CLASSESAFFAIRES
ACTUALITÉS ▪ SÉMINAIRES ▪ PERSPECTIVES

Blakes

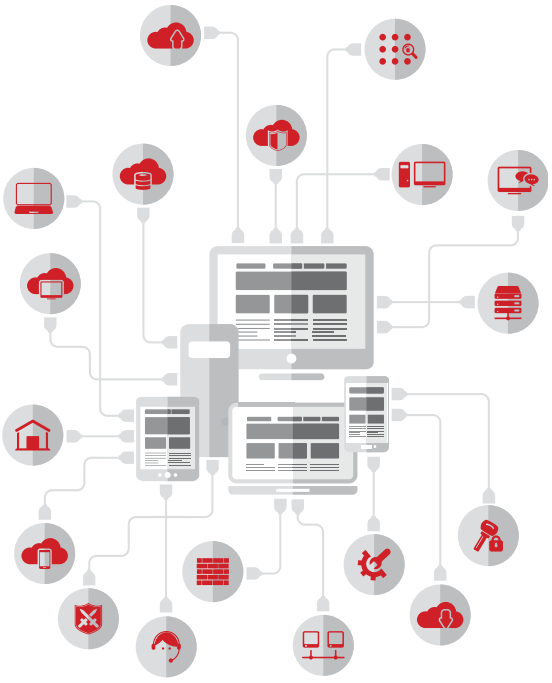
Le darknet sous les projecteurs :
Ce que toute entreprise devrait savoir

Sheldon Burshtein

En général, la plupart des gens n'utilisent qu'une seule des trois couches qui composent l'Internet. La couche couramment utilisée et accessible à l'aide de moteurs de recherche est appelée Web visible ou Web surfacique (*clearnet* ou *surface Web*). Elle représente environ 4 % du contenu de l'Internet. En plus de cette couche, l'Internet comporte le Web invisible (*deep Web*) et le darknet. C'est sur le darknet que sont publiées les données piratées, et cette tendance devrait prendre de l'ampleur pour les communications, les activités commerciales, le terrorisme et les cybercrimes.

QU'EST-CE QUE LE WEB INVISIBLE?

Le Web invisible, aussi appelé Web profond, a été développé par l'armée américaine et est différent du darknet. Il a d'abord été conçu dans les années 1970 pour isoler des réseaux de l'Advanced Research Projects Agency Network (ARPANET) et cacher l'emplacement et les adresses IP des activités militaires des États-Unis à des fins de sécurité. Les armées, les gouvernements et les organismes d'application de la loi comptent toujours parmi les principaux utilisateurs du Web invisible.



Le Web invisible se compose de contenu non indexable, de pages de contenu dynamique et de contenu autrement protégé qui n'est pas accessible au moyen des navigateurs et moteurs de recherche réguliers. Le Web invisible comprend d'importantes bases de données, des bibliothèques et des sites Web réservés à des membres qui sont inaccessibles au grand public; les sites sont plutôt protégés ou cachés de manière à ce que seul le public cible y ait accès. Des ressources théoriques tenues par des universités et d'autres institutions forment la majeure partie du contenu du Web invisible. Il est désormais communément utilisé pour le stockage de renseignements en ligne.

QU'EST-CE QUE LE DARKNET?

De manière générale, un darknet est un ensemble de réseaux faisant appel à des technologies qui permettent aux utilisateurs de communiquer et d'interagir dans l'anonymat. Le terme « darknet » a été utilisé pour différencier les réseaux distribués privés et anonymes des réseaux publics. Il a ensuite évolué et désigne maintenant un réseau distribué décentralisé qui ne possède pas d'index central et qui intègre la protection de la vie privée par chiffrement et des caractéristiques d'anonymat des utilisateurs dans le but principal de partager des renseignements uniquement avec des membres de confiance.

L'objectif d'un darknet est de créer un réseau fermé de communication sécuritaire de manière à éviter d'être détecté ou infiltré, afin que l'accès aux sites Web soit anonyme. Le projet Freenet constitue l'un des premiers exemples de darknet. Il s'agit d'une plateforme pair à pair utilisée de manière anonyme pour partager des dossiers, clavarder ainsi que naviguer sur des *freesites* (des sites Web accessibles uniquement sur la plateforme Freenet), et publier de tels sites, sans craindre la censure. En outre, il permet de créer des réseaux privés pour que le contenu d'un site Web particulier soit accessible seulement aux personnes à qui un accès a été donné manuellement. Le réseau privé I2P, un exemple plus moderne, offre également le stockage intégré de fichiers, des courriels sécurisés, une fonction de clavardage et des blogues.

Désormais, le terme darknet désigne également la troisième couche de l'Internet, celle qui est « cachée ». En raison de l'anonymat offert aux utilisateurs, le darknet accueille maintenant une gamme d'activités et d'opérations Internet clandestines, notamment la violation des droits de propriété intellectuelle, la cybercriminalité et le terrorisme.

FONCTIONNEMENT DU DARKNET

Le darknet fait appel au « routage en oignon », une technique qui permet la communication anonyme sur un réseau informatique. Le routeur en oignon (*the onion router, ou Tor*) est un logiciel gratuit de cryptage nécessaire pour accéder au darknet. Le nom choisi pour le système symbolise les nombreuses couches d'un oignon. Le logiciel Tor a été développé au milieu des années 1990 par le Naval Research Laboratory (le « NRL ») des États-Unis.

En 2002, le NRL a lancé une version publique de Tor, ce qui a permis à tous de télécharger et d'utiliser Tor pour naviguer sur le Web visible dans l'anonymat et pour visiter des sites Web anonymes du darknet. Plusieurs millions de personnes utilisent Tor au quotidien. Par conséquent, bon nombre de sites Web ont émergé sur le darknet.

Chaque site Web du darknet possède sa propre adresse IP *.onion* contenant une combinaison alphanumérique de 16 éléments suivie de la désignation *.onion*, par exemple, a1b2c3d4e5f6g7h8.onion. Un utilisateur doit connaître l'adresse .onion pour accéder au site Web voulu. Le domaine *.onion* n'est pas reconnu parmi les domaines de premier niveau établis ou soutenus par la Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN).

Le darknet est populaire chez les blogueurs et les journalistes vivant dans des territoires où la censure et l'emprisonnement politique sont monnaie courante. On y retrouve de nombreux forums. Facebook possède un site Web sur le darknet, conçu pour les utilisateurs qui visitent le site Web par l'entremise de Tor, pour échapper à la surveillance et à la censure. Plus d'un million d'utilisateurs accèdent à Facebook de cette façon chaque mois.

MARCHÉS DU DARKNET

Un aspect central du darknet est le nombre de marchés en ligne vendant des biens contrefaits, piratés et illégaux. Par exemple, des utilisateurs peuvent être redirigés d'un site du Web visible à un site Web du darknet sans le savoir, notamment par une page Web non indexée dont le nom ressemble beaucoup au nom de domaine du site Web officiel d'une marque. Cela peut également se produire par un clic sur une publicité qui contient un lien vers un site du darknet dans les résultats d'un moteur de recherche ou par des applications mobiles ou des courriels contenant des liens redirigeant les utilisateurs vers des sites Web non indexés du darknet.

Le marché le plus populaire du darknet était Silk Road, jusqu'à sa fermeture par le gouvernement américain. Le particulier qui exploitait ce site a été reconnu coupable de nombreux crimes, dont pour complot visant à violer diverses lois. Il a dû payer plus de 180 M$ US d'amendes et a été condamné à la prison à vie sans libération conditionnelle.

Dès que le gouvernement a fermé Silk Road, une autre personne a mis en place Silk Road 2.0 et a rapidement été accusée des mêmes crimes que l'exploitant du premier site. De nombreux autres marchés du darknet, comme Alpaca, Cloud 9, Hydra et Pandora, ont été retirés par les autorités au moyen de « pots de miel », c'est-à-dire des sites Web mis en place pour attirer et piéger des personnes prenant part à des activités illégales.

Malgré tout, de nombreux autres marchés continuent de prospérer sur le darknet, dont Abraxas, Agora, AlphaBay, Andromeda (anciennement Dark Bay), BlackBank, Blue Sky, Evolution, The Free Market, Middle Earth, Nucleus, Outlaw Market, Pirate Market, RAMP et Tochka. Certains sont accessibles sur invitation seulement, mais fonctionnent comme un marché sur le Web visible.

Les marchés du darknet comprennent généralement tous les attributs d'une foire commerciale en ligne : pages de fournisseur, évaluations de produits, listes de produits, service à la clientèle et procédures de règlement des différends. Nombre d'entre eux effectuent uniquement des opérations avec une devise virtuelle, qui utilise la cryptographie comme moyen de sécurité, notamment les bitcoins. (Pour en savoir davantage, consultez notre article paru en septembre 2015 intitulé *Payez-vous comptant, par carte de crédit ou en bitcoins? Avantages et inconvénients de la monnaie numérique*)

L'absence d'un moteur de recherche efficace a été pendant longtemps l'une des caractéristiques contribuant aux volets clandestins du darknet. Cependant, le moteur de recherche Grams indexe désormais certains des principaux marchés du darknet se trouvant sur Tor.

AUTRES CRIMES SUR LE DARKNET

Des sondages ont révélé que les biens les plus couramment vendus sur les marchés du darknet sont les drogues illicites, les cartes de crédit, les armes ainsi que les biens contrefaits et piratés. La monnaie virtuelle, la fraude, le piratage, les canulars, l'hameçonnage et le terrorisme constituent les services les plus fréquemment achetés sur ces marchés.

Les dossiers obtenus dans le cadre d'atteintes à la protection des données sont souvent publiés et mis en vente sur le darknet. Par exemple, des pirates ont publié sur le darknet des renseignements concernant les membres du site de rencontres Ashley Madison.

Par ailleurs, des études indiquent que la pornographie juvénile est très recherchée sur le darknet. Dans un procès pour pornographie juvénile aux États-Unis, il a été révélé que le Federal Bureau of Investigation avait pris le contrôle de PlayPen, le service de pornographie juvénile connu le plus important du darknet, au moyen d'une technique d'enquête de réseau visant à obtenir les adresses IP et MAC des utilisateurs et ainsi obtenir des preuves de la vente de pornographie par les accusés.

L'utilisation croissante du darknet comme plateforme pour la violation de propriété intellectuelle ainsi que pour des crimes commerciaux ou autres force les entreprises à prendre conscience des répercussions actuelles et futures du darknet sur leurs activités.

COMMUNIQUEZ AVEC NOUS

Sunny Handa
514-982-4008
sunny.handa@blakes.com

Sheldon Burshtein
416-863-2934
sb@blakes.com