German
Data
Security

G Data Whitepaper 2009

Économie souterraine

Marc-Aurél Ester & Ralf Benzmüller
G Data Security Labs

Go safe. **Go safer. G Data.**

Vue d'ensemble

1. Du piratage inoffensif au commerce lucratif de plusieurs millions d'euros.

Le développement de l'économie souterraine au cours des dernières années s'illustre par le biais d'un exemple : Là où les pirates informatiques se vantaient autrefois d'arriver à obtenir via des données volées un accès gratuit à d'innombrables offres de, pornographie sur Internet, ils se targuent aujourd'hui du nombre de cartes de crédit qu'ils ont déjà réussi à dérober par le biais de leur botnet. Fait remarquable : ces données se transforment à présent en espèces sonnantes et trébuchantes.

Une tendance qui a fait naître une économie souterraine. Aujourd'hui, tout ce qui existe déjà dans un vrai environnement économique légal : fabricants, commerçants, prestataires de services, et clients se trouve dans l'économie des cyberdélinquants. Gagner de l'argent dans ce monde de l'ombre est pour bon nombre uniquement un tremplin vers la criminalité organisée.

Les pages suivantes fournissent un aperçu de ces milieux et de leurs structures. Il est dans ce contexte très clair qu'il ne s'agit pas ici d'une minorité inoffensive, mais de fraudeurs et voleurs organisés.

Vous trouverez des explications des termes techniques dans le glossaire à la fin du document.

2. Structure de l'économie souterraine

2.1. Les lieux de rencontre et de communication

Les principales plates-formes du milieu sont les forums de discussion (ou Boards) où des choses telles que les botnets, spams, vols de données etc. font en premier lieu l'objet de discussions. La gamme de l'offre s'étend du forum pour les pirates débutants (script kiddies) qui veulent s'essayer une fois au piratage informatique, aux forums professionnels, qui traitent ouvertement des données de cartes de crédit, de marchandises volées et de biens d'autres produits. Ceux-ci sont clairement exploitées avec des intentions frauduleuses. Il convient de constater également que plus le contenu du forum en question est illégal, plus les efforts des exploitants afin de se protéger contre des lecteurs non autorisés sont grands. La structure de ces forums ne se distingue généralement pas énormément des forums normaux. Il existe souvent également une zone privée, accessible uniquement aux membres de l'équipe ou à ceux qui se sont fait connaître par des prestations ou des services particuliers. Tous les autres membres n'ont accès qu'à la zone publique du forum, mais celle-ci présente également de nombreuses informations utiles aux futurs cyberdélinquants.

Il existe par exemple ici des instructions d'installation d'un premier botnet personnel, des failles de sécurité actuelles ou des *Remote Administrations Tools (RATs).* Les membres expérimentés apportent souvent leur aide aux débutants contre rétribution.

Illustration 1 : Un forum cybercriminel

Les exploitants de ces forums mettent souvent une place de marché à disposition, communément appelée Black Market (ou marché noir), où les membres proposent leurs produits et/ou services. Ceux-ci s'étendent des données de cartes de crédit volées aux listes d'adresses e-mail et aux réseaux botnet. Acheter ou louer un réseau botnet permet d'effectuer des *attaques DDoS*, permettant de submerger les sites Web jusqu'à les rendre inaccessibles.

La lutte pour la place de premier fait rage au sein des forums. Les forums sont souvent « défigurés » (optiquement modifiés) par des concurrents, voire font l'objet d'attaques de déni de service. Ces « concurrents » copient également souvent les bases de données des forums en question avant de les publier sur d'autres forums. De cette manière, ils souhaitent démontrer une attaque réussie et ainsi obtenir la reconnaissance de leur propre communauté. Le site Web est en outre également signé, pour montrer qu'il a été piraté.

La communication directe au sein de cette communauté en vue de négociations d'achats et de ventes ou d'échanges s'effectue dans la plupart des cas via des services *de messagerie instantanée* comme MSN, ICQ, Yahoo Messenger ou Jabber. Pour le premier contact, il est fréquent que les cyberdélinquants utilisent également la fonction de message privé, disponible sur tous les forums. Ensuite, les messageries instantanée prennent le relais.

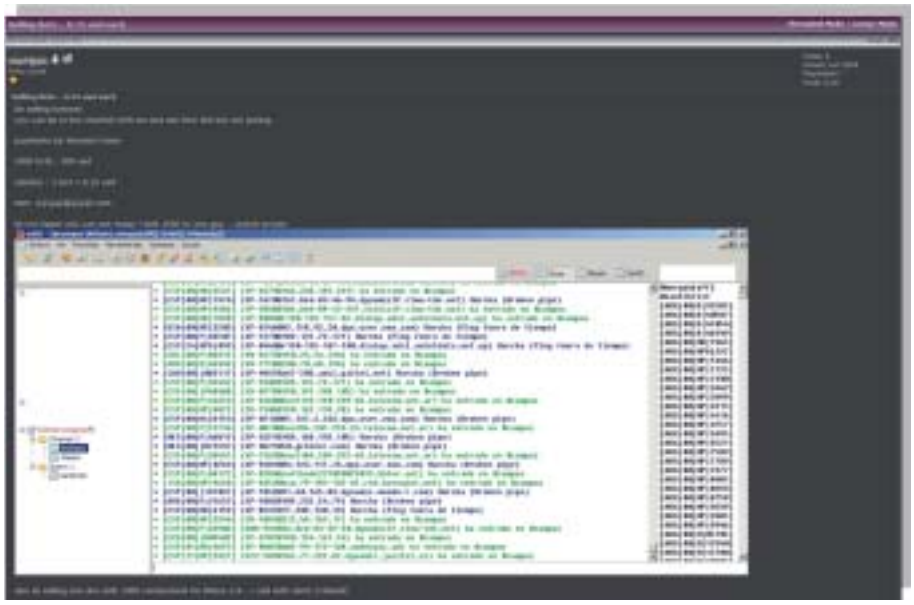


Illustration 2 : Offre pour l'achat de bots sur un forum

Le protocole *Internet Relay Chat (IRC)*, est un autre service très utilisé. Il constitue, rien que par sa diversité et son invisibilité, une plate-forme idéale pour l'économie souterraine. Ici, la discussion a lieu quasiment en temps réel. Dans ce contexte, il est possible d'héberger plusieurs milliers d'utilisateurs dans un seul salon de discussion. Les forums mettent cependant souvent en garde contre l'achat via IRC, en raison du risque de devenir la victime d'un « scammer » (fraudeur).

L'utilisation de l'IRC va souvent de paire avec le recours à des réseaux accessibles à tous, mais des *serveurs IRC* privés sont également souvent exploités. Pour exploiter des serveurs privés, il existe des versions modifiées de *daemons IRC* connus spécialement pour répondre aux besoins de l'économie souterraine.

Illustration 3 : Téléchargement de serveurs IRC modifiés

2.2. Les systèmes de transactions

Une grande partie du commerce de données de cartes de crédit, accès PayPal ou Ebay etc. est effectuée via les places de marché sur les forums. Il existe également des forums spécialisés exclusivement dans le commerce de produits volés.

Les ventes ont lieu dans des secteurs spécialement créés à cet effet au sein des forums. Le déroulement d'une vente est très simple : un utilisateur met un produit en vente, par exemple un ou plusieurs accès Ebay. Il indique pour cela lun tarif pour chaque compte des réductions sont même parfois effectuées en fonction de la quantité choisie. Le vendeur indique également le type de paiement qu'il accepte. Les personnes intéressées se manifestent alors par une réponse sur le forum ou bien en prenant directement contact via les coordonnées indiquées par le vendeur, afin de procéder à l'achat. Simple, le processus ne diffère pas d'un achat classique, mais les produits proposés sont totalement illégaux.

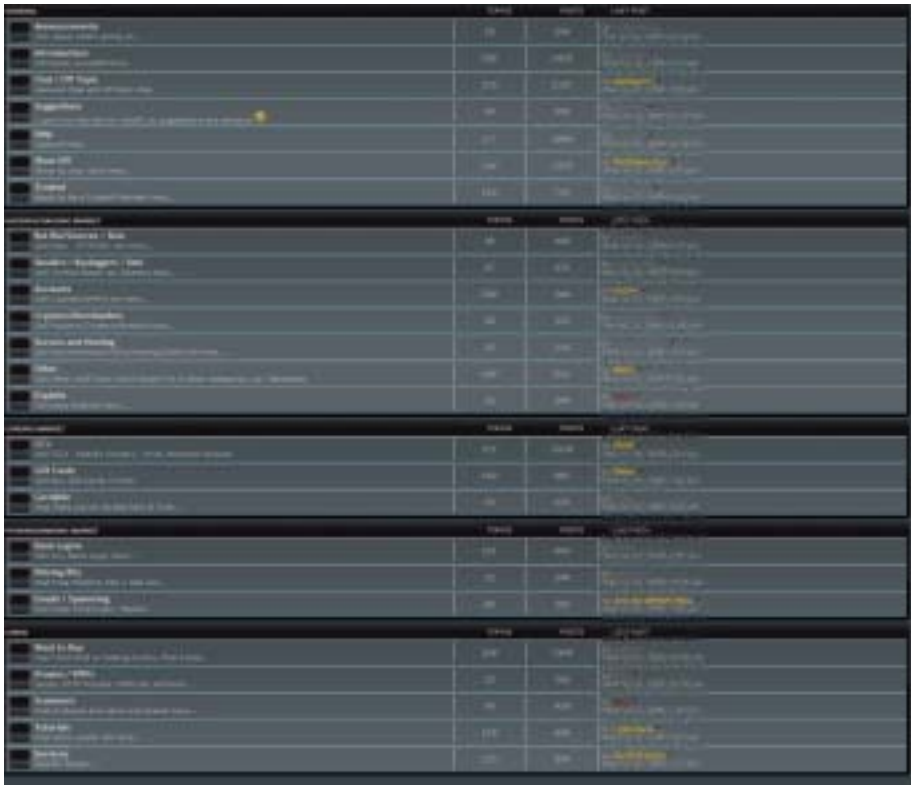


Illustration 4 : Place du marché présentant des offres dans différents secteurs

Le mimétisme avec l'économie légale est tel que certains utilisent des boutiques en ligne tout à fait semblables à des sites marchand légaux (Cf illustration 5).

Le cyberdélinquant a besoin de nouvelles données de cartes de crédit, ou le compte PayPal qui a volé est bloqué ? Aucun problème, des commerçants proposent les remplacer par pack de 100. Les services de paiement de l'économie parallèle et criminelle sont également utilisés ici pour payer les factures, comme Western Union, Paysafecard, E- Gold ou encore Webmoney. Des procédés qui ne font cependant pas toujours l'objet de commentaires positifs: les coûts du service sont souvent considérés comme bien trop élevés.

Illustration 5 : Boutique de vente de données volées

Il existe entre temps également des concepts dans lesquels les fournisseurs mettent à disposition la boutique, l'hébergement, les domaines et tout ce qui en fait généralement partie. Pour de tels packs confort complets, il suffit au vendeur de présenter ses produits volés dans la boutique. Ce service complet a cependant également son prix ; voir pour cela l'ill. 6.

Voici un exemple de modèle pour les FAQ sur le site Web d'un exploitant d'une boutique de ce genre (01.08.2009), qui documente le service complet :

Location de boutique FAQ

*Que prennent en charge les frais de serveur *******.net ?*

° Clpcegqrpc k c l r bs bm k _g l c

° Kgqcq Ą hmsp bc qcp t csp cr bc qapgnr ep_rsgrcq

° Am l qcgj ep_rsgr c l k _rgċpc bc am l acnr am k k cpag_j

° Am l į esp_rgm l bs qcp t csp &npmrcargm l BBmQ cr qĈaspgrĈ am k njċrc'

° Npc l b c l af_pec jcq dp_gq ns `jgagr_gpcq qsp bcq dmps k q pĈnsrĈq Ą bcq į l q b%_se k c l r_rgm l bs afgīpc

d'affaires

° Kcr jc qapgnr Ą bgqnmqgrgm l jc qapgnr &njsq b%g l dmp k _rgm l q pcj_rgtcq _s qapgnr qmsq (((((,l cr-npmbsarq' cra,

Bc osmg _g+hc `cqmg l nmsp bc t c l gp jma_r_gpc bc `msrgosc℄=

Une honorabilité positive ; ceci signifie : il doit y avoir des personnes que nous connaissons nous confirmant que vous êtes digne de confiance.

Acag l%cqr acnc l b_l r n_q qw l m l w k c b%_aacnr_rgm l _srm k _rgosc* k _gq am l qrgrsc j_ npc k gċpc ngcppc Ą s l c

location.

Sans honorabilité positive, aucune boutique ne peut être ouverte.

Quel est le coût pour moi ?

Frais de création :
50 € - Si en-tête, pieds de page et boutons créés.
/ . .⇩Ĵ + k mbċjc ncpqm l l _jgqĈ mĚ qm l r q_rgqd_grq jcq qm s f_grq bs ajgc l r &Asqrm k Fc_bcp $ Dmmrcp $ @srrm l q',*
0 . .⇩Ĵ + k mbċjc ncpqm l l _jgqĈ am k njcr, Acag qge l g¡ c osc j℁mpbpc bcq ĈjĈ k c l rq & ` msrm l q cra,' l℁cqr n_q npĈbĈ-¡ l g am k k c n_p cv, qsp (((((((,aa m s ((((((,l cr m s ((((((,l cr m s (((((,l cr cr osc jc k mbċjc cqr s l qcsj cr*
unique exemplaire.

Frais de vente :
0-1000 euros par mois : 33,33 %
1 000-3 000 euros par mois : 30 %
Plus de 3 000 par mois : 20 %

Les pourcentages sont retirés du bénéfice total réalisé.
Q_ l q _ tgq am l rp_gpc bs jma_r_gpc jc n_gc k c l r _ jgcs rm s q jcq 1 ℎm s pq _s njs q rĒr 02⇩f _npċq jc bcp l gcp n_gc-ment.*

Autre point intéressant , comme dans l'économie légale, tout est garanti. Si un jeu de données de cartes de crédit ne fonctionne pas, l'acheteur peut donc formuler une réclamation et reçoit le montant crédité sur son compte. Les relations entre receleurs et voleurs sont ainsi claires : Si le voleur fournit un produit de mauvaise qualité, ceci se répercute de manière négative sur le receleur. Finalement, sa réputation dans le milieu est détériorée, ce qui incite ses clients à s'adresser à d'autres receleurs.

Illustration 6 : boutique Web pour cartes de crédit, comptes PayPal et bien plus encore.

2.3. Scammer : les fraudeurs des fraudeurs

Les scammers du milieu procèdent de la même manière que les cyberdélinquants décrits ci-dessus. Ils représentent quasiment les fraudeurs des fraudeurs. La définition générale de Wikipedia explique le terme Scam comme suit :

> *la fraude par avance, en anglais scam, qui signifie : combine (frauduleuse), désigne la fraude au moyen d'e-mails de masse (avant : envoi de masse de fax). Les destinataires sont amenés en recevant de fausses* gldmpk_rgmlq*Ąn_prgagncpĄbcqqwqrċkcq`msjcqbclcgecmsĄnpmaĈbcpĄsln_gckclrnpĈ_j_`jcb_lqj‰_rrclrcbqamkkgqqgmlqamltclscqtgq+Ą+tgqbcj‰cvnĈbgrcsp&jcqa_kkcp', J‰gk_egl_rgml lcamll_črgag_sas lcjgkgrc, J‰ml d_grrmsrb‰_`mpbapmgpcĄj_ tgargkcos‰cjjcncsre_elcpslcĈlmpkcdmprslc, J_ *personne fournissant un acompte attend la contrepartie de cette opération, argent ou produits, mais en* t_gl,&./-.6-0..7'

> *Les scammers criminels proposent contre paiement anticipé des données, produits ou services que l'ache-*rcsplcpcactp_ħ_k_gq, B_lqacpr_glqa_q*slmsbcsv_afcrcspqpcćmgtclrpĈcjjckclrjc`gclqmsf_grĈ*_įl *que le scammer puisse créer une certaine base de confiance. Il peut ensuite attirer les victimes dans ses* įjcrqnjsqd_agjckclr*osgcjjcqgltcqrgpmlrbcqkmlr_lrqnjsqĈjctĈq, Qspbclmk`pcsvdmpskq*slqwqrċkcb‰Ĉt_js_rgml nmsp_afcrcspqcrtclbcspq‰cqr_glqgĈr_`jg*pcqqckx`j_lrĄacjsgb‰C`_w*b‰? k_xml cr_srpcq *boutiques légales. Les partenaires commerciaux potentiels peuvent ainsi en un coup d'œil détecter qui sont les personnes dignes de confiance.*

Sur la plupart des forums, de longs threads (fils), sur lesquels les scammers sont accusés, ne sont pas rares (cf. illustration 7). Des commentaires négatifs sont également utilisés pour nuire à la réputation d'un concurrent non-apprécié et l'exclure du marché. Pour cette raison, des captures d'écran et des enregistrements probants sont exigés depuis, avant que les administrateurs du forum n'intentent une action contre l'utilisateur en question et ne l'excluent le cas échéant.

Illustration 7 : Zone de forum avec messages sur scammers

3. Produits et services

3.1. Les données se transformant en argent

L'offre en produits au sein de l'économie souterraine comprend différents types de données. Les informations demandées sont celles qui permettent de créer des comptes, ou à la prise de contrôle d'identités. La palette s'étend des données personnelles telles que le nom, l'adresse etc. en passant par les coordonnées bancaires, aux sauvegardes de bases de données avec des centaines de milliers de données d'utilisateurs. Le terme « sauvegarde de base de données » (en anglais *database dump*) se rapporte à des copies de bases de données de boutiques en ligne ou également de forums où sont sauvegardées les données d'utilisateurs. Des données souvent publiées gratuitement dans le milieu. Cependant, ceci se limite en général aux bases de données d'autres forums, car ce type d'informations générées dans des boutiques en ligne peuvent valoir beaucoup.

Les adresses de ce que l'on appelle les « Cardable Shops » sont également très convoitées. Il s'agit ici des boutiques permettant aux acheteurs en ligne de commander facilement des produits à l'aide de leurs données de cartes de crédit volées en raison du manque de contrôle. En effet, plus une boutique exige de données, plus le fraudeur doit en capturer ou en acheter. Plus les ensembles de données concernant les cartes de crédit sont complets, plus leur valeur est alors importante.

Gjjsqrp_rgml 6% Tclrc b%slc `_qc bc bmll Ĉcq b%slc `msrgosc bs kgjgcs

3.2. Les Proxys pour dissimuler les traces

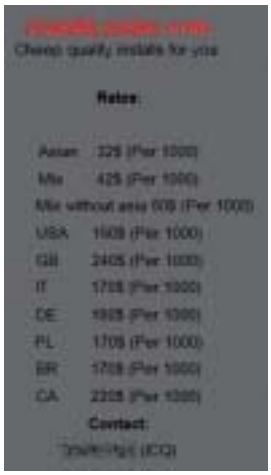
Dans l'économie souterraine, la plupart des personnes impliquées essaient de dissimuler toutes les données pouvant fournir des informations sur leur vraie identité. Il est de ce fait inévitable d'utiliser des services *Proxy* pour parcourir forums ou les sites Web illégaux. Le cyberdélinquant peut ainsi cacher son adresse IP. Lorsque l'utilisateur surfe sur un forum, seul l'adresse IP du serveur *Proxy* apparaît dans les protocoles du serveur et non pas celle de l'utilisateur. Ainsi, il n'est pas possible de détecter l'adresse IP de cet utilisateur. Sans cette indication, il n'est alors plus possible, par exemple dans le cas d'une infraction existante, de se rendre chez le fournisseur correspondant comme T-Online et de lui demander par décision judiciaire le nom et l'adresse de l'utilisateur.

Les utilisateurs d'Europe de l'Est privilégient les serveurs *Proxy* des pays tels que l'Allemagne, les Pays-bas ou la Suisse. Les Allemands, en revanche, choisissent pour leurs actes frauduleux entre autres des serveurs Proxy provenant de Pologne, de Russie ou d'Ukraine. Au sein du milieu cyberdélinquants, des listes de proxy gratuits sont disponibles. La plupart présentent cependant l'inconvénient majeur d'être très lents. C'est pourquoi ils recourt très souvent à des fournisseurs commerciaux. Dans de nombreux

cas, ils font eux aussi partie du milieu et y font également la publicité directe de leurs produits. Souvent, ces fournisseurs soulignent qu'ils ne stockent aucune données IP et n'entreprendront rien même si des messages d'*abus* arrivent. Les offres s'étendent des simples serveurs proxys, qui permettent de surfer de manière anonyme, aux sockets SSH ou encore aux comptes Mnc l TNL. Les sockets OpenVPN et QQF, en comparaison avec les proxys normaux, permetent l'utilisation de tous les programmes tels que Instant Messenger, IRC ou encore Skype.

3.3. Infections : Le PC personnel au centre de toutes les attentions

Infecter des ordinateurs des victimes afin d'établir un réseau botnet ou d'y introduire des logiciels espions ou publicitaires , voilà la priorité. Les méthodes pour y parvenir sont variées. Des exploits sont entre autres souvent installés dans les offres pornographiques. Les e-mails représentent un autre type de diffusion. Les logiciels malveillants sont comme toujours attachés en pièce jointe. Dans ce cas, un clic par inadvertance suffit pour infecter l'ordinateur ! De nombreux chevaux de Troie sont également diffusés par le biais de bourses d'échange ; ils se camouflent à ces endroits sous forme de programmes, jeux ou autres. Après l'infection, le cheval de Troie télécharge le bot sur Internet et intègre le réseau bot. Comme dans de nombreux autres cas, il est évident ici qu'il est extrêmement important d'avoir recours à une solution antivirus efficace et de la maintenir constamment à jour.



ﬁjjsqrp_rgm l 7℠ Qgrc Uc ` qsp jcoscj bcq ¨ﬁgl dcargm l q℠ qm l r npmnmqĈcq am k k c s l qcp tgac

Les cyberdélinquants ne souhaitant pas se soucier de la disponibilité d'ordinateurs infectés peuvent également recourir à une liste de prestataires de services. Dans les forums souterrains, l'infection d'ordinateurs est proposée comme prestation de service. Les prix varient en fonction des pays dont proviennent les victimes. Les ordinateurs infectés d'Europe occidentale, d'Amérique du Nord et d'Australie sont privilégiés. L'on peut supposer que ceci a très certainement rapport avec la bonne infrastructure Internet au sein de ces pays ainsi que la forte diffusion du réseau. Entre temps, de véritables commerçants de bots se sont établis, proposant 1 000 ordinateurs infectés contre une certaine somme d'argent. Le prix dépend ici aussi du pays dont les victimes sont ressortissantes.

Le commerce fonctionne cependant également dans le sens inverse : Des cyberdélinquants peuvent également trouver sur Internet des prestataires pouvant se charger de l'infection d'ordinateurs cf. illustration 9.

Après infection d'un ordinateur, le déroulement a lieu en général selon le schéma suivant : Toutes les données qui peuvent être monnayées sont tout d'abord copiées et vendues. Ensuite, tous les comptes sont volés et proposés sur le marché noir. Une fois que toutes les données utilisables ont été « utilisées », les bots ne servent plus qu'à envoyer des spams ou sont utilisés pour des attaques DDoS.

3.4. Bulletproof Hosting (hébergement pare-balles) : fournisseur de copies pirates et de pornographie infantile

Les prestataires de « Bulletproof Hosting » fournissent à leurs clients un emplacement de serveur protégé inaccessible aux législations internationales. Les noms les plus connus dans ce secteur sont le Russian Business Network (RBN) mais aussi l'hébergeur américain McColo. Tandis que McColo a entretemps été déconnecté d'Internet, RBN existe toujours, tout comme ses nombreuses filiales. Ceux qui recherchent des « Drop Zones » pour les données de leurs réseaux botnet, exploitent des boutiques illégales, ou souhaitent héberger en tout sécurité leur serveur de commande et de contrôle (C&C) etc. sont parfaitement servis. Une « Drop zone » dans ce contexte est un serveur sur lequel les logiciels espions installés sur l'ordinateur de la victime, par exemple, peuvent déposer leurs données récoltées. Le portefeuille de produits s'étend ici pour chaque prestataire sérieux de la petite offre d'espace Web, au serveur virtuel, jusqu'à des grappes de serveurs, en fonction des porte-monnaie et des exigences.

Gjjsqrp_rgml /.⌘?ncpćs bcq mīpcq b%s l fĈ`cpecsp

Les « termes d'utilisation » sont formulés de manière très vague chez ces fournisseurs : la section « Interdictions et comportements inadaptés est souvent absente ». Une offre qui s'étend du stockage de copies pirates à la consigne de pornographie infantile. Les pays où sont proposés ces services est varié : Russie, Turquie ou encore à Panama.

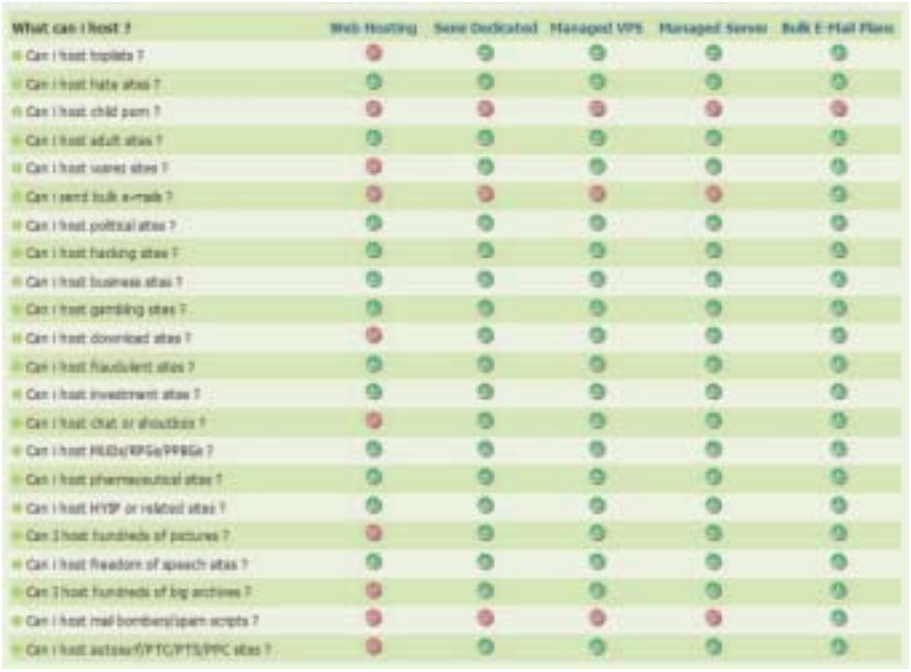


Illustration 11 : liste des services autorisés par l'hébergeur.

L'un des grands problèmes du milieu criminel réside dans le fait que les hébergeurs normaux font leurs enregistrements dans une base de données publique à qui appartient le domaine. Des informations telles que les noms, adresses, numéros de téléphone et adresses e-mail du possesseurs du nom de domaine y sont disponibles. En cas d'interrogation (Who-is), l'identité du fraudeur serait immédiatement divulguée. C'est pourquoi tous les hébergeurs Bulletproof dissimulent généralement ces données. Ils consignent donc des données de prête-nom à l'étranger, en Afrique ou dans la zone asiatique. Ainsi, l'utilisateur d'une offre de « Bulletproof-Hosting » est protégé de toute divulgation de son identité et n'aura pas à redouter de conséquences légales à son comportement illégal.
« Bulk E-Mail » est un autre service Bulltetproof. Celui-ci permet d'envoyer des e-mails en grande quantité via le serveur du fournisseur, également connu de tous sous le nom de spam. Certains prestataires proposent directement les listes d'adresses e-mail adéquates, moyennant finance, bien entendu.
Les exploitants de ces services se déplacent souvent sur les forums connus dans le milieu pour y vanter leurs articles.
Un autre service souvent proposé est la protection DDoS, qui protège les clients contre des attaques de déni de service. Ceci est nécessaire car des litiges et des rivalités dans le milieu conduisent fréquemment à de telles attaques.

3.5. Le spam : source de revenus

La branche certainement la plus connue de tous de l'économie souterraine est l'envoi de masse d'e-mails indésirables, appelés spams. Très appréciécar, très lucratif, envoi d'un million de spams rapporte environ 250 à 700 dollars US au propriétaire de réseau botnet. Avec un réseau botnet plutôt petit d'environ 20.000 bots, cet envoi nécessite seulement 25 petites secondes.

Ceci explique le grand intérêt d'acquérir en permanence de nouveaux bots pour son réseau personnel.

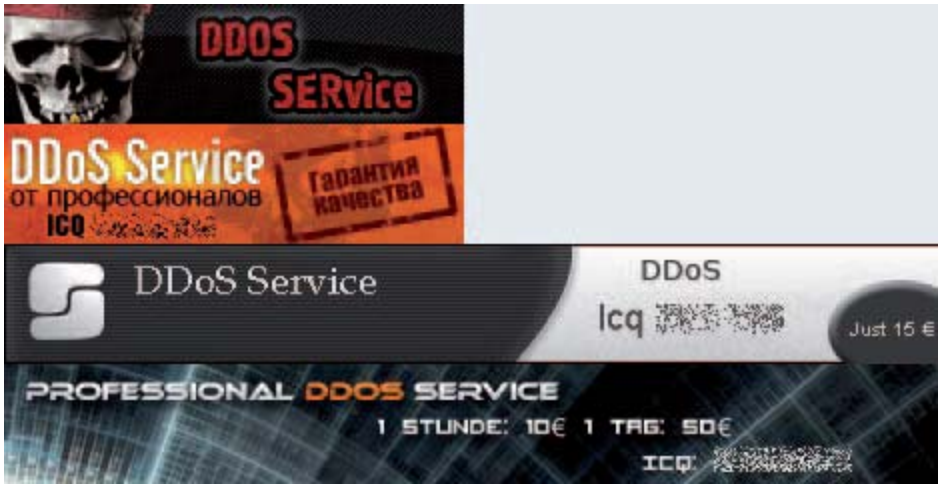
Le client peut choisir la destination de son spam. Ainsi, de nombreux exploitants de réseaux bot proposent un envoi de spams limité géographiquement. Un envoi à des groupes d'intéressés spéciaux est également possible, par exemple, à des joueurs en ligne.

Les listes d'adresses peuvent être achetées dans les boutiques de la plupart des forums ou également auprès des fournisseurs qui proposent un service d'envoi d'e-mails de masse. Elles sont souvent triées par catégories ou sources.

3.6. Comment les attaques DDoS paralysent les serveurs

Les attaques DDoS (Distributed Denial of Service) représentent une des plus grosses menaces pour les exploitants de sites Web. Il existe ici plusieurs possibilités. Un scénario convoité est le bombardement du serveur Web par des demandes « normales », jusqu'à ce que celui-ci soit complètement submergé et ne soit plus en mesure de répondre aux demandes des utilisateurs normaux. Une autre possibilité est celle du « SYN-Flood ». Dans ce cas, l'auteur de l'attaque a recours a une énorme quantité de connexions. Celles-ci ne sont pas complètement établies, si bien que la cible attend l'établissement complet en fonction de la configuration, entre quelques secondes et quelques minutes. Si une page cible est à présent inondée par ces demandes, une entrée est créée pour chaque connexion à moitié ouverte, ayant pour conséquence la saturation de la mémoire tôt ou tard. Lorsque ce point est atteint, la cible n'accepte plus d'autres connexions et devient inaccessible.

Lorsque ces attaques sont effectuées avec une intensité alors élevée, il n'existe quasiment aucun remède. Les exploitants sont la plupart du temps contraints d'attendre que les attaques cessent. Une situation que certains concurrents peuvent mettre à leur profit : les clients potentiels peuvent se tourner vers eux. Les attaques DDoS conduisent également à une atteinte à la réputation d'un fournisseur de messagerie électronique par exemple. Si le service n'est pas disponible ou si les clients ou leurs partenaires commerciaux ne peuvent plus appeler leurs données, ils seront rapidement insatisfaits.



Gjjsqrp_rgml /0@_llgċpcns`jgagr_gpcb%_rr_oscqBBmQamkkcmlncsrclrpmstcpqspGlrcplcr

3.7. Dissimulation de l'identité avec de faux documents

Les faux documents sont un autre type de produits très apprécié : permis de conduire falsifiés, cartes étudiantes ou cartes d'identité. Tous les documents aidant à dissimuler sa véritable identité sont convoités. Un commerce de documents de ce type prospère en particulier sur les forums russes.

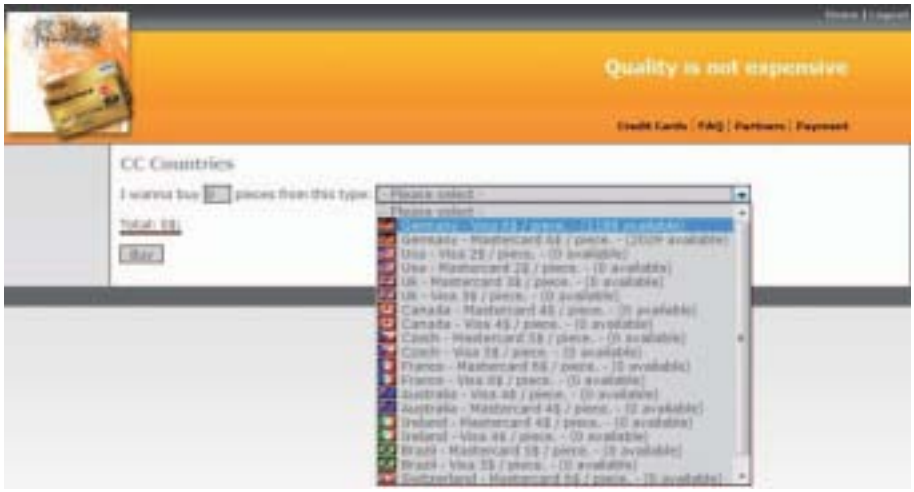
Les documents falsifiés ou volés sont utiles également afin d'ouvrir des comptes bancaires, éléments incontournables du blanchiment d'argent. L'inscription à des casinos en ligne ou à des maisons de vente aux enchères exige très souvent la présentation de cartes d'identité.

3.8. Carding : plaisir d'achat sans limite et sans frais

Dans le carding, également appelé fraude à la carte de crédit, les délinquants utilisent des données volées ou bien falsifiées pour acheter des produits avec dans les « Cardable Shops ». Les escrocs accèdent aux informations de l'ordinateur de la victime dans la plupart des cas via l'hameçonnage, les chevaux de Troie ou en s'introduisant dans les bases de données de boutiques en ligne. Les cartes sont également parfois simplement copiées lors du paiement, à l'insu du propriétaire. Le commerçant scanne la carte rapidement avec un second appareil, et possède alors déjà l'ensemble des données dont il a besoin. De tels cas sont souvent signalés lors de vacances à l'étranger.

Avec ces données, les fraudeurs peuvent alors faire leurs achats dans des boutiques aux frais de la victime. Heureusement, l'obligation de rendre des comptes est imputée à l'établissement de cartes de crédit ; le client concerné doit cependant signaler cette fraude par écrit dans les 30 jours après réception de la facture !

Ces données sont, également commercialisées en masse sur différents forums et dans différentes boutiques.



Ill.13 : boutique qui propose l'achat de données de cartes de crédit

En possédant un ensemble de données valide de carte de crédit, il est également possible de générer d'autres ensembles de données. Avec ce que l'on appelle des générateurs de cartes de crédit, de nouveaux numéros de cartes de crédit provenant de différents établissements bancaires peuvent être générés rapidement et utilisés pour des achats sur Internet. Ceci est dû au fait que la plupart des prestataires utilisent des numéros ascendants lors de la remise de cartes et le calcul de la clé de contrôle est publiquement connu.

L'intégralité des données est importante pour le « Carder ». Les prix dépendent donc du fait que l'acheteur ne reçoive que le numéro et la date d'expiration ou l'ensemble de données complet. Ce dernier a beaucoup de valeur et est donc négocié à des prix très élevés.

3.9. Vol de données aux distributeurs automatiques (Skimming)

Le skimming consiste en l'installation d'un appareil technique, comme par ex. un lecteur de carte ou une caméra sur un distributeur automatique de billets. Le lecteur de carte lit la carte de la victime, tandis que la caméra filme l'entrée du code PIN. En raison de cette procédure publique, la réticence pour ce type de fraude est bien plus élevée que pour une simple fraude en ligne. En outre, les frais d'équipement sont bien plus élevés. Dans des forums spécialisés, l'on parle de quelques milliers d'euros pour acquérir le matériel nécessaire. De plus, le fraudeur court toujours le risque de voir son kit de skimming découvert et saisi.

Gjjsqrp_rgml /28 Bgqrpg` srcsp bc `gjjcr k_lgnsjĈ &qmspac28 Npcqqc nmjgagċpc @_tgċpc bs 01-.6-.5'

Les malfaiteurs proviennent très fréquemment d'Europe de l'Est. Les distributeurs automatiques dans les grandes villes sont en particulier menacés, car ils font l'objet d'un débit de cartes bien plus important que dans les petites villes. Le danger d'être surpris est aussi infiniment supérieur.

Dans le passé, ces installations de skimming ont été découvertes à de nombreuses reprises par des clients attentifs et signalées à la police ou à la banque. Depuis, elles sont fabriquées par des professionnels si bien qu'elles sont difficilement reconnaissables par des amateurs.

3.10. L'hameçonnage

L'hameçonnage permet d'accéder à quasiment toutes sortes de données. Le fraudeur a besoin de coordonnées bancaires ? Aucun problème, il crée de fausses pages bancaires, envoie via son réseau botnet une grande quantité de spams avec des liens à sa page et il lui suffit alors d'attendre jusqu'à ce que les données des personnes tombées dans son piège lui parviennent. La quantité de données est ici quasi inépuisable. Tout ce qui peut générer de l'argent est demandé, comptes de jeux vidéo, données de cartes de crédit, accès aux banques en ligne. Les comptes de paris en ligne ou de casinos en ligne sont tout aussi convoités. Les délinquants en abusent souvent pour blanchir l'argent qu'ils ont extorqué en fraudant.

La quantité des produits vendus au sein de l'économie souterraine est quasiment illimitée. Si l'on regarde dans les forums du milieu, des comptes MySpace ou bien Twitter volés sont parfois également vendus ou échangés. Les fraudeurs ont pour objectif d'accéder à autant de données personnelles que possible sur la victime. Ainsi, ils peuvent ensuite prendre l'identité de la victime et l'utiliser à ses propres fins.

3.11. Comment fonctionne une attaque de masse : les réseaux botnet et leur structure

Les exploits permettent aux fraudeurs d'installer des chevaux de Troie et des vers sur les ordinateurs de leurs victimes. Les exploits sont des faiblesses dans le système d'exploitation ou dans l'un des programmes déjà installés sur l'ordinateur, pouvant être exploités. Pour que le logiciel antivirus ne fonctionne pas immédiatement, les chevaux de Troie sont codés par des crypteurs, afin de dissimuler leur code. Pour ces crypteurs, des versions publiques sont disponibles, cependant généralement inutilisables en raison de leur grande diffusion. Ce qu'ils produisent est directement détecté par la plupart des logiciels antivirus. En outre, des versions privées sont disponibles, cependant commercialisées uniquement contre espèces. Les programmeurs de crypteurs proposent généralement leurs services sur des forums. D'outils sont très demandés et souvent proposés en tant que services. En effet, des logiciels malveillants créés avec des crypteurs et des packers ne peuvent pas être détectés sur la base de leur signature, dès lors que leur signature n'est pas précisément consignée dans la base de données. Ces versions uniques, vantées également comme serveurs « Fully UnDetectable » (FUD), peuvent ensuite ne pas être trouvées pendant un certain temps par les logiciels antivirus.

Le fonctionnement est similaire avec les bots : la plupart des bots disponibles ont des segments cachés. Les bots sont des petits programmes qui tournent généralement de manière inaperçue en arrière-plan de l'ordinateur de la victime et effectuent diverses actions : attaques DDoS, spams ou lecture des entrées sur le clavier, etc. Les fonctionnalités disponibles sont en fonction du tarif du Bot : plus il est cher, plus il est complet.

Pour gérer le réseau botnet, des serveurs de commande et contrôle (C&C Server) sont utilisés. Les bots installés sur l'ordinateur de la victime se connectent de manière autonome à ce serveur de contrôle et attendent les ordres de leur maître. Il existe différents concepts pour ce serveur C&C : Certains bots s'inscrivent dans l'IRC et entrent dans un canal spécial. Pour des raisons de sécurité, des serveurs IRC presque toujours privés sont utilisés (cf. illustration 15). Dans le canal, ils attendent ensuite de recevoir des ordres.

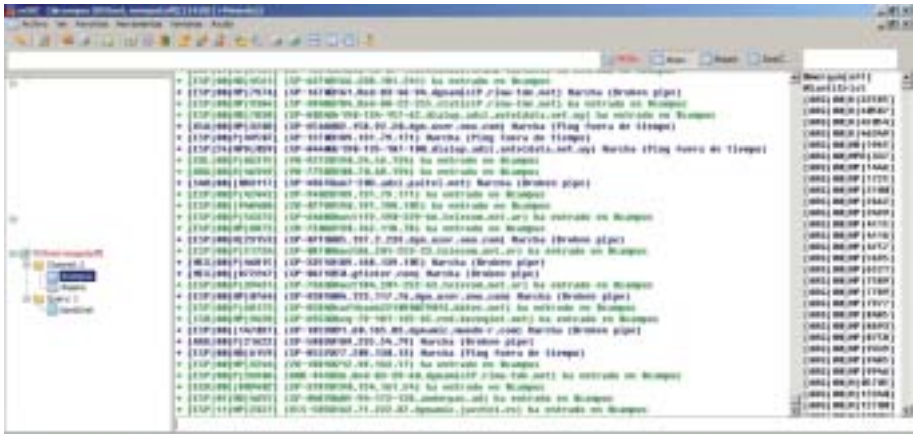


Illustration 15 : Canal IRC avec bots

Une possibilité souvent utilisée est la gestion via une interface Web (cf. illustration 16). La console de gestion est alors accessible après la saisi d'un nom d'utilisateur et d'un mot de passe. Dans cette interface Web, différentes possibilités sont disponibles en fonction des fonctionnalités du bot. Des statistiques sont proposées, expliquant combien de bots sont en ligne, combien ont été infectés en tout ou également de quels systèmes d'exploitation il s'agit. Des mises à jours de l'interface peuvent également être effectuées.

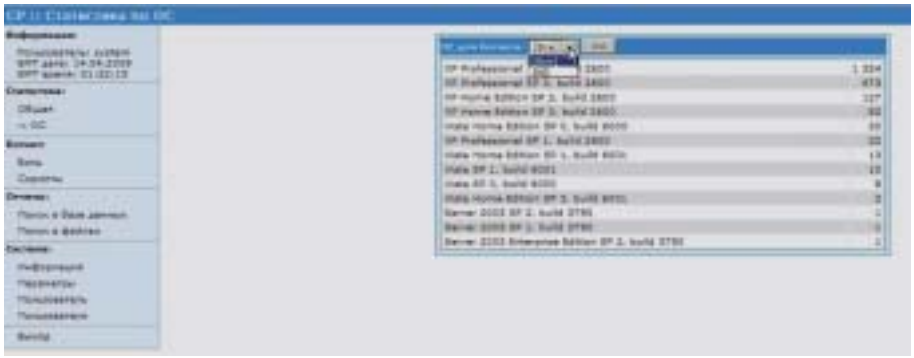


Illustration 16 : Interface Web d'un réseau botnet

Lorsqu'un cheval de Troie vient de s'installer sur l'ordinateur de la victime, il télécharge généralement un bot sur Internet. Les services des hébergeurs Bulletproof sont souvent utilisés en tant que sources de téléchargement. Si un fraudeur veut avoir un réseau botnet, il s'adresse alors au programmeur, pour lui acheter une version. Les bots sont souvent proposés en code binaire ou en code source, sachant que les prix pour le code source sont de 5 à 10 fois plus élevés.

Des RAT (Remote Administration Tools) sont également souvent utilisés. Ils permettent au cyberpirate d'accéder directement à l'ordinateur de la victime. Il peut alors y vérifier les actions effectuées par l'utilisateur et voir par exemple si son Bot n'a pas été installé dans le «honeypot» d'un éditeur de logiciel antivirus.

Dans ce cas c'est une mauvaise affaire : la version actuelle de son bot sera alors rapidement détectée par tous les logiciels antivirus actuels. Il devra de nouveau crypter le bot et mettre à jour toutes les installations, avant que les scanners éventuellement installés ne se mettent en route et nettoient le système.

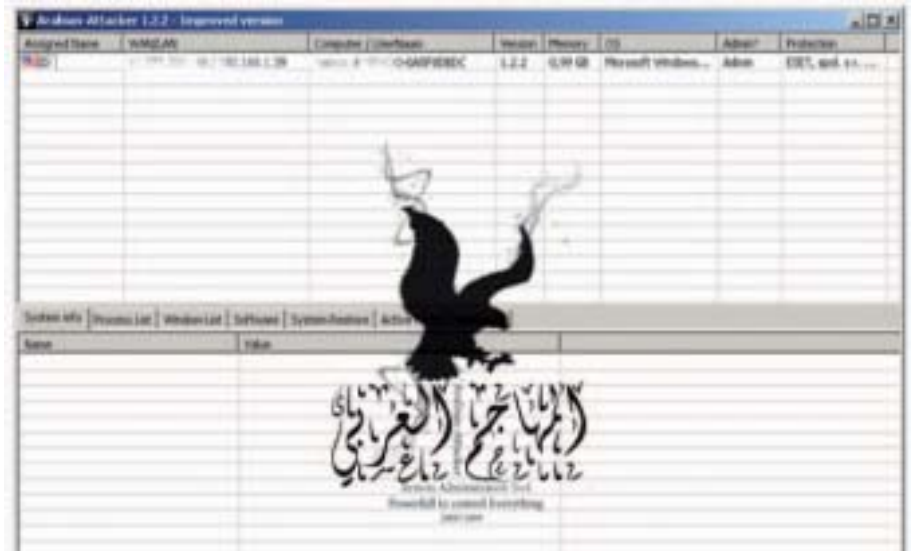


Illustration 17 : Client RAT

Cette méthode est souvent entreprise par des véritables professionnels. Elle demande cependant bien plus d'efforts que l'installation automatique. La créativité du fraudeur ne connaît quasiment aucune limite lorsqu'il s'agit de diffuser ces RAT. Il peut les placer via des « drive-by downloads » sur l'ordinateur des victimes, les introduire dans des réseaux P2P ou les envoyer en pièce jointe dans des millions d'e-mails.

Les « stealers » sont également très répandus. Ils sont utilisés pour le vol de données de compte. Les stealers sont diffusés via les mêmes voies que les RAT et les chevaux de Troie. Seule une solution antivirus de bonne qualité, surveillant tous les points d'entrée, constitue ici une bonne protection, par exemple le navigateur via un filtre HTTP ou l'accès e-mail avec un outil d'analyse des e-mails.

4. Le problème du blanchiment

Malgré la grande diversité des outils et des approches, tous ont un objectif commun : gagner de l'argent ! L'un des principal problème se pose une fois que les fraudeurs ont extorqué leur argent. Il existe de nombreuses approches permettant de procéder au « cashout ». Le cashout consiste à transformer l'argent virtuel en argent réel, sans que la provenance de l'argent ne puisse être repérée. Dans de nombreux cas, des produits sont achetés sur Internet via les données de cartes de crédit volées ou également avec de l'argent stocké sur des comptes Paypal volés. Pour ne pas se faire surprendre lors de la transmission des produits, les produits sont livrés 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 également être utilisés, ce sont les « Housedrop ».

Gjjsqrp_rgml /6ß Mīpcq bc bpmn xmlcq b_lq s l dmps k

Une autre méthode consiste à déplacer de l'argent via des casinos en ligne. Ainsi, l'argent peut par exemple être versé avec le compte PayPal volé auprès du casino en ligne. L'inscription au casino n'a bien entendu pas lieu avec les vraies données, mais avec des données falsifiées. Des évaluations sont à cet effet disponibles sur bon nombre de forums. Elles mentionnent quels portails de casinos ou de paris sportifs sont plus coulants sur les informations nécessaires à l'ouverture d'un compte. Les comptes volés qui ont déjà été certifiés sont dès lors fortement appréciés. L'argent sale déposé par ce biais est alors rapidement transféré vers d'autres comptes bancaires bien réels mais tout aussi illégaux, les « bank drop ». Le bank drop est un compte ouvert sous un faux nom. Une brique indispensable qui

assure un total anonymat. Une étape qui constitue sans nul doute l'un des plus gros problèmes des cyberescrocs. Rien d'étonnant donc à ce que les instructions et les outils permettant d'accéder à un compte anonyme soient proposées à des prix très élevés. Les solutions s'étendent de la corruption d'un agent de la poste, jusqu'à l'achat de cartes d'identité falsifiées permettant d'ouvrir un compte. Autant de solutions qui demandent savoir faire et technique de piratage. Des compétences qui ne manquent pas et qui se négocient sur le marché parallèle...

5. L'eCrime en progression

L'époque où le milieu des pirates informatiques était composé principalement d'adolescents masculins qui se promenaient sur internet pour se divertir et par intérêt technique est depuis longtemps révolue. La désignation « pirate informatique » pour la nouvelle génération qui sévit dans cette économie souterraine est donc tout simplement fausse. Il s'agit en effet de fraudeurs possédant des connaissances techniques, sans distinction entre le perceur de coffre-fort et les autres fraudeurs classiques. Dans le milieu, tout tourne autour de l'argent et des millions sont réalisés chaque année, que ce soit par vol actif de victimes oupar l'envoi de spams. Les auteurs sont souvent réunis en bandes possédant une structure organisationnelle professionnelle, dans lesquelles chacun a une mission.

Pour l'utilisateur, ceci signifie qu'il est de plus en plus important de protéger son ordinateur contre des influences nuisibles. Ceux qui se promènent encore aujourd'hui sur Internet sans recourir à une solution antivirus et de pare-feu performante risquent de devenir les victimes de ces fraudeurs. Ce danger est d'autant plus grand à une époque où les maisons de vente aux enchères et les banques en ligne font partie du quotidien.

La manipulation de ses données personnelles constitue un autre point primordial. De nombreux utilisateurs n'hésitent pas à entrer diverses données personnelles dans leurs profils de réseaux sociaux, sans penser qu'ils les livrent ainsi aux fraudeurs. En effet, même une information apparemment insignifiante comme sa date de naissance peut aider le fraudeur à compléter les données de la carte d'identité.

Une tendance croissante consiste à modifier les sites Web des victimes à l'aide des données de compte qui sont volées sur leur ordinateur. Pour cette raison, les prestataires de sécurité conseillent, en cas d'infection, de contrôler non seulement l'ordinateur, mais également le site Web par exemple, que l'on exploite. Les conséquences peuvent dans le cas contraire être fâcheuses : Si les fraudeurs intègrent des logiciels malveillants, l'exploitant est alors tenu responsable.

Annexe 1 :

Liste de prix pour des articles souterrains

Cet aperçu comporte des prix pour des produits et des services tels qu'ils ont été négociés dans la période de juin et juillet 2009 dans les forums souterrains. La différence de prix, définie par les remises et l'habileté à négocier, est large.

Produit	**Prix min.**	**Prix max.**
RAT en fonction des propriétés	20,00 €	100,00 €
Stealer	5,00 €	40,00 €
Cartes d'identité/permis de conduire volés en fonction de la qualité de la contrefaçon	50,00 €	2500,00 €
Fichier bot (prix en fonction des propriétés et du programmeur)	20,00 €	100,00 €
Code source bot	200,00 €	800,00 €

Service	**Prix min.**	**Prix max.**
Hébergement, en fonction de l'étendue du service, de l'espace Web à plusieurs serveurs	5,00 €	10000,00 €
Service FUD	10,00 €	40,00 €
Attaques DDoS par heure	10,00 €	150,00 €
Installations de bots par 1 000, prix dépendant de la situation géographique	50,00 €	250,00 €
1 million de spams à des destinataires spéciaux, par ex. joueurs augmentent le prix	300,00 €	800,00 €

Données	**Prix min.**	**Prix max.**
Bases de données : le prix dépend des contenus et du volume précis de la base de données, il s'agit de l'achat de la base de données	10,00 €	250,00 €
Données de cartes de crédit : les prix dépendent de l'intégralité des données. Un simple numéro de CC avec date a peu de valeur. Plus les informations sont nombreuses, plus le prix est élevé.	2 €	300 €
1 million d'adresses e-mail, les adresses vérifiées ou groupes d'intéressés sont plus coûteuses	30,00 €	250,00 €

Comptes	**Prix min.**	**Prix max.**
Compte steam, le prix dépend de la quantité de jeux installés	2,00 €	50,00 €
Compte WoW, en fonction de l'étendue des données et du niveau des caractères dans le compte	5,00 €	30,00 €
Compte Packstation, les prix dépendent de l'étendue des données présentes et du fait qu'il soit falsifié ou volé	50,00 €	150,00 €
Compte PayPal, plus des données de compte sont présentes, plus le prix est élevé	1,00 €	25,00 €
Compte Click & Buy	10,00 €	35,00 €
Comptes e-mail avec mails privés, les prix varient en fonction des négociants	1,00 €	5,00 €

Annexe 2 :

Glossaire

Account : Droit d'accès à un système informatique. Celui-ci se compose, de manière générale, d'un dispositif de reconnaissance de l'utilisateur (identification de l'utilisateur) et d'un mot de passe secret.

Administrateur : Gestionnaire d'un système de réseau qui possède des droits d'accès illimités et qui est responsable pour le suivi et l'administration de ce réseau.

Crypteur : Les crypteurs servent à encoder des fichiers afin de compliquer la détection des logiciels malveillants aux logiciels antivirus.

DoS (Denial of Service) : 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 deviennent incapable d'assurer leurs services et s'écroulent 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.

E-mail : Electronic mail ou courrier électronique, l'une des applications essentielles d'Internet. Une multitude de courriers professionnels et privés est envoyée chaque jour sous forme électronique. Les messages électroniques sont, certes, très utiles, mais représentent aussi l'une des principales voies de propagation des programmes nuisibles. Les vers se multiplient souvent en raison du fait qu'ils envoient des e-mails automatiques dont la pièce jointe contient un ver. Les auteurs de virus tentent, par tous les moyens de camouflage et de tromperie, d'inciter les destinataires à ouvrir les pièces jointes. D'autres e-mails incitent leur lecteur à se rendre sur des pages Web dont les contenus sont infectés. Certains e-mails HTML installent même le ver directement à l'ouverture de l'e-mail. Pour contrer ce risque, le logiciel antivirus prévoie des mécanismes de protection des programmes de messagerie électronique, qui détectent et suppriment les virus avant qu'ils ne soient involontairement activés par l'utilisateur.

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

FAQ : Réponses à des questions fréquemment posées (en anglais, frequently asked questions) autour d'un sujet spécifique.

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 : Le « File Transfer Protocol » (= protocole de transfert des fichier) est un 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 publiques. Certains virus et chevaux de Troie installent leur propre serveur FTP, sur lesquels on peut télécharger des fichiers sur des ordinateurs infectés.

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

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 troyens. En détournant la page de démarrage ou la fonction de recherche, les browser 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 browser hijackers utilisent souvent les failles de sécurité et les points faibles des systèmes pour s'y implanter profondément. Ils s'attaquent le plus souvent à Internet Explorer. La suppression de ces fonctions de commande est souvent très difficile. L'un des Browser Hijacker les plus fameux est CoolWeb.

ICMP : ICMP (Internet Control Message Protocol) Protocole faisant partie de TCP/IP et qui sert à transférer des messages d'erreur ainsi que des paquets d'informations et de contrôle.

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.

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

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.

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. Un représentant de cette espèce s'appelle Padodoor.

Login : Procédures de connexion, d'enregistrement et d'authentification (généralement par mot de passe) d'un utilisateur pour accéder à un système informatique.

OpenVPN : OpenVPN 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 OpenVPN. Dans ce cas, seul l'IP de l'ordinateur qui permet d'établir une connexion est émis.

P2P (Peer to Peer) : Le réseau « Peer to Peer » ne possède pas de serveur central, et tous les ordinateurs reliés agissent séparément avec les mêmes droits.

Patch : Module réparant des erreurs ou comblant des lacunes de sécurité dans un logiciel. Le Patch ne fait que remplacer les fichiers erronés, et non pas la version complète du logiciel.

Payload : Payload est désigne en anglais la Fonction destructrice d'un virus (littéralement). L'activation de cette action peut être liée à une condition, un élément déclencheur (payload trigger). La définition de fonction destructrice est remise en question, car certains chercheurs taxent aussi l'utilisation des ressources de système et la bande de transmission de Payload.

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. La plupart des tentatives de hameçonnage s'adressent aux clients de banques possédant des services en ligne (CityBank, Postbank), aux utilisateurs de services de paiement (Paypal), aux abonnés des FAI (AOL) ou aux clients des commerçants en ligne (eBay, Amazon). Souvent la victime est conduite sur de fausses pages Internet, par courriel ou messagerie instantanée, prêtant à confusion avec de véritables pages.

Posting : Message publié sur Internet dans un groupe de discussion, une liste de diffusion ou un forum.

Protocole : Langage de communication entre différents ordinateurs au sein d'un réseau. Un protocole comporte un ensemble de règles qui contrôle l'échange d'informations. Exemples de protocoles : FTP, HTTP, POP3 ou TCP/IP.

Provider : Prestataire proposant un accès à Internet.

Proxy : Un proxy 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.

Copie pirate (angl. Warez) : Copie non autorisée d'un programme effectuée illégalement à partir d'un produit original. Toute possession ou réalisation de copie illégale est puni par la loi de protection de la propriété.

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

Server : Programme mettant des données ou des services à la disposition de postes clients.

Skype : Skype permet de téléphoner via Internet soit depuis son propre PC soit depuis un téléphone adapté. Les destinations potentielles sont ici d'autres ordinateurs sur Internet ainsi que le réseau fixe et mobile.

Social Engineering : Tactiques de persuasion utilisées par un pirate informatique pour obtenir des informations d'une personne, qu'il pourra utiliser ensuite pour nuire à la personne ou à sa structure. Souvent sont utilisés des procédés d'intimidation, afin d'obtenir les codes d'accès ou mots de passe.

Stealer : Ils servent en premier lieu à espionner des accès à l'ordinateur de la victime.

Spams : Au milieu des années 90, ce mot désignait la diffusion massive du même message dans les forums Usenet. Le concept lui-même se réfère à un sketch des Monty Python. Depuis lors, le mot a pris plusieurs significations. De manière générale, il désigne tous les courriers électroniques non sollicités. Dans un sens plus strict, il désigne tous les courriers publicitaires : Les vers, canulars, courriers de hameçonnage et réponses préenregistrées ne font pas partie des spams.

Spammer : Personne qui envoie des spams.

Logiciels espions (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, analyser le comportement de navigation, ou pour espionner les données d'accès bancaire ou d'Online-Accounts.

SSH (Secure Shell) : Secure Shell est en particulier répandu sur Linux et Unix. Ce protocole permet d'accéder à une connexion codée à des ordinateurs à distance. Il est également possible de dissimuler les connexions via des ordinateurs sur lesquels l'on est connecté.

Chevaux de Troie : L'expression « cheval de Troie », référence historique, décrit un programme qui fait croire à l'utilisateur qu'il possède une fonction particulière normale. Mais les chevaux de Troie contiennent en plus un segment caché, qui leur permet de pénétrer dans les ordinateurs infectés et leur donne un accès presque total au système, à l'insu de l'utilisateur. Les méthodes de camouflage des chevaux de Troie sont quasiment illimitées. Mais ces programmes insidieux prennent aussi souvent la forme d'écrans de veille ou de jeux envoyés par e-mail. Un seul démarrage suffit pour que le parasite infecte le système.

Update : Mise à jour de données et de programmes (par exemple, logiciels, données antivirales, bases de données). Le logiciel G Data Security vous permet de mettre régulièrement à jour les signatures virales via Internet (mise à jour de virus). Vous pouvez actualiser également le logiciel antivirus même à l'aide d'une mise à jour du logiciel.

Virtuel : Décrit un environnement qui n'est pas fondé sur la vie réelle, mais qui est généré par ordinateur. On parle un peu confusément de réalité virtuelle (VR).

PC zombie : Ordinateur contrôlable à distance à partir d'un backdoor. Comme dans les films de genre, la machine zombie obéit uniquement à son maître caché dont elle exécute les commandes le plus souvent nuisibles. La plupart du temps, de nombreux Zombies sont réunis sous forme de réseaux appelés robots.