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

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES

DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Importation de véhicules de luxe de l'Allemagne vers Nice : Une fraude à la TVA de 3,2M€ découverte

Six personnes de la région de Nice ont été mises en examen dans une affaire de fraude à la TVA sur des voitures allemandes importées en France via le site Le Bon Coin. Le préjudice est estimé à 3,2 M€.

Trois protagonistes de cette fraude ont été écroués jeudi dernier et trois autres placés sous contrôle judiciaire, a précisé Eric Antonetti, chef du groupe d'intervention régional (GIR) de Paca.

Ce système de fraude est assez répandu. Les garages allemands acceptent régulièrement un paiement en liquide à condition d'avoir un numéro de société en France.

"Ils payaient en liquide des véhicules dans ce pays en créant des sociétés éphémères et empochaient le montant de la TVA, soit 20% sur chaque transaction, en revendant ces voitures", a indiqué une source policière à Metronews.

Un blanchiment d'argent pour du trafic de stupéfiants?

Le groupe de fraudeurs mis en examen la semaine dernière avait ainsi créé huit sociétés en l'espace d'un an gérées notamment par des hommes de paille connus pour trafic de stupéfiants.

Ces sociétés ont enregistré quelque 16 millions d'euros d'achats de véhicules à prix imbattables, représentant une fraude à la TVA de 3,2 millions d'euros, précise le commissaire qui a enquêté en collaboration avec les douanes de Nice.

L'origine des paiements est indéterminée. Or *"ce système est très pratique pour blanchir l'argent de trafics de stupéfiants"*, a souligné Eric Antonetti.

Lien : **http://www.nicematin.com/faits-divers/importation-de-vehicules-de-luxe-de-lallemagne-vers-nice-une-fraude-a-la-tva-de-32m-decouverte-15347**

Trafic de stupéfiants et blanchiment d'argent : Plus d'un million d'euros saisis

Dix-sept personnes ont été interpellées mercredi en France et trois autres en Suisse dans le cadre du démantèlement d'un réseau de blanchiment lié à un trafic de stupéfiants. Le butin saisi lors des perquisitions est impressionnant : plus d'un million d'euros en espèces. Le réseau aurait déjà importé en France plus de huit tonnes de cannabis.

Les autorités ont procédé à 17 interpellations en France. Le réseau démantelé mercredi était spécialisé dans l'importation de cannabis en Europe puis dans le blanchiment de l'argent tiré de la revente.

Un butin impressionnant

Les perquisitions ont été fructueuses et le butin saisi est considérable : Plus d'un million d'euros en espèces, 2.800 dollars six, lingots d'or (d'une valeur à l'unité de 41.000 euros), deux photos d'art d'une valeur d'un million d'euros.

Plus d'une centaine d'enquêteurs étaient mobilisés mercredi dans le cadre de cette enquête.

Des interpellations et des biens saisis en Suisse

Parallèlement, en Suisse, trois responsables présumés du réseau de blanchiment ont été interpellés en présence de policiers français. Et en Suisse aussi, les biens saisis sont nombreux : un million de francs suisses en espèces, 160 montres de collection, pour une valeur estimée à deux à trois millions de francs suisses, une quantité importante de bijoux de luxe

Une enquête initiée il ya plusieurs mois

Le parquet de Paris s'est saisi en avril d'une enquête initiée deux mois plus tôt à Nanterre portant sur un vaste trafic d'importation de cannabis entre le Maroc, l'Espagne et la région parisienne.

L'enquête a permis de découvrir que ce réseau avait déjà importé plus de huit tonnes de cannabis en France, pour une valeur à la revente de 40 millions d'euros. Le produit des ventes était réinjecté dans une machinerie complexe de blanchiment d'argent.

Selon le parquet, *"les flux financiers sont considérables : il apparaît qu'uniquement entre mai et octobre 2012, près de 12 millions d'euros ont ainsi été collectés"* dans le cadre de ce réseau d'une *"ampleur inédite»*.

Les gardes à vue peuvent durer 96 heures, à l'issue desquelles les suspects pourraient être déférés devant le juge d'instruction en vue d'une mise en examen éventuelle.

Lien : http://www.francetvinfo.fr/societe/justice/trafic-de-stupefiants-et-blanchiment-d-argent-plus-d-un-million-d-euros-saisis_1630471.html

Les "banquiers" des stups dans les filets de la PJ

En matière de lutte contre la drogue, les saisies d"espèces sont monnaie courante, si l'on ose dire. Cette fois cependant, la police judiciaire peut se targuer d'avoir raflé la banque. Où l'on retrouve une "sainte" alliance devenue un classique des réseaux criminels, la jonction entre un milieu maghrébin spécialisé dans le commerce du cannabis d'origine marocaine et un milieu juif versé dans la finance internationale opaque.

Partie d'un gros trafiquant de cannabis de la région parisienne, plus précisément de Mantes-la-Jolie, un homme d'origine marocaine soupçonné de brasser la marchandise à la tonne, l'enquête a rapidement mis les policiers de l'office central de répression du trafic de stupéfiants sur la piste d'un important collecteur de fonds. Un "banquier" occulte membre d'une fratrie implantée depuis des années à Genève, où deux de ses frères ont pignon sur rue sous la bannière d'importantes banques de la place.

La lessiveuse mise à jour par les enquêteurs de l'office central de répression de la grande délinquance financière (OCRGDF) fonctionnait de manière assez simple. Les bénéfices du trafic étaient distribués à des commerçants installés ayant fortement besoin d'argent en espèce pour faire tourner leur "boutique". Parmi eux, des rois de la confection, des entrepreneurs du BTP, mais aussi un architecte, un avocat parisien,... et une élue verte parisienne, tous suspectés aujourd'hui de blanchiment d'argent. Tous devaient disposer d'un compte en banque en Suisse, où l'argent refaisait surface. Il ne

restait plus au "banquier" qu'à expédier les fonds vers la Grande Bretagne, d'où ils revenaient entre les mains du dealer, prêts à être réinvestis dans le trafic.
Côté suisse, une véritable salle de coffre clandestine a été découverte, une caverne d'Ali Baba versions stups dans laquelle étaient entreposés lingots d'or, bijoux, montres, pour une valeur qui pourrait atteindre les 10 millions d'euros. Une prise sans précédent dans une affaire qui devrait faire exploser le compteur des saisies d'avoirs criminels, sans compter les millions d'euros que ne manquera pas de réclamer le fisc aux "honnêtes" entrepreneurs suspectés d'avoir contribué à blanchir cet argent (dont ils se défendent de connaitre l'origine criminelle, à l'instar de l'élue parisienne, dont l'avocat dénie toute participation à un réseau de blanchiment).
Lien : **http://www.marianne.net/fredericploquin/Les-banquiers-des-stups-dans-les-filets-de-la-PJ_a95.html**

Europol : Arrestation du gang derrière les trojans bancaires ZeuS et SpyEye

Les services de police de six pays européens différents ont mis fin aux activités illicites d'un gang ukrainien de cybercriminels soupçonnés du développement**,** de la distribution et du déploiement des malwares bancaires Zeus et SpyEye.
Selon le rapport sur le site officiel d'Europol, les autorités ont arrêté cinq suspects entre le 18 et le 19 juin, tous membres présumés d'un gang de cybercriminels accusé d'avoir infecté des dizaines de milliers d'ordinateurs dans le monde avec des logiciels malveillants et des chevaux de Troie bancaires.
Le groupe cybercriminel présumé aurait distribué et utilisé les malwares bancaires Zeus et SpyEye dans le but de voler de l'argent à plusieurs grandes banques en Europe et à l'extérieur. Le gang a constamment modifié ses chevaux de Troie afin de passer outre les protocoles de sécurité des banques et ont utilisé massivement des réseaux de "mules" à des fins de blanchiment d'argent.
"Sur les forums undergrounds spécialisés, ils ont activement vendu des informations bancaires piratées et des logiciels malveillants", a déclaré jeudi Europol dans un communiqué, *"tout en vendant des services de piratage et étant à la recherche de nouveaux partenaires pour facilité la coopération dans d'autres activités cybercriminelles annexes."*
Chaque cybercriminel du groupe présumé avait sa propre spécialité. En outre, le gang a été impliqué dans le développement de logiciels malveillants infectant spécifiquement les terminaux de paiement commerciaux et le piratage de services de location dédiés aux fraudeurs en ligne (sur le Deep Web principalement).
Plus de 2 millions d'euros en dommages et intérêts
Selon les responsables, le gang aurait causé des dommages financiers estimés à plus de 2 millions d'euros. L'opération a été menée par l'équipe d'enquête conjointe (JIT), et faisait partie d'une initiative lancée par Europol durant l'année 2013, qui a abouti à 60 arrestations à ce jour.
Il y a deux mois, les autorités ont mis à terme au botnet BeeBone, qui avait infecté plus de 12 000 ordinateurs dans le monde. En outre, l'initiative en cours a entraîné la chute du botnet Ramnit, responsable à lui seul de plus de 3,2 millions d'infections d'ordinateurs dans le monde entier.
L'année dernière, le FBI et Europol ont démantelé le botnet Zeus GameOver, même si ce dernier a pu revenir un mois après.

Lien : https://www.undernews.fr/malwares-virus-antivirus/europol-arrestation-du-gang-derriere-les-trojans-bancaires-zeus-et-spyeye.html

Caution de 500.000 euros payée en liquide : L'individu interpellé

Medhi B., mis en examen pour trafic de stupéfiants, a été arrêté dans la nuit de jeudi à vendredi sur l'A48 par les policiers de la brigade anticriminalité de Grenoble, rapporte "Le Dauphiné".

Fin de cavale pour Medhi B. Ce Grenoblois de 31 ans, mis en examen notamment pour trafic de stupéfiants, a été arrêté dans la nuit de jeudi à vendredi sur l'A48 par la brigade anticriminalité de Grenoble, rapporte *Le Dauphiné*. L'homme avait été libéré après avoir payé une caution de 500.000 euros en liquide avant finalement de faire l'objet d'un mandat d'arrêt européen.

Une interpellation sans incident. L'individu se trouvait à bord d'un voiture avec deux jeunes filles lorsqu'il a été repéré par les policiers. Ces derniers ont dû faire usage d'un stop-stick (une barre qui permet d'intercepter le véhicule) mais l'interpellation s'est déroulée sans incident.

Du blanchiment d'argent pour payer la caution ? Originaire du quartier Mistral à Grenoble, cet homme de 30 ans est mis en examen pour trafic de stupéfiants, association de malfaiteurs et blanchiment en bande organisée. Ses avocats avaient réclamé une remise en liberté à quelques mois de son procès, fixé à septembre.

Le 27 mai, la justice avait donné son aval à la condition dissuasive qu'il verse une caution de 500.000 euros. Quelques jours plus tard, 29 personnes s'étaient présentées à la régie du tribunal de grande instance de Lyon avec des sommes de 7.000 à 70.000 euros en billets de 500, le parquet décidant alors d'ouvrir une enquête pour blanchiment d'argent.

Une décision "incompréhensible" selon les avocats. Le parquet avait également fait appel de la décision de le libérer. La cour d'appel lui a donné raison, estimant que les faits qui lui sont reprochés sont suffisamment graves pour qu'il reste en prison en attendant son procès. Un mandat d'arrêt a donc été émis à son encontre. Sa cavale a pris fin cette nuit.

Lien : http://www.europe1.fr/faits-divers/caution-de-500-000-euros-payee-en-liquide-lindividu-interpelle-2814145

Comment le rêve de l'argent facile se termina en fiasco

L'un des plus gros scandales financiers de Suisse sera traité dès lundi par le Tribunal pénal fédéral. Le jongleur de la finance bâlois Dieter Behring comparaît pour escroquerie et blanchiment d'argent. Quelque 2000 épargnants de Suisse et de l'étranger auraient été lésés de 800 millions de francs au total. Le prévenu nie les accusations.

Régulièrement, les épargnants rêvent d'argent facilement gagné. Et régulièrement, des financiers réussissent à les attirer avec de belles promesses. Ainsi, à la fin des années 1990, Dieter Behring est célébré comme un gourou de la bourse et un jongleur de la finance. Cet ancien laborantin en chimie se vante d'avoir déchiffré le «code génétique» des marchés financiers.

Apparemment, il réussit là où peu d'autres réussissent, à savoir faire fructifier des avoirs grâce à des placements à faible risque sur les marchés financiers, tout en générant de hauts rendements. Des milliers de clients mordent à l'hameçon. Mais en 2004, le système Behring, ou plus précisément le «système commercial Behring», ainsi que le qualifie l'acte d'accusation du Ministère public de la Confédération, s'effondre.

C'est sur cet acte d'accusation que se baseront les débats contre Dieter Behring devant le Tribunal pénal fédéral. L'ex-financier âgé aujourd'hui de 61 ans est accusé d'escroquerie par métier et de blanchiment d'argent qualifié. Le procès débute ce lundi 30 mai.

Une longue enquête

Soupçonné d'escroquerie, Dieter Behring a été arrêté en 2004 déjà et a passé environ six mois en détention préventive. Grâce à une caution d'un million de francs, il a pu sortir de prison, mais a dû déposer son passeport. Ont suivies de longues investigations sur un dossier extrêmement compliqué, qui ont duré onze ans.

Le Ministère public de la Confédération s'est retrouvé sous pression, le délai de prescription étant de 15 ans seulement pour certains délits. De leur côté, de nombreuses personnes lésées étaient désespérées, car elles avaient perdu beaucoup d'argent, certaines même toute leur fortune, des petits épargnants comme de gros investisseurs.

Dans l'acte d'accusation, qui compte 84 pages, le système Behring est décrit de façon minutieuse. Selon l'accusation, l'ex-financier promettait des gains assurés et durables grâce à un «logiciel conçu pour les marchés financiers».

«Une construction virtuelle»

Toutefois, il semble que l'ex-gourou de la bourse utilisait l'argent que lui confiaient les épargnants et les intermédiaires surtout pour boucher les trous de son système financier, un genre de système boules de neige. «Incontrôlé, arbitraire et illégal», estime Tobias Kauer, le procureur de la Confédération en charge du dossier. Selon lui, il s'agissait d'une «construction virtuelle exploitée à travers un système de répartition».

Quelque 2000 personnes auraient été lésées entre 1998 et 2004; la somme totale escroquée est énorme: plus de 800 millions de francs, selon le Ministère public, alors que Dieter Behring aurait pour sa part encaissé des centaines de millions de francs.

Dieter Behring se rendait également à l'étranger pour attirer les épargnants; il faisait des présentations dans des hôtels de luxe à Buenos Aires, Miami, Londres et Santo Domingo. Lors de ses exposés, il utilisait sciemment le drapeau suisse et des photos en lien avec la Suisse dans le but de donner une impression sérieuse, selon le Ministère public.

Des montres chères et des grands vins

En tous les cas, Dieter Behring ne se privait visiblement de rien. Sa société QED Consulting AG, du groupe Moore-Park, d'abord sise à Riehen (BL), élit ensuite domicile en ville de Bâle dans un immeuble qu'il acquiert pour 30 millions de francs. L'homme aimait également les montres de luxe et les bijoux. C'est en tout cas ce qu'il ressort du chapitre consacré au blanchiment d'argent dans l'acte d'accusation.

Il en achète pour 5,3 millions de francs. A cela s'ajoutent 170'328 francs dépensés en bons vins, afin de satisfaire «son plaisir coûteux de collectionneur et de bon vivant». Etant donné que Dieter Behring devait savoir que ses revenus étaient issus d'activités délictuelles, il s'agit donc pour le Ministère public d'un cas évident de blanchiment d'argent. En outre, l'ex-financier se versait des salaires nets allant de 328'000 (2011) à 627'000 francs (2003).

Le prévenu rejette les accusations

L'accusé, qui habite depuis dans un village du canton d'Argovie, rejette catégoriquement la présentation des faits de l'accusation. Il rend les intermédiaires responsables de l'effondrement de son système. Sur sa page web, avec son épouse Ruth, Dieter Behring regrette «profondément les grosses pertes essuyées par les personnes lésées par Moore Park», mais ajoute: «Nous aussi nous avons perdu tout ce que nous avions construit au cours des dernières décennies».

Et il poursuit: «Contrairement à tous les préjugés et les accusations véhiculés par les médias, mais aussi malheureusement par les enquêteurs, nous avons la conscience tranquille et nous mettrons tout en œuvre pour apporter la lumière dans cette catastrophe sombre et compliquée».

Le procès doit durer jusqu'au 1er juillet 2016, avec des interruptions. La lecture du jugement est prévue pour le 30 septembre. La Cour sera constituée de trois juges et présidée par Daniel Kipfer, le président du Tribunal pénal fédéral.

Lien : http://www.swissinfo.ch/fre/economie/le-financier-dieter-behring-devant-la-justice_comment-le-r%C3%AAve-de-l-argent-facile-se-termina-en-fiasco/42176192

Aéroport Roland Garros
Un imam de Mayotte voyageait avec 54 000 euros en liquide

La somme non déclarée a été consignée par la Douane et l'homme laissé en liberté

Un imam de Mayotte a été intercepté par les douaniers à l'aéroport Roland Garros ce lundi 22 août 2016. Il transportait 54 000 euros en espèces sans avoir fait aucune déclaration aux Douanes, ce qui est interdit. La somme a été consignée par les Douanes. L'homme, qui a déclaré être en route pour un pèlerinage à la Mecque, a été laissé en liberté. Il a quitté La Réunion. "Le procureur n'a pas été prévenu car il n'y avait pas de souci de blanchiment d'argent" déclare la Douane interrogée par Imaz Press Réunion. "Nous poursuivons les investigations pour connaître la provenance de l'argent" ajoute la Douane**.**

Lorsqu'il a été intercepté par les douaniers, l'homme a déclaré que l'argent allait servir à payer son voyage et son séjour à la Mecque dans le cadre du hadj, le pèlerinage annuel des Musulmans sur les lieux saints de l'islam.

En transportant cette somme, "la personne a commis un manquement à l'obligation déclarative des devises et valeurs" explique la Douane à Imaz Press Réunion avant de rappeler qu'aux termes de la loi "toute personne transportant des sommes (espèces, chèques, actions…) et valeurs d'un montant égal ou supérieur à 10 000 euros est tenue de les déclarer aux Douanes à son arrivée où à son départ du territoire" français.

Après avoir intercepté le voyageur - en provenance de Mayote après avoir transité par Maurice, semble-t-il -, les douanes ont cherché à savoir si cet important transport de fonds en liquide pouvait être lié à une tentative de blanchiment d'argent. Cela n'a pas été établi, et "nous n'avons pas prévenu le procureur de la République et nous avons laissé la personne en liberté après avoir consigné la totalité des 54 000 euros" déclare la Douane avant d'ajouter que le mis en cause "a quitté La Réunion pour aller faire son pèlerinage"

L'administration douanière précise toutefois qu'elle poursuit son enquête afin de déterminer la provenance de l'argent. Quant à savoir quelle action sera possible contre le voyageur si une origine frauduleuse des fonds est établie, la Douane répond : "tous les signalements nécessaires seront alors faits et l'on se chargera de les diffuser"

Lien : http://www.ipreunion.com/actualites-reunion/reportage/2016/08/24/la-somme-non-declaree-a-ete-consignee-par-la-douane-aeroport-roland-garros-un-iman-de-mayotte-voyageait-avec-54-000-euros-en-liquide,48827.html

Pirates informatiques
Multiples arrestations dans l'underground français

La période semble propices aux autorités françaises. En effet, de multiples arrestations concernant des cybercriminels ont eu lieu sur le territoire. Parmi les pirates informatiques, on retrouve entre autre des carders, des skimmers et des spécialistes du phishing.

La première arrestation a eu lieu en Haute-Marne, grâce à ce que l'on peut appeler de la chance : lors d'un banal contrôle routier, les gendarmes ont mis la main sur du matériel permettant de piéger les distributeurs automatiques de billets dans le but de copier les données des cartes bancaires et d'intercepter le code PIN secret des utilisateurs à leur insu.

Tout l'arsenal de skimming était caché dans la voiture contrôlée, avec à son bord, deux ressortissants bulgares âgés d'une quarantaine d'années. D'après l'Est Républicain, les deux présumés pirates auraient commis leur méfait en Franche-Comté vers fin février 2014. Au total, 100 000 euros auraient été détournés via six banques basées à Besançon, Saint-Vit et Dole durant leur campagne malveillante. Les clones des cartes bancaires ainsi interceptées ont été utilisés en Bulgarie et au Vietnam.

Bonne prise direz-vous mais ce n'est pas tout ! Plusieurs autres pirates français ont été arrêtés, un à un depuis fin avril. Citons par exemple le pirate Downi, un jeune internaute accusé d'avoir piraté des bases de données de sites Web et réalisé du carding et de la fraude bancaire en ligne. Les autorités en ont profité pour appréhender tous ses complices dans la foulée, ces derniers l'aidant à blanchir l'argent et à gérer les diverses opérations. Le montant de la fraude présumée n'a pas été divulgué.

Idem pour H0udini_r.u, un jeune internaute connu par les autorités pour des faits de piratage informatique, fraîchement sorti de deux semaines de détention à l'EPM, un établissement pénitentiaire pour mineurs basé dans les Yvelines. La aussi, le motif est la fraude bancaire, et le vol entre autres, de 950 euros sur un compte bancaire français.

Lien : https://www.undernews.fr/hacking-hacktivisme/pirates-informatiques-multiples-arrestations-dans-lunderground-francais.html

Le FBI démantèle un énorme botnet piloté par un hacker russe

La justice américaine a donné un coup fatal à un gang de pirates qui a siphonné plusieurs dizaines de millions de dollars par des virements frauduleux, réalisés grâce à des données bancaires subtilisées par le virus « Gameover ZeuS ».

L'opération avait pour nom de code « Tovar » et s'est soldée par la mise à mort de l'un des plus importants réseaux botnet de la planète. Hier, lundi 2 juin, le ministère américain de la Justice a annoncé le démantèlement d'un réseau de pirates informatiques, qui a dérobé plusieurs millions de dollars à des entreprises et à des consommateurs au moyen d'ordinateurs infectés dans une dizaine de pays.

« Gameover Zeus est le réseau le plus sophistiqué que le FBI et nos alliés ont jamais tenté de démanteler », a déclaré Robert Anderson, haut responsable de la police fédérale, lors d'une conférence de presse à Washington.

Le virus « Gameover Zeus », apparu en septembre 2011, avait pour principal objectif de voler les informations bancaires et autres données confidentielles sur des disques durs infectés. D'après les enquêteurs du FBI, il serait responsable de plus de 100 millions de dollars de pertes après avoir infecté entre 500.000 et un million d'ordinateurs dans le monde, dont un quart aux Etats-Unis. Son administrateur, le Russe Evgeniy Mikhailovich Bogachev, 30 ans, a été inculpé par un grand jury de Pittsburgh, en Pennsylvanie (est), de piratage informatique, fraude financière et bancaire, et blanchiment d'argent.

Le ministère de la Justice a en outre annoncé le démantèlement d'un autre virus informatique, baptisé « Cryptolocker », apparu en septembre 2013, qui cryptait les ordinateurs de ses victimes et exigeait une rançon en échange des mots de passe permettant d'en libérer à nouveau l'accès. La rançon dépassait souvent les 700 dollars par victime, portant à plus de 27 millions de dollars les sommes ainsi dérobées en deux mois d'activité sur plus de 234.000 ordinateurs infectés. Le virus était en général contenu dans un courriel prétextant délivrer un message audio ou la confirmation d'une livraison.

Dans ce cas aussi, Bogachev, identifié par les surnoms « Slavik » ou « Pollingsoon », est accusé d'avoir orchestré cette vaste escroquerie informatique, selon une plainte déposée dans le Nebraska (centre). *« Bogachev et les membres de son réseau ont inventé et perpétré le type de cybercrimes auxquels vous ne croiriez pas dans un film de science-fiction »*, a déclaré Leslie Caldwell, procureure générale adjointe.

Comment les services gouvernementaux ont-ils procédé pour démanteler ces deux réseaux ? Le 7 mai, le FBI a pu saisir à Donetsk et Kiev, avec l'aide des autorités ukrainiennes, des serveurs dits de « commande et contrôle ». Ce qui leur a permis d'identifier le cerveau de toutes ces opérations et de préparer le démantèlement d'un point de vue technique et juridique. Le week-end dernier, les enquêteurs américains ont alors infligé le coup fatal.

En quelques jours, des serveurs ont été saisis dans sept pays avec l'aide des forces de police locales : Canada, France, Allemagne, Luxembourg, Pays-Bas, Ukraine et Royaume-Uni. Parallèlement, plus de 300.000 ordinateurs zombies ont été identifiés et « libérés ». En effet, les forces de police ont fait en sorte que les logiciels malveillants ne communiquent plus avec les serveurs encore sous contrôle des cybercriminels, mais soient redirigés vers une infrastructure mise en place par la justice américaine.

Ont également participé à l'opération le Centre européen du cybercrime (EC3), ainsi que des acteurs du secteur privé, comme Dell, Microsoft, Afilias, Deloitte ou encore Symantec.

Des criminels de haut vol

L'acte d'accusation rédigé par la justice américaine montre que Bogachev et ses complices étaient loin d'être des petites frappes, mais un gang professionnel qui n'avait peur de rien. Les données financières récupérées grâce à « Gameover Zeus » leur ont permis de siphonner 7 millions de dollars auprès d'une banque de Floride du Nord. Deux entreprises américaines ont perdu, chacune, environ 190.000 dollars à la suite d'un virement frauduleux. Ils ont même dépouillé une tribu indienne dans l'état de Washington, qui a vu disparaître 277.000 dollars de son compte en banque.

Lien : http://www.01net.com/actualites/le-fbi-demantele-un-enorme-botnet-pilote-par-un-hacker-russe-620980.html

Cybercriminalité : 3 millions de dollars de récompense pour retrouver Evgueni Mikhaïlovitch Bogachev

Evgueni Mikhaïlovitch Bogachev est recherché par le FBI, qui offre jusqu'à trois millions de dollars de récompense pour le retrouver. Il est considéré comme l'un des plus importants cybercriminels en activité.

Evgueni Mikhaïlovitch Bogachev, un cybercriminel russe activement recherché

Le FBI est à la recherche de l'un des plus importants cybercriminels en activité et offre jusqu'à trois millions de dollars de récompense pour le retrouver ou disposer d'informations permettant son arrestation. Evgueni Mikhaïlovitch Bogachev**,** également connu sous le pseudo de « lucky12345 » ou « slavik » est accusé d'avoir injecté un virus au sein de plus d'un million d'ordinateurs et d'avoir été l'administrateur du réseau qui a implanté ce malware. Il est soupçonné d'être à la tête du malware GameOver Zeus, un botnet qui a permis de dérober plus de 100 millions de dollars.

GameOver Zeus fait son apparition en 2011

GameOver Zeus est un malware apparu en 2011, qui fait suite au célèbre botnet « Zeus », découvert en 2007. Le logiciel malveillant que le cybercriminel russe aurait implanté dans de nombreux ordinateurs permettrait de voler des données, notamment des codes d'accès offrant la possibilité d'accéder à des services financiers. Entre 500 000 et un million d'ordinateurs auraient été infectés sur la planète. Le hacker russe est poursuivi par Washington pour piratage informatique, fraude électronique et bancaire, blanchiment d'argent et crime organisé.

William Brownfield, chargé de la coopération judiciaire internationale au Département d'Etat a indiqué que Bogachev est peut-être le plus important cybercriminel de la planète. Une banque située en Floride aurait vu disparaître 7 millions de dollars de l'un de ses comptes en 2012 suite à l'infection de l'un de ses ordinateurs par le botnet en question. L'enquête menée par le FBI sur ce malware a impliqué plusieurs pays dont les Pays-Bas, l'Australie, le Royaume-Uni, la France, la Suisse, l'Italie, le Japon ou encore le Luxembourg.

Le hacker de 31 ans, activement recherché par le FBI, vivrait en Russie. L'enquête sur GameOver Zeus a débuté en Pennsylvanie en 2012 et une première opération de police s'était déroulée le 23 mai 2014 avec pour objectif de couper les lignes de communication entre les ordinateurs piratés et le réseau qui est à l'origine du botnet. Les enquêteurs ont également découvert que le hacker russe effectuait du chantage auprès des propriétaires d'ordinateurs infectés et leur réclamait une rançon pour qu'ils puissent s'en resservir convenablement.

Lien : http://www.zone-numerique.com/cybercriminalite-3-millions-de-dollars-de-recompense-pour-retrouver-evgueni-mikhailovitch-bogachev.html

Evgueni « Fantomas » Bogatchev, l'insaisissable hackeur russe

Inculpé en février 2015 en Pennsylvanie pour crime organisé, piratage informatique, fraude électronique, financière et bancaire et blanchiment d'argent, Evgueni Bogatchev est devenu à seulement 31 ans le cybercriminel le plus recherché au

monde, avec une récompense affichée à 3 millions de dollars (2,6 millions d'euros) pour tout renseignement amenant à sa capture.

Le 7 mai 2014, les autorités ukrainiennes aidées par le FBI investissent deux bâtiments situés l'un à Donetsk, l'autre à Kiev. A l'intérieur, plusieurs centres de « commande et de contrôle » (C & C) d'un réseau d'ordinateurs-zombies (ordinateurs infectés sous contrôle) éparpillés un peu partout dans le monde. Gameover Zeus (GoZ), c'est son nom, est l'un des « botnets » les plus sophistiqués et les plus lucratifs au monde, avec plus d'un million de machines sous son contrôle, et plus de 100 millions de dollars de gains estimés depuis son apparition en septembre 2011.

Avec cette prise, fruit d'un travail de plusieurs années, les enquêteurs peuvent enfin localiser l'ensemble des serveurs propageant les virus, pour la plupart situés en Allemagne, au Canada, en France, au Luxembourg, aux Pays-Bas, au Royaume-Uni et en Ukraine. Une fois la totalité des serveurs stoppés, ce sont plus de 300 000 ordinateurs zombies qui sont ainsi « libérés ».

Et parmi les ordinateurs de commande et de contrôle récupérés, les enquêteurs mettent la main sur un serveur de discussions en ligne utilisé par les pirates pour leurs communications internes. Son analyse va permettre de dessiner plus clairement les contours de cette société secrète.

L'opération « Tovar » est un succès presque total : les enquêteurs américains ont aussi et surtout réussi à démasquer et impliquer le cerveau de toutes ces opérations, l'insaisissable pirate russe Evgueni Bogatchev. Mais ils ne sont pas parvenus à l'arrêter.

Voitures de luxe, voilier et armes de poing

Né le 28 octobre 1983, Evgueni Mikhailovich Bogatchev résidait dans la petite station balnéaire d'Anapa, 60 000 habitants, sur les bords russes de la mer Noire, jusqu'en mai. Il y occupait la totalité du sixième étage – transformé en forteresse – d'un discret immeuble de 14 étages rue Lermontova, avec Valentina, sa femme, et leur bébé.

Selon *Paris Match* qui est allé enquêter sur place, le 14^{e} et dernier étage lui appartenait également, ainsi qu'une société écran, « LLC Standart », installée au rez-de-chaussée d'un immeuble anonyme dans la ville de Krasnodar, distante de quelque 150 km d'Anapa.

Passionné de voitures et de bateaux de luxe, Evgueni Bogatchev possédait plusieurs bolides de marques allemandes et américaines qu'il changeait très régulièrement, mais également, selon le FBI, un yacht amarré dans la marina proche, avec lequel il faisait régulièrement des balades en mer Noire, allant peut-être jusqu'en Bulgarie, Géorgie, Roumanie, Turquie ou même en Ukraine.

La dernière tentative des autorités américaines pour mettre fin à ses agissements il y a un an aurait quelque peu bouleversé cette tranquillité relative : ses voisins ont en effet assisté au départ précipité, dans la nuit du 31 mai 2014, de toute la famille dans une voiture de luxe, deux jours seulement avant que Bogatchev n'apparaisse en tête de la célèbre « Most Wanted List » du ministère de la justice américain. Aurait-il été prévenu ? A-t-il flairé les complications ? Quoi qu'il en soit, les lumières de l'appartement 101, qui restaient habituellement allumées jour et nuit, sont maintenant définitivement éteintes.

Selon des informations publiées en février dans le *Daily Mail*, Bogatchev serait titulaire d'un port d'armes de poing et posséderait également des armes de chasse. D'après l'un de ses voisins, « Fantomas » – comme il était surnommé dans le quartier pour sa ressemblance avec le célèbre méchant – n'est sûrement pas allé bien loin puisque leur chauffeur personnel a continué de venir régulièrement relever le courrier et payer ses factures.

Puis, en octobre 2014, c'est « *une femme, grande, belle, l'air sympathique,* [qui] *est venue s'affranchir de toutes les créances des Bogatchev. Elle a payé cash* », rapporte *Paris Match*, citant les gestionnaires de l'immeuble.

Surveillance bienveillante

Pourtant, et depuis de nombreux mois, les autorités américaines étaient en contact avec leurs homologues russes sur ce délicat dossier. Le FBI aurait même transmis dès 2013 suffisamment d'informations aux services russes du FSB pour enquêter sur celui qui est soupçonné depuis longtemps d'être l'instigateur de plusieurs réseaux internationaux de fraudes bancaires.

Mais, toujours selon le *Daily Mail*, qui a questionné Aslan Vladimirovich Goshokov, un responsable de la police locale, aucune demande d'arrestation ne lui est jamais parvenue au nom de Bogatchev, dont le casier judiciaire est toujours vierge en Russie. Mieux : questionnés dans la rue, des habitants d'Anapa n'hésitent pas à voir en Bogatchev un héros de la nation, méritant plus une médaille que la prison, pour avoir tenu tête et dépouillé des représentants du « grand capital ».

« Hackeur du futur »

Côté technique, les avis des différents experts ayant étudié les codes sources de Zeus ou de Cryptolocker (logiciel de racket en ligne qui a énormément rapporté à Bogatchev) sont dithyrambiques : *« C'est un hackeur du futur, l'un des plus brillants qui soit*, selon Tom Kellerman, responsable de la cybersécurité chez l'éditeur d'antivirus Trend Micro. *Gameover Zeus, fils prodigue de la première version de Zeus, est en tout point plus sophistiqué que l'original. »* Don Jackson, chercheur en sécurité informatique du laboratoire Dell SecureWorks, note que sur les forums fréquentés par les escrocs en ligne, le logiciel était devenu dès 2007 « *une sorte de best-seller* », finement programmé, ne ralentissant pas les ordinateurs infectés, difficilement détectable et surtout constamment amélioré par son créateur, « *à un rythme effréné, comme un projet vivant de codage* ».

Moins d'un an après sa première détection, Zeus avait déjà été transformé en une suite logicielle de piratage, du malware (virus) au botnet (réseau de machines sous contrôle), en passant par le spyware (logiciel espion), les outils d'administration de serveurs de commandes et de contrôle (C & C) et même un outil d'attaque par déni de service (attaques dites DDoS).

Le « Business Club »

Car c'est bien d'une entreprise de racket à l'échelle mondiale dont rêve Bogatchev lorsqu'il commence, dès l'âge de 25 ans, à se faire remarquer pour ses exploits sur la scène underground russe. Utilisant les pseudos de « Slavik », « Lucky12345 », « Pollingsoon » pour les plus connus, mais aussi « A-Z », « Monstr », « Umbro », « IOO » ou encore « Nu11 », le jeune hackeur russe est déjà en train de jeter les bases d'un empire du cybercrime organisé.

Le 5 août, lors de la convention « Black Hat » à Las Vegas, un rapport écrit par le FBI et les sociétés de sécurité Crowdstrike et Fox-IT a détaillé l'ampleur du système en place. Après avoir minutieusement décodé les archives des conversations saisies en 2014, Michael Sandee, l'expert du cabinet Fox-IT, a pu déterminer que le groupe – qui se faisait appeler le « Business Club » – était composé d'un comité directeur d'une demi-douzaine de leaders principalement originaires de la région de Krasnodar, et d'une cinquantaine de membres – essentiellement russes : techniciens support jour et nuit, fournisseurs de malwares, ou passeurs d'argent, qui ne pouvaient intégrer le « club » qu'en s'acquittant d'un droit d'entrée conséquent.

Accords avec le gouvernement russe

Le club fonctionnait sur les relations de confiance entre membres. Tous recevaient une part équitable des profits, qui provenaient essentiellement du piratage de comptes en banque. Les membres de ce gang « travaillaient » selon un rythme de bureau classique (de 9 heures à 17 heures, du lundi au vendredi), ciblant l'Asie et l'Australie le matin, l'Europe en milieu de journée, pour terminer en vidant des comptes américains en début de soirée. Tout l'argent siphonné transitait ensuite vers des banques chinoises de la province d'Heilongjiang, au nord de Vladivostok, à la frontière avec la Russie, que des mules se chargeaient de rapatrier ou d'investir dans la région.

Mais Evgueni Bogatchev, créateur du système et chef avisé, n'a pas tout divulgué à ses acolytes. Et pour cause. Soupçonné d'avoir passé des accords avec le gouvernement russe selon les experts des cabinets de sécurité, il aurait progressivement modifié le code source de son botnet pour le transformer dès l'automne 2013 – lors du début du conflit avec l'Ukraine – en système d'espionnage décentralisé ciblant des ordinateurs en Ukraine, en Géorgie, mais aussi en Turquie, visant notamment la direction du ministère des affaires étrangères turc et la Turkish KOM, une unité spéciale de la police.

Selon Michael Sandee, Bogatchev recherchait des informations sur le conflit à la frontière turco-syrienne, là précisément où ont vraisemblablement eu lieu des livraisons d'armes et des actions de mercenaires russes. A l'heure actuelle, et selon les dernières informations de la justice américaine, Bogatchev résiderait toujours en Russie avec sa famille, quelque part entre Anapa et Krasnodar.

Lien : http://www.lemonde.fr/pixels/article/2015/08/27/evgueni-fantomas-bogatchev-bogatchev-l-insaisissable-hacker-russe_4738498_4408996.html