الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ا م

LETTRE D'INFORMATION : BON A SAVOIR (N°17)

Etude au cœur du carding et du Deepweb

Une étude-reportage par Lycroft Eugenia. Comme vous le savez il existe un véritable business d'escroquerie et de fraudes sur le net. Voici un article complet pouvant être qualifié d'étude-reportage sur le carding.

Qu'est ce que le carding ?

Il s'agit des fraudes à la carte bancaire sur le net (achat, vols, blanchissement de fonds…). Nous nous intéresserons au carding général ainsi qu'à ses dérivés (trafic de faux-papiers, blackmarket, etc…).

Le *"**deepweb**"*, représentant 70% de l'internet n'est pas référencé par les moteurs de recherche tels que Google ou Yahoo!

Véritable nid de tous les excès, il s'agit d'un endroit favorable et apprécié pour les groupuscules de carders.

Quelques recherches et de "bons contacts" suffisent pour vite trouver quelques adresses et aboutir à de telles annonces :

Et non, vous ne rêvez pas, les cartes bancaires sont tellement abondantes qu'elles ne coûtent que 10$ soit environ 8 euros pour des modèles européens !

Ce n'est pas tout, nous avions ici affaire à de petits vendeurs isolés, sachez que certains se réunissent et mettent en place un véritable système de vente sécurisé. Rappelez-vous les deux grandes places de marchés dédiées à la vente de CVV de par le monde qui ont été démantelées cette année…

Ici un groupe de carder distribue gratuitement un stock de numéros de cartes bancaires valides afin de se faire promouvoir :

Certains n'hésitent pas non plus à recruter publiquement :

Les comptes PayPals, Liberty Reserve et Moneybookers (la plupart étant volés via des malwares) se vendent dans chaque BlackMarket et certains sites en sont mêmes spécialisés :

Une question se pose alors :

Comment ces carders obtiennent-ils ces numéros de cartes bancaires et ces comptes ?

A cette question il y a plusieurs réponses.

Le **phishing** est responsable d'une partie non négligeable des données en circulation. Pour rappel, il s'agit de mails ou de faux sites se faisant passer pour votre banque (ou tout autre organisme officiel) voir même, plus récemment via des appels téléphoniques.

Ceux-ci vous demandent de saisir vos identifiants et/ou vos coordonnées bancaires et c'est alors qu'ils les obtiennent.

Ensuite arrive le piratage de sites Web. Si vous avez fait des achats en ligne, le site web conserve certaines de vos données bancaires en cas de litige pendant un temps défini. Dès l'instant ou le site web est piraté et que sa base de données à été corrompue et dérobée par un pirate informatique après une intrusion sur le serveur, les données personnelles et bancaires pourront alors être remises à des carders.

Plus actifs et plus efficace encore, voici les malwares. Les botnets comme SpyEyes ou Zeus sont équipés pour dérober les comptes bancaires et les numéros de cartes de crédit. Ils embarquent des "grabbers" qui sont capables d'intercepter et d'enregistrer les données des formulaires par exemple.
D'autres virus sont spécialisés dans le vol d'identifiants, ils sont appelés Stealers ou Password Stealers. C'est le moyen le plus rapide de récupérer des données privées sur des ordinateurs. Certains sont relativement accessible du fait qu'ils se vendent à bas prix par rapport aux botnets.

Interview

Afin d'en savoir plus sur les carders, nous avons décidé de réaliser une interview avec un carder français :

Lycroft: nos lecteurs aimeraient en savoir plus sur le carding. Auriez-vous une courte définition à leur proposer?

CarderX: La définition la plus courte et complète que je puisse donner et celle qu'on utilise le plus régulièrement.

Le carder est une personne qui va commander sur des sites e-commerce, tel que C-discount, pour ne citer que lui. C'est celui qui va commander l'objet en question et faire de son mieux pour que la transaction soit acceptée et que l'objet convoité quitte les entrepôts.

Le carding en général regroupe donc, les usurpateurs de coordonnées bancaires (ceux qui, donc vont nous vendre les numéros de carte de crédits) Le carder (que je viens de citer plus haut) et le dropper, c'est la personne qui va réceptionner le colis d'un quelconque moyen afin de le renvoyer au carder en échange d'argent, ou qui va le revendre afin d'envoyer un pourcentage au carder souvent du 50/50 Il arrive aussi, mais rarement, que le carder drop lui même son colis.

J'espère que la réponse est assez complète, n'hésitez pas à me demander des précisions.

Lycroft: vous avez parlé de dropper. Vous pourriez expliquer le dropping-shipping à nos lecteurs?

CarderX: Le drop-shipping (et là on parle bien de carding, le drop-shipping à de multiples définitions suivant comment il est utilisé et par qui il est proposé)

Le drop-shipping donc est souvent proposé par de gros carders qui ont un stock de produits récupérés plutôt conséquent, on parle là de 50 iPad, 30 Macbook, 80 iPhone par exemple.

Le drop-shipper (celui qui propose le produit) recherche donc des personnes pour vendre ses produits sur des sites de vente (eBbay, Priceminister etc.)

Le revendeur (celui qui a accepté le contrat) va donc mettre des annonces, sur son compte personnel pour vendre les objets du carder/drop-shipper, une fois la vente finalisée (objet acheté, payé) le revendeur va donner la part due au dropshipper et celui-ci une fois l'argent reçu va expédier le colis à l'adresse de l'acheteur.

Le revendeur, dans tous ça, conserve tout l'argent qui est au delà du montant demandé par le carder

Imaginons que le carder en demande 250 € et que la vente s'est finalisée à 564, le revendeur empoche 314 €

Lycroft: concernant le carding. Quelles précautions utilisez-vous pour éviter le tracing?

CarderX: Alors, tout dépend de la mobilité du carder, vous avez des carders qui vont utiliser un netbook, acheté en cash dans une boutique de reventes d'objets d'occasion, comme Cash Converter afin de ne pas être lié à l'ordinateur d'une quelconque façon qu'il soit. Et ils utilisent les hotspot, Mac Donald, hotels, hotspot dans la rue tel que SFR et Freewifi (ils achètent les identifiants qui ont été usurpés à des victimes de stealer).puis se cachent derrière un vpn et un socks, selon la localité originale de la carte de crédit qu'ils utilisent.

D'autres, vont utiliser leur propre PC et la connexion d'un voisin, changer leur adresse MAC, changer les DNS pour ceux de google se mettre sous VPN, se relier à un RDP, puis un autre VPN et utiliser le socks correspondant à la localité de la carte.
CarderX: personnellement j'utilise cette deuxième option.
Lycroft: En France, d'après vos connaissances pensez-vous le carding très organisé? (nombreux réseaux). Pensez-vous que la police est efficace et empêche votre « travail »?
CarderX: D'après mes connaissances, le carding n'est pas assez évolué à mon gout, d'ailleurs, même les communautés virtuelles (forums, en l'occurrence) sont très peu développées et ce n'est pas vraiment un gros problème, au contraire.
Mais il est certains que nous sommes de petits joueurs comparé à nos amis US.
La police ?
Mouarf, la police ne s'occupe pas de ça, vraiment ! C'est à peine si ils prennent les dépôts de plaintes..
Une émission est passé sur France 2 il y a de ça un an et demi.
Les flics avouaient eux-mêmes préférer coincer des dealer dans les cages d'immeuble, c'est direct, c'est du flagrant délit, ça ne coute rien, et ça augmente les statistiques, et là se crée le fameux (faux) sentiment de sécurité..
La France n'a ni les moyens financier ni les moyens intellectuels pour le faire. Vous avez déjà entendu parler d'une brigade contre le cyber-crime ? A part la BEFTI qui ne fait qu'arrêter des uploaders sur boards warez ? Non. Et encore, les uploaders qui se protègent derrière un simple VPN ne se font pas avoir..
En vérité, en France, il faut vraiment avoir fait de grosses conneries.. La seule façon qu'ils ont trouvé pour qu'un carder se fasse attraper, c'est de faire partir un flic déguisé en livreur de la poste (comme le fait la douane avec les gros colis de contrefaçons..)
CarderX: Mais c'est aussi pour ça qu'il y a les droppers.
Lycroft: Vous connaissez la fraude des faux-papiers. Vous y avez déjà eut un quelconque rapport. Si oui est-ce possible d'avoir votre expérience
CarderX: La fraude réelle, non, aucunement, pour le moment.
La fraude virtuelle, de faux scans, rien de bien compliqué, des graphistes en herbe, sur certains forums vous vendent :
Faux justifs de domiciliation, faux scans d'identité, faux scans de carte de crédit et tous ça avec toutes les valeurs que vous souhaitez. Pour environ 15à25 €, selon la board, selon le contact, la qualité du produit etc.
Ces faux « papiers » servent à passer les contrôles de vérifications imposés par fia-net, entre autres.
c'est tout ce que je peux dire à ce sujet. Je ne suis pas très renseigné sur ces pratiques de faussaires.
Lycroft: que pouvez-vous nous dire sur le skimming?
CarderX: Le skimming, je n'y trempe pas du tout.
Ce sont des dispositifs qui copient la bande magnétique de la carte bancaire… et une camera enregistre le code de la carte, ensuite les personnes s'en servant envoient les données à des contacts en thailand etc.. Afin de cashout le tout et se font renvoyé l'argent par Wester union, ou d'autres moyens que je n'ai à ma connaissance. thailand, aux pays du maghreb, ça dépend. Mais je ne suis pas calé du tout là dedans) »

Le shiping-droping

A titre d'explications sur le shipping-droping voici l'explication donné par notre « carderX » :
« Le drop-shipping (et là on parle bien de carding, le drop-shipping ayant de multiples définitions suivant comment il est utilisé et par qui il est proposé). Le drop-shipping donc est souvent proposé par de gros carders qui ont un stock de produits récupérés par le biais de

cartes bancaires volées plutôt conséquent, on parle là de 50 iPads, 30 Macbooks, 80 iPhones par exemple.
Le drop-shipper (celui qui propose le produit) recherche donc des personnes pour vendre ses produits sur des sites de vente légaux (Ebay, Priceminister, le Bon Coin, etc).
Le revendeur (celui qui a accepté le contrat de revente) va donc mettre des annonces, sur son compte personnel pour vendre les objets du carder/drop-shipper, et une fois la vente finalisée (l'objet acheté et payé), le revendeur va donner la part due au drop-shipper et celui-ci une fois l'argent reçu va expédier le colis à l'adresse de l'acheteur.
Le revendeur, dans tout ça, conserve tout l'argent qui est au-delà du montant demandé par le carder. Imaginons que le carder en demande 250 € et que la vente s'est finalisée à 564 €, le revendeur empoche donc les 314 € restant. »

Le cashout

Lorsqu'un carder a dérobé des identifiants de cartes bancaires, il lui faut blanchir l'argent. Ces procédés de blanchissements sont appelés cashout. Voici des exemple d'annonces sur des techniques de cashout :

La fraude aux faux-papiers

Des carders se spécialisent aussi dans la falsification de documents, sur une offre un carder nous propose d'accéder à son « catalogue », sécurisé par mot de passe et en suivant ses recommandations :
Vous remarquerez la présence des hologrammes ainsi que la qualité faisant qu'il est très difficile de pouvoir affirmer qu'il s'agit d'un faux. Même les pays de l'est, comme la Pologne, sont touchés.
Après avoir contacté un de ses carders pour en savoir plus sur ce business, celui-ci a montré ses templates éditables. Il s'agit de fichiers .psd, Photoshops éditables. Ainsi les carders peuvent y insérer des noms, photos et même signature.
Il y a aussi de nombreuses templates pour carte bancaires et surtout des papiers d'identité, des permis pour tout les états des États-Unis, quelques pays d'Europe de l'est et les plus grands pays Europe de l'ouest.
Les carders se renseignent aussi sur les méthodes employées par les polices afin de débusquer ces faux-papiers comme le prouve ce fichier pdf crée par la police expliquant comment reconnaitre de faux papiers.
Ainsi les carders peuvent bypass (dépasser, passer outre) les systèmes de vérifications mis en œuvre par les polices. Ces derniers n'hésitent pas à développer des logiciels pour parfaire leurs faux-papiers, tels que des générateurs de codes barres par exemple ou encore la modification des bandes magnétiques.

Autres fraudes relatives au carding

Voici des captures d'écran de la page d'acceuil d'un Blackmarket vous résumant le « reste » :

Conclusion

A la suite de cette étude nous pouvons conclure sur le fait qu'internet peut donner accès à des trafics pour n'importe qui tels que le trafic d'armes, de drogues, de faux-papiers, de données bancaires etc…
Le fait le plus effrayant est que n'importe qui peut avoir accès aux méthodes, à l'achat et à la vente de ce type de produits.
https://www.undernews.fr/undernews/reportage-etude-au-coeur-du-carding-et-deepweb.html

Découvrez le « deep web »,

Dans les profondeurs du Web : Armes, drogues, êtres humains : les trafics se dématérialisent et investissent ce que l'on appelle le "deep web", la partie immergée d'Internet. Ce "web

profond” est aujourd’hui le théâtre d’affrontements sans répit entre dealers et forces de police, entre terroristes et agences de renseignements. Mais c’est aussi la dernière zone dans laquelle notre vie privée numérique se trouve en sécurité

L e 15 juillet, à Pittsburgh, le procureur américain David Hickton, cheveux gris et costume sombre, annonçait la dernière victoire du FBI dans la lutte contre la cybercriminalité. “Nous avons démantelé un réseau de pirates criminels que beaucoup croyaient impénétrable”, a-t-il déclaré sur fond de drapeau américain. Le lendemain matin, dans plusieurs pays, plus de 70 personnes étaient inculpées, interpellées ou voyaient leur domicile perquisitionné dans le cadre de “la plus grande opération policière internationale jamais menée contre un forum en ligne de cybercriminels”. L’enquête de dix-huit mois conduite par le FBI visait les utilisateurs du site Darkode, aujourd’hui accusés d’escroquerie bancaire, de blanchiment d’argent et de conspiration en vue de commettre une fraude informatique. Leurs méfaits atteignaient des proportions inédites : l’un d’eux avait réussi à s’introduire dans les réseaux sécurisés d’entreprises comme Microsoft et Sony ; un autre avait récupéré des informations privées sur plus de 20 millions de personnes. Deux semaines plus tard pourtant, le principal administrateur de Darkode répondait aux autorités depuis un nouveau site. “L’essentiel de notre équipe est à l’abri, ainsi que nos membres les plus importants, écrivait-il alors. Il semblerait que l’opération visait principalement les membres les plus récents ou des gens qui n’étaient plus actifs depuis des années. Le forum sera de retour.” Et il promettait que l’organisation allait se réorganiser à partir de l’une des régions les plus secrètes du web – le “Darknet” (ou “darkweb”) –, une partie du web impossible à faire disparaître puisque ce sont les autorités fédérales qui l’ont créée et qui en financent toujours le développement. Pour accéder au Darknet, où l’anonymat est pratiquement garanti pour tous, y compris les criminels, il faut utiliser le navigateur Tor, un logiciel gratuit qui masque à la fois votre localisation et votre activité sur le réseau. Conçu par un laboratoire de recherche de l’armée américaine, le Naval Research Lab (NRL), et financé à 60 % par le département d’Etat et le ministère de la Défense, Tor devait à l’origine servir de réseau de communication sécurisé pour les agences gouvernementales ainsi que pour les dissidents résidant dans des pays à régime autoritaire. Aujourd’hui, il sert aussi bien pour le meilleur que pour le pire. Côté pile, Tor a permis à des militants de communiquer pendant le “printemps arabe”, il a offert un refuge à des victimes

Le harcèlement en ligne et a permis à des citoyens ordinaires de surfer sur la Toile sans être traqués par les mouchards publicitaires. Côté face, c’est aussi un sanctuaire pour des criminels comme Ross Ulbricht, le fondateur – aujourd’hui emprisonné – du site Silk Road [sorte de supermarché de la drogue], les auteurs du récent piratage contre le site de rencontre Ashley Madison et les membres de forums comme Darkode. Utilisé à la fois par des militants et des criminels, Tor devient de plus en plus problé- matique pour les autorités : à peine supprimés, les sites illégaux repoussent comme du chiendent. De la bataille pour faire régner la loi sur cet espace de non-droit qu’est le Darknet dépend peut-être la protection de nos vies privées en ligne aux Etats-Unis et dans le reste du monde. Le Darknet, résume David Hickton, “c’est le Far West d’Internet”. I maginez le web comme un iceberg : la plupart des internautes ne voient que le web “de surface”, soit toutes les infos, les ragots et le porno qu’une simple recherche sur Google vous permet de trouver. Plongez sous la surface et vous découvrirez le “deep web”, le web profond, c’est-à-dire l’ensemble des données qui ne sont pas indexées par les moteurs de recherche classiques et qui sont incomparablement plus nombreuses que celles que l’on peut observer “en surface”. Cela inclut tout ce qui se trouve protégé en surface par un paywall (comme le site Netflix), un mot de passe (votre boîte électronique) ou le moteur de recherche interne d’une page donnée (lorsque vous recherchez dans des archives judiciaires, par exemple). Et, comme les sites qui se trouvent là ne peuvent pas non plus être trouvés en passant par des moteurs de recherche classiques, c’est dans le web profond que se cache le

Darknet. La principale différence [entre les deux notions], c'est qu'il s'agit d'un choix délibéré de la part des utilisateurs et des sites du Darknet, qui tiennent à leur anonymat et veulent rester introuvables au commun des mortels, qui n'utilise pas le navigateur Tor.

Les autorités ont créé le darknet et le financent

Ce logiciel qui vous permet de surfer sur le web de surface – exactement comme Firefox ou Safari – est aussi la clé pour accéder aux coulisses d'Amazon ou à des sites comme Silk Road. La plupart des utilisateurs de Tor ont recours à ce navigateur pour des raisons parfaitement légales de protection de leur vie privée. En fait, d'après les estimations du Tor Project – l'organisation non marchande financée par le gouvernement américain et chargée de la maintenance du logiciel –, le Darknet ne représente que 3 % du trafic réalisé avec Tor. (Et seule une infime partie de ce pourcentage concerne des activités criminelles.) Mais, en raison de sa nature opaque et mystérieuse, le Darknet évoque généralement un sinistre fourre-tout regroupant tout ce que l'on peut trouver de pire en ligne, des groupes terroristes aux réseaux pédophiles, en passant par le trafic de drogue et les hackers mercenaires. Certains des aspects les plus inquiétants du Darknet sont en effet remontés à la surface ces derniers mois. En mai, le fondateur de Silk Road – qui avait vendu pour près de 200 millions de dollars de drogue à des consommateurs du monde entier – a été condamné à la prison à perpétuité. En août, des pirates informatiques ont publié des informations personnelles sur 36 millions d'utilisateurs du site de rencontres extraconjugales Ashley Madison. Enfin, en mai, c'est vers le Darknet que se sont portés tous les regards après que l'organisation Etat islamique (EI) a revendiqué la fusillade perpétrée au Texas en marge d'un concours de caricatures du Prophète. En dépit des coups de filet spectaculaires contre des sites comme Darkode ou Silk Road, les activités du Darknet restent florissantes. D'après une étude publiée en août par des chercheurs de l'université Carnegie Mellon [à Pittsburgh], la vente de drogue et d'autres produits de contrebande rapporterait chaque année près de 100 millions de dollars sur ces sites invisibles où les transactions sont réalisées à l'aide de bitcoins, cette monnaie virtuelle qui ne nécessite ni carte de crédit ni établissement bancaire.

Les enquêteurs n'ont pas seulement affaire à des réseaux criminels capables de rester invisibles sur la Toile, ils sont également confrontés à un afflux massif d'utilisateurs ordinaires à la recherche de produits illicites. Car, contrairement à ce que beaucoup pensent, il n'est pas nécessaire d'être un petit génie de l'informatique pour accéder au Darknet. En fait, il est même étonnamment facile de vendre ou d'acheter des biens et services illégaux : lancez le logiciel Tor et vous vous retrouverez sur un navigateur semblable à tout autre, à l'exception de la vitesse de navigation, très ralentie à cause des sché- mas de routage complexes des données.

"Ici c'est Le far west d'internet"

Au lieu de finir en ".com" ou ".org", les adresses des sites du Darknet se terminent en ".onion" (d'où leur surnom de "sites oignons"). Google n'indexant pas ces "sites oignons", il vous faudra utiliser les moteurs de recherche rudimentaires du Darknet ou des répertoires comme Hidden Wiki ou Onion Link pour trouver votre destination. Les sites marchands du Darknet ressemblent à n'importe quelle autre plateforme commerciale, sauf qu'en lieu et place des ustensiles de cuisine ou décorations de jardin vous trouvez des benzodiazépines, des stupéfiants et des Kalachnikov d'occasion. P aul Syverson, membre du NRL, est le créateur du logiciel Tor. "Nous savions pertinemment que des gens malintentionnés pourraient s'en servir, explique ce mathématicien de 57 ans. Mais notre objectif, c'était de proposer un outil aux gens honnêtes qui ont besoin de protection." Réputé dans le monde entier depuis sa création, en 1923, le NRL est notamment l'inventeur du radar et du GPS. En 1995, Syverson et son équipe imaginent un moyen de sécuriser les communications en ligne. L'idée est de permettre à qui que ce soit de partager des informations sans révéler ni son identité ni sa localisation. Après avoir obtenu un financement du ministère de la Défense, Syverson recrute

deux jeunes diplômés du Massachusetts Institute of Technology (MIT), Roger Dingledine et Nick Mathewson, pour mener à bien son projet. Imaginez un espion prenant le train entre Paris et Berlin. Il est facile de le suivre s'il prend une ligne directe entre les deux villes mais, s'il fait Paris-Amsterdam, AmsterdamMadrid, puis Madrid-Berlin, la tâche devient beaucoup plus ardue. C'est la logique qu'ont adoptée Syverson et son équipe. Au lieu de prendre un train direct pour Berlin, l'utilisateur de Tor passe par une série aléatoire d'ordinateursrelais qui masquent son véritable point de départ. C'est ce qu'on appelle le routage "en oignon" [Tor est l'acronyme de The Onion Router], c'est-à-dire par couches successives. Si le logiciel Tor était réservé aux militaires, toutes ses activités seraient logiquement en lien avec le gouvernement. Mais, poursuit Syverson, "nous voulions créer un réseau capable d'accueillir toutes sortes d'utilisateurs, de manière que nul ne puisse savoir si vous êtes un malade du cancer qui recherche des informations ou bien un soldat de la marine". Pour ce faire, Syverson et son équipe prennent alors une décision "fondamentale pour la sécurité du système" : ils choisissent de faire de Tor un logiciel libre et open source, c'est-à-dire que n'importe qui dans le monde peut l'utiliser et l'améliorer. Accessible au grand public depuis 2003, Tor circule rapidement dans les milieux universitaires et chez les défenseurs de la vie privée. Très vite, il devient le navigateur préféré – et le plus fiable – des internautes désireux de ne laisser aucune trace sur le web. Ses premiers utilisateurs ne sont pas des criminels, mais des dissidents. L'un d'entre eux, Nima Fatemi, est un Iranien de 27 ans, tout vêtu de noir. Devenu l'un des principaux propagateurs du logiciel, il apprend aux internautes du monde entier comment l'utiliser pour lutter contre les régimes dictatoriaux. "Nous avions besoin de quelque chose de différent pour nous connecter en toute sécurité, se souvient-il. J'ai trouvé Tor et je me suis dit : 'C'est ça qu'il nous faut.' Ça nous a permis d'avoir l'esprit tranquille." Au cours de l'été 2009, Fatemi prend des photos de manifestations pro-démocratie à Téhéran et se retrouve pourchassé par les forces de police. Les photos qu'il publie sur Facebook et Twitter témoignent de la répression menée par le gouvernement iranien contre les dissidents. De plus en plus étroitement surveillé, il se tourne alors vers le logiciel Tor pour continuer à travailler dans le secret de l'anonymat et aider ses camarades militants à échapper à la police. Fatemi organise des ateliers privés pour apprendre à sa famille et à ses amis comment utiliser le réseau Tor, dont la sécurité croît avec le nombre d'utilisateurs : plus il y a d'ordinateurs connectés, plus il y a de "nœuds" pour brouiller les traces. "Nous avons diffusé ce logiciel partout", assure-t-il. Dans les dix ans suivant sa sortie, le navigateur Tor se répand ainsi massivement dans les cercles militants, en partie grâce aux efforts de l'Electronic Frontier Foundation [EFF, une ONG qui défend la liberté d'expression sur Internet], qui a financé son développement et le présente encore aujourd'hui comme l'un des meilleurs outils de lutte pour la démocratie. Alors que le Tor Project bénéficie encore largement des financements du ministère de la Défense américain, Mathewson et Dingledine continuent à faire évoluer leur logiciel et la communauté qui l'entoure. Aujourd'hui, la popularité du navigateur dépasse toutes ses espérances, reconnaît Mathewson, grand amateur de science-fiction de 38 ans. "Je reçois des courriels de gens qui me disent : 'Je suis à peu près sûr que votre logiciel m'a sauvé la vie.' Ce à quoi je réponds que je suis bien content qu'ils soient en vie, mais je ne suis qu'un programmeur informatique. J'espère juste ne pas faire de boulette !" L e 27 janvier 2011, Ross Ulbricht annonce sous le pseudonyme Altoid le lancement imminent de Silk Road [littéralement, la "route de la soie"], le premier marché noir sur le Darknet. Gérant son site sous le nom de Dread Pirate Roberts, Ulbricht est le premier à exploiter pleinement le potentiel criminel de Tor. Il s'agit moins d'une prouesse technique que d'une idée nouvelle. N'importe qui peut déjà créer son site illégal dans les profondeurs du Darknet, où il est aussi difficile d'identifier les auteurs des contenus que ceux qui les consultent. Mais Ulbricht va encore plus loin en utilisant le bitcoin comme monnaie d'échange, ce qui lui permet de rendre

les transactions tout aussi intraçables. A l'été 2011, le terme "Darknet" fait son apparition dans les médias et le discours des politiques.

"Votre Logiciel m'a sauvé la vie"

En novembre 2013, le magazine Time évoque en une "un repaire de criminels où cohabitent les drogues, le porno et les vidéos de meurtres". Un mois plus tôt, on a appris grâce à un document publié par Edward Snowden que l'Agence nationale de sécurité américaine (NSA) considérait le logiciel Tor comme une menace potentielle. Lors d'une réunion ultraconfidentielle en 2012, l'agence notait : "Nous ne pourrons jamais entiè- rement lever l'anonymat des utilisateurs de Tor, mais nous pouvons en identifier un très petit nombre." (Contactée par Rolling Stone, la NSA s'est refusée à tout commentaire.) Toujours d'après les révélations de Snowden, l'agence de renseignements britannique [le MI6] conteste le caractère pro-démocratie du navigateur Tor, jugeant les "utilisations pseudo-légitimes" mineures par rapport aux "mauvais usages" qui sont faits du Darknet. Les autorités commencent alors à chercher de nouvelles manières d'infiltrer le Darknet. En juillet 2015, Interpol organise sa première formation pour "identifier les méthodes et stratégies utilisées par les réseaux du crime organisé pour échapper à toute détection sur le Darknet". Le même mois, le directeur du FBI, James Comey, explique devant la commission judiciaire du Sénat l'impuissance de ses agents face aux communications cryptées. "Les outils qu'on nous demande d'utiliser sont de moins en moins efficaces", déclare-t-il. Des courriels récemment rendus publics montrent pourtant qu'au moins une société semblait détenir la solution. Installée à Milan, Hacking Team est une entreprise de sécurité informatique qui fournit aux gouvernements des outils pour lutter contre les criminels, les activistes et les agitateurs du Darknet. "Il est possible de neutraliser/décrypter le Darknet dans sa totalité. La technologie existe. Faites-nous confiance", écrivait le directeur de cette société, David Vincenzetti, dans un courriel adressé au directeur du FBI. L e responsable de l'innovation à la Darpa, l'agence en charge des projets de recherche avancés pour le ministère de la Défense américain, est un homme jovial aux cheveux blancs, ancien concepteur de jeux vidéo. Dans une salle de conférences du quartier général de l'agence à Arlington, en Virginie, Dan Kaufman m'explique sur un écran haute définition comment la Darpa tente de remporter le jeu du gendarme et du voleur à l'ère numérique. A titre d'exemple, il me montre une annonce vantant les services d'une prostituée appelée Cherry, une jeune femme mince, asiatique, qui semble avoir 19 ans mais qui pourrait en avoir 30. Mesurant 1 m 62, les cheveux bruns aux épaules, l'annonce précise qu'elle n'a ni tatouage ni piercing. Cherry est l'une des victimes de la traite des femmes organisée au niveau international, qui, d'après les estimations du département d'Etat américain, frapperait entre 600 000 et 800 000 femmes chaque année. Avec près de 100 millions de dollars de profit annuel, c'est l'une des activités les plus florissantes du crime organisé dans le monde. Comme tous les autres trafics – d'armes ou de drogue –, cette activité s'est délocalisée, délaissant la rue pour les profondeurs du web : forums anonymes, messageries cryptées, services d'abonnement et autres sites invisibles pour les moteurs de recherche. C'est cette lacune qui a incité la Darpa à intervenir. "Nous sommes partis d'un constat simple : tout ça est terrible, nous ne pouvons pas rester les bras croisés."

Memex, L'arme des enquêteurs pour sonder le web caché

La Darpa a donc créé Memex, un moteur de recherche capable de sonder le deep web et le Darknet. Memex peut effectuer des recherches sur le web profond, trouver des sites et stocker des données qui permettront de les purger, exactement comme Google sur le web de surface. Il s'agit de la dernière et principale arme des enquêteurs pour jeter de la lumière sur le web caché. Kaufman me fait une démonstration : avec la seule adresse électronique de Cherry, Memex fait apparaître en un clic toute une liste d'informations, dont des numéros de téléphone, des adresses de salons de massage et des photos en lien avec les annonces. Le créateur du moteur de recherche Memex s'appelle Christopher White. Ancien responsable des

programmes de la Darpa, cet homme de 33 ans a d'abord fait ses classes comme haut responsable de la Darpa en Afghanistan avant de s'intéresser, il y a quelques années, au Darknet. L'idée lui est venue après avoir visité plusieurs agences gouvernementales et constaté leur niveau d'impréparation dans la lutte contre la cybercriminalité. "Ils utilisaient Google et Bing pour leur travail, se souvient-il. Les informations qu'ils recherchent ne leur sont pas accessibles par ces moyens, elles se trouvent dans les méandres du Darknet." Les agences gouvernementales et les forces de police coopèrent désormais étroitement avec la Darpa afin de calibrer Memex au plus près de leurs besoins. Il s'agit également d'explorer les possibilités offertes par ce moteur de recherche pour démasquer les recruteurs de l'organisation Etat islamique qui se cachent sur le réseau. Cette technologie est le produit d'une industrie en plein essor consacrée à la "domestication" du Darknet. Moyennant des sommes pouvant aller jusqu'à 500 000 dollars, des entreprises d'évaluation des "menaces liées au renseignement" promettent à leurs clients de passer le Darknet au peigne fin à la recherche d'éventuels pirates. D'après le cabinet de recherche technologique Gartner, ce marché pourrait représenter 1 milliard de dollars d'ici à 2017. Ce passage à la lumière du Darknet ne risque-t-il toutefois pas de faire disparaître le dernier espace de vie privée sur Internet ? Les défenseurs des libertés espèrent que l'arrivée du moteur de recherche Memex ne mettra pas en péril les internautes du Darknet qui respectent les lois. "Memex est un outil incroyable et fascinant, mais, comme n'importe quelle autre technologie, il peut servir à faire le bien autant que le mal", soulignait récemment un blogueur spécialiste de la sécurité en ligne. Pour l'heure, les policiers du Darknet ont toutefois de bonnes raisons de se réjouir. En dépit de leurs rodomontades, les anciens membres du forum Darkode n'ont pas encore redonné signe de vie (ce qui ne signifie pas qu'ils ne sont pas là) et les premières condamnations d'internautes devraient bientôt tomber. Mais, pendant que le FBI célèbre ses victoires, les gens dont la vie dépend de l'anonymat continuent à se battre. En août, la Cour suprême d'Arabie Saoudite a examiné le cas de Raif Badawi, un blogueur de 31 ans arrêté en juin 2012 et condamné à dix ans de prison et 1 000 coups de fouet, accusé d'avoir critiqué des religieux. Raif Badawi illustre bien l'importance de maintenir des zones d'anonymat et de liberté sur Internet, zones qui n'existent que grâce au logiciel Tor, sans lequel le Darknet n'existerait pas. Pour la représentante de la Californie au Congrès, Zoe Lofgren, les autorités ne devraient pas oublier pourquoi ce logiciel a été créé. "Tor a été développé avec le soutien du gouvernement américain pour défendre la liberté, at-elle déclaré. C'est pourquoi nous plaidons pour son maintien, c'est sa raison d'être." Alors que la bataille du Darknet fait rage, le navigateur connaît une popularité croissante. Facebook propose désormais une version ".onion" de son site pour ceux qui se sentent un peu trop épiés. Invité à un évé- nement organisé par l'organisation de défense de la vie privée et des libertés civiles Epic, le PDG d'Apple, Tim Cook, a ironisé sur les tentatives menées par le gouvernement pour pirater des appareils privés. "La suppression des dispositifs de cryptage de nos appareils – telle que la souhaitent certains à Washington – ne servirait qu'à nuire aux citoyens honnêtes qui nous confient leurs données", a-t-il argué. D'autres navigateurs, comme Firefox, devraient bientôt proposer des fonctionnalités Tor, prophétise Mathewson, qui espère que cette méthode sera "le mode de communication par défaut sur Internet" d'ici cinq ans. Mais la partie de cache-cache sur le Darknet est loin d'être terminée. Même si de nombreux militants utilisent cet outil pour rendre le monde meilleur, il y aura toujours des criminels pour s'en servir. Et des policiers pour les traquer.

http://www.bsavenir.fr/2015/12/14/decouvrez-le-deep-web-lensemble-des-donnees-non-indexees-par-les-moteurs-de-recherche-classiques/

Qu'est-ce qui se passe dans le Deep Web ?

Des spécialistes en sécurité web ont conçu un outil de recherche permettant d'analyser les activités cybercriminelles sur la toile

Pour ne pas se faire repérer, les cybercriminels opèrent généralement dans l'ombre d'internet. Ils font des échanges discrets depuis Deep Web, une face cachée d'internet qui n'est pas indexée au sien des moteurs de recherche. On peut y trouver des pages Dark Web qui ne sont accessibles qu'avec des outils spéciaux comme I2P, Tor ou Freenet. Il y a aussi les sites hébergés au sein de domaines alternatifs qui ne sont pas sous la gestion de l'Icann et qui ne sont pas compatibles avec les résolveurs DNS courants. C'est notamment le cas du '.BIT'.

Durant la conférence 'Black Hat Europe', des spécialistes en sécurité web ont proposé DeWA (Deep Web Analyzer). Il s'agit d'un moteur de recherche permettant de mettre à jour une partie des contenus masqués. Le but est d'identifier la pratique des cybercriminels. Leur système cherche les URL localisées sur plusieurs sources, dont les listes de Dark Web, et analyse chaque page. Celles-ci sont ensuite traduites via le service Google Traduction, puis sauvegardées, indexées et synthétisées depuis un nuage de mots-clés.

En seulement 2 ans, DeWA a pu amasser 611 000 URL sur 20 500 domaines. 75% du contenu est en anglais. Le protocole utilisé est souvent HTTP. Les spécialistes ont aussi pu découvrir plus de 100 domaines consacrés aux échanges par IRC. En tout, cette analyse permet de connaître diverses activités illégales : drogues, faux passeports, armes, informations bancaires, blanchiment d'argent…

Et ce qui choque le plus ce sont les offres de tueurs à gages. On y trouve un site de meurtre à la demande. Il se fonde sur un financement participatif. Plusieurs personnes indiquent un nom et placent un pot. L'assassin prend la somme quand son contrat est achevé. Toute cette démarche se fait de manière anonyme. Sur ce site, il n'y a que 4 personnes qui sont inscrites jusqu'à présent. Et aucune somme d'argent n'a été déposée.

Le Deep Web est aussi une structure permettant de gérer les réseaux de botnets et de **propager des malwares**. À titre d'exemple, c'est à travers le réseau Tor que le malware Vawtrak est diffusé. Pour ne pas se faire détecter, les adresses IP sont cryptées par stéganographie.

http://webmag.fr/2016/01/deep-web/

Plongée au coeur du "Deep Web"
Comment fonctionne le Web clandestin ?

Le "Deep Web" est en quelques sortes la partie immergée de l'Internet que vous connaissez tous, invisible aux yeux des moteurs de recherche et inaccessible aux non initiés. En bref, c'est une zone de non droit où la cybercriminalité rejoint la criminalité. Explications.

Comment y accèdent-on ?

TOR (The Onion Router), IP2 Web ou encore Freenet. Ces moyens permettent non seulement de naviguer incognito mais aussi d'héberger des sites en leur sein. Ces derniers ne sont accessible qu'en connaissant leur adresse exacte et de ce fait, ils ne sont pas indexés par les moteurs de recherche. Cela implique qu'il faut avoir des connaissances dans le milieu afin d'y accéder.

Que pouvons-nous y trouver ?

Des produits physiques et virtuels (dématérialisés) y sont présents. La liste est longue et on ne peut mentionner qu'une partie qui représente la majorité des ventes illégales actuelles :

- drogues diverses (cannabis, héroïne, cocaïne, opium, Barbituriques, Amphétamines, LSD, et des dizaines d'autres psychotropes
- armes en tout genre
- services de piratage professionnel
- faux papiers et fausse monnaie
- malwares (trojans/botnets, password stealers, keyloggers, crypters FUD, binders, ransomwares, etc)
- hébergement "bulletproof" & VPN sans logs
- informations bancaires volées (dumps de cartes de crédit et identifiants bancaires en ligne)
- matériel volé ou acquis illégalement via le carding (blanchiment d'argent)
- photos et vidéos illégales (torture, pédopornographie, etc)
- documents classés secret défense

Quels sont les moyens de paiement qui y sont utilisés ?

Les monnaies virtuelles sont à l'honneur dans ce monde underground, le but étant bien entendu que ce genre de monnaie ne laisse aucune trace des transaction et permet aux deux parties de rester dans l'anonymat. Ces monnaies sont nombreuses et l'on peut en citer quelques unes :

- Bitcoin (cryptomon0naie)
- PayPal (dans certains cas seulement, les transactions peuvent êtres tracées)
- Liberty Reserve (récemment fermé par le FBI)
- Webmoney
- PerfectMoney

Les cartes prépayées anonymisées sont aussi très prisées des criminels. Tous ces nouveaux moyens de paiement en vogue dans l'underground n'offrent aucun contrôle possible de la part des institutions financières mondiales ou des autorités.

Pourquoi ces réseaux clandestins sont intouchables ?

Comme souvent, les autorités se retrouvent démunies face aux technologies avancées des cybercriminels. Le chiffrement de bout en bout est omniprésent et le seul moyen semble d'attendre que la cible commette un faux pas et révèle ainsi son identité (ou du moins une adresse IP pouvant être tracée afin de remonter jusqu'à ce dernier).

https://www.undernews.fr/undernews/plongee-au-coeur-du-deep-web-comment-fonctionne-le-web-clandestin.html

Drogues, armes, malwares, tueurs à gages… à la découverte du Deep Web

Des chercheurs en sécurité ont développé un moteur de recherche qui analyse les activités cybercriminelles qui se trament à l'ombre de la Toile. Les résultats sont, parfois, choquants.

Pour éviter d'être découverts, les cybercriminels opèrent toujours de façon cachée. Leurs échanges sont discrets, ils se tiennent au plus profond du « Deep Web », cette partie de la Toile qui n'est pas indexée par les moteurs de recherche usuels. On y trouve bien sûr les places de marché du Dark Web, accessibles uniquement par des logiciels spéciaux comme Tor, I2P ou Freenet. Mais aussi des sites hébergés dans des domaines alternatifs non gérés par l'Icann et qui ne sont pas pris en charge par les résolveurs DNS classiques. C'est le cas par exemple du .BIT adossé au Namecoin, de la Toile libertaire d'OpenNIC et Name.space ou de l'Internet parallèle de l' « église césidienne » (si, si ça existe).

A l'occasion de la conférence Black Hat Europe 2015, qui se tient à Amsterdam, les chercheurs en sécurité Marco Balduzzi et Vincenzo Ciancaglini ont présenté leur « Deep Web Analyzer » (DeWA), un moteur de recherches qui permet de faire remonter une partie de ce contenu caché. L'objectif étant de mettre en lumière les tendances et les usages du monde de la cybercriminalité.

Leur système aspire des URLs trouvés sur diverses sources - forums publics, listes dans le Dark Web, Twitter, Pastebin, Reddit, etc. - puis analyse les pages. Elles sont traduites par le service Google Traduction, puis stockées, indexées et synthétisées au travers d'un nuage de mots-clés.

En l'espace de deux ans, DeWA a mis la main sur 611 000 URLs de 20 500 domaines. Sans surprise, il apparaît que la langue du cybercrime est l'anglais, qui représente 75 % du contenu aspiré. Loin derrière arrive le russe et le français. Le protocole le plus utilisé est, de loin, HTTP. Mais les chercheurs ont également trouvé plus d'une centaine de domaines dédiés aux échanges par IRC.

Au final, il se dégage de cette analyse une grande variété d'activités illégales. Les chercheurs sont tombés sur des sites de ventes (drogues, armes, passeports, données bancaires…), des services de blanchiment d'argent, des sites de révélations d'informations personnelles (« doxing ») pour provoquer une vindicte populaire (vis-à-vis d'agents du FBI ou de célébrités par exemple), etc.

Parmi les choses les plus choquantes figurent les services de tueurs à gage avec tarifs à la clé. *« En tant que chercheurs, il nous est impossible de savoir si ces services sont vrais ou non. C'est aux forces de l'ordre de se pencher sur cette question. D'ailleurs, nous coopérons régulièrement avec elles »*, souligne Vincenzo Ciancaglini.

L'un des sites de cette catégorie macabre était particulièrement étonnant : un service de meurtre à la demande basé sur le financement participatif. Des personnes ajoutent un nom et mettent au pot. L'assassin récupère la somme après avoir rempli son contrat. Et le tout se fait de manière anonyme. *« Pour l'instant, seules quatre personnes figurent sur ce site et personne n'a mis de l'argent. Il s'agit probablement d'un hoax »*, estiment les chercheurs.

Enfin, le Deep Web sert également d'infrastructure technique pour piloter les réseaux de botnets et diffuser les malwares. Le malware Vawtrak, par exemple, utilise Tor pour diffuser auprès des machines zombies les adresses IP des serveurs de commande et contrôle. Pour rendre la détection encore plus compliquée, ces adresses sont codées par stéganographie dans des images d'icône.

http://www.01net.com/actualites/drogues-armes-malwares-tueurs-a-gages-a-la-decouverte-du-deep-web-929845.html

Le deep web, le côté obscur de la toile

Dans les bas fonds du web, inaccessibles via Google, pirates, dealers et même tueurs à gages naviguent incognito.

À la base, le deep web c'est…

Une partie du web accessible en ligne, mais non référencée par les moteurs de recherche classiques (Google, Explorer, Bing, Yahoo, etc.). Ces derniers possèdent des programmes appelés « robots d'indexation » qui parcourent le web à la recherche de liens hypertexte pour découvrir de nouvelles pages. Mais certaines pages sont isolées, indépendantes ou parfois écrites dans des formats illisibles par ces robots. Ces données « invisibles » constituent le deep web. Seuls 3 à 10% des pages seraient en fait indexées sur le web, comme l'expliquent Chris Sherman et Gary Price dans leur livre *The Invisible Web*. Il existerait plus d'un trilliard de données « cachées » des moteurs de recherche généralistes

Certains documents sont trop volumineux. Certaines bases de données sont trop complexes pour que leurs contenus soient indexés. Et certains individus (grosso merdo des nerds qui s'y connaissent en bidouille) choisissent délibérément de ne pas référencer leur site. Pour « privatiser » l'information. Une seule façon d'accéder à ces pages : connaître leur url. Le développeur du site va alors choisir de diffuser l'adresse à quelques personnes, qui peuvent ensuite la faire circuler grâce au bouche à oreille. Le *deep web* ou le club VIP des ingénieurs informaticiens..

Au fin fond de cette partie immergée du net, certains outils de reconnaissance, eux-mêmes indétectables par les moteurs de recherche classiques et capables de décrypter des pages invisibles pour ces derniers, ont vu le jour. Et se sont vite transformés en bottin 2.0 des criminels…

Le côté dark du deep

Synonyme d'anonymat, le *deep web* a rapidement hébergé tous types de marchés noirs : des drogues aux armes. Le *Hidden Wiki* (sorte de jumeau maléfique de Wikipédia) se charge de référencer ces portes d'entrées sur le « *dark web* ».

On y trouve des sites non commerciaux, comme *Shroomtastic*, un forum pour « apprendre à faire pousser des champignons hallucinogènes et s'amuser ». Et des sites commerciaux, comme *Silk Road*, le plus connu. Un marché clandestin sur lequel on peut acheter toute sorte de drogues, grâce à une monnaie anonyme, virtuelle et universelle qui se passe des banques : le bitcoin.*Silk Road*, le plus connu. Un marché clandestin sur lequel on peut acheter toute sorte de drogues, grâce à une monnaie anonyme, virtuelle et universelle qui se passe des banques : le bitcoin.

L'offre commerciale, illégale et considérable, ne s'arrête pas aux drogues : *CoinFog* permet de blanchir de l'argent ; *Killer For Hire* offre les services de tueurs à gage ; *All Purpose Identities* propose de fabriquer de fausses cartes d'identité et *EuroArms* vends des AK47, des Glock, etc. Sans parler de tous les sites porno déviants et pédophiles.

Avant de s'orienter du côté obscur de la force, mieux vaut mesurer les risques. Personne ne vous poursuivra pour avoir flâné sur le deep web. En revanche, les sanctions pour des transactions illégales sont loin d'être virtuelles. En février 2013, Paul Leslie Howard, trafiquant lié à Silk Road, s'est fait attraper en Australie. Jugé coupable par le tribunal de Melbourne pour vente de cocaïne, amphétamines, LSD et marijuana, il encourt de trois à cinq ans de prison.

Et pourtant les marchés clandestins sont légions. Car les acheteurs, eux, n'ont encore jamais été inquiétés. Le « dark web » assure à ses internautes une ultra-sécurisation de la navigation. Pour cause, l'accès à cette partie du net promet, pour les novices, d'être un vrai parcours du combattant. Accrochez-vous.

Envie de faire vos premiers pas dans le *deep web* ?

L'entrée dans le *dark web* et ses pages ultra-sécurisées, souvent cryptées, se fait via des réseaux décentralisés de routeurs comme Tor, le plus connu et « maintream », ou d'autres outils comme Freenet, I2P, etc. Des programmes qui garantissent, plus ou moins, l'anonymat de votre connexion, en modifiant par exemple constamment votre adresse IP, qui devient alors très compliquée à identifier. Disons… pour le FBI. Vos requêtes passent par une multitude de relais à travers le monde, appelés « nœuds ». Le traçage de la requête originale devient alors quasi impossible. (Ceci n'est pas tiré d'un épisode des Experts.), le plus connu et « maintream », ou d'autres outils comme Freenet, I2P, etc. Des programmes qui garantissent, plus ou moins, l'anonymat de votre connexion, en modifiant par exemple constamment votre adresse IP, qui devient alors très compliquée à identifier. Disons… pour le FBI. Vos requêtes passent par une multitude de relais à travers le monde, appelés « nœuds ». Le traçage de la requête originale devient alors quasi impossible. (Ceci n'est pas tiré d'un épisode des Experts.)

Avant de vous rendre sur Tor, prenez quand même quelques précautions supplémentaires. Commencez par vous armer d'un solide antivirus. Au risque de choper tout un tas de virus pas jolis, jolis. Équipez-vous ensuite d'un VPN (un réseau privé virtuel qui masque le réseau local depuis lequel vous surfez). Ce n'est pas obligatoire, ça fait ramer l'ordi – la navigation sur le *deep web* est déjà lente – mais ça renforce les barrières de sécurité. Une fois que vous aurez téléchargé Tor, faites gaffe d'ajuster chaque paramètre d'installation**. Certaines pages web, par défaut, récupèrent des informations sur votre connexion (notamment grâce aux cookies). Quelques réglages suffisent à garantir leur suppression. Et assurer votre invisibilité., faites gaffe d'ajuster chaque paramètre d'installation**. Certaines pages web, par défaut, récupèrent des informations sur votre connexion (notamment grâce aux cookies). Quelques réglages suffisent à garantir leur suppression. Et assurer votre invisibilité.
Vous voilà au cœur de la matrice. Attention à ne pas vous y perdre…
http://www.neonmag.fr/le-deep-web-le-cote-obscur-de-la-toile-313974.html

Deep Web
Arrestation du fondateur de Sheep Marketplace lors de l'achat d'une villa

Thomas Jiřikovský, le propriétaire présumé de l'un des **sites** les plus populaires du Darknet, "Sheep Marketplace", a été arrêté après le blanchiment d'environ 40 millions de dollars, ce qui en fait une des plus grandes escroqueries dans l'histoire du Deep Web.
Après l'arrestation de propriétaire de Silk Road, Ross Ulbricht, en 2013, Sheep Marketplace est devenu la place de marché underground la plus célèbre sur le réseau anonyme Tor. Les clients du marché noir y affluait pour la vente de produits illicites, en particulier les médicaments.
Mais après quelques semaines seulement, Sheep Marketplace a soudainement disparu après avoir été déconnecté par son propriétaire, qui avait été soupçonné d'avoir volé massivement des Bitcoins, montant estimé à 40 millions de dollars au moment où la valeur de marché du Bitcoin atteint des sommets historiques. Peu de temps après cette escroquerie au Bitcoin, un habitué du Darknet, Gwern Branwen, publie un "dox" sur le propriétaire présumé qu'il a lui-même identifié : Thomas Jiřikovský.
Cela est du à une erreur de Jiřikovský qui a oublié de cacher son identité et adresse résidentielle sur Internet, qui a été exposée par sa page Facebook. Cependant, immédiatement après la fuite de son identité, Jiřikovský a nié en bloc son implication dans la place de marché illicite Sheep Marketplace.
Lors d'une enquête pour ce vol d'argent en ligne, la police tchèque a remarqué un jeune programmeur suspect qui a tenté d'acheter une maison de luxe d'une valeur de 8,7 millions de couronnes tchèques (soit $ 345 000 USD) en Lusace, une région en République tchèque, sous le nom de son grand-père. Le complément d'enquête a révélé qu'en janvier de l'année dernière, un compte bancaire au nom d'Eva Bartošová, 26-ans, a reçu un énorme virement de près de 900 000 couronnes, émis par une société étrangère de change de Bitcoins. Bien entendu, la jeune femme était incapable de justifier l'origine de l'argent…
Selon les médias tchèques, Eva Bartošová est la femme de Thomas Jiřikovský, qui l'aurait aidé à transférer l'argent volé sur son compte de banque fraîchement créé. La division économique de la police tchèque a enquêté sur l'argent des Jiřikovský et a constaté que la maison avait été entièrement achetée en utilisant les Bitcoins incriminés.
Rappelons aussi qu'un autre grand marché de la drogue du Deep Web « Evolution », a soudainement disparu il y a quelques jours à peine, et que les rumeurs qui circulent sur ses propriétaires indiquent qu'une gigantesque arnaque aurait touché les utilisateurs après le vol

de plusieurs dizaines de millions de dollars en Bitcoin. Une chose est sûre, le Darknet et le Bitcoin se portent mal !
https://www.undernews.fr/hacking-hacktivisme/deep-web-arrestation-du-fondateur-de-sheep-marketplace-lors-de-lachat-dune-villa.html

Deep Web : 20'000 lieues sous Google

« Près de 90% du contenu du Web échappe aux moteurs de recherche. C'est le «Deep Web» ou la face immergée de l'iceberg numérique. Un territoire invisible et profond où cohabitent incognito «whistleblowers», blogueurs dissidents, dealers, pédophiles et tueurs à gages. Bienvenue dans les abysses de la matrice.

La presse anglo-saxonne le surnomme «le plus grand conseiller en pornographie infantile au monde». Arrêté début août par le FBI, Eric Eoin Marques de son vrai nom est accusé d'être le cerveau de Freedom Hosting, un service web accessible sur le réseau anonyme Tor qui héberge des milliers de forums pédophiles. Cet Irlandais de 28 ans aurait favorisé l'échange de milliers de fichiers de pornographie infantile et conseillé d'autres pédophiles sur la manière d'abuser sexuellement des enfants sans se faire arrêter.

En Australie, Paul Leslie Howard croupit dans une prison de Melbourne en attendant le verdict du tribunal. Le trafiquant de 32 ans encourt jusqu'à 5 ans d'emprisonnement pour la vente de cocaïne, amphétamines, LSD, MDMA et marijuana. Une large palette de substances illicites qu'il se procurait et fournissait à des prix défiant toute concurrence sur la Silk Road (la route de la soie), la plateforme commerciale uniquement accessible sur le réseau anonyme Tor. Paul Leslie Howard et Eric Eoin Marques, deux cybergangsters au sein d'une nébuleuse criminelle cachée active sur le «Deep Web».

Les milliards d'internautes lambda l'ignorent. Le Web tel que nous le connaissons n'offre que 10% seulement de son contenu. C'est la pointe visible de l'iceberg. Les 90% restants représentent la face cachée de la Toile, soit plus d'un trilliard de données accessibles en ligne, mais invisibles des moteurs de recherche classiques. On l'appelle le «Deep Web» (Web profond) ou Web invisible, un cyberespace insondable et abyssal dont l'entrée et le contenu ne s'offrent qu'à une poignée d'initiés.

Profondeurs obscures

Le Web est à l'image d'un océan. A sa surface, les moteurs de recherche classiques. Avec l'aide de leurs robots d'indexation, ils parcourent les pages web en naviguant de lien en lien. Les moteurs de recherche aspirent, archivent et indexent le contenu de chaque page visitée. Cette matière visible et accessible à tous est stockée dans les serveurs. Ainsi, Google dispose de plus de 1 million de serveurs dans le monde, tout comme Microsoft. Yahoo! en compte plus de 50 000 et Facebook 180 000. Ces serveurs connectés entre eux hébergent notamment les milliards de pages web aspirées sur lesquelles nous surfons.

Lorsque l'internaute s'immerge dans la matrice, il rencontre des pages web isolées, indépendantes, volumineuses, écrites dans des formats illisibles pour les robots d'indexation, donc des moteurs de recherche classiques. A partir d'une profondeur de 200 mètres, là où la lumière du jour ne filtre pas, on pénètre dans les abysses de la Toile, où le surf est anonyme. Les ressources du Web invisible sont de grande qualité, car générées par des experts – informaticiens, hackers et hacktivistes. Un territoire où se côtoient le meilleur, mais aussi le pire de la Toile (pédophilie, images morbides, réseaux de tueurs à gages, trafic de drogue…). Bienvenue dans les profondeurs obscures de la matrice.

Immenses ressources documentaires

L'universitaire Michael K. Bergman fait figure de pionnier dans l'exploration du «Deep Web». A la fin des années 1990, l'Américain effectue sa première plongée. Il remonte dans

ses filets une pêche miraculeuse. Le Web profond regorge d'immenses ressources documentaires sous forme de bases de données en ligne. On y trouve notamment l'ensemble du contenu des bibliothèques numériques, celles du Congrès américain par exemple, de la BNF-Gallica ou de la National Library of Medicine pour ne citer qu'elles. «Une richesse à couper le souffle», s'exclamera Michael K. Bergman à sa remontée, tant «la valeur du Web profond est incommensurable».

Pourquoi les fichiers jouent-ils à cache-cache ? Les documents et bases de données présents dans le Web profond sont trop volumineux ou trop complexes pour que leurs contenus soient indexés, donc visibles. Parallèlement, plusieurs internautes (des as du code informatique) choisissent délibérément de ne pas renforcer leur site pour privatiser l'information et préserver l'anonymat. L'unique manière d'accéder au contenu de ces pages est de connaître leur URL, soit leur adresse internet. Le développeur du site choisit ainsi de la divulguer à quelques élus. On retrouve ainsi dans ce «club VIP» les membres de WikiLeaks, les groupuscules libertaires d'Anonymous ou les activistes du Printemps arabe, qui conversent à leur guise et échangent des centaines de milliers de documents dans le plus grand secret.

Prévenons celui qui voudrait faire ses premières brasses dans le «Deep Web». Dans les profondeurs, tout est question d'anonymat. On accède aux pages ultra-sécurisées, souvent cryptées, via des réseaux décentralisés de routeurs, c'est-à-dire les appareils par lesquels transite l'information entre les ordinateurs. Le plus connu est le réseau Tor (The Onion Router), constitué de multiples strates comme des pelures d'oignon. Une fois à l'intérieur, vous êtes anonyme puisque le réseau Tor modifie constamment votre adresse IP (le numéro d'identification de votre ordinateur, comme il existe des numéros de téléphone). Vous surfez dans votre salon genevois alors que le NSA vous localisera à Acapulco. En conclusion, la traçabilité de vos recherches en ligne devient quasi impossible.

Dernier rempart libertaire

L'exploration peut commencer. Faut-il encore connaître l'adresse précise du site recherché. Dans les bas-fonds du Web, un lien internet prend la forme d'une succession de lettres et de chiffres se terminant par un .onion et non .com : http://dppm78fxaaccguzc.onion. Le projet Tor est géré par des bénévoles qui assurent aux utilisateurs un anonymat complet en ligne. Le réseau est un outil essentiel à certaines luttes politiques, au point que Reporters sans frontières le recommande dans son kit de survie numérique. Qui s'y connecte? Des hackers, des cybercriminels, mais aussi des opposants politiques, des blogueurs dissidents et des journalistes.

Les sites, chats et forums qui peuplent ce réseau sont réunis dans un «Hidden Wiki», soit un Wikipédia caché. Cette encyclopédie obscure rassemble toutes les tendances. On y trouve aussi bien la liste des sites tenus par des opposants au président syrien Bachar el-Assad que celle des défenseurs d'une «Europe blanche». D'autres plateformes invitent à financer la lutte islamique. La pornographie y tient une place de choix, du X classique aux tendances les plus déviantes. Mais l'anonymat garanti par le réseau Tor attire aussi les pires criminels.

Tueurs à gages et blanchiment d'argent

Le «Deep Web» a son côté obscur : le «Dark Web», où les marchés clandestins sont légion. On y trouve des sites non commerciaux, comme Shroomtastic, un forum pour «apprendre à faire pousser des champignons hallucinogènes». Et des sites commerciaux. Le plus connu se nomme Silk Road (route de la soie). L'offre illégale y est pléthorique. Le site CoinFog permet de blanchir de l'argent, Killer for Hire fournit les services de tueurs à gages pour 9200 francs. All Purpose Identities explique la fabrication de faux papiers d'identité. EuroArms vend des AK-47, des kalachnikovs russes pour 680 francs. Sans parler de la longue liste de drogues, des produits Apple de contrebande à petit prix et des poisons utiles à l'élaboration de cocktails mortels.

Sur ce marché clandestin, les transactions se font dans une monnaie virtuelle : le bitcoin. Cette dernière a été créée en 2009 par un certain Satoshi Nakamoto – son nom d'emprunt. Les bitcoins sont générés par des algorithmes. Ils sont échangeables via un logiciel de partage pair-à-pair à installer sur son ordinateur. L'utilisateur met à disposition une partie de la capacité de calcul de son ordinateur au réseau et peut ainsi échanger de la monnaie virtuelle. Sa particularité ? Elle est intraçable. Les 5 grammes de résine de cannabis s'échangent à 0,59 bitcoins, soit 63,33 francs au dernier cours de change.
Selon l'étude de Nicolas Christin, professeur français à l'Université de Carnegie Mellon, en Pennsylvanie, le volume total des ventes du site Silk Road représentait l'an passé 1,3 million de francs par mois, dont 100 000 reversés aux administrateurs. Le chercheur et enseignant en sécurité informatique à l'EPFL, Philippe Oechslin, fait preuve de prudence : «Les outils cryptographiques sont si performants qu'il est impossible de remonter un circuit criminel pour le quantifier», explique l'expert, également fondateur d'Objectif sécurité, la société spécialisée dans la sécurité des systèmes d'information.
Le seul moyen de débusquer un cybercriminel reste de le pousser à la faute. Car pour livrer de la drogue ou une kalachnikov achetés sur Silk Road, il faut une adresse physique de livraison. Mais là aussi, les criminels disposent de boîtes aux lettres anonymes. Les marchés clandestins ont donc de beaux jours devant eux. D'autres sites comme Atlantis et Black Market Reloaded voient le jour sur le même modèle que Silk Road. Si ces plateformes sont parfois victimes d'attaques informatiques qui les mettent hors service, elles échappent au contrôle de la police, impuissante devant cette pieuvre qui profite des limites de la coopération internationale en matière de lutte contre la criminalité.
La «magie» du réseau Tor est qu'il est utilisé tant par l'Etat américain et son agence de renseignement (NSA) que par ses opposants. Les pionniers du réseau l'ont pensé pour le bien de la communauté numérique. Ils revendiquent le secret et la sécurité au milieu de l'océan qu'est le Web. «Il en va de la protection de l'information et de la sécurité des whistleblowers comme Edward Snowden ou Julian Assange», ajoute Philippe Oechslin. A mesure que la sphère privée des internautes s'effrite et que les gouvernements outrepassent les lois pour surveiller les communications, le besoin de confidentialité en ligne grandit. Les révélations sur le programme d'espionnage Prism de la NSA n'ont rien arrangé.
Malgré son apparente anarchie, le Web visible devient de plus en plus contrôlé. Il est surtout l'objet d'intenses convoitises commerciales de la part des fournisseurs d'accès à Internet. Petit à petit, les moteurs de recherche classiques – Google en tête – se cherchent des chemins dans le Web profond. Mais l'exploration vers les grands fonds promet d'être longue et semée d'embûches ».
https://olivierdemeulenaere.wordpress.com/2013/08/25/deep-web-20000-lieues-sous-google/

Blanchiment de l'argent du carding (Cash Out) par les cybercriminels

Blanchir l'argent émanant de la cybercriminalité et plus particulièrement du carding est une affaire hautement risquée. Le processus est lourd, long, coûteux et les intermédiaires ne sont pas fiables. Comment procède les pirates aujourd'hui pour réaliser un Cash Out (Ca$h Out) ?
Les opérations cybercriminelles à grande échelle peuvent permettre de passer outre la plupart des pièges et aux opérations illégales de devenir beaucoup plus rentables et sûres, surtout lorsque les cybercriminels réussissent à dissimuler leurs activités frauduleuses au sein d'entreprises légitimes en cours d'exploitation aux États-Unis. Ils sont de plus en plus nombreux à faire cela.
Un nouveau type de service underground a vu le jour et est commercialisé par et pour des cybercriminels. La réexpédition (par exemple via des mules, ndlr) de marchandise achetée par

le biais de cartes bancaires volées (carding) a toujours été la façon la plus courante et populaire pour les pirates informatiques et carders se situant à l'étranger d'encaisser l'argent de leurs actes cybercriminels commis sur le territoire américain ou européen.
Les cyberescrocs s'appuient très souvent sur ce genre de service de réexpédition à l'international pour le déplacement et l'acheminement de matériel électronique et d'autres biens qui sont achetés avec des cartes de crédit piratées, puis expédiés à l'étranger pour être vendus pour de l'argent "cash". De nombreux fraudeurs utilisent des carte bancaires volés pour payer des étiquettes d'expédition de l'US Postal Service et de FedEx (aussi appelées les "étiquettes noires") mais les principaux fournisseurs d'expédition semblent être à même de mieux en mieux à bloquer et intercepter ce type de paquet. La preuve en est, on ne compte plus les plaintes de cybercriminels sur les forums underground spécialisés du Deep Web…
En conséquence, les cybercriminels se tournent de plus en plus vers un service plus fiable : les marques blanches d'expédition qui sont payées avec des comptes bancaires offshores dédiés exclusivement à la cybercriminalité et financés par l'intermédiaire de sociétés bidon, mais apparemment légitimes aux États-Unis.

Retirer de l'argent cash, le Graal pour tout pirate informatique

Dans le cas d'une violation d'une boutique en ligne qui expose des données bancaires (numéro de carte, date d'expiration et CVV), ces dernières sont généralement utilisées pour acheter de l'équipement électronique à prix élevé dans boutiques en ligne connues pour être "cardable", c'est à dire non regardant sur l'identité de l'acheteur (pas de copie numérique de pièce d'identité demandée par exemple) et proposant l'expédition de la marchandise à une adresse différente de l'adresse de facturation.
Dans le cas des violations sur les moyens de paiements physiques où les attaquants utilisent un logiciel malveillant afin de compromettre les opérations bancaires effectuées en caisse et de recueillir des données qui peuvent être utilisés pour fabriquer de nouvelles cartes, les fraudeurs emploient des équipes annexes spécialisées et équipées techniquement qui utilisent les données dérobées pour créer des cartes contrefaites pour ensuite acheter des marchandises à prix élevé à des grandes surfaces ou voyager.
Dans tous les cas envisageable de fraude bancaire, l'un des moyens les plus lucratifs pour les fraudeurs se situant à l'étranger pour encaisser l'argent des cartes de crédit piratées, est d'avoir des produits brevetés expédiés à l'étranger, où l'électronique et autres articles de luxe se vendent généralement un prix beaucoup plus élevé que dans les États-Unis ou en Europe (les derniers iPads et iPhones, par exemple).
L'étape la plus difficile dans tout ce processus est de faire sortir les marchandises des États-Unis ou d'Europe, car un pourcentage élevé de détaillants refusent tout simplement de les transporter vers des pays tels que la Russie et l'Ukraine en raison du taux élevé de fraude dans ces régions.
Traditionnellement, les fraudeurs réussissent à contourner ce type de restriction en se tournant vers des services qui s'appuient sur les « mules » pour procéder à la réexpédition des marchandises. Ces précieux intermédiaires sont recrutés localement pour réexpédier les paquets après avoir reçu la marchandise à leur domicile. Ces mules dédiées à la réexpédition reçoivent plusieurs colis contenant des produits électroniques qui ont été achetés avec des cartes bancaires volées et également des étiquettes prépayées et pré-adressée d'expédition. Ces personnes mal informées que sont les mules sont responsables de s'assurer que les marchandises sont réexpédiées rapidement et avec précision.
Malgré cela, l'année dernière, ce mode de fonctionnement a toutefois rencontré des problèmes, de plus en plus de cybercriminels utilisateurs de services réexpédition ayant rapportés qu'une grande part de leurs paquets ont été interceptés ou annulés. Apparemment, les compagnies maritimes sont de mieux en mieux équipées pour procéder à la détection des étiquettes d'expédition qui sont payées illégalement.

Des services innovants dédiés à la cybercriminalité

Face à ces nouvelles difficultés engendrant de lourds coûts de fonctionnement, la cybercriminalité internationale s'est organisée et a créé des services undergrounds 100% dédiés à leurs activités illégales, permettant de transporter la marchandise à bon port avec un important taux de succès (la livraison est garantie ou remboursée, ndlr).

Aucun nom ne sera cité dans cet article à but purement informatif. Cependant, il faut s'avoir que ces services sont poussés par la criminalité organisée mondiale et difficiles à stopper. De plus, les tarifs sont entre 15 et 20% moins chers que les transporteurs légitimes, permettant des marges maximales aux utilisateurs et ainsi, amplifier leurs profits.

Là encore, la majorité de ces service en marque blanche se trouvent en Russie.

Une façon de récupérer et d'augmenter les gains blanchis

Retirer l'argent volé à un distributeur automatique de billets à l'autre bout du monde via une carte de débit clonée est certes efficace mais il ne donne pas la possibilité au cybercriminel de réinvestir cet argent dans l'achat de biens ou dans toute autre façon de le faire fructifier.

Les réseaux criminels sont reliés pour un maximum d'efficacité. Grâce à ces nouveaux réseaux undergrounds très discret et délocalisés, une autre forme de fraude est née, dont le but est d'extraire le maximum de valeur des activités cybercriminelles.

https://www.undernews.fr/fiches-pirates/techniques-de-pirates-comment-les-cybercriminels-blanchissent-largent-carding-cashout