SIMPLY SECURE

INCURSION DANS LE BLACKMARKET

LES EXPERTS DU G DATA SECURITYLABS DEVOILENT LES DESSOUS DES MARCHES CYBERCRIMINELS.

I. CYBERCRIMINALITÉ

L'économie numérique a considérablement évolué au cours de cette dernière décennie, la cybercriminalité a suivi. Ainsi, alors qu'en 2000 deux étudiants philippins concevaient le vers « I Love You » par simple jeu (infection de 3 millions d'ordinateurs en quelques jours), en 2012 ce sont par exemple 39 personnes qui étaient jugées pour avoir infecté plus de 13 millions d'ordinateurs et dérobé 100 millions de dollars avec le Botnet Zeus. Cette monétisation de la cybercriminalité repose aujourd'hui sur des systèmes d'échanges parallèles parfaitement structurés.

Les principales plates-formes cybercriminelles sont des forums à l'apparence peu différente des sites légaux. Mais dans la partie privée, seulement accessible aux membres, se cachent des places de marché (blackmarket) où chaque membre propose produits et services. Failles, données de cartes de crédit, adresses email, location de botnet, etc. sont proposées. Mais aussi d'autres produits de la vie réelle : faux passeport, drogues, armes, etc. tout s'achète et se vend. De véritables boutiques spécialisées sont aussi disponibles sur Internet. Annoncées par bannières publicitaires sur les forums, elles proposent l'achat en gros de données (numéro de carte bancaire, compte PayPal). Des achats qui disposent même d'une garantie de retour en cas de non-validité des données.

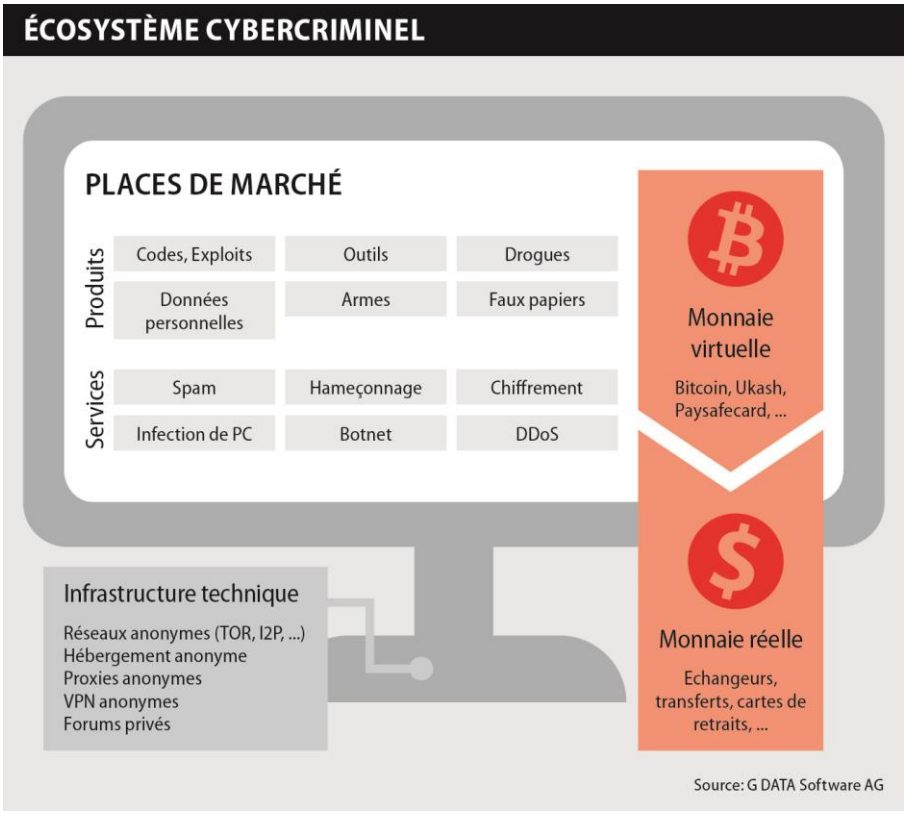


Illustration 1 : l'écosystème cybercriminel

Comme toute économie parallèle, la non-traçabilité des flux d'argent est une priorité. C'est là qu'intervient la monnaie virtuelle, et bitcoin comme fer de lance ! Avec les monnaies anonymes, les cybercriminels peuvent alors commercer en toute tranquillité.

Si commercer virtuellement est simple et sans grand risque, convertir sa monnaie virtuelle en argent réel est plus compliqué compte tenu des contrôles opérés par les services judiciaires et fiscaux. Mais comme pour tout problème, des solutions existent…

Une lutte efficace contre le cybercrime, et les infections digitales qui en découlent, passe par une bonne connaissance de ses rouages. Tout au long de ce dossier, les experts du G DATA SecurityLabs livrent un aperçu de cette nébuleuse qu'est le blackmarket.

II. LE BLACKMARKET, PLACE DES ÉCHANGES

Parmi les infractions cybercriminelles, on peut recenser le vol ou le détournement de données personnelles, le vol d'identifiants bancaires, la falsification de papiers d'identité, l'espionnage, l'organisation d'actes de piratages destinés à désorganiser des entreprises, des médias, ou encore la diffusion de logiciels malveillants.
Pour réaliser ce type de méfaits, il est rare de disposer de toutes les compétences et ressources requises. Pour cela, les cybercriminels peuvent se reposer sur la puissance du web. Mais ils n'utilisent pas les acteurs classiques du web pour commercer entre eux, ils n'exploitent pas les réseaux courants pour mener leurs transactions délictueuses. Le décor de leurs agissements est communément appelé blackmarket. Sous ce terme générique sont recensés des réseaux spécialisés sur lesquels il est possible de vendre, louer, ou acheter des produits ou services délictueux. Hormis l'accès qui est logiquement plus confidentiel, les caractéristiques de ces places de marché diffèrent peu des forums et sites de ventes grand public. Sur ces espaces, certains offreurs utilisent publicités et offres spéciales pour attirer le client. Ces plateformes ont également opté pour des systèmes de notation inspirés des forums ou sites d'enchères légaux. Ainsi, l'acheteur est assuré de la qualité du vendeur. En cas de doute sur le produit, le risque reste limité : beaucoup sont garantis. Un numéro de carte bancaire qui ne fonctionne pas, un code qui pose problème, avec certains fournisseurs et sur certains forums, c'est du satisfait ou remboursé !

A. Un marché de plusieurs milliards d'euros

Difficile de disposer de données tangibles sur ces réseaux par nature opaques.
À chaque nouveau démantèlement de trafic, à chaque intervention des autorités pour fermer une de ces places de marché occultes, ce sont des préjudices de centaines milliers d'euros qui sont révélés.

À la fin de l'année 2014, le FBI a par exemple tenté de mettre un terme à Silk Road 2.0. Ce site exclusivement accessible depuis le réseau anonyme Tor, avait réussi à fédérer en une année d'existence près de 100 000 clients (entre fin 2013 et fin 2014). En septembre, les ventes réalisées sur le site auraient généré environ huit millions de dollars. Silk Road prélevait une commission de 8 à 15% sur chaque transaction. Un exemple parmi tant d'autres des volumes d'argent échangés en toute illégalité…

B. Le deep web n'est pas le darknet

Afin de comprendre quelles sont les sources d'approvisionnement du blackmarket, il convient de différencier deux termes fréquemment utilisés : deep web et darknet. Tous deux associés à la cybercriminalité, ils n'en restent pas moins totalement différents dans leur approche et leur fonctionnement.
Le deep web englobe tous les contenus web non indexés. Bien qu'ils ne soient pas protégés en accès, ils ne peuvent pas être trouvés par l'intermédiaire d'un moteur de recherche classique. C'est l'opposé du clear Web : la partie visible du Web et facilement accessible à partir d'un moteur de recherche.

Le darknet est un réseau encore plus profond dans lequel ses utilisateurs ne se connectent qu'à des personnes de confiance. La plupart du temps, ces réseaux sont de petite taille et généralement lents. Un darknet peut être créé par n'importe quelle personne et pour n'importe quel objectif. Mais la technique est le plus souvent utilisée spécifiquement pour créer des réseaux de partage de fichiers. Le dark web est quant à lui la partie Web (composées de pages web) du darknet. Le dark web est accessible via des systèmes d'anonymisation, dont Tor est

le plus connu (voir chapitre III.C.). Mais d'autres outils tels qu'I2P permettent également d'accéder et de créer des réseaux anonymes dans le darknet.

III. STRUCTURES TECHNIQUES

Pour échanger, commercer, et s'organiser, le tout anonymement, les cybercriminels ont besoin de structures techniques dédiées. Vous trouverez ci-dessous la base technique du système.

A. Forums

Les forums du blackmarket fonctionnent comme les sites de petites annonces du Clear Web. Les offres de vente sont postées directement dans les rubriques thématiques du forum. Si les annonces sont consultables par tous les utilisateurs enregistrés du forum, une fois le contact établi, les échanges s'effectuent le plus souvent via les canaux de messagerie instantanée (voir chapitre III.E.), jugés plus discrets. Certaines offres (numéros de carte, programmes malveillants, services) sont diffusées simultanément sur plusieurs forums. L'anglais et le russe sont les langues les plus couramment utilisées sur ces Forums.

B. *Proxy* et VPN anonymes

Naviguer sur les réseaux de manière anonyme est une nécessité pour les cyberdélinquants. Deux techniques sont principalement utilisées pour masquer l'adresse IP de leur machine. Les *proxys* anonymes sont une première possibilité. Mais compte tenu de leur limitation technique, les connexions VPN anonymes leur sont généralement privilégiées. La technologie VPN englobe l'ensemble des connexions de la machine, ce qui garantit l'anonymat de toutes les actions que peut entreprendre l'attaquant. Bien entendu, *proxys* et VPN anonymes sont proposés par des fournisseurs localisés dans des pays peu enclins aux coopérations judiciaires.

C. Tor

Le réseau décentralisé Tor répond lui aussi au besoin d'anonymisation recherché par les cybercriminels. Ce réseau Internet superposé dit en Oignon se compose de plusieurs couches, appelées nœuds, ayant pour principe de transmettre de manière anonyme les flux TCP : après un nœud, il est dans quasi impossible de remonter l'adresse IP d'une connexion Internet. Cette capacité d'anonymisation fait du réseau Tor une plateforme de choix pour le cybercrime, si bien que la plupart des espaces de ventes et des forums utilisent ce réseau.

D. Serveurs bulletproof

Ces serveurs sont, si l'on s'en réfère à la traduction littérale, à l'épreuve des balles. Ils proposent des hébergements sans prendre en considération le type de données qui seront stockées ou l'usage qui en sera fait. Des contenus illégaux allant de productions régies par le droit d'auteur (film, musiques…) aux images pédopornographiques y sont stockés. Ces serveurs exploitent certaines failles de l'architecture DNS pour associer plusieurs adresses IP à une URL parmi lesquelles la technique *fast flux* qui rend très difficile l'identification de ces serveurs. Le second usage courant de ces serveurs bulletproof, c'est la mise en place de serveurs de C&C (contrôle et commande) qui permettent de prendre le contrôle d'ordinateurs infectés par un *trojan* dans le cadre de création de réseaux *botnet* (voir chapitre VIII.).

E. Messageries instantanées

Très utilisée il y a quelques années, la messagerie instantanée ICQ a aujourd'hui été supplantée par des solutions concurrentes (Skype, Talk, etc.). Elle reste toutefois ouverte à tous et certains aficionados continuent à utiliser cette plateforme pour discuter entre amis. La plateforme est aussi très utilisée par les cybercriminels. Dans la plupart des annonces postées sur les forums, les cybercriminels indiquent leur identifiant de messagerie instantanée ICQ afin de discuter plus librement des conditions et de réaliser la transaction. Certains vendeurs ont même développé des boutiques spécifiques à travers cette plateforme. Des protocoles automatisés, fonctionnant par codes numériques, permettent de passer des commandes sans même sortir d'ICQ.
ICQ n'est pas la seule messagerie utilisée. Elle subit la concurrence de différents autres outils comme Jabber. Jabber peut également agir en complément d'ICQ : il exploite le protocole XMPP (le standard de la messagerie instantanée, également utilisé par la majorité des autres acteurs) et, en y ajoutant le module OTR (off the record), permet de chiffrer l'ensemble des conversations.

F. IRC

Acronyme d'Internet Relay Chat, l'IRC est un autre protocole de communication qui a connu ses heures de gloire dans les années 2000. Ce système de communication prend principalement la forme de groupes de discussion sur lesquels les intervenants se connectent à travers un canal spécifique. Conversation individuelle et transfert de fichiers sont aussi possibles. Fortement concurrencé par la simplicité des messageries instantanées, l'IRC est moins utilisé aujourd'hui dans les usages courants. Mais compte tenu des possibilités d'anonymisation et de communication de groupe, c'est encore un système particulièrement apprécié des cybercriminels.

G. Messagerie mobile

Le côté pratique des messageries instantanées sur mobiles gagne également le secteur cybercriminel. Afin de communiquer en toute impunité, notamment pour finaliser des transactions commencées en ligne, un nombre croissant de cybercriminels optent pour les messageries cryptées disponibles sur mobile. Plusieurs solutions, telle que par exemple la messagerie Threema, sont proposées par l'offreur dans ses annonces afin de pouvoir le contacter plus directement.

IV. LIEUX D'ÉCHANGES

Pour commercer, des places de marchés spécifiques sont créées. Elles utilisent les techniques de stockage et d'anonymisation présentées plus haut. Ces lieux d'échanges utilisent les monnaies virtuelles pour toutes les transactions (voir chapitre X.).

A. WebStore

Les Shops sont l'équivalent des sites de commerce électronique du clear web. On peut distinguer les shops professionnels qui sont dévolus à l'achat de numéros de cartes bancaires (*carding*) et dont les offres sont structurées, des shops amateurs par nature plus volatiles. Les shops évoluent très rapidement et quelques semaines suffisent pour voir exploser l'offre disponible.

B. SilkRoad Reloaded

Sans doute l'un des plus importants blackmarket au monde connu comme le supermarché de la drogue et des armes. Il a succédé à SilkRoad et à SilkRoad 2.0, successivement fermés par le FBI. On y trouve des kits de piratage informatique, de faux permis de conduire, passeports, documents d'assurance ainsi que des services clé en main de piratage ou de voies de faits et violences physiques. SilkRoad Reloaded a fait son apparition en janvier 2015, non plus via Tor, mais via le réseau anonyme I2P.

C. DeepBay

Concurrent de SilkRoad, DeepBay est accessible via Tor. Supermarché de la drogue, c'est une place de marché très active qui utilise notamment Twitter pour racoler de nouveaux clients. Drogues, métaux, données, armes, tabac ou encore contrefaçons, les rubriques sont aisément accessibles.

D. Pandora

Cette place de marché particulièrement réputée offre un large éventail de produits et services illicites. Pandora est sans doute l'un des espaces sur lequel les drogues et produits stupéfiants circulent le plus. Mais nul n'est prophète en son pays et Pandora a subi une attaque en 2014 et a vu s'envoler près de 250 000 $ en bitcoins.

E. Agora

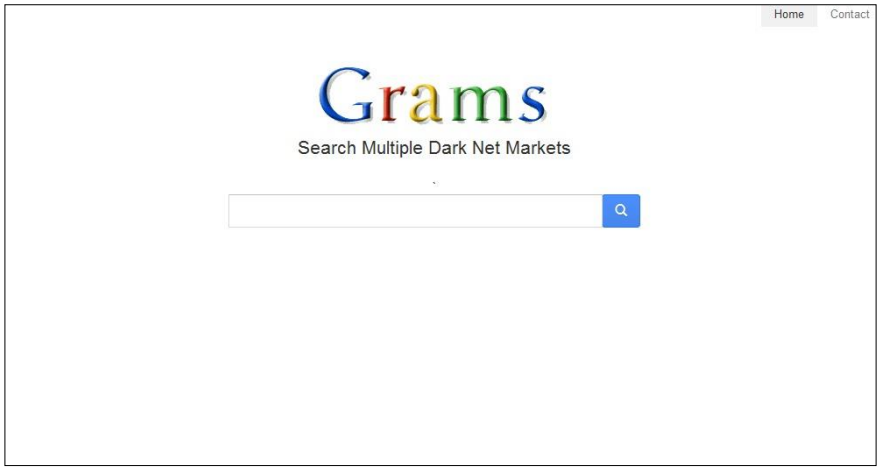
Agora est l'une des places de marché les plus populaires du deep web avec près de 9000 références disponibles. Seulement accessible par invitation, cette plateforme est aussi régulièrement hors ligne (https://dnstats.net/market/Agora).

V. RÉSEAUX ANONYMES ET RÉSEAUX PUBLICS

Pour se déplacer sur le web parallèle, il n'est pas question de recourir aux outils de recherche classiques. Ces derniers, normés, standardisés, n'indexent pas les contenus illicites et quand bien même ils le feraient, ils conservent dans leurs logs et historiques, l'ensemble des traces laissées par les requêtes des internautes. Dès lors, pour naviguer dans le web profond et réaliser des transactions sur le blackmarket, les cybercriminels se sont dotés d'outils spécifiques.

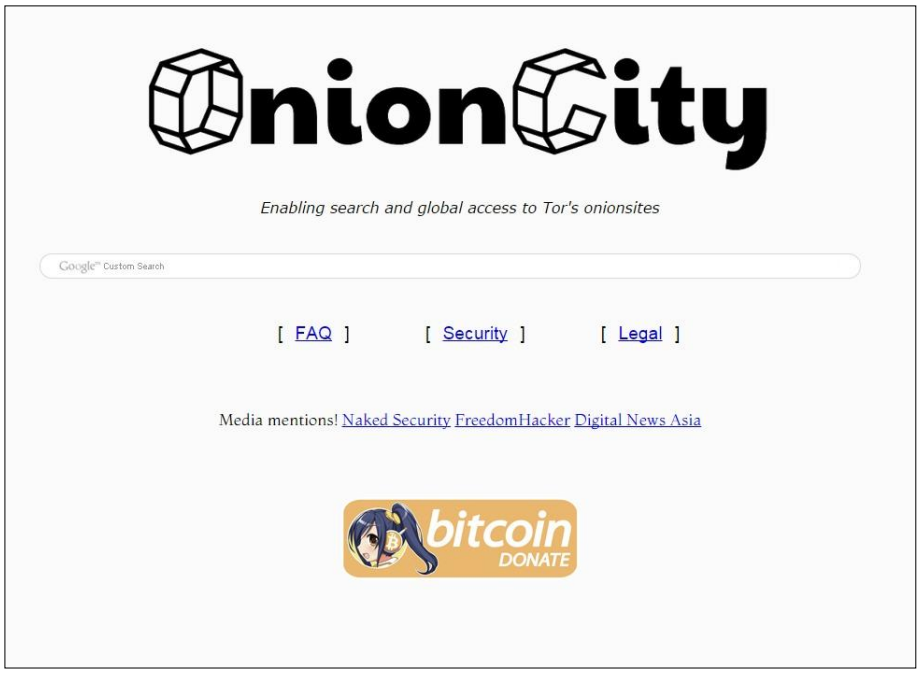
A. Grams

Grams est un moteur de recherche qui a vu le jour en 2014. Il est conçu pour mener des recherches sur les différents lieux d'échanges. Grams indexe notamment les produits disponibles sur Agora, Pandora, et Silk Road 2. Les listings de contenus indexés sont actualisés toutes les 72 heures.



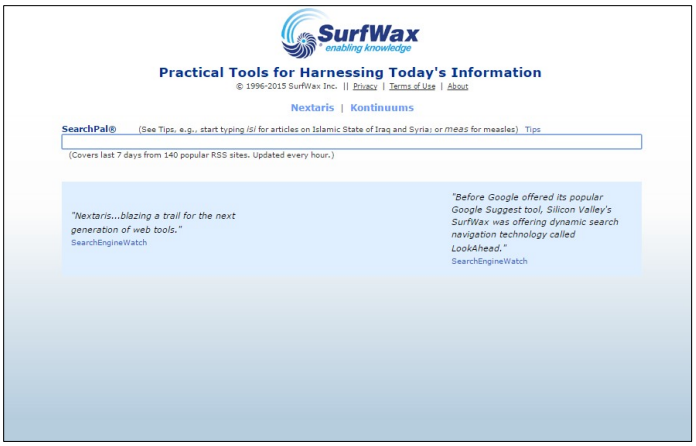
B. OnionCity

Onion.City est un moteur de recherche destiné au DarkNet et alimenté par le proxy Tor2Web. Ce dernier lui permet d'accéder en profondeur au réseau d'anonymisation TOR. Il détecte et indexe ainsi des sites .onion en agrégeant les services undergrounds pour les rendre ensuite disponibles via un simple navigateur Web.



C. Surfwax

Conçu pour afficher les résultats de plusieurs moteurs de recherche en même temps, Surfwax est un métamoteur qui autorise la création des *searchsets*. L'utilisateur peut ainsi composer ses propres ensembles personnalisés (listes) des sources qui peuvent alors être enregistrées. Surfwax est un outil particulièrement adapté à la recherche deep web, car il récupère des informations émanant de sources que les moteurs de recherche classiques ne prennent pas en considération.



D. Torsearch

Véritable porte d'entrée sur le réseau TOR, ce moteur de recherche est un passage incontournable pour pénétrer sur les blackmarkets et sites illicites du deep web. Considéré comme le Google du deep web, Tor Search fait figure de référence.

E. Memex, le moteur deep web officiel

Memex est un moteur de recherche qui permet d'inspecter la partie invisible de la Toile, que les autres moteurs de recherche n'indexent pas. Ce moteur de recherche a été développé par le DARPA (Defense Advanced Research Projects Agency) qui est un laboratoire de recherche de l'armée américaine. Memex n'est pas utilisé par les cybercriminels, mais il permet de mesurer l'importance du deep web, mais également du darknet ! Ainsi, son inventeur Chris White avance l'hypothèse que ce nouveau moteur pourrait devenir un outil à destination des forces de police, capables dès lors de rechercher sur le dark web les ventes de produits illégaux (http://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/).

VI. PRODUITS DISPONIBLES

Sur le blackmarket, tout s'achète et tout se vend, surtout si c'est illégal ! Trois grandes catégories de biens coexistent : les outils logiciels ou matériels d'attaque (logiciels malveillants, matériel de *skimming*, etc.), les biens liés au banditisme classique (drogue, arme, faux papiers d'identité, matériels de création de fausses cartes bancaires…), et les données utilisateurs volées (email, numéro de carte bancaire, etc.), autrement dit les cibles potentielles.

A. Logiciels malveillants

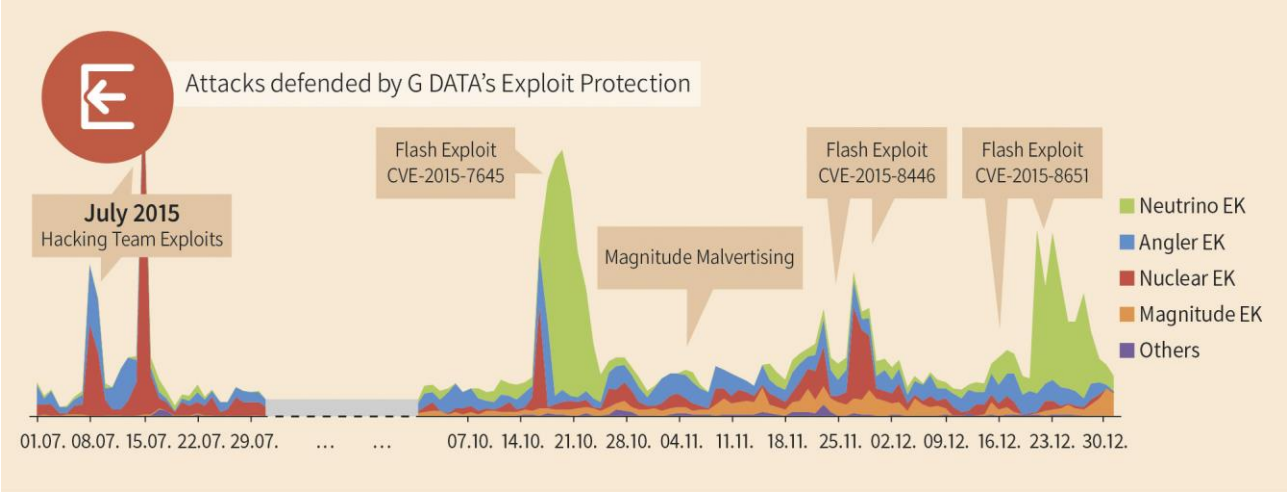
L'appellation générale de logiciel malveillant regroupe au sens large l'ensemble des codes malveillants développé dans le but de contrôler ou d'infecter les machines.
Les places de marché étant multiples et les moyens d'échanges opaques, quantifier le volume des codes malveillants échangés sur ces plateformes est impossible. Mais en se basant, non pas sur les ventes des codes, mais sur leur utilisation, il est possible d'avoir une vision assez précise des typologies de codes échangés. Les statistiques du G DATA Security Labs, basées sur le nombre de signatures antivirales générées, permettent de donner les grands axes de répartition des familles de codes nuisibles. Les *trojan* constituent la principale catégorie de codes utilisés, et donc probablement échangés sur les places de marché. Le *trojan* est la boîte à outils du cybercriminel. Beaucoup plus ciblés sur l'activité mercantile, les *adwares* connaissent une forte croissance. Ces codes enregistrent les activités et les processus d'un ordinateur (habitudes de navigation, par exemple) et affichent des publicités dans les fenêtres des navigateurs. Les *adwares* ont de plus l'avantage d'être souvent dans la zone grise, autrement dit à la limite de la légalité, si bien que les risques pour leurs utilisateurs sont quasi nuls. Les téléchargeurs (*downloader*) ont pour mission de charger ou de copier un fichier sur l'ordinateur infecté. En tant que module indispensable à toute infection, ils sont eux aussi très présents sur les places de marché cybercriminels.

1. Ransomware/Crypter

Bien que faisant partie de la grande famille des malware, les *ransomware* constituent une catégorie à part sur les sites de vente. Ces logiciels malveillants bloquent l'ordinateur et exigent le paiement d'une rançon pour en rendre le contrôle à son propriétaire. Les plus évolués chiffrent les documents contenus sur le disque dur, empêchant toute tentative de récupération. Ces programmes, camouflés dans des documents, soi-disant légitimes (fichier bureautique, économiseur d'écran), sont massivement diffusés par envoi de spam. L'attaquant n'a alors plus qu'à attendre que les destinataires tombent dans le piège.

2. Exploits

Les exploits sont des programmes informatiques qui mettent en œuvre l'exploitation d'une vulnérabilité, d'une faille, dans un logiciel. Chaque exploit est spécifique à une version du logiciel et permet d'en exploiter une vulnérabilité. L'exploitation d'une faille dans un logiciel vulnérable offre des possibilités d'augmentation de privilèges dans le système d'exploitation et ainsi l'exécution de code malveillant. La finalité de ce type d'attaque est généralement la prise de contrôle de la machine attaquée. En tant que porte d'entrée pour l'infection, l'exploit est un des outils les plus recherchés sur le blackmarket. Les tarifs de ces exploits évoluent en fonction du logiciel ciblé et de sa nouveauté. Ainsi, un exploit 0day (non diffusé sur Internet et non corrigé par l'éditeur) touchant Windows (le système d'exploitation majoritairement utilisé) peut se négocier pour plusieurs milliers, voire plusieurs dizaines de milliers d'euros. Dernièrement, la boutique dédiée TheRealDeal a vu le jour sur le réseau anonyme Tor. Cette nouvelle place de marché se présente comme le lieu de vente privilégié pour les exploits techniquement avancés et à forte valeur.



Graphique 2 : détection des attaques via l'exploit kit Nuclear.

La commercialisation d'exploit est une activité lucrative qui flirte bien souvent entre légalité et illégalité. Des sociétés ayant pignon sur rue se sont également spécialisées dans la recherche et la commercialisation d'exploit 0day. Les grands éditeurs souhaitant limiter les failles dans leurs programmes, ils sont prêts à dépenser beaucoup d'argent pour acheter ces exploits.

B. Tutoriels pour les nouveaux

Inutile d'être un spécialiste pour bénéficier des facilités du blackmarket. Comme sur le clear web, les tutoriels ont le vent en poupe sur les réseaux parallèles. Pour savoir comment utiliser un proxy, utiliser tel ou tel exploit kit, ou tout savoir sur les différents systèmes de protection des cartes bancaires, des tutoriels sont disponibles à la vente. Ces modes d'emploi en anglais sont vendus accompagnés de leurs captures d'écrans légendées, à l'image de ce que l'on peut trouver dans la presse spécialisée pour apprendre à configurer un logiciel ordinaire. Certains tutoriels (au format PDF) sont gratuitement mis à disposition dans des forums du

blackmarket, d'autres sont vendus une trentaine d'euros. Les thématiques sont variées et les tarifs augmentent en fonction de la technicité de l'exercice.

C. Matériel à la vente

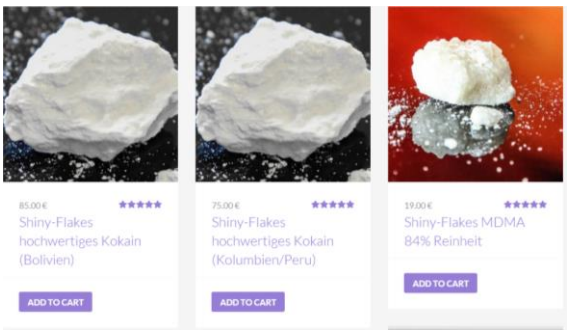
Le blackmarket ne se résume pas à des places de marché dédiées aux programmeurs. Un pan entier est également consacré aux échanges mafieux et criminels. Faux papiers, armes, drogues, médicaments et matériels divers sont proposés en toute impunité.

1. Faux papiers, pour tous les usages

Les faux papiers (passeport et pièces d'identité), sont des produits courants sur les marchés parallèles et largement utilisés dans les milieux criminels. La création de faux papiers reste une pratique onéreuse. Une fausse carte d'identité d'un pays européen se négocie aux alentours des 1000 € sur les sites spécialisés. Quant au passeport, il faut compter environ 4000 €. Il est à noter que les tarifs diffèrent en fonction du pays.

2. Armes et drogue en libre-service

Bien qu'ils soient réels, les liens entre blackmarket et banditisme sont difficilement faits par le grand public. L'image stéréotypée des filières mafieuses colle difficilement à celle des réseaux informatiques pirates. Mais deux catégories de produits que sont les armes et la drogue remettent la finalité du blackmarket en perspective. Internet constitue ainsi une plateforme de commerce privilégiée pour la drogue. Des commerces plus ou moins organisés ont été créés sur des places de marché accessibles via le réseau Tor. Cocaïne, héroïne, ecstasy, marijuana s'achètent par exemple en Bitcoin (BTC). Du côté des armes, le constat est également identique. Il est ainsi aisé de se procurer un revolver sur des sites de vente en ligne.



3. Carding et skimming

Générer des revenus par le piratage de cartes bancaires est une des activités privilégiées des réseaux mafieux cybercriminels. Ceci passe en premier lieu par l'utilisation d'informations de cartes bancaires (numéro, date d'expiration et code de vérification) volées sur des plateformes de commerce électronique légales, mais également par la création et l'utilisation de fausses cartes dans des magasins ou distributeurs de billets physiques. Mais créer de tels systèmes nécessite du matériel. Parce que de tels achats ne sont pas aisés dans le commerce et parce qu'ils pourraient également alerter les autorités, l'offre est disponible sur les marchés parallèles. Lecteurs de bandes magnétiques, imprimantes de cartes, système de collecte à poser sur les distributeurs automatiques de billets, tout le matériel nécessaire au vol et piratage des cartes est disponible. Bien entendu, ce matériel est également disponible dans des boutiques légales, mais elles ne permettent pas l'anonymat proposé sur le blackmarket.

VII. DONNÉES DISPONIBLES : DESCRIPTION ET TARIFS

Les données personnelles sont l'essence même du commerce cybercriminel. Sur ce domaine, le marché se segmente entre ceux qui volent les données, ceux qui les vendent et ceux qui les utilisent. Un email, une pièce d'identité, un compte de réseau social ou encore un numéro de carte bancaire, toute donnée est valorisable.

A. Adresses email

L'email est une des ressources nécessaires pour les activités cybercriminelles. Même si les attaques par infection de sites Internet (drive by) se généralisent, les tentatives d'infection et hameçonnages par email restent présentes. Dans cette optique, disposer d'une base email valide est un atout. Pour la collecte, plusieurs méthodes existent. La plus simple consiste à scanner les forums et pages web à la recherche d'adresse email. Une autre consiste à pénétrer les systèmes de base de données de web marchands ou de fournisseurs d'accès Internet. Enfin, il est également possible de récupérer une base email plus ou moins grande dans l'ordinateur infecté d'une victime.

B. Données de comptes email

Disposer d'accès à des comptes email est une ressource très intéressante pour un cybercriminel. L'espace de stockage proposé dans les Webmail étant croissant, beaucoup d'utilisateurs y laissent la totalité de leur correspondance. Avoir accès à cet espace ouvre donc un large éventail d'attaques et de fraudes. L'une des plus courantes consiste à usurper l'identité de la victime en envoyant un email à ses contacts. Sous prétexte d'un voyage à l'étranger qui se passe mal, le délinquant demande aux contacts d'envoyer une somme d'argent dans un pays étranger. Une campagne d'infection ciblant les contacts de la victime est également envisageable : la probabilité qu'une cible ouvre un document provenant d'un de ses contacts est plus importante. L'accès aux autres comptes de la victime est également à envisager : via les emails de récupération, il est aisé de récupérer identifiants et mots de passe de sites marchands, réseaux sociaux, et système de paiement (PayPal). Autant d'informations pouvant ensuite être utilisées pour d'autres méfaits ou revendues sur le blackmarket.
Pour se procurer des comptes email, plusieurs solutions sont possibles. Les attaquants ayant pour finalité la revente de ces données réalisent des campagnes d'hameçonnage dédiées. Les bases email en poche, ils réalisent des campagnes spécifiques. Qui n'a pas reçu de faux emails émanant d'Orange, Free ou SFR les invitant à confirmer leur identifiant et mot de passe ? D'autres cyberdélinquants, dont la finalité est d'utiliser les comptes emails pour leurs activités illégales, peuvent opter pour l'achat. Les tarifs proposés évoluent en fonction du pays ciblé et du degré de validation des informations (compte validé). À titre d'exemple, 40 000 comptes email (identifiants et mot de passe) non validés se négocient environ 20 dollars…

C. Cartes bancaires

Acheter frauduleusement des biens et des services sur Internet est une activité courante pour les cyberdélinquants. Pour cela, l'utilisation de cartes bancaires volées est nécessaire. Inutile de disposer de véritables connaissances techniques pour acquérir ce type de données personnelles. Les places de marché regorgent de cartes bancaires volées. Sur les sites de vente, les cartes disponibles sont triées en fonction du type de carte, de la date de validité, du pays d'émission, etc. le paiement se fait en ligne. Les prix varient de 1 € à 100 € et dépendent des places de marchés, du volume d'achat, du type de carte ou du pays d'émission. Bien sûr, le processus de validation de la carte joue un rôle important sur le tarif. En moyenne une carte bancaire internationale française est vendue aux alentours des 50 €.

D. Fullz : l'identité complète

Tout connaître d'une personne est possible et sur le blackmarket ce type d'information coûte moins 100 € ! Les *fullz* comprennent toutes les informations d'un individu. L'identité complète comprend les noms et prénoms, la date et le lieu de naissance, l'adresse postale, les numéros de téléphone, les comptes emails (et leurs identifiants) ou encore les numéros de carte bancaires. Certains *fullz* peuvent même contenir les identifiants d'accès au compte bancaire de l'individu. Avec ces données, les possibilités de nuisances sont infinies. Usurpation d'identité en ligne, transfert bancaire, extorsion, attaque ciblée dans l'entreprise de l'individu, sont possibles. Cela peut aussi aller jusqu'à la location de voiture, de chambres d'hôtel ou d'appartements jusqu'à la création de sociétés. Autant de démarches qui impliquent juridiquement l'individu en cas de non payés ou de poursuites.

VIII. BOTNET – OUTIL DE CHOIX DU CYBERCRIMINEL

Face à de nombreuses actions internationales visant à arrêter les serveurs de commandes et de contrôle, les réseaux *botnet* connaissent depuis ces dernières années une décroissance notable. Mais ils ne restent pas moins un outil de choix pour les cybercriminels. Contrôler un réseau de PC zombies offre un large choix d'activités cybercriminelles. Revue de détail.

A. Le botnet : définition

Un *botnet* (ro**bot net**work) est un ensemble d'ordinateurs infectés et contrôlés à distance par une personne dans le but de les utiliser à des fins délictueuses. L'architecture d'un *botnet* (la connexion Internet de chaque ordinateur contrôlé) peut être utilisée pour de multiples actions : envoi de spam, campagne d'hameçonnage, distribution de codes malveillants, DDoS (Distributed Denial of Service qui sature les serveurs informatiques de la cible et le rend indisponible pour un temps donné), etc. Mais le contenu des ordinateurs contrôlés peut aussi être utilisé : données bancaires, identifiants d'email ou de boutique en ligne collectée sur les postes des utilisateurs peuvent faire l'objet d'une exploitation délictueuse ou d'une revente.

B. Écosystème du botnet

En tant que système complexe, le *botnet* requiert différentes compétences, et implique l'interaction de plusieurs intervenants qui commercent sur les places de marchés parallèles. Les codes malveillants nécessaires à l'infection et au contrôle (incluant le serveur de contrôle et de commande) sont les points de départ de cette action cyberdélinquante : sans code adapté, pas d'infection possible. C'est à ce niveau qu'interviennent les programmeurs : des milliers de codes malveillants de tout type sont disponibles à l'achat sur les forums spécialisés. Une fois le code en poche, il s'agit alors de le diffuser au plus grand nombre. Sans compétence interne, le délinquant peut faire appel à des services dédiés. Il faut compter entre 20 et 100 € pour l'infection de 1000 ordinateurs, le prix est en fonction de la localisation des systèmes. Plusieurs éléments entrent en compte pour définir le tarif des clients infectés. Les pays disposant de connexion réseau plus rapide sont plus intéressants. Les habitants des pays les plus riches sont aussi les plus recherchés : leurs cartes bancaires et données personnelles assurent une plus grande rentrée d'argent à l'attaquant.
Au final, il aura fallu débourser plusieurs milliers d'euros pour constituer le *botnet*. Il est alors temps de le rentabiliser. Son propriétaire va alors pouvoir compter sur les données qu'ils renferment. En fonction de la qualité des internautes infectés, il va récupérer sur les machines infectées les identifiants d'emails, de réseaux sociaux voire de comptes bancaires. Autant de données valorisables sur les places de marchés. L'illustration 2 n'est bien entendu qu'une vision limitée de l'écosystème cybercriminel global. Fournisseurs d'infrastructures (serveurs bulletproof), structures spécialisées dans le blanchiment d'argent (conversion de bitcoin en monnaie réelle), délinquants spécialisés dans l'achat frauduleux sur des sites de commerce électronique, etc. une multitude d'autres acteurs du blackmarket bénéficieront directement ou indirectement de ce *botnet*.

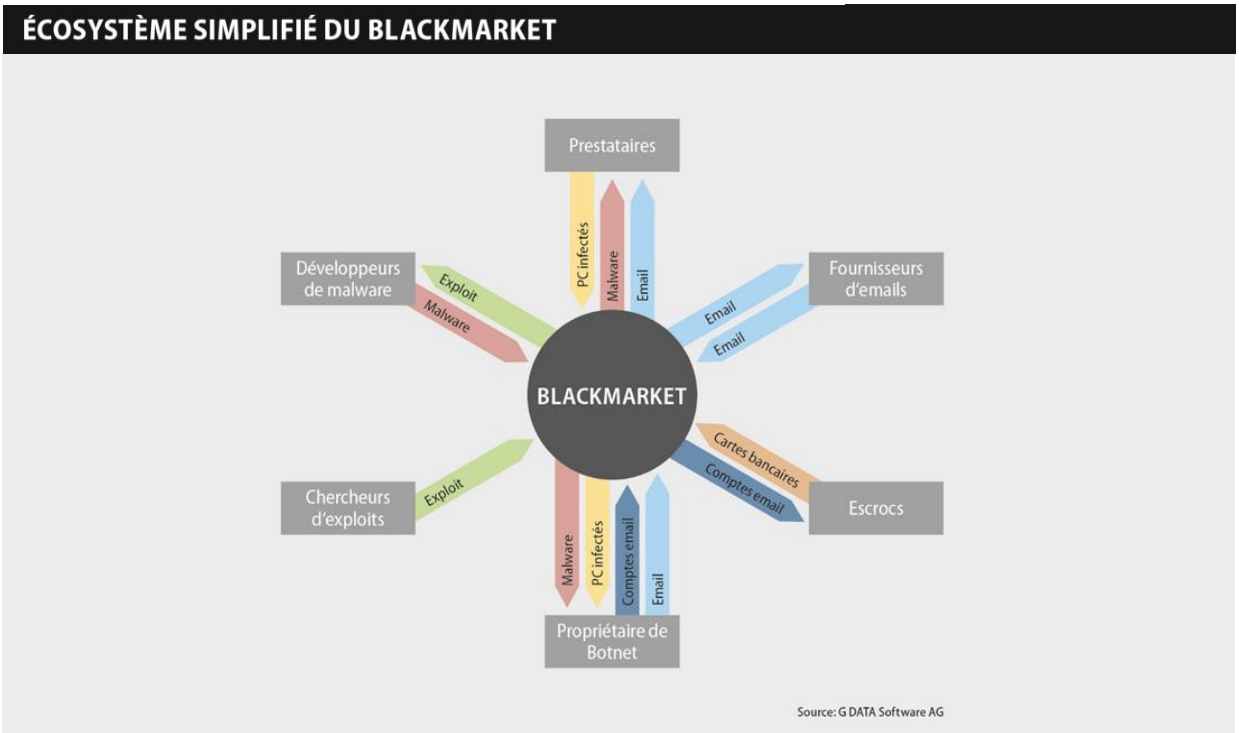


Illustration 2 : écosystème des botnet

IX. SERVICES A LA DEMANDE

Il ne faut pas imaginer que les cybercriminels soient tous de fins techniciens, des informaticiens avertis. Dans le banditisme classique, chacun a ses spécialités. Sur le secteur cybercriminel, il en est de même. Lorsqu'ils ne maîtrisent pas une technique, les réseaux organisés s'approvisionnent en services et en compétences.

A. Attaques DDoS

Lorsqu'un cybercriminel souhaite mener une attaque sur une ou plusieurs cibles sans disposer nécessairement du savoir-faire ou des outils nécessaires, il peut passer une annonce spécifique sur le blackmarket, ou bien encore répondre à une offre d'un pirate sur ces mêmes réseaux. Lorsque l'on souhaite acheter une attaque DDoS par exemple, la prestation est facturée le plus souvent au volume d'attaque par heure, par jour ou par semaine. Pour une attaque ciblée sur un site, les tarifs varient à l'heure entre 10 et 200 €.

B. Spam

Envie d'inonder le web d'un message publicitaire ou subversif ? Sur le blackmarket, il suffit de souscrire à un service d'envoi, le plus souvent hébergé sur un serveur bulletproof, afin d'éviter que la source de la campagne soit traçable. Plusieurs facteurs influent sur le tarif : le volume de message adressé, mais aussi la qualité du service d'envoi et sa capacité à détourner des dispositifs de protection comme les Captchas.

C. Installation de Bot

Les *botnets* sont des outils privilégiés pour les cybercriminels. Mais comme dans la plupart des cas sur le blackmarket, chaque étape de création fait appel à des sous-traitants. Le déploiement du code malveillant fait partie des étapes incontournables. Des acteurs spécialisés vendent ce service à ceux souhaitant agrandir ou constituer un botnet. Ce type de prestataires facture entre 20 et 100 € pour du bot sur 1000 ordinateurs situés en Europe. Un tarif aussi bas démontre que la procédure est rapide. L'infection de site Internet vulnérable par l'utilisation d'exploit kits est privilégiée. Elle permet de rapidement toucher des internautes non protégés.

D. Attaques d'hameçonnage

Sur le blackmarket, une campagne d'hameçonnage peut se mettre en place assez simplement. Avec les kits clés en main, inutile d'être un spécialiste. Il est possible de créer une page Internet falsifiée en quelques minutes sans connaissances particulières. En fonction de la notoriété des établissements ciblés et de la qualité des kits (soin graphique, orthographe soignée, etc.), les prix fluctuent entre 10 et 30 € par page créée. Cette page créée et stockée sur des serveurs web piratés, il suffit au cybercriminel d'attirer les victimes potentielles. Là encore pas besoin de grandes connaissances et de matériel. Il suffit d'acheter une base d'adresse email et de la diffuser par des systèmes d'envoi dédiés. L'attaque complète n'aura finalement coûté que quelques centaines d'euros.

E. Chiffrement à la demande (FUD)

La création d'un code malveillant passe par une étape incontournable qui consiste à masquer le contenu du programme. Ce masquage (obfuscation), basé sur l'utilisation d'un « packer », permet de rendre plus difficile le code nuisible indétectable aux solutions de sécurité et aux analyses. Mais parce que masquer les composants d'un programme est une tâche techniquement complexe, les programmeurs peuvent faire appel à des services de chiffrement à la demande à travers des sites spécialisés : contre moins de 10 euros, le code transmis à travers un formulaire est automatiquement chiffré. Le tarif de cette prestation dépend du prestataire, et donc de la qualité du chiffrement, mais également du volume demandé, une décote étant réalisée en fonction du volume. Une analyse multi scanner, comme expliquée dans le paragraphe suivant, finalise la procédure en montrant au client que le camouflage est effectif. Il peut alors récupérer son code par téléchargement.

F. Multi Scanner

Toute création d'un nouveau code malveillant passe par une ultime étape : la vérification de sa non-détection par les logiciels antivirus. Pour un usage légal, un multi scanner tel que VirusTotal fait l'unanimité. Mais avec cette solution, tout code scanné non détecté est automatiquement envoyé aux éditeurs pour analyse. Autant dire qu'il est hors de question pour un programmeur de codes nuisibles d'utiliser une telle solution. C'est pourquoi des sites spécialisés de multi scanners anonymes sont disponibles. Pour moins d'un euro, il est possible de faire scanner anonymement et simultanément son code avec 35 antivirus. Pour les gros consommateurs, un paiement mensuel à 30 € est proposé.

X. DU VIRTUEL AU REEL

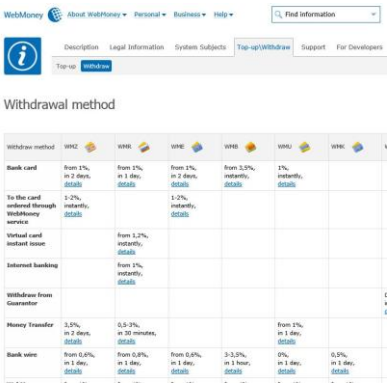
S'il existe bien des réseaux de cyberterroristes qui souhaitent avant tout déstabiliser le système et l'opinion, ce sont bien des motivations crapuleuses qui animent le blackmarket. L'argent est donc le nerf de la guerre sur le Web profond et les trafics en tous genres finissent toujours par se solder par une transaction financière. Ce passage du virtuel au réel est l'étape la plus dangereuse pour les cybercriminels, car elle peut permettre aux autorités d'établir un lien avec le délinquant. Mais plusieurs solutions existent pour éviter les risques. Monnaies virtuelles et ingénieux systèmes de blanchiment sont disponibles.

A. Le système de monnaies virtuelles

Quelle que soit la monnaie virtuelle considérée, c'est dans la volatilité du dispositif que résident les germes de la cybercriminalité. Même si ces monnaies n'ont a priori jamais été pensées pour contrevenir à la légalité, elles présentent toutes les caractéristiques susceptibles de faciliter les transactions illégales. Des dizaines de monnaies numériques, existant pour certaines depuis plus d'une décennie, sont en concurrence sur Internet. Pour la plupart chiffrées, elles peuvent servir à tous types d'échanges (légaux et illégaux) en se substituant à des services de

paiement régulés. En théorie, la création d'un compte permettant d'utiliser un système de monnaie virtuelle implique que l'authenticité de l'utilisateur soit vérifiée et qu'il justifie de son identité avec des documents officiels. Mais nous l'avons vu : il est aisé de se procurer ce type de documents sur le blackmarket. Lorsque le cybercriminel dispose enfin de son propre compte, il peut recevoir des sommes. Il peut bien entendu utiliser cet argent virtuel pour acheter produits et services sur le blackmarket, ou toute autre place qui reconnaît ces monnaies.
Mais la plus grande difficulté réside dans l'injection de ces monnaies dans le système économique légal. Autorités financières et services fiscaux sont attentifs aux mouvements financiers suspects. Mais là encore, les cybercriminels peuvent compter sur des pays peu regardants sur les législations financières.

1. WebMoney



Parmi les stars des paiements sur le blackmarket, Webmoney fait office de figure historique. Cette solution a vu le jour en 1998 en Russie. Elle revendique aujourd'hui 28 millions d'utilisateurs dans le monde. Ce système de transferts permet de réaliser des transactions et d'effectuer des paiements en ligne. Différents porte-monnaie sont disponibles chez Webmoney en fonction des pays/zones géographiques (WMZ pour les États-Unis, WME pour l'Europe, etc.). Chaque porte-monnaie offre des taux de conversion en fonction des zones et permet plus ou moins de passages dans l'économie réelle (en fonction des législations en vigueur).

2. Bitcoin

Bitcoin est la monnaie en vogue depuis ces dernières années. Bitcoin est parfaitement anonyme. Ce système qui a vu le jour en 2009 repose sur le principe d'une unité de compte. Chaque Bitcoin est identifié par son histoire depuis sa création jusqu'à la date présente où un agent le détient, à travers toutes les transactions dans lesquelles ce Bitcoin est impliqué et qui sont reconnues par les signatures cryptographiques qui ainsi l'avalisent. Le 9 février 2011, la valeur du Bitcoin atteignait la parité avec le dollar. En juin 2011, le taux de change dépasse les 31 $, avant de retomber sous les 4 $ en décembre. Le 29 novembre 2013, la valeur d'un Bitcoin dépasse celle de l'once d'or. Au cours actuel, un Bitcoin vaut environ 211 $. Les Bitcoins figurant dans les transactions dont un compte est bénéficiaire peuvent être réutilisés par le titulaire de ce compte dans des transactions dont il est l'émetteur, à condition qu'il puisse justifier de son identité au moyen de sa signature cryptographique, les comptes eux-mêmes étant anonymes. Les Bitcoins ainsi échangés constituent une monnaie cryptographique, qui a vocation à être utilisée en tant que moyen de paiement. En juillet 2013, la Thaïlande a été le premier pays à interdire le Bitcoin, rejoint ensuite par la Chine, et la Russie.

B. Blanchiment des gains

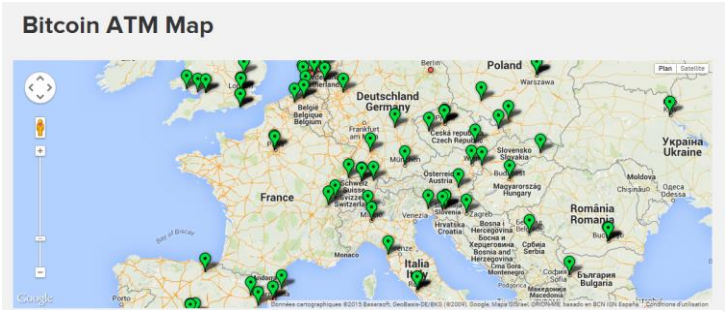
1. Achat sur le commerce électronique

Dans les cas les plus simples, et pour les petits volumes, les cybercriminels se rémunèrent par l'achat de produits sur les sites d'commerce électronique classiques. Ceux-ci peuvent être réalisés à partir de monnaies virtuelles (sur

les boutiques qui prennent en charge ces moyens de paiement), mais également à partir de cartes bancaires ou de comptes Paypal volés. Pour acheter en toute sécurité les délinquants se font livrer les produits achetés dans des « drop zones ». Des intermédiaires, généralement enrôlés via des spams comme messagers ou personnes qualifiées en logistique, sont chargés de transférer les produits. L'intermédiaire est bien rétribué pour sa prestation, souvent sous forme de produits commandés en même temps que ceux du fraudeur. Maisons et appartements vides peuvent également être utilisés, ce sont les *House drop*.

2. Blanchiment des monnaies virtuelles

Si l'injection dans le système économique légal de sommes d'argent provenant de systèmes de monnaies virtuelles est techniquement possible, elle reste juridiquement compliquée pour ceux les ayant acquis par des actions douteuses. Certaines plateformes telles que WebMoney propose un panel de solutions afin de disposer de sa monnaie virtuelle dans la vie réelle. Il est par exemple possible d'injecter de l'argent dans des cartes prépayées, compatibles avec les systèmes de cartes les plus courants, ce qui constitue la méthode offrant le plus grand anonymat. Les transferts bancaires sont également possibles. Mais ces mouvements pouvant alerter les autorités financières, les délinquants optent pour des comptes bancaires de personnes dupées (mules), ou ouverts à l'aide de fausses identités. Avec les Bitcoins, il existe de puissants réseaux de change comme Zipzap (qui revendique 25 000 implantations au Royaume-Uni, 240 000 en Russie). Des distributeurs de monnaies prenant en charge les Bitcoins font également leur apparition. Ils permettent de retirer des euros en échange de la monnaie virtuelle.



Source : http://bitcoinatmmap.com

3. Jeux en ligne comme passerelle

Les jeux d'argent sont des moyens de blanchiment intéressants pour les réseaux mafieux. Par le jeu des moyens de dépôts et de transferts, il est possible de transformer des monnaies virtuelles en monnaies réelles. Sur certains portails dédiés, il est par exemple possible de trier les casinos en fonction des méthodes de dépôt proposées. Une fois l'argent sur ces espaces de jeux, il est possible après quelques parties de récupérer son argent à travers un virement sur un compte bancaire. Sous prétexte de gain, les sommes sont alors blanchies. Dans ce contexte, il est à noter que les casinos en ligne utilisés pour ces transactions sont là encore domiciliés dans des pays aux législations financières légères, ce qui empêche toute remontée d'information par les autorités financières.

4. Virements bancaires

Même s'ils ont recours aux monnaies virtuelles et portefeuilles électroniques, les cybercriminels finissent toujours par monétiser ce capital pour en disposer dans le monde physique. La solution la plus fréquemment exploitée par les malfrats consiste à publier des annonces sur le blackmarket (ou parfois par le biais de spams) afin de recruter des « mules ». Ces dernières acceptent de recevoir des sommes qu'elles redistribuent ensuite sur d'autres comptes après avoir prélevé une piètre commission. La promesse repose sur un travail facile et exécuté à domicile…

XI. LES TARIFS DU BLACKMARTKET

Produits	Prix min	Prix max
RAT	Gratuit	300 $
Stealer	Gratuit	150 $
Crypter	Gratuit	150 $
Bot (programme)	Gratuit	10 000 $
Bot (code source)	Gratuit	15 000 $
Tutoriel	Gratuit	50 $
Kit exploit (location au mois)	50 $	2 000 $
Services		
Service de chiffrement (FUD)/programme	2 $	20 $
Attaques DDoS / heure	10 $	200 $
Installations de *bot* pour 1000 (Europe)	20 $	100 $
Données		
Fullz (Europe)	20 $	70 $
American Express (Europe)	Gratuit	50 $
Mastercard Gold (France)	Gratuit	50 $
Carte Visa Premier (France)	Gratuit	50 $
Passeport (Europe)	150 $	2 000 $
Carte d'assuré social (États-Unis)	150 $	2 000 $
Permis de conduire (États-Unis)	150 $	2 000 $
Un million d'adresses email	10 $	150 $
Comptes		
Compte Steam	Gratuit	150 $
Accès compte bancaire	Gratuit	50 $
Compte PayPal	Gratuit	50 $

XII. LES TERMES DE LA CYBERCRIMINALITÉ

Adresse IP : adresse Internet Protocol, adresse numérique servant à l'identification des ordinateurs dans un réseau TCP/IP. Cette adresse comprend quatre chiffres (par exemple, 193.98.145.50). Elle se compose de deux parties : 1. Adresse du réseau logique 2. Adresse de l'hôte à l'intérieur du réseau logique. Puisque nous ne sommes pas capables de retenir des adresses IP, nous utilisons normalement des noms de domaine pour naviguer sur Internet.

Packer : ils servent à encoder des fichiers afin de compliquer la détection des logiciels malveillants aux logiciels antivirus.

Carding : le trafic de numéro de carte bancaire est une des activités privilégiées sur le blackmarket.

DoS (Denial of Service) : attaque qui consiste à bombarder un ordinateur (le plus souvent un serveur web) avec un nombre de requêtes très important. Ainsi, il devient incapable d'assurer son service et s'écroule sous la charge.

DDoS (Distributed Denial of Service) : une attaque Distributed-Denial-of-Service repose sur le même principe qu'une attaque DoS normale, à la seule différence qu'il s'agit ici d'une attaque répartie. Ces attaques sont souvent effectuées à l'aide de milliers de PC zombies.

Dump : un dump est une image de quelque chose, par exemple une copie d'une base de données.

Exploit : code permettant d'exploiter une faille de sécurité dans un ordinateur cible pour exécuter un code de programmation.

Flooding : terme générique désignant différentes possibilités de surcharger ou de bloquer certains ordinateurs d'un réseau par un afflux massif de requêtes.

File Transfer Protocol : protocole de transmission pour l'échange de données entre deux ordinateurs. Le FTP ne dépend pas du type du système d'exploitation et du mode de transfert. Contrairement au HTTP, le FTP construit une connexion et la conserve durant tout le processus de transfert.

FTP server : serveur mettant à disposition des internautes des fichiers et des répertoires à télécharger. Le plus souvent, le nom d'utilisateur « Anonymous » et une adresse électronique personnelle permettent de se connecter aux serveurs FTP publics. Certains virus et *trojan* installent leur propre serveur FTP, sur lequel on peut télécharger des fichiers sur des ordinateurs infectés.

FUD (Fully UnDectable) : « Fully UnDetectable » signifie que les données (qui ont été créées avec le packer), ne peuvent être détectées par aucun logiciel antivirus.

Hameçonnage : tentative de collecter des données personnelles, comme les identifiants, mots de passe, numéros de carte de crédit, codes d'accès aux comptes bancaires, etc., par le biais de faux sites web ou de messages électroniques falsifiés.

Hijacker : programme qui s'installe de manière invisible et qui modifie les paramétrages du navigateur (par exemple, la page de démarrage) et de ses fonctions (par exemple, la fonction de recherche). Les hijackers entrent donc dans la catégorie des *trojan*. En détournant la page de démarrage ou la fonction de recherche, les navigateurs Internet hijackers conduisent l'utilisateur vers des pages web (souvent pornographiques). Parfois, ils font apparaître des barres de menu ou des fenêtres supplémentaires qu'il est impossible de supprimer ou de fermer. Les navigateurs Internet hijackers utilisent souvent les failles de sécurité et les points faibles des systèmes pour s'y implanter profondément. La suppression de ces fonctions de commande est souvent très difficile.

Internet Relay Chat (IRC) : protocole permettant à deux personnes ou plus de communiquer par écrit de manière instantanée via Internet.

Keylogger : un *keylogger* (enregistreur de frappe) permet d'enregistrer les entrées sur le clavier et de les envoyer le cas échéant. Les mots de passe et données personnelles peuvent ainsi être extorqués.

Messagerie instantanée : communication directe entre deux ou plusieurs personnes. Les messages écrits sont envoyés immédiatement (Instant) et apparaissent dans l'instant chez l'interlocuteur. Tous les participants doivent généralement être connectés chez le même prestataire.

VPN : un VPN permet d'établir des connexions encodées avec d'autres ordinateurs ou dans d'autres réseaux. Il est possible de dissimuler l'intégralité de son trafic Internet via une connexion VPN. Dans ce cas, seul l'IP de l'ordinateur qui permet d'établir une connexion est émis.

Payload : il image en anglais la fonction destructrice d'un virus. L'activation de cette action peut être liée à une condition, un élément déclencheur (*payload trigger*).

PC zombie : ordinateur contrôlable à distance à partir d'une porte dérobée (backdoor). La machine zombie obéit à son maître qui la contrôle à partir d'un serveur de commandes et de contrôle (C&C). La plupart du temps, les PC Zombies sont réunis sous forme de réseaux appelés botnet.

Proxy : il sert d'intermédiaire entre l'expéditeur et le destinataire, sachant que le destinataire ne connaît pas l'adresse de l'expéditeur, mais seulement celle du *proxy*.

RAT (Remote Administration Tool) : outils permettant aux fraudeurs de commander à distance l'ordinateur des victimes.

Skimming : attaque consistant à copier les informations de cartes bancaires d'utilisateurs par la transformation ou la manipulation de distributeurs automatiques de billets ou de moyens de paiement (distributeurs d'essence).

Social Engineering : tactiques de recherche utilisées par un pirate informatique pour obtenir des informations d'une personne ou d'une structure, qu'il pourra utiliser ensuite pour lui nuire.

Spyware : logiciel qui enregistre les activités et les processus exécutés sur un ordinateur et qui transmet ces informations à des tiers. Souvent, les *Spyware* sont exploités pour des encarts publicitaires ou analyser le comportement de navigation.