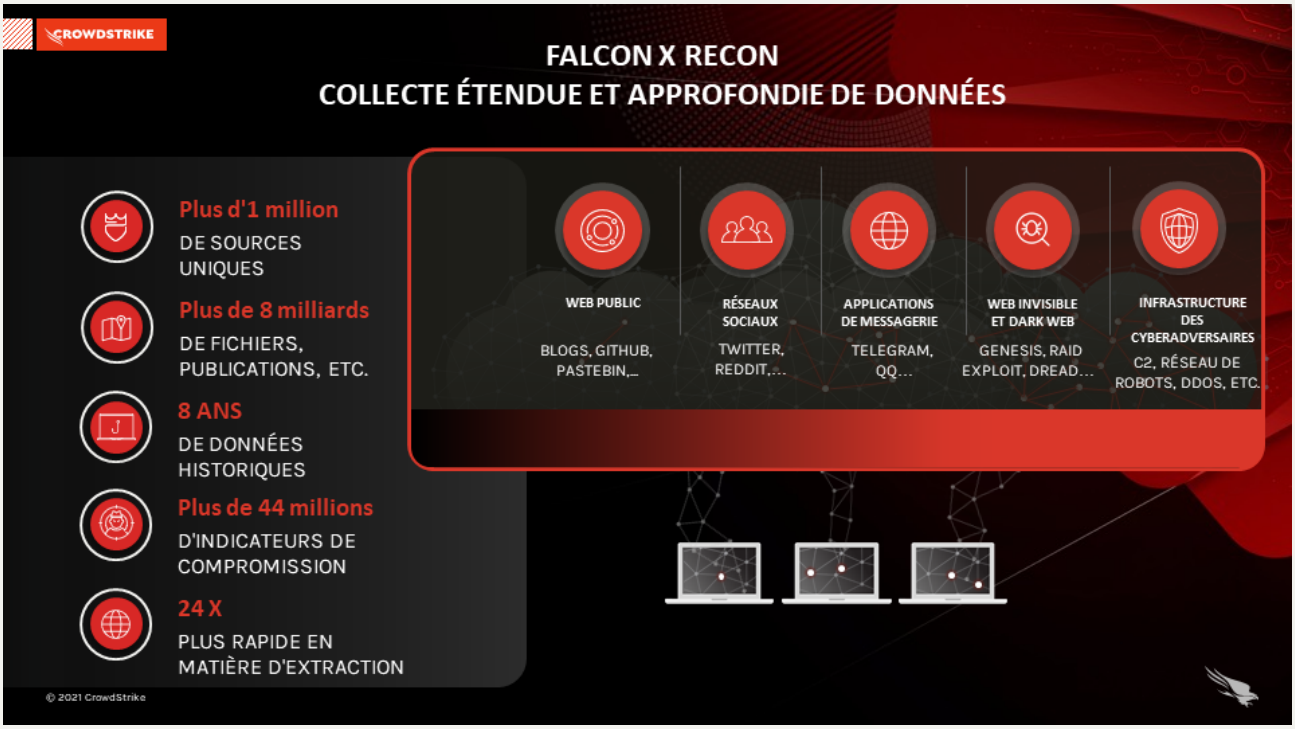
Rentabilité accélérée : prise de mesures immédiates contre le cyberrisque grâce à une plateforme native au cloud soutenue par des experts

POURQUOI CHOISIR FALCON X RECON ?

Falcon X Recon fournit des informations détaillées sur le Web souterrain. La solution vous aide à identifier et investiguer les menaces externes qui pèsent sur votre entreprise, à une vitesse et avec une couverture inégalées.

À la fois très évolutive et performante, la solution de CrowdStrike offre les avantages suivants :

- Elle collecte en permanence des données provenant de plus d'un million de sources uniques. Elle conserve plus de 8 milliards de pages, de messages et de fichiers, et en extrait des données 24 fois plus vite que les solutions concurrentes.
- Elle procure une visibilité sur l'historique des activités des cyberadversaires.
- Elle fournit plus de 44 millions d'indicateurs de compromission.
- Elle utilise des appâts et des filets disséminés dans le monde entier pour attirer les cyberadversaires et identifier les réseaux de robots, les attaques par déni de service distribué (DDoS) et les autres cybermenaces qui rôdent.



CONCLUSION

Les cybercriminels sont tapis dans les sombres recoins de l'Internet, prêts à dérober vos données, à escroquer vos clients et à tirer profit de la réputation de votre entreprise. Mettez un terme à leurs agissements avec Falcon X Recon. Grâce à notre solution, vous pouvez déployer des stratégies proactives pour déjouer les fraudes, les compromissions de données, les campagnes de phishing et autres cybermenaces ciblant votre entreprise.

Pour découvrir comment Falcon X Recon peut aider votre entreprise à identifier les menaces externes et à atténuer les risques, visitez la page **https://www.crowdstrike.com/products/threat-intelligence/falcon-x-recon/**.

À PROPOS DE CROWDSTRIKE

CrowdStrike, leader mondial de la cybersécurité, redéfinit la sécurité pour l'ère du cloud en proposant une plateforme de protection des endpoints et des workloads conçue spécifiquement pour empêcher les compromissions. L'architecture à agent léger unique de la plateforme CrowdStrike Falcon® s'appuie sur l'intelligence artificielle à l'échelle du cloud pour offrir une visibilité et une protection en temps réel au sein de l'entreprise et prévenir les attaques sur les endpoints et les workloads, qu'ils soient connectés ou non au réseau. Optimisé par la base de données propriétaire CrowdStrike Threat Graph®, CrowdStrike Falcon met en corrélation en temps réel cinq billions d'événements liés aux endpoints identifiés chaque semaine dans le monde, qui viennent enrichir l'une des plateformes de données les plus avancées au monde en matière de sécurité.

Avec la plateforme cloud CrowdStrike Falcon, les clients bénéficient d'une protection renforcée, de performances supérieures et d'une efficacité immédiate.

Vous ne devez retenir qu'une seule chose à propos de CrowdStrike : **We stop breaches.**

Commencez l'évaluation gratuite d'un antivirus de nouvelle génération

Pour en savoir plus, consultez le site **www.crowdstrike.fr**.