



Le web underground en France

Sous le sceau de la vigilance

Cédric Pernet
Trend Micro Cybersafety Solutions Team

MENTIONS LEGALES

Les informations sont fournies dans ce document à titre d'information et de sensibilisation. Elles ne constituent en aucun cas des conseils d'ordre juridique. L'information contenue dans ce document ne s'applique pas à toutes les situations et peut ne pas refléter la situation la plus actuelle. Aucun des éléments présentés ne doit être appliqué tel quel sans validation juridique par rapport aux spécificités, faits et conditions réelles. Trend Micro se réserve le droit de modifier le contenu de ce document sans notification au préalable.

La traduction française de ce document est proposée à titre pratique uniquement. La précision et la stricte conformité de la traduction par rapport à la version originale ne sont pas garanties. En cas d'incompréhension ou de doute, merci de vous référer à la version originale de ce document. Toute différence entre la version traduite et l'originale n'engage aucunement la responsabilité de Trend Micro, ni celle du traducteur.

Bien que des efforts aient été réalisés pour présenter des informations précises et à jour, Trend Micro ne peut garantir la parfaite précision et l'exhaustivité des informations fournies. En utilisant ce document, vous acceptez de le faire en assumant toutes les responsabilités qui y sont liées. Trend Micro s'exonère de toute responsabilité et garantie, implicite ou explicite. Trend Micro, ainsi que les différentes parties impliquées dans la création, la production, la traduction et la fourniture de ce document s'exonèrent de toute responsabilité vis-à-vis de dommages pouvant résulter de l'application et de l'utilisation de ce document, ou d'éventuelles erreurs ou omissions. Toutes les informations de ce document sont fournies en l'état.

Sommaire

3

Introduction

4

Anatomie de
l'underground français

11

L'offre au sein de
l'underground français

29

Conclusion

31

Références

Si le web underground nord-américain devait disposer d'un équivalent, ce serait probablement l'underground français. L'exploration de l'underground américain¹ permet de comprendre qu'il s'agit d'un "réservoir transparent", ouvert aussi bien aux hackers technophiles qu'aux cybercriminels et forces de l'ordre. L'underground français, en revanche, est parfaitement dissimulé au sein du Dark Web et se veut, en outre, particulièrement vigilant.

La méfiance est d'actualité au sein de cet environnement, et aussi importante que dans l'underground Japonais. Les systèmes de babillards électroniques (BBS) japonais utilisent des CAPTCHA pour filtrer les utilisateurs et s'assurer qu'ils sont bien du pays ou, du moins, qu'ils communiquent en japonais. En France, on va plus loin : les forums, places de marchés et autres autoshops ("boutiques" tenues par un seul vendeur) exigent d'y adhérer ou imposent un processus de validation avant toute participation. Les administrateurs de forums ne permettent à un demandeur d'en être un membre actif qu'après obtention d'un certain score de réputation, et certains forums classent leurs utilisateurs selon le critère de l'expérience. Les novices sont traités différemment des cybercriminels plus expérimentés qui disposent d'un statut premium (Elite, Administrateur, membre de confiance...)

Les intermédiaires dépositaires de fonds (escrows) constituent un impératif au sein de l'underground français, toute comme en Russie³ et en Allemagne⁴. Ces tiers de "confiance" s'assurent qu'acheteurs et vendeurs obtiennent leur dû respectif suite à une transaction. Mais contrairement aux marchés underground dans ces deux derniers pays, la mise à l'index est une réalité en France : chaque forum dispose de son "mur de la honte" où s'affichent ceux ayant fait preuve de malhonnêteté et d'activité frauduleuse au sein de la communauté. Il arrive souvent que les propriétaires et/ou membres de ces forums y inscrivent leurs rivaux pour leur porter préjudice. Les luttes d'influence entre les places de marchés sont communes, dans l'objectif de recruter toujours plus de membres ou de récupérer le pouvoir d'achat des membres de marchés rivaux, en sachant que les cybercriminels français fréquentent souvent plusieurs marchés.

Contrairement aux marchés plus importants et établis - Russie et Chine⁵ notamment - l'underground français reste relativement petit, regroupant environ 40 000 cybercriminels (du novice à l'expert) et générant de 5 à 10 millions d'Euros par mois, selon les données de la Gendarmerie Nationale et de la Police Nationale. Il se rapproche des caractéristiques de l'underground allemand et de ses offres de niche. Les cybercriminels français font appel à des marchés de plus grande envergure pour l'essentiel de leurs besoins (malware, outils connexes, services...) La majorité des outils offerts sur ces marchés souterrains ne peut être utilisée qu'à des fins de fraudes ciblant un public francophone. Parmi ces outils et ressources, on trouve des passe-partout d'accès aux boîtes aux lettres (pass PTT), des contrefaçons de reçus/factures ou des services d'ouverture de compte bancaire notamment. Un passe-partout permet notamment de dérober des documents personnels dans un but de détournement d'identité. Les factures et reçus contrefaits peuvent ternir la réputation des entreprises censées les avoir émises. De leur côté, les services d'ouverture de compte et le vol de données de carte de paiement permettent aux criminels de mener leurs fraudes bancaires. Mais attention, les cybercriminels ne trouvent pas tous les outils dont ils ont besoin au sein de l'underground français et s'essayent donc à créer leurs propres outils. C'est notamment le cas des ransomware conçus localement⁶, sans doute la menace de sécurité la plus importante à ce jour. Les cybercriminels proposent également des fichiers de données (identifiants utilisateur détournés notamment) et des outils tels que des « binders » qui facilitent les attaques sur le grand public et les entreprises.



Pendant toute l'année dernière, les équipes R & D de Trend Micro ont étudié des marchés souterrains nationaux et leur spécificités. Le marché français semblait prometteur et n'a pas manqué de nous surprendre, dans son état actuel de croissance et de développement ... Ces spécificités nationales doivent être prises en compte dans le dispositif de réponse nationale, mais plus largement connues en Europe et mondialement. C'est pourquoi nous continuons à travailler localement avec les services compétents : la BEFTI (Préfecture de Police), le C3N (Gendarmerie Nationale) et la SDLC (Direction Centrale de la Police Judiciaire) ; et avec les autres services de Police en Europe et dans le monde, via EUROPOL et INTERPOL pour un monde numérique plus sûr.

~ Loïc Guézo,
Cybersecurity Strategist SEUR, Trend Micro



SECTION 1

Anatomie de l'underground
français

Anatomie de l'underground français

À quoi ressemble l'économie souterraine de la cybercriminalité en France ? Quelle est sa structure ? Quelles sont les spécificités françaises ? Voici quelques-unes des questions auxquelles nous allons maintenant répondre, en mettant notamment l'accent sur ce qui rend l'underground cybercriminel français différent de ses homologues dans le monde.

Prudence et vigilance sont de rigueur

Le cybercriminel français, tout comme ses homologues d'ailleurs, est obnubilé par une idée : éviter de se faire coincer par les forces de l'ordre. Mais contrairement à ces mêmes homologues, il est probablement plus prudent. Il en est persuadé : ici, les loups se dévorent entre eux. Chaque forum propose ainsi une fonction pour signaler tout acte malhonnête ou frauduleux, avec souvent un "mur de la honte" qui répertorie leur auteur. Et ce climat de méfiance ne s'arrête pas là. Au-delà de cette délation, il arrive souvent que les propriétaires et/ou membres de ces forums s'en prennent à leurs rivaux et à leur offre. Il arrive souvent que des places de marché se lancent dans des guerres l'une contre l'autre, dans l'objectif de s'attirer le pouvoir d'achat de nouveaux membres. Les cybercriminels sont, en effet, souvent membres de plusieurs places de marché. Lors d'un événement récent, les membres de deux places de marchés - A et B - ont été témoins d'un affrontement entre ces deux entités. La place de marché A a identifié ses membres appartenant également à la place de marché B. Les administrateurs ont ensuite détourné les identifiants des membres du marché A pour tenter de pirater les comptes de ces utilisateurs sur le marché B. Les administrateurs ont ainsi pu détourner tous les bitcoins associés aux comptes utilisateurs piratés (pour les titulaires de compte utilisant les mêmes identifiants sur les deux places de marché). Cependant, les administrateurs de la place de marché attaquée ont su réagir rapidement en annulant toutes les transactions bitcoin non garanties, sans doute après avoir été avertis par les victimes.

Lors de nos recherches, nous avons assisté à la disparition soudaine d'un forum majeur, ce qui semble être assez "commun" au sein de l'underground français. Forums et marchés émergent et disparaissent régulièrement, sans doute par crainte des forces de l'ordre et conséquence des guerres menées entre marchés. Les cybercriminels français craignent que les forces de l'ordre ne surveillent furtivement et en

permanence leurs mouvements. Face à ce risque, les forums misent sur un mécanisme de vérification. Les administrateurs de forums ne permettent à un demandeur d'être un membre actif qu'après obtention d'un certain score de réputation. Le score de réputation d'un membre augmente à chaque post pertinent publié ou transaction frauduleuse réussie sur le forum. Plus votre score de réputation est élevé, plus vous êtes une personne de confiance (en clair, vous ne faites pas partie des forces de l'ordre). Au-delà des scores de réputation, certains forums classent leurs utilisateurs selon le niveau d'expérience. Les novices sont traités différemment des cybercriminels plus expérimentés qui disposent d'un statut premium (Elite, Administrateur, membre de confiance, ...)



V.I.P.



Lieu : France
Inscription : 10/01/2015
Messages : 1 310

 [MP](#)

Rèputation : 149 / 16

Laisser un avis : + / -

 [Voir Son Store \(97.67% \)](#)

Figure 1: la réputation d'un utilisateur au sein d'une place de marché est affichée sur son profil.

Cette forme de paranoïa collective est sans doute aussi la principale raison pour laquelle les cybercriminels chiffrent leurs communications. Tous les forums étudiés offrent la possibilité de chiffrer les messages, même ceux acheminés via le système de messagerie privé. Les administrateurs des babillards sont d'ailleurs parfois suspectés de consulter les messages privés. Ceci est peut-être dû à un incident passé, lorsqu'un membre de la communauté underground de cybercriminels a divulgué des messages privés de plusieurs forums aux forces de l'ordre.

La défiance règne donc au sein de l'underground français, ce qui explique sans doute la présence des tiers de confiance ("escrow" en anglais) qui jouent le rôle d'intermédiaire dans une transaction bipartite. Ces tiers s'assurent que les acheteurs reçoivent leur produit acheté et que les vendeurs reçoivent leur argent, après perception d'une commission évidemment. Cette commission est généralement de 7% pour les transactions d'un montant inférieur à 500 € et de 5 % pour les montants au-delà de 500 €. Contrairement à la Russie et à l'Allemagne, le montant maximal de la transaction "assurée" par un tiers est de 1 000 € sur certaines places de marché françaises. Lorsque ce seuil est atteint, il doit patienter jusqu'à ce que toutes les transactions soient traitées, avant d'en accueillir de nouvelles.

Ces tiers sont si courants au sein de l'underground français que la place de marché IBM (Intelligence Black Market) dispose de son propre système semi-automatisé. Les tiers de confiance perçoivent 4% du montant de chaque transaction. Ce système, appelé "Autoescrow Platform" est hébergé de manière indépendante, et fonctionne même si le forum est en maintenance ou connaît des soucis de connectivité. La sécurité est par ailleurs renforcée grâce à un mécanisme d'authentification à deux facteurs.



The image shows a login interface for the 'AUTOESCROW PLATFORM'. At the top, the logo 'AUTOESCROW PLATFORM' is displayed in blue, bold, uppercase letters. Below the logo, the text 'IBM Auto Escrow' is shown in a grey bar. The interface contains two input fields: 'Nom de compte' (Account name) and 'Mot de passe' (Password). Below these fields, there is a link that says 'Pas encore inscrit ? Inscrivez vous.' (Not yet registered? Register now.). At the bottom, there is a large blue button labeled 'Valider' (Validate).

Figure 2 : interface d'authentification de la plateforme Autoescrow

Si l'underground nord-américain s'apparente à un "réservoir de verre", qui accueille les hackers technophiles et reste visible aux cybercriminels et aux forces de l'ordre, l'underground français, en revanche, est à l'exact opposé. Il est plus proche de l'underground allemand et réside entièrement dans les tréfonds d'Internet, à savoir le Dark Web.

Quelle différence entre place de marché et autoshop ?

Globalement, il existe 3 canaux de vente de biens et services illégaux au sein de l'underground français. Certains fraudeurs se contentent de faire la promotion de leur offre au sein des places de marché populaires. D'autres préfèrent rester furtifs, sans promotion mais en cherchant à contacter des acheteurs potentiels identifiés. Enfin, les autoshops sont très communs et une particularité française, à savoir des "boutiques" gérées par les vendeurs eux-mêmes.

Les forums disposent parfois de leur propre place de marché. Si certains de ces marchés s'identifient simplement via une requête sur un moteur de recherche, elles sont néanmoins généralement bien cachées. Les places de marché cybercriminelles françaises ne sont pas si différentes de celles de Russie, de Chine ou du Brésil. De nombreux outils et logiciels malveillants sont proposés à des tarifs très compétitifs. Y accéder requiert parfois de régler un abonnement ou de passer via un processus de vérification.

Au final, l'underground français et celui du Japon, sont moins confiant que ceux d'autres pays. Leurs forums (babillards au Japon) nécessitent une forme d'authentification pour obtenir un accès.



Key generator

1HZg1fSbg4oiop8XjqGgS7si9syBkcisnT

Pour obtenir votre **key** d'inscription au forum Black Hand, envoyer €50 (soit : **0.13490543 BTC**) à l'adresse BTC ci-dessus

Figure 3 : un marché underground français qui exige des frais d'adhésion de 50 € (en bitcoins).

Ce sont néanmoins les autoshops qui sont les plus visibles au travers de leur promotion sur de nombreux forums et places de marché. Chaque autoshop est géré et opéré par un individu. Ce dernier est en contact direct avec les clients et prospects. Les transactions de biens et de services illégaux sont ainsi plus directes.



Figure 4 : un autoshop français proposant des stupéfiants

Les autoshops sont tellement populaires en France que certains cybercriminels tirent leurs revenus de la prestation de service de création d'autoshops. Pour 400 €, ils vous proposent un autoshop hébergé (Dark Web ou Clear Web), complet et disposant d'un système de gestion de contenus (CMS), actif en quelques heures. Le service porte sur l'enregistrement du nom de domaine, l'installation, l'hébergement, la personnalisation et même la sauvegarde.



Figure 5 : exemple de système de gestion de contenu dans le cadre de la création d'autoshops

Bitcoins et cartes prépayés : les moyens de paiement préférés dans l'underground français

Les problématiques de confiance, vis-à-vis des forces de l'ordre et des pairs, constituent sans doute la principale raison pour laquelle les cybercriminels n'acceptent que deux formes de paiement : les Bitcoins et les cartes prépayées PCS.

L'utilisation de bitcoins offre un certain niveau d'anonymat aux utilisateurs. Cette monnaie virtuelle s'échange et se transfère simplement, sans exiger d'identification puisque cette monnaie n'est pas réglementée.

Les cartes prépayées, disponibles un peu partout en France ou en ligne, sont populaires auprès des acheteurs. Certains marchands n'exigent d'ailleurs aucune identification des acheteurs qui se procurent ou rechargent leur carte prépayée. Seul un numéro de téléphone mobile valide est requis, ce qui reste assez simple à obtenir. Ces cartes se sont donc imposées comme idéales pour les achats illégaux.

Les cartes prépayées sont devenues si populaires que certains cybercriminels vendent de telles cartes avec de fausses cartes d'identité et informations personnelles (adresse personnelle, email et une carte SIM qui est utilisée pour enregistrer la carte prépayée). Les acheteurs se contentent ainsi d'utiliser des fausses cartes prépayées pour percevoir le paiement des produits/services illicites commercialisés.

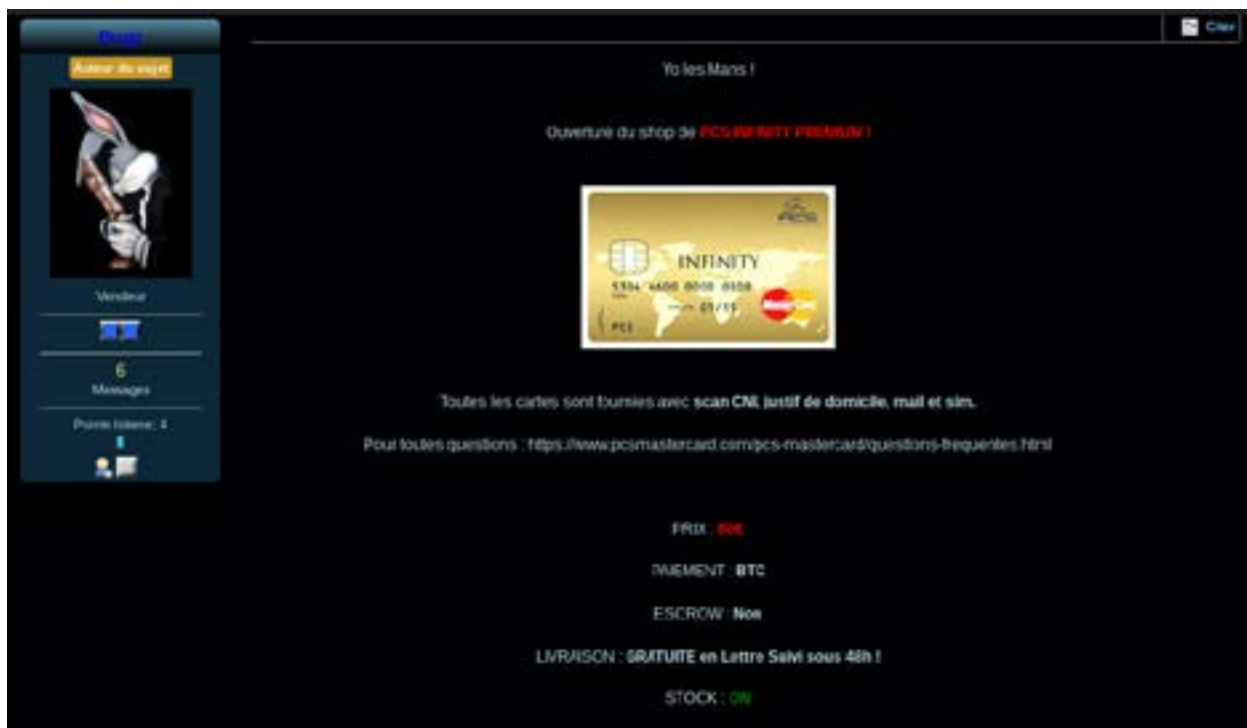


Figure 6 : publicité pour une carte prépayée avec fausses informations personnelles pour 80 €

A dark, industrial interior, possibly a factory or workshop, with a large circular graphic overlay. The scene is dimly lit, with light coming from windows in the background. The structure is made of dark metal beams and supports. The floor is cluttered with various objects, including what looks like a roll of material. The overall atmosphere is gritty and historical.

SECTION 2

L'offre au sein de
l'underground français

L'offre au sein de l'underground français

Comme tout marché cybercriminel, l'offre au sein de l'underground français est diversifiée. Certains produits et services sont propres à la France et les logiciels malveillants sont nombreux. À noter que nos recherches ont, pour l'essentiel, porté sur les cinq plus grandes places de marché de l'underground français, et sur deux forums qui ne sont pas directement associés à des marchés.

Armes, passe-partout, fausses factures, stupéfiants...

Des armes de petite catégorie

Chaque marché cybercriminel propose des armes à la vente. Mais en France, cette offre porte, pour l'essentiel, sur des armes discrètes en lieu d'armes puissantes et d'envergure.



Figure 7 : "Pen gun" proposé à la vente pour 150 € dans un marché underground

Ces armes discrètes, qu'il s'agisse de poings américains ou de couteaux de petit format, sont bon marché, à partir de 10 € seulement. Ils sont souvent présentés comme des armes sans danger. On peut donc se procurer des couteaux flexibles d'un format carte de crédit (10 €) ou des stylo-pistolets d'un calibre 22 long rifle (150 €). Des armes certes petites mais dont le port reste illégal au titre de la législation française.

Mais attention, il est aussi possible de se procurer des armes lourdes. Ils coûtent bien plus chers, de 650 à 1800 €, un tarif élevé qui s'explique par l'interdiction de la possession de ce type d'arme en France.

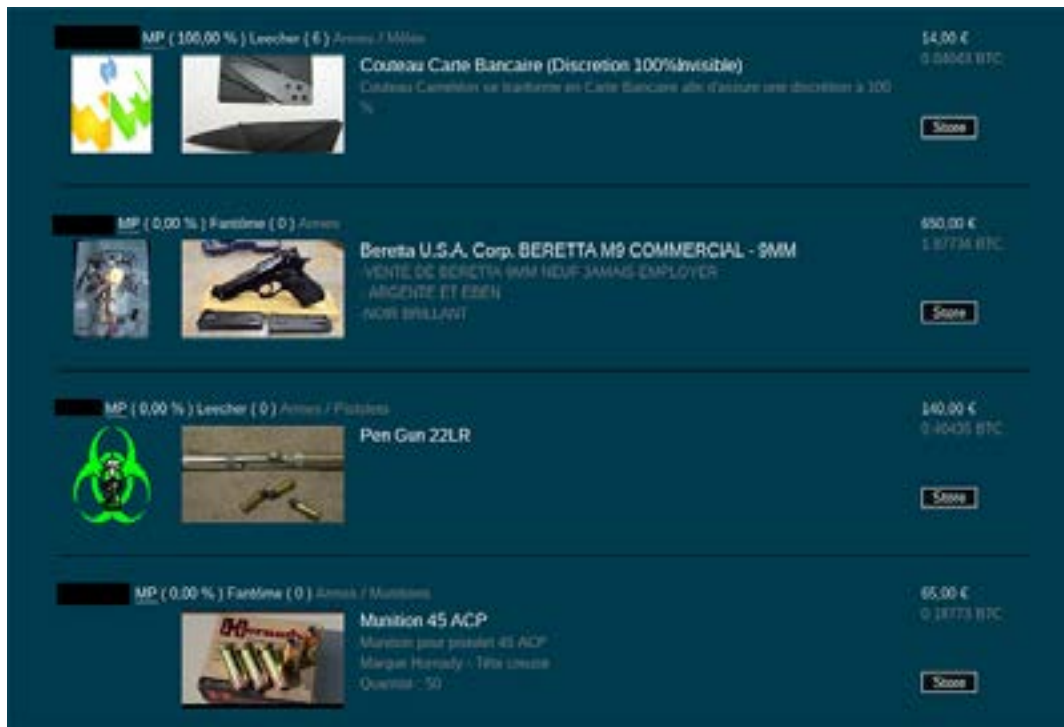


Figure 8 : exemples d'armes à feu disponibles au sein de l'underground français

Notons également que des fichiers sont proposés pour l'impression d'armes en 3D. Un pack de fichiers, proposé à seulement 4 € chacun, permet d'imprimer 12 armes à feu différentes (AK-47, Glock 17/22 et MAC-10 notamment). Ce tarif est si bas qu'il en devient inquiétant, même si l'offre n'inclut pas les instructions d'assemblage des pièces imprimées en 3D.

Kits de suicide et d'euthanasie

Plus dérangeant encore, nous avons aperçu dans un forum un vendeur proposant un "KIT DE SUICIDE/ MEURTRE ou EUTHANASIE, 100% de réussite". Cet utilisateur souhaitait connaître si son offre pouvait rencontrer une demande, avant de produire les kits. Deux kits différents étaient proposés - par injection ou prise orale - au tarif de 500€ si l'acheteur utilisait le kit lui-même. Mais pour utiliser ce kit sur un tiers, le tarif était deux fois plus important. Ce vendeur n'a cependant pas trouvé d'acheteurs, tout du moins publiquement.

Dans un fichier de base de données récupéré auprès d'un autre forum d'une place de marché, nous avons trouvé un fil de discussion entre ce même vendeur et un acheteur potentiel. L'acheteur souhaitait obtenir ce kit pour une utilisation sur autrui, ce qui ressemble fort à un assassinat. Un marchandage a eu lieu, au bout duquel un prix de 600 €, payé en Bitcoins, a été défini.

Passe-partout pour boîtes aux lettres

Certains fournisseurs de services de livraison, comme La Poste, disposent de passe-partout (appelés également Pass PTT) capables d'ouvrir les boîtes aux lettres de leurs clients. Mais ce que ces clients ignorent est que ces clés passe-partout sont disponibles sur certains forums underground, à des tarifs très abordables. Nous avons ainsi identifié un vendeur proposant 25 de ces clés pour 220 € seulement. D'autres vendent ces clés à l'unité au tarif de 15 €, par trois pour 35 € et 12 clés pour 115 €.

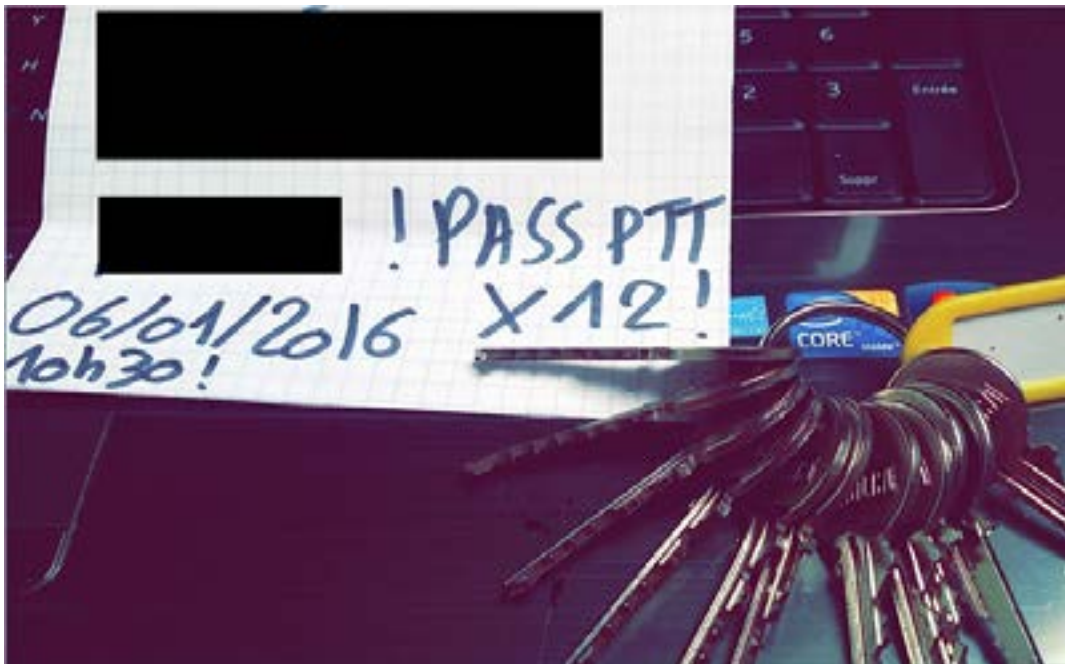


Figure 9 : Pack de 12 clés proposé à 115 €.

Si la quasi-totalité des boîtes aux lettres peuvent être ouvertes en France à l'aide de seulement 4 types de passe-partout, certains autres peuvent être achetés pour ouvrir des boîtes aux lettres dans des régions précises du pays. Certaines de ces clés ouvrent également des portes et verrous (autres que ceux des boîtes aux lettres) dans des villes cibles (passages dans les transports publics ou entrées d'immeubles privés par exemple).

Les passe-partout sont si populaires que certains individus peu scrupuleux en proposent des fichiers d'impression 3D, gratuitement. Cette disponibilité étendue de passe-partout permet aux cybercriminels de mettre la main sur les paquets et courriers présents dans les boîtes aux lettres, et notamment sur les documents personnels ou officiels nécessaires à des opérations de détournement d'identité.

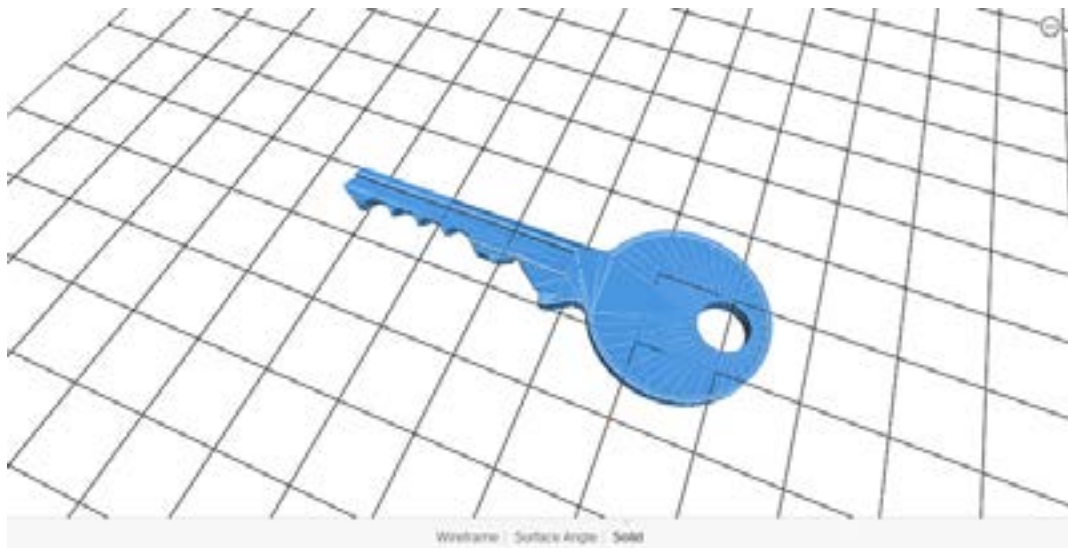


Figure 10 : un fichier d'impression 3D gratuit pour réaliser un passe-partout pour boîtes aux lettres

Facture, reçus, cartes grises et chèques contrefaits

Des documents contrefaits se vendent également au sein de l'underground français. À l'image de toutes les contrefaçons, ces documents sont conçus pour sembler aussi authentiques que possible.



Figure 11 : une fausse facture pour des enceintes Hercules XPS 101

Les principales enseignes de la grande distribution en France (Amazon, Pixmania, Darty, etc.) font souvent l'objet de détournement pour ces contrefaçons. Dans le type de fraude qui s'en suit, les acheteurs sont piégés : ils doivent payer davantage pour un produit, et ce, à l'insu de l'enseigne. Le différentiel de prix va dans la poche du fraudeur. Une autre utilisation de ces fausses factures consiste à rendre légitime des objets ayant été volés.

Des cartes grises contrefaites sont également disponibles au sein de l'underground français. Ceci permet à des malfaiteurs de vendre des voitures volées à un prix très intéressant. Le temps que l'acheteur réalise l'arnaque, probablement lors du changement de carte grise, le vendeur a disparu depuis belle lurette.



Figure 12 : une fausse carte grise proposée à 500 €.

Les chèques contrefaits, de leur côté, sont utilisés pour régler des achats en magasin. Puisqu'il n'existe pas de détecteur de faux chèques, certains utilisent des chèques contrefaits correspondant à des cartes d'identité, elles aussi falsifiées, pour acheter produits et services. Bien sûr, l'acheteur aura disparu avant que la banque ne se rende compte de la fraude. Les faux chèques sont vendus entre 70 et 100 € pour 10 chèques.

Services d'ouverture de compte bancaire

L'ouverture d'un compte bancaire en France implique que le requérant présente une pièce d'identité, des justificatifs de domicile et de revenus, ainsi que d'autres documents. Ces documents ne font pas réellement parti du métier des cybercriminels. Une demande d'ouverture de compte bancaire implique également souvent de se présenter physiquement, une condition peu acceptable par des cybercriminels qui préfèrent la discrétion. Les cybercriminels français se contentent donc le plus souvent de fraudes qui ne requièrent aucun transfert ou service bancaire.

Cependant, certains d'entre eux devant transférer des montants importants détournés des comptes des victimes, peuvent faire appel à des pairs susceptibles d'ouvrir un compte bancaire pour eux. Ce service est facturé relativement cher, autour de 700 €, compte tenu des risques qui y sont associés.



Figure 13 : publicité pour un service d'ouverture de compte bancaire français proposé à 700 €.

À noter que des documents de formation sont proposés entre 400 et 500 € pour ceux qui veulent ouvrir un compte bancaire par eux-mêmes.

Points de permis de conduire

Le permis de conduire français est soumis à un système de points qui en assure la validité. Un jeune conducteur dispose de 6 points contre 12 pour les plus expérimentés. Les points sont déduits en cas d'infraction constatée, et selon la gravité de celle-ci.

De nombreux radars et caméras permettent de surveiller le trafic et de pénaliser les excès de vitesse et autres infractions. Mais ces radars se focalisent généralement sur la plaque d'immatriculation arrière des véhicules, ce qui ne permet pas d'identifier le conducteur avec certitude. Il devient alors possible de déduire les points de pénalité sur le permis d'un tiers, si ce permis est mentionné sur le formulaire que reçoit la personne incriminée pour régler l'amende et effectuer le retrait des points.

C'est la raison pour laquelle des cybercriminels proposent des points de permis à la vente.



Figure 14 : message d'un membre d'un marché s'interrogeant sur l'intérêt de vendre des points.

Les malware proposés au sein l'underground

Ransomware

Le ransomware (rançongiciel) est en passe de devenir la plus grande des menaces de sécurité à ce jour, si ce n'est déjà le cas. C'est la raison pour laquelle il n'est guère étonnant que des variantes de ransomware soient commercialisées au sein de l'underground français.

Nous avons identifié deux cybercriminels vendant des ransomware. Ces logiciels semblaient être conçus sur mesure pour des victimes françaises. Un des ransomware, en phase finale de développement, était présenté sous forme de copies d'écran illustrant son fonctionnement. Le rançongiciel exigeait un paiement de la rançon sous forme de Bitcoins, de carte prépayée ou de carte Paysafe.

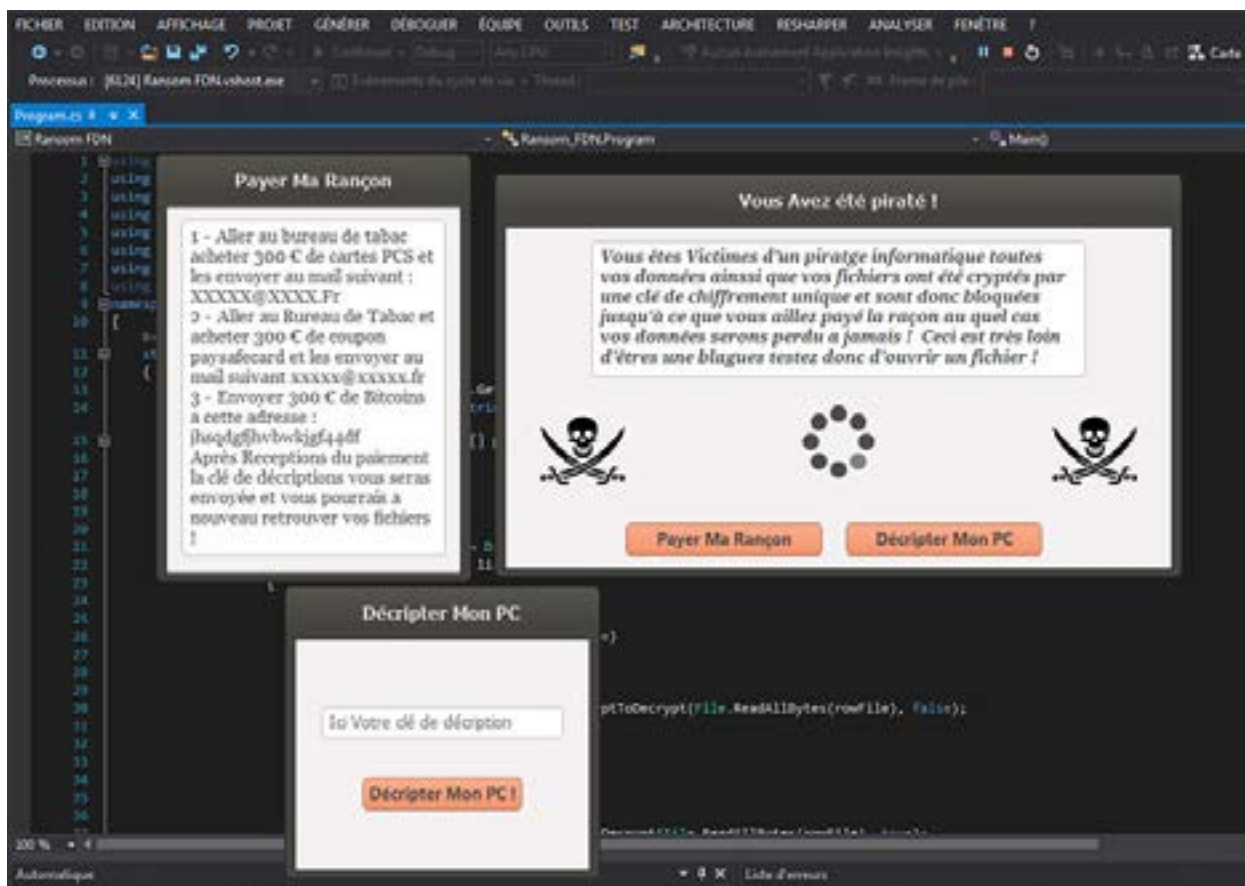


Figure 15 : copie d'écran illustrant le développement d'un ransomware français.

La seconde variante de ransomware, proposée à 100 euros, exigeait un règlement en Bitcoins.

bounty MP (0.00 %) Confirmé (0) Autres

BOUNTY

Ransomware FDN BITCOIN
Un petit RANSOMWARE pour demander des rançons en BTC à vos victimes

100.00 €
0.27346 BTC

Store

RANSOMWARE FDN FERMER

Mot de passe pour le décryptage

Selection du STUB

Votre EMAIL

Votre WALLET

Montant de la rançon

CREATION DU RANSOMWARE

Figure 16 : interface de la seconde variante de ransomware



Figure 17 : demande de rançon de la seconde variante de ransomware

Outils d'accès distant, chevaux de Troie et autres malware

Selon nos observations, la majorité des cybercriminels français se procure leurs chevaux de Troie et autres outils d'accès distants (ou RAT pour Remote Access Tools) auprès de marchés underground anglophones. Le seul outil d'accès distant "made in France", toujours utilisé à ce jour, est Dark Comet conçu par Jean-Pierre Lesueur¹⁰, connu sous le pseudo de "DarkCoderSc." DarkComet a été développé entre 2008 et 2012, avant que DarkCoderSc ne décide d'y mettre en terme, l'outil ayant été utilisé lors d'une attaque liée au conflit syrien. L'outil reste néanmoins encore disponible en ligne et utilisé par des cybercriminels, même s'il est détecté par toutes les solutions de sécurité dans sa version sans obfuscation, packaging ou chiffrement important.

Nous avons également identifié un projet en cours de conception d'un outil d'accès distant, mais ce projet apparaît lent et sans réelle orientation.

Binders de fichiers

Les cybercriminels français ont pour habitude d'utiliser des logiciels et outils malveillants achetés sur d'autres marchés underground. Certains d'entre eux, cependant, choisissent de créer et de vendre leurs propres outils, adaptés aux spécificités de l'underground français. Nous avons identifié un tel outil, un binder (outil d'obfuscation de malware, qui mixe le code du malware avec un logiciel légitime pour éviter toute détection) non commercialisé, ni distribué sur aucun forum ou place de marché.

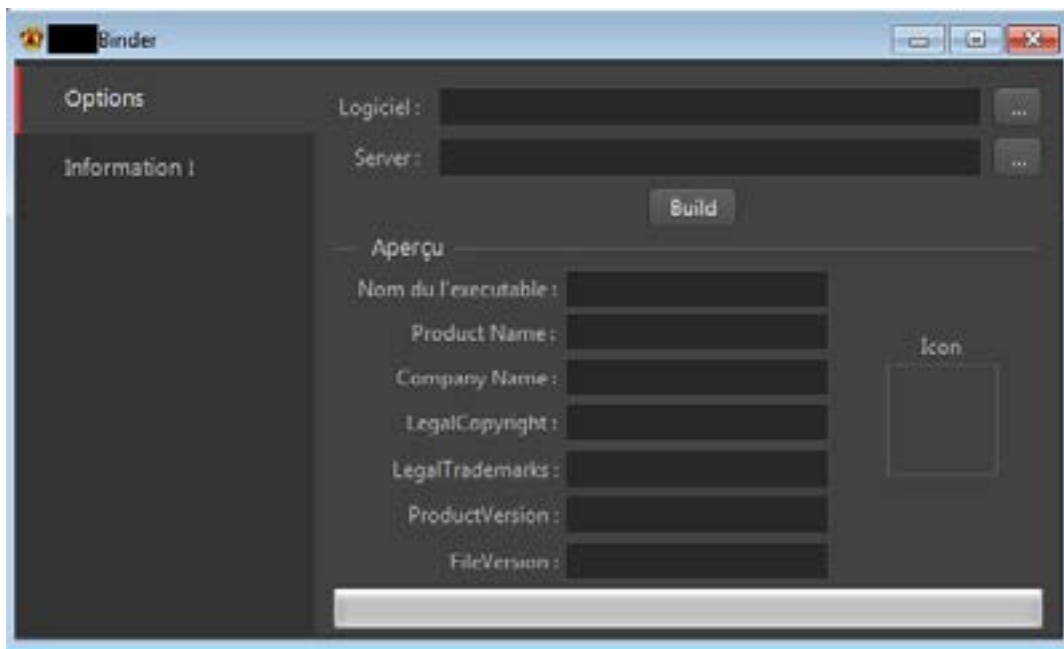


Figure 18 : binder créé par un développeur français mais qui n'est ni promu, ni vendu.

Cet outil s'avère particulièrement intéressant, puisque son concepteur est français (son nom figure dans la section d'information de l'interface utilisateur). L'interface contient également un message à l'intention de deux des connaissances du développeur, également des concepteurs français de malware. Nous pensons que ces trois développeurs utilisent l'outil en question, ainsi que quelques autres individus triés sur le volet.

Stupéfiants

À l'instar de l'underground cybercriminel nord-américain, le trafic de drogue va bon train au sein de l'underground français. Le cannabis ou le hachisch se vend entre 6 et 15 € le gramme, selon sa qualité et son origine. Sont également vendus : cocaïne, héroïne, MDMA, ecstasy, LSD et autres champignons. Les dealers de drogue ne vendent néanmoins qu'au sein du pays, une précaution qui évite de se faire détecter lors des transactions transfrontalières.

LES CONDITIONS

- Steath Impeccable** - Brise vue + garantie sans odeurs ni molécules
- Envoie Lettre prioritaire** - Pour mon anonymat - LP J+1 - Pas de refund
- Escrow accepté** - Je ne suis pas garant de votre drop - Envoyé, c'est payé
- Envoi à partir de France vers routes destinations**
- PCS acceptés** - Je passe par un échangeur dont voici les tarifs :
 - Coupons jusqu'à 100 € = + 20% sur le prix en Btc
 - Coupons de plus de 100€ = + 15% sur le prix en Btc

LES PRIX

1/2 G Pour 45€ (90€/g)	3 G Pour 225€ (75€/g)
1 G Pour 80€ (80€/g)	4 G Pour 295€ (74€/g)
2 G Pour 155€ (77€/g)	5 G Pour 365€ (73€/g)
10 G Pour 700€ (70€/g)	
20 G Pour 1300€ (65€/g)	

Pour de plus grosses quantités, merci de me contacter par MP chiffré PGP.

Logos: bitcoin, ESCROWOK, PCS

Images: Three photographs showing white crystalline substances (cocaine) on a red surface, with a German flag and a coin visible in the background of each photo.

Figure 19 : publicité pour de la cocaïne

Contrairement aux autres pays, les drogues récentes de type « sels de bains » et nouvelles substances psychoactives ne sont pas disponibles au sein de l'underground français, à la date de rédaction de ce document.

Autres produits et services illicites

Les numéros de cartes de paiement, informations personnelles et documents d'identification sont également proposés à la vente dans des autoshops. Un fichier de base de données complète se négocie à environ 400 €.

Pricing Plans

CC FR CLASSIC	CC FR GOLD/1ER	CC FR PREMIUM
✓ 20 EUROS / CARTE	✓ 25 EUROS / CARTE	✓ 30 EUROS / CARTE
✓ basic support	✓ priority support	✓ priority support
BUY NOW	BUY NOW	BUY NOW

Payment Methods

- J'accepte uniquement le BTC comme moyen de payement
- Pour me contacter, merci d'utiliser PGP, vous pouvez trouvez ma clé public sur ma page de profil directement

Figure 20 : publicité pour des données volées de carte de paiement



AUTO'SCAN v3

- Documents d'identité
- Justificatif de domicile *New*
- Fiche de Paie
- Carte Bancaire
- Brevet d'Identité Bancaire
- Autres documents *New*
- Mon Panier

Bienvenue sur Auto'Scan : Générateur de documents FR et étrangers.

... toujours en ligne

Effet Scan-impression *

Nom * : DESMOULINS

Prénoms (s) * : JACQUES
Séparez les prénoms avec une virgule

Sexe * : Homme

Taille (en cm) * : 180

Date de naissance * : 10/11/1976

Ville de naissance * : NANCY (54)



SAMPLE

Figure 21 : publicité d'Auto'Scan v3 (autoshop) pour des scans de qualité de fausses cartes d'identité.

Le tableau suivant répertorie les produits et services illicites commercialisés au sein de l'underground français :

Produit/Service	Tarif
Service de chiffrement indétectable	4 – 100 €
Hébergement de type Bulletproof	10 €
Kit de phishing	100 – 500€
Page de phishing	5 €
Service de création d'un site de phishing	299 €
Location de réseau botnet (100–150 bots/jour)	95 €
Carte d'identité nationale falsifiée	60 €
Carte PMR (Personne à Mobilité Réduite) falsifiée	40 €
Pack de documents falsifiés (carte d'identité et justificatifs d'identité)	50 –100 €
Papier Teslin (utilisé pour créer des cartes nationales d'identité, 200 feuilles)	167 €
Service de retouche de document PDF, avec modification de données	8 €
Faux billets (300€ en billets de 20)	135–150 €
Faux chèques avec bénéficiaire spécifique (10 chèques)	70–100 €
Logs comprenant des sites Web vulnérables (100 sites vulnérables à l'injection SQL)	30 €
Accès à un site Web vulnérable	1–2 €
Service d'analyse de vulnérabilités logicielles (analyse du code source)	219 €
Données de cartes de paiement volées (dépend de la limite et du solde)	9–23 €
Skimmer de distributeur de billets	800 €
Clonage de carte de paiement (selon le seuil)	40–110 €
Accès à un compte Paypal piraté	5–10 €
Accès à un compte Amazon piraté	10 €


Produit/Service	Tarif
Carte cadeau falsifiée	50% de la valeur de la carte
Accès à un compte Facebook piraté	0,50 €
Accès à un compte Gmail/webmail français, Spotify ou Netflix piraté	1 €
Accès à un compte Leboncoin, Wi-Fi d'un FAI, Cdiscount, Pixmania, LDLC, Zalando, Auchan ou 3Suisses	2 €
Accès à un compte PlayStation piraté (+ 20 jeux)	3 €
Fichier de base de données piraté	400 €
Fichiers de configuration de sites bancaires volés	50 €

Tableau 1 : liste de produits/services vendus au sein de l'underground français

L'underground français, à l'image de ses homologues de pays tiers, compte de nombreux novices et nouveaux arrivants. De nombreux cybercriminels proposent à la vente des tutoriels et kits de formation. Le tableau suivant indique le tarif de ces documents :

Sujet du tutoriel ou document de formation	Tarif
Ouverture d'un compte bancaire dans le cadre d'une fraude	450 €
Comment convertir le solde de cartes de crédit en bitcoins	250 €
Fraude à la carte bancaire	29 – 150 €
Comment convertir un solde Paypal en bitcoins	100 €
Injection SQL	60 €
Comment monétiser l'accès à des comptes Paypal piratés	60 €
Affiliation et cybercriminalité : comment ça marche	30 €
Comment obtenir un nombre illimité de remboursement sur Amazon	25 €
Comment utiliser un outil d'accès distant ?	20 €
Comment envoyer et recevoir des produits et paiement illicites de manière anonyme ?	10 €
Comment propager un malware ?	2 €

Tableau 2 : tutoriels et kits de formation et leurs prix

A dark, grainy black and white photograph of an industrial interior. The scene is dimly lit, with a prominent glowing circular light effect in the center. The word "Conclusion" is centered in the middle of the image. The background shows structural elements like beams and a window with multiple panes. A bright light source is visible in the upper right corner. The overall atmosphere is somber and industrial.

Conclusion

Conclusion

Alors que l'underground français n'est pas comparable à ses homologues étrangers en termes de taille et de puissance, son offre spécifique en fait néanmoins une niche très particulière de l'économie cybercriminelle. Après tout, il n'existe aucun autre marché offrant des outils et services répondant parfaitement aux spécificités françaises.

Le climat de méfiance qui rend les acteurs de l'underground français particulièrement précautionneux et furtifs, est un défi pour les forces de l'ordre et les fournisseurs de solutions de sécurité. Nous avons cependant pu identifier des schémas spécifiquement français utilisés par les cybercriminels, ce qui est un bon début. Les informations de veille recueillies lors de nos plongées dans les territoires cybercriminels peuvent aider les forces de l'ordre et le législateur à pallier certaines faiblesses de l'arsenal de défense physique, logiciel et réglementaire. Seule une collaboration continue entre les acteurs de la sécurité et les forces de l'ordre permettra de sécuriser davantage l'univers des échanges numériques.

Références

1. Kyle Wilhoit et Stephen Hilt. (7 décembre 2015) *Trend Micro Security News*. “North American Underground: The Glass Tank.” consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/north-american-underground-the-glass-tank>.
2. Trend Micro Incorporated (1 Mars 2016). *Trend Micro Security News*. “Cybercrime and the Deep Web.” Consulté le 21 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercrime-and-the-deep-web>.
3. Max Goncharov. (28 juillet 2015). *Trend Micro Security News*. “Russian Underground 2.0.” Consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools>.
4. Forward-Looking Threat Research (FTR) Team. (8 décembre 2015). *Trend Micro Security News*. “U-Markt: Peering into the German Cybercriminal Underground.” Consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/u-market-the-german-cybercriminal-underground>.
5. Lion Gu. (23 novembre 2015). *Trend Micro Security News*. “Prototype Nation: The Chinese Cybercriminal Underground in 2015.” Consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/prototype-nation-the-chinese-cybercriminal-underground-in-2015>.
6. Trend Micro Incorporated (14 juin 2016). *Trend Micro Security News*. “Ransomware 101: What, How, and Why.” Consulté le 21 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works>.
7. Olivier Dumons et Yves Eudes. (1er octobre 2015). *LeMonde.fr*. “Plusieurs Sites de Vente de Drogue du «Deep Web» Français Piratés” Consulté le 17 juin 2016, http://www.lemonde.fr/pixels/article/2015/10/01/plusieurs-sites-de-vente-de-drogue-du-deep-web-francais-pirates_4780425_4408996.html.
8. FTR Team. (12 janvier 2016) *Trend Micro Security News*. “Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015.” Consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-cybercriminal-underground-2015>.
9. Akira Urano. (13 octobre 2015). *Trend Micro Security News*. “The Japanese Underground.” Consulté le 15 juin 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-japanese-underground>.
10. Sylvia Edwards Davis. (30 septembre 2014). *French Entrée*. “Driving Licence in France FAQ.” Consulté le 15 juin 2016, <https://www.frenchentree.com/living-in-france/driving/driving-licence-faq/>.
11. BBC. (10 juillet 2015). *BBC News*. “Spy Code Creator Kills Project After Syrian Abuse.” Consulté le 16 juin 2016, <http://www.bbc.com/news/technology-18783064>.

Un rapport proposé par

TrendLabs

Le centre mondial de support technique et de R&D de TREND MICRO

Trend Micro™

Fort de 27 ans d'expérience, Trend Micro Incorporated (TYO: 4704; TSE: 4704) compte parmi les leaders mondiaux des solutions de sécurité et continue d'innover afin de sécuriser les échanges d'informations numériques de ses clients. Nos solutions pour le grand public, les entreprises et les organisations gouvernementales, déploient une sécurité multicouche permettant de protéger les informations sur les équipements mobiles, les Endpoints, les passerelles, les serveurs et le Cloud. Trend Micro concrétise une protection évoluée des données, grâce à des technologies simples à déployer et à gérer, et s'adaptant à un environnement évolutif. Toutes nos solutions sont optimisées par notre infrastructure Cloud de renseignements sur les menaces Smart Protection Network™ (SPN), et sont prises en charge par plus de 1 200 chercheurs en sécurité à travers le monde.



Securing Your Journey
to the Cloud

www.trendmicro.com