vaadata

Ethical Hacking Services

COMMENT PRÉVENIR LES ATTAQUES ET IDENTIFIER LES FUITES DE DONNÉES SUR LE DARK WEB

LIVRE BLANC

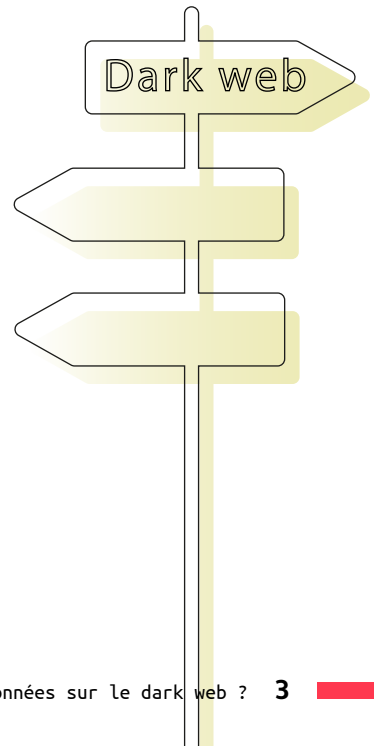
SOMMAIRE

Introduction

La croissance des cyberattaques est un phénomène qui touche toutes les entreprises, quels que soient leur taille ou leur domaine d'activité. Dans ce contexte, la prise de conscience des risques est réelle. Elle se traduit par la mise en place de mesures de sécurité proactives et préventives parmi lesquelles la sensibilisation de tous les collaborateurs, la formation des équipes techniques, la réalisation de tests d'intrusion sur les systèmes informatiques, etc.

Pour prévenir les cyberattaques, il est nécessaire de maîtriser les informations publiquement accessibles sur votre entreprise. Cela implique notamment d'explorer le web à la recherche de données sensibles, dans le but de réduire le volume d'informations exposées, ou du moins d'éliminer les informations représentant un risque de sécurité. Et pour aller encore plus loin, il est possible d'adopter une position « d'éclaireur » - autrement dit de « reconnaissance » - afin d'identifier les stratégies et les plans d'attaques des pirates informatiques sur leur terrain de jeu favori : le dark web.

L'objectif de ce livre blanc est de passer en revue l'écosystème du dark web, d'en décrire les mécanismes et les tactiques utilisées par des attaquants pour compromettre vos actifs critiques, puis de vous présenter comment Vaadata peut vous aider à réduire votre surface d'attaque en identifiant les risques sur le web en tenant compte des spécificités du dark web.



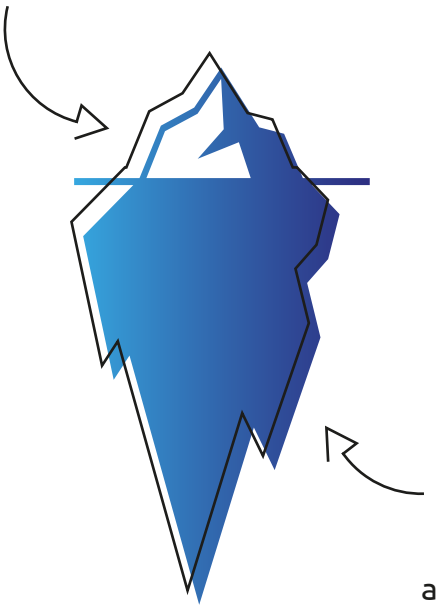
1. Le dark web, réel danger pour votre entreprise

1.1. Qu'est-ce que le dark web ?

Avant d'entrer dans le vif du sujet, quelques précisions sur le dark web afin de mieux comprendre sa nature.

Le web est très souvent représenté en trois strates : le web visible, le deep web et le dark web.
Vous connaissez sûrement l'image de l'iceberg très souvent utilisée pour illustrer ces trois strates.

Le web visible, comme son nom l'indique, comprend toutes les pages indexées et accessibles via n'importe quel moteur de recherche (Google, Bing, etc.). Il représenterait environ 5 à 10 % de la totalité d'Internet. C'est le web auquel tout le monde a accès en effectuant des requêtes sur les moteurs de recherche.



Par opposition au web visible, le deep web regroupe toutes les pages et sites web existants mais non indexés par les moteurs de recherche (environ 90 à 95 % du web donc). Il s'agit par exemple de toutes les pages uniquement accessibles via une authentification (intranets, services accessibles via abonnement, comptes bancaires, etc.) ou de pages expressément non indexées.

À l'intérieur du deep web se trouve un sous-ensemble de contenus connu sous le nom de dark web, inaccessible via les navigateurs web communs. On peut le définir comme un ensemble de réseaux privés chiffrés, aussi appelé dark nets (tels que TOR – The Onion Router -, I2P – Invisible Internet Project - ou Freenet), permettant d'accéder à du contenu qui leur est propre. La différence principale entre le deep web et le dark web est donc la nécessité d'utiliser un logiciel spécifique pour y accéder.

Bien que célèbre pour son utilisation par des personnes malveillantes, le dark web n'a rien d'intrinsèquement illégal. En effet, il désigne simplement un moyen d'accéder ou d'héberger du contenu web dans l'anonymat. Il peut donc être utilisé à des fins légitimes. C'est d'ailleurs le cas dans des pays où l'activité sur Internet est fortement surveillée ou qui disposent de lois locales strictes en matière de censure ou de contrôle des réseaux. Dans ces pays, le dark web est une bouée de secours et un canal indispensable pour éviter l'oppression et la persécution. Dans des sociétés plus libres, il constitue également un outil permettant de garantir le respect de la vie privée et de l'anonymat sur Internet. Par ailleurs, de nombreuses organisations disposent d'un site web sur le dark web. C'est le cas de nombreuses ONG ou grands journaux.

Le revers de la médaille : ce respect de la vie privée et cet anonymat, qui protègent des persécutions et des publicités ciblées, font également du dark web un terreau fertile pour la cybercriminalité. On y retrouve diverses activités illicites : trafic d'armes, trafic de drogues, partage et vente de données personnelles ou professionnelles, ressources permettant de réaliser des cyberattaques telles que des malwares par exemple.

Le dark web regorge en effet de forums et de marketplaces potentiellement nuisibles pour les entreprises, qui doivent se saisir du problème et gagner en visibilité sur ce canal afin d'identifier les menaces, traiter les incidents potentiels et réduire les risques pour leurs actifs critiques. Mais avant de revenir sur cette question centrale, quelques précisions sur le fonctionnement du dark web.

1.2. Accéder au dark web : focus sur le fonctionnement de TOR

Il existe plusieurs technologies utilisées pour accéder au dark web (I2P et Freenet notamment), mais la plus connue et la plus étendue reste de loin le réseau TOR (The Onion Router) avec environ deux millions d'utilisateurs quotidiens selon le site metrics.torproject.org (site rattaché au projet TOR qui fournit des statistiques d'utilisation du réseau).

Développée au sein des services de renseignement militaires américains au milieu des années 90 et disponible en Open source depuis 2003, sa fonction première est de permettre la navigation sur le web sans compromettre l'identité des utilisateurs.

En effet, TOR est à la fois un réseau de routeurs et un protocole de chiffrement, permettant une anonymisation forte des échanges en ligne. Il est fondé sur le principe du « routage en oignon », qui multiplie les intermédiaires entre le client d'où est émis une requête et le serveur auquel cette requête s'adresse, tout en chiffrant l'ensemble de la chaîne de transmission. Cela garantit l'impossibilité de retracer l'activité jusqu'à l'utilisateur final.

À la différence du TCP qui requiert de connaitre les adresses IP du client et du serveur pour établir une communication entre eux, dans le protocole de TOR, la connexion client-serveur se fait sans que le client ni le serveur ne connaissent leurs adresses IP respectives. Pour ce faire, le client TOR transmet sa requête à un premier proxy TOR, qui la transmet à un deuxième proxy ne connaissant lui-même que l'adresse du chemin précédent, et qui le transmet ensuite à un troisième et dernier proxy qui assumera la connexion avec le serveur. C'est la raison pour laquelle ce type de routage est dit « en oignon ».

Par ailleurs, une fois la connexion établie, TOR utilisera la même route pendant une courte période avant de générer un nouveau chemin. Cela permet de renforcer l'anonymat des utilisateurs et de contrer les attaques visant à connaitre le contenu d'un échange via TOR, notamment les attaques Man In the Middle.

TOR, au même titre que les autres dark nets, a donc permis la création de pages web accessibles uniquement via des navigateurs TOR, avec un nom de domaine en .onion. C'est cet ensemble de pages web que l'on nomme communément le dark web. Et contrairement au web visible qui est très interconnecté et accessible, le dark web est très fragmenté.

Aujourd'hui, le réseau TOR compterait plus de 65 000 URL uniques en .onion. Une étude réalisée en 2018 par Hyperion Gray a répertorié environ 10 % de ces sites et constaté que la plupart d'entre eux ont pour fonction de faciliter la communication, par des forums, des salons de discussion et des hébergeurs de fichiers et d'images, et le commerce sur des places de marché. Ces rôles fonctionnels, en particulier ceux liés à la communication, permettent de nombreux usages considérés comme légaux et légitimes dans les sociétés libres.
Par ailleurs, une étude de 2016 de la société de recherche Terbium Labs, pour laquelle 400 sites en .onion ont été sélectionnés au hasard et analysés, indiquait que plus de la moitié de tous les domaines du dark web étaient en fait légaux. Sur près de 200 noms de domaines classés comme illégaux par Terbium Labs, plus de 75 % étaient des places de marché, alimentées principalement par le Bitcoin et d'autres cryptomonnaies comme le Monero.

1.3. Panorama des menaces cyber sur le dark web

En raison de l'anonymat qu'il confère, le dark web a vu naître et se développer toutes les formes de cybercriminalité, avec l'émergence de nombreux sites illégaux. On peut les décomposer en deux grandes catégories.

D'un côté, on retrouve des forums abordant des discussions de tout genre et où le partage de ressources (tutoriels, comptes piratés, etc.) est très présent.

De l'autre, de nombreuses places de marché proposent toutes sortes de produits et services et intègrent des fonctionnalités de dépôt de monnaie (Bitcoin, Monero principalement), paiement après livraison, systèmes de notes et avis, achat/vente et livraison en quelques clics.

Certaines sont spécialisées dans la vente de données professionnelles (identifiants, coordonnées, documents, etc.), et d'outils permettant de réaliser des cyberattaques ciblées : malwares, ransomwares, exploits de type zero-day (attaques ciblant des vulnérabilités qui n'ont pas encore été corrigées et qui ont donc de grandes chances de réussir), etc. Il existe également des fournisseurs de services qui, contre rémunération, peuvent donner accès à l'infrastructure de botnets. Cela permet à l'acheteur de réaliser des attaques de déni de service distribué (DDoS) à grande échelle.

Certains sites proposent également des services de piratage à la demande. On y retrouve les tarifs des prestations proposées, une description des compétences et spécialités de chaque pirate proposant ses services : ingénierie sociale, attaques web, attaques sur des réseaux, etc.

2. Reconnaissance et identification de la surface d'attaque

Les spécialistes en cybersécurité appellent « reconnaissance » la démarche consistant à rechercher un ensemble d'informations disponibles sur le web au sujet d'une cible donnée (par exemple au sujet d'une entreprise, ou d'un service en ligne en particulier).

Ce que l'on nomme reconnaissance consiste à collecter tout type d'informations (adresses IP, DNS, informations sur l'architecture du SI et les technologies utilisées, organigramme et coordonnées, documents internes, diverses données techniques ou business, etc.) accessibles et potentiellement utilisables dans le cadre d'une cyberattaque. Cette démarche nécessite des compétences ainsi que certains outils spécifiques.

La plupart des audits de sécurité commencent par une phase de « reconnaissance », qui permet d'orienter certaines recherches et parfois d'identifier directement des vulnérabilités liées à des fuites de données. Il existe aussi des audits de sécurité exclusivement focalisés sur la reconnaissance, qu'on peut appeler audits de reconnaissance ou audits d'exposition. L'objectif est alors de cartographier la surface d'attaque d'une entreprise pour ensuite contrôler et limiter les informations visibles et disponibles pour des attaquants, autrement dit réduire la surface d'attaque.

Les recherches sur le dark web ne sont pas systématiquement incluses dans les audits de reconnaissance. En effet, au vu des spécificités du dark web, exposées dans la première section de ce livre blanc, il est à la fois utile mais complexe d'inclure des recherches sur le dark web dans une démarche de reconnaissance. Cela nécessite des compétences et des outils spécifiques au dark web. C'est l'objet principal de ce livre blanc que de présenter ce que l'on peut attendre d'un audit de reconnaissance incluant des recherches spécifiques sur le dark web, également appelé audit d'exposition dark web.

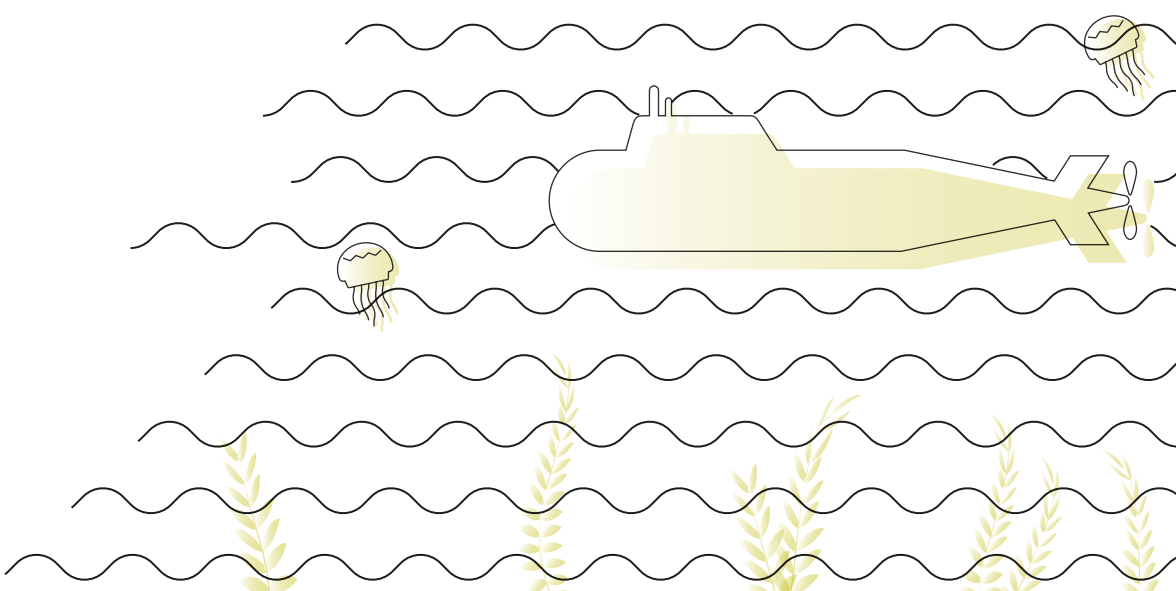
3. Réaliser un audit d’exposition dark web avec Vaadata

3.1. Notre service

3.1.1. Approche

Un audit d’exposition dark web consiste en un audit de reconnaissance plus approfondi, car incluant des recherches sur le dark web. Notre approche pour ce type d’audit repose sur des recherches manuelles, complémentées par l’utilisation d’outils spécialisés dans la recherche de données « open source ».

Les recherches manuelles utilisent notamment les Google dorks et l’exploration du web public. La liste des outils utilisés comprend notamment des outils d’interrogation de serveurs DNS, des APIs de recherche OSINT, des services tiers réputés de bases de données liées aux noms de domaines, des outils internes développés sur mesure, ainsi que des outils de recherche professionnels permettant d’extraire des données depuis des communautés infiltrées sur le dark web.

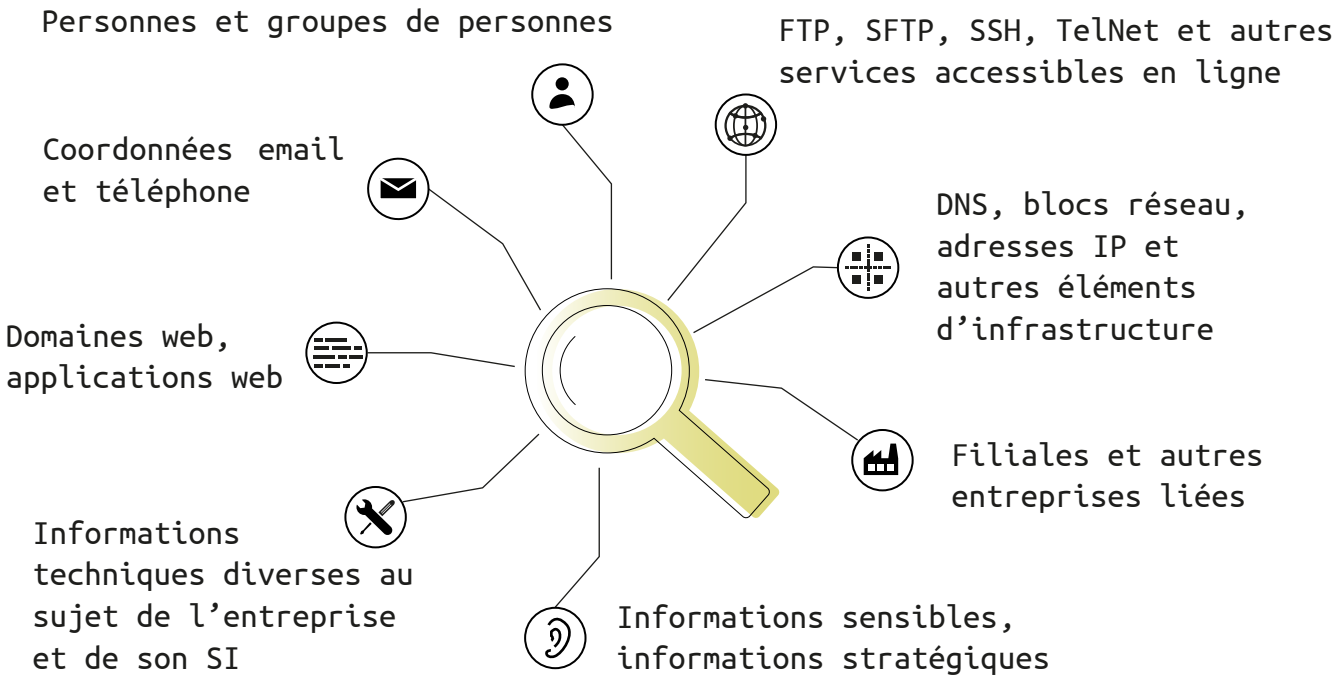


3.1.2. Méthodologie

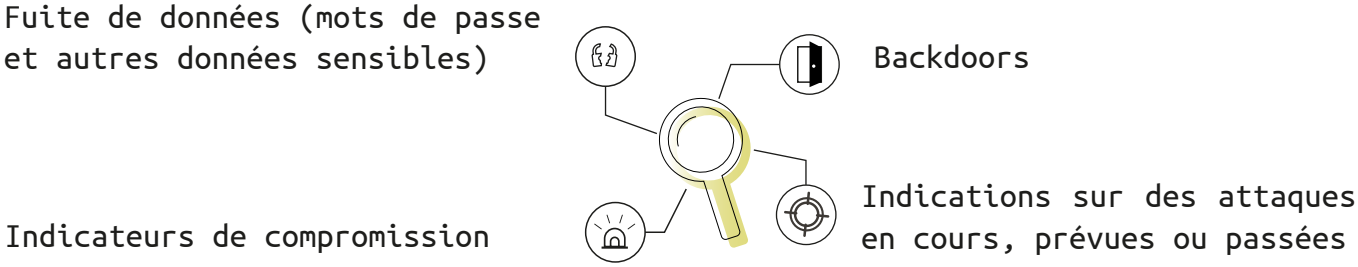
La méthodologie consiste à identifier d'abord les éléments de base que l'entreprise expose sur Internet. À partir de ces éléments, nous recherchons ensuite d'autres éléments liés et exposés sur le web.

Par exemple :
Sont identifiés en premier lieu les noms de domaines et les personnes clés de l'entreprise, identifiables sur le web.

Par la suite, il devient possible d'identifier de nouveaux éléments tels que :



Pour ce qui concerne plus spécifiquement le dark web, le type d'éléments identifiables pourra concerner :



3.1.3. Outils de recherche sur le dark web

Les outils de recherches que nous utilisons sont des outils professionnels hautement sophistiqués permettant de crawler le dark web pour remonter des informations provenant de communautés ayant des activités illicites.

La valeur de ce type d'outils repose sur un travail d'investigation permettant de recenser des sites cachés et non indexés (forums, marketplaces, chats, etc.) afin de permettre de les crawler. De plus, la plupart des sites liés à des activités illicites étant fermés par login/mot de passe, et conçus pour être non accessibles aux non-membres d'une communauté spécifique, un travail continu d'infiltration de ces communautés est nécessaire pour obtenir des accès permettant d'intégrer ensuite le contenu des sites à l'outil de crawling. Il s'agit d'un travail au long cours, comparable à celui qu'effectuent des spécialistes chargés d'enquêter sur des activités criminelles.

Cela explique pourquoi les outils permettant de crawler le dark web étaient initialement réservés aux services des gouvernements. Les entreprises ayant conçu ces outils les ont par la suite mis à disposition de grandes entreprises ayant besoin de protéger leurs activités. Pour les petites et moyennes entreprises, ces outils sont peu accessibles en raison de l'investissement en coût et en expertise qu'ils représentent.

3.1.4. Livrables

Le livrable obtenu suite à un audit d'exposition dark web est un rapport répertoriant l'ensemble des éléments ayant pu être identifiés.

En règle générale, plus l'entreprise est de grande taille et plus elle possède un historique sur le marché, ainsi qu'un système d'information existant de longue date, plus le volume d'information récoltable sera potentiellement important.

Mais d'autres facteurs entrent en compte pour déterminer l'exposition potentielle d'une entreprise sur le dark web. Typiquement, le secteur d'activité, l'exposition médiatique, et le fait d'avoir déjà subi des attaques informatiques. Ainsi une petite entreprise spécialisée dans le bitcoin présente un niveau potentiellement élevé de risque, et donc un volume potentiellement important d'informations récoltées par des communautés malveillantes.

3.1.5. Expertise et valeur ajoutée

La valeur de notre service d'audit d'exposition dark web repose non seulement sur des outils hautement sophistiqués (tels que décrits en 3.1.3.) mais également sur les compétences et l'expérience des auditeurs en charge de la prestation.

Ces compétences reposent sur trois piliers : la maitrise des outils, l'expérience en reconnaissance, et l'expérience du pentest.

La maitrise des outils permet de bien les utiliser, et notamment de bien filtrer les données, qui peuvent représenter une masse importante, puis de savoir interpréter les résultats.

L'expérience en reconnaissance permet de savoir quoi chercher sur le dark web. Plus précisément, le fait de commencer par des recherches sur le web visible permet d'identifier des mots clés spécifiques au client, ainsi que des adresses IP, des noms de domaines, et d'autres informations qui serviront ensuite de point de départ pour des recherches sur le dark web. C'est une des raisons pour lesquelles l'audit d'exposition dark web comprend une approche globale de la reconnaissance avec des recherches sur le web visible avant de conduire des recherches sur le web caché. Parmi les autres raisons, la principale est qu'il est très souvent possible d'identifier des éléments sensibles et des fuites de données via le web visible, donc qu'il est nécessaire de s'intéresser au web visible avant de se concentrer plus spécifiquement sur le dark web.

Enfin, l'expérience en pentest permet aux auditeurs de se placer facilement du point de vue d'un attaquant, afin d'interpréter les résultats des recherches en fonction de leur utilisation possible dans le cadre d'une cyberattaque. En effet, parmi les informations remontées, on peut trouver par exemple des contenus de fuites de données (fichiers à disposition, contenus de serveurs piratés), pouvant aussi être commercialisés sur des marketplaces spécialisées dans la revente de données, ainsi que des discussions concernant des attaques en cours, futures ou passées. L'expérience en pentest permet de mieux faire la part des choses entre ce qui est hautement sensible et ce qui l'est moins. Dans certains cas, les auditeurs peuvent être amenés à investiguer davantage en téléchargeant voire en achetant des contenus, pour vérifier ce qu'ils permettent réellement en termes d'utilisation. Ce type d'opération nécessite de multiples précautions et une forte expertise en cybersécurité afin d'éviter de se faire piéger et de créer des brèches de sécurité dans sa propre entreprise.

3.2. Démocratiser les recherches sur le dark web auprès des startups et PME

3.2.1. Enjeu de sécurité pour les startups et PME

À l'heure actuelle, on constate un intérêt croissant pour les investigations sur le dark web. Pour toute entreprise, réduire sa surface d'attaque permet de se protéger contre les cybermenaces, et le fait de connaitre les informations disponibles sur le dark web à son sujet fournit des pistes pour identifier des attaques passées ou potentiellement à venir.

Pour une PME ou une startup, l'enjeu prioritaire est d'identifier les informations la concernant sur le web public. En effet, la surface d'attaque se compose de nombreux éléments accessibles en ligne mais non répertoriés : des sites de staging, des anciennes versions d'applications, des documents internes involontairement partagés en ligne, des fuites de données publiquement accessibles, etc. La plupart des entreprises sont surprises en constatant ce qu'il est possible d'obtenir à leur sujet via un travail de reconnaissance classique.

Investiguer le dark web ne constitue pas une priorité de sécurité pour de nombreuses startups et PME, car il existe d'autres sujets plus urgents permettant de renforcer leur niveau de sécurité.

Cependant, conduire des recherches rapides sur certains de leurs mots clés sensibles leur permettrait d'obtenir des informations utiles sans que cela ne représente un investissement important.

De plus, pour certaines catégories de startups et PME, typiquement celles présentes dans des secteurs sensibles (finance, cryptomonnaies, sécurité, infrastructures publiques, etc.), investiguer le dark web présente un réel intérêt. Les principaux freins se situent au niveau des moyens, à la fois parce qu'internaliser des compétences sur le sujet aurait peu de sens, et parce que les outils permettant de crawler le dark web représentent un budget réellement élevé.

3.2.2. Notre engagement en faveur des startups et PME

Notre expérience conséquente auprès de clients startups, qui représentent environ 50 % de nos missions de sécurité, nous amène à leur proposer des prestations adaptées à la réalité de leurs besoins et de leur budget.

Ainsi, nous mettons à la disposition de nos clients startups et PME notre expertise de la sécurité, pour leur proposer des audits techniques avec un périmètre progressif au fur et à mesure de leur développement et de l'augmentation de leur niveau d'exposition aux risques.

Concernant l'exposition sur le dark web, il est possible de conduire des recherches très courtes mais à forte valeur ajoutée, par exemple une ou deux journée(s) de reconnaissance « classique » (sur le web visible) à laquelle s'ajoute une demi-journée ou une journée de recherches sur le dark web.

Nous mettons alors à la disposition de nos clients startups et PME notre expertise de la reconnaissance à laquelle s'ajoutent des outils très haut de gamme, inaccessibles à l'échelle d'une seule startup ou même d'une seule grosse PME.

Ce type de prestation est simple à mettre en place car il ne nécessite quasiment aucun transfert d'informations vers le prestataire spécialisé.

En résumé

Si le dark web n'est pas toujours synonyme de cybercriminalité, comme nous avons pu le voir dans la première partie, il représente néanmoins un risque de sécurité pour les entreprises. En effet, des échanges sur les forums du dark web peuvent concerner des projets de cyberattaques, tandis que certaines marketplaces permettent de vendre et acheter des données piratées. D'où l'intérêt d'analyser le contenu publié sur le dark web au sujet d'une entreprise.

Réaliser un audit d'exposition dark web consiste à rechercher des informations concernant votre entreprise disponibles sur le web visible, puis à s'infiltrer sur des sites cachés et réservés à des cercles fermés. Néanmoins, l'exploration du dark web peut constituer une opération « périlleuse » pour certaines entreprises. En effet, rares sont les entreprises disposant du temps et des ressources nécessaires pour analyser le volume d'informations disponibles sur le web visible, et plus encore sur le dark web. De plus, explorer le dark web comporte de nombreux risques d'être arnaqué ou piraté, pour une personne non spécialiste de ce sujet.

C'est pourquoi nous proposons un service reposant à la fois sur une expertise reconnue et des outils premium, accessible pour nos clients. Nous nous sommes basés sur notre expérience auprès de plus de 200 clients pour lesquels nous effectuons du pentest, afin de concevoir un service spécifiquement adapté aux besoins des grandes entreprises comme de jeunes startups souhaitant maîtriser leur exposition sur le web visible et caché.

Ainsi, les informations remontées lors d'un audit d'exposition dark web pourront être de différentes natures : liste des éléments d'infrastructure informatique exposés en ligne, liste des coordonnées exposées en ligne, fuites de données (identifiants, mots de passe, documents confidentiels concernant votre entreprise, etc.), malwares et kits d'exploitation destinés à votre entreprise ou votre secteur d'activité, informations concernant des backdoors, etc.

Contactez-nous pour échanger plus en détail sur votre besoin concernant votre exposition sur le web visible et sur le dark web.

A PROPOS DE VAADATA

VAADATA est une société spécialisée en tests d'intrusion. Nous proposons des audits de sécurité en boite noire, en boite grise et en boite blanche, ciblant différents périmètres : plateformes web, applications mobiles, objets connectés, infrastructure et réseaux, ingénierie sociale.

Nous visons à démocratiser le pentest avec des offres adaptées aux startups comme aux grandes entreprises. Nous comptons environ 200 clients, parmi lesquels Crédit Agricole, Heineken, Esker, Dext, Malt, Friendsurance…

VAADATA est une entreprise certifiée CREST. Notre équipe technique possède les certifications suivantes : CEH, OSCP, GWAPT, OSWE, AWS Certified Security & AWS Certified Solutions Architect, CISSP, PMP.

vaadata
Ethical Hacking Services

12 Rue des Tuileries
69009 LYON
FRANCE

+33 (0)4 37 92 98 85

contact@vaadata.com

@vaadata

Vaadata

www.vaadata.com