



La présente traduction est préliminaire et ne représente pas la version finale.

LE 3^{EME} CONGRES MONDIAL CONTRE L'EXPLOITATION SEXUELLE DES ENFANTS ET DES ADOLESCENTS

**La coalition financière contre la pornographie mettant en scène des enfants:
Une étude de cas sur la façon dont le secteur privé, la police et les organisations non gouvernementales s'allient pour combattre la pornographie mettant en scène des enfants**

Buts

Cet article tâche de décrire les mécanismes, les avantages et les défis de la Coalition Financière Contre la Pornographie Mettant en Scène des Enfants (CFPMSE) pour les participants du 3^{ème} Congrès Mondial. La CFPMSE est issue d'une collaboration unique entre le secteur privé, la police et les organisations non gouvernementales. Nous espérons que les participants aux 3^{ème} Congrès Mondial feront usage de cette information pour qu'ils établissent de semblables partenariats public-privé dans le monde entier.

Cet article donne:

- une présentation générale de la CFPMSE et de ses sponsors, du Centre International des Enfants Disparus et Exploités (CIEDE) et son équivalent américain, le Centre National des Enfants Disparus et Exploités (CNEDE) ;
- des statistiques et une description du contexte de l'exploitation des enfants et, plus spécifiquement, de la pédo-pornographie à caractère commercial ;
- des exemples sur l'aspect pratique de l'action de la CFPMSE et de ce qui a été accompli aussi bien que des défis à venir.

Contexte

La Coalition Financière Contre la Pornographie Mettant en Scène des Enfants, formée en 2006, est une association inédite entre le secteur privé et le secteur public dans la lutte contre la pornographie infantile commerciale. Elle regroupe d'importantes banques, des compagnies de carte de crédit et d'institutions intermédiaires, des sociétés de portage et des entreprises de prestations de services sur Internet. La CFPMSE avance à grands pas vers son objectif de perturber les transactions commerciales liées à la pédo-pornographie en traçant les flux financiers et en fermant les comptes de paiement employés par ces entreprises illégales.

Ce qui rend la CFPMSE unique est qu'elle ne suit pas le modèle traditionnel de responsabilité sociale des entreprises fondé sur des donations ou des contributions. Son action est avant tout opérationnelle, et tandis que certaines compagnies ont apporté une contribution, cela ne constitue pas un condition requise pour prendre part à la coalition.

La CFPMSE est mandatée et dirigée par le Centre International des Enfants Disparus et Exploités (CIEDE) et le Centre National des Enfants Disparus et Exploités (CNEDE) basé aux Etats-Unis.

Le CIEDE a pour but d'identifier et de coordonner un réseau global des organisations combattant l'exploitation sexuelle et l'enlèvement d'enfant. Le CIEDE vient en aide aux enfants et aux familles en: mettant en place les ressources globales pour retrouver les enfants disparus et pour empêcher l'exploitation sexuelle d'enfant ; créant des centres et des filiales nationaux dans le monde entier ; établissant un réseau international pour diffuser les images et les informations sur les enfants disparus et exploités ; offrant des formations à la police, aux procureurs, aux juges, aux professionnels juridiques, aux organisations non gouvernementales et aux fonctionnaires de gouvernement ; enfin, en prônant l'ajustement des lois, des traités et des systèmes pour protéger les enfants dans le monde entier.

Le CNEDE est une organisation à but non lucratif mandatée par le congrès des Etats-Unis et travaillant en partenariat avec le ministère de la justice américain. Depuis 24 ans, le CNEDE a fonctionné sous la tutelle du congrès pour faire office de centre de ressources et de bureau central sur les enfants disparus et exploités. Ce mandat statutaire inclut des fonctions opérationnelles spécifiques requises par le congrès américain, notamment une ligne d'appel directe et gratuite 24 heures sur 24 pour signaler toute information sur un enfant disparu ou exploité appelée "CyberTipline" ; un système de gestion des cas pour la police et les familles ; l'assistance technique aux agences policières dans l'identification et la localisation des agresseurs sexuels récalcitrants; ainsi qu'une multitude de programmes pour arrêter l'exploitation sexuelle des enfants.

Problématique

S'attaquer à la croissance alarmante de l'exploitation sexuelle des enfants et des adolescents est une priorité pour les participants du 3ème Congrès Mondial. Définir l'étendue du problème est un défi pour la communauté de défense des droits des enfants. Le CIEDE et le CNEDE fournissent les statistiques suivantes :

- Au cours des 10 ans qui ont suivi la création de CyberTipline, le CNEDE a reçu et a traité plus de 600.000 signalements. L'écrasante majorité de ces cas a trait à la pornographie mettant en scène des enfants. Jusqu'ici, les prestataires de service électronique ont rapporté au CyberTipline plus de 5 millions d'images d'enfants sexuellement exploités. En 2007, le CNEDE a connu une augmentation des signalements dans presque toutes les catégories : 23% d'augmentation des signalements de pédo-pornographie, augmentation de 66% des signalements de séduction en ligne ; 58% des cas de prostitution d'enfant, 10% des cas de tourisme sexuel impliquant des enfants et une augmentation de 9% des signalements de brutalité sur enfant.
- Des enfants de plus en plus jeunes sont pris pour victimes et les images deviennent plus explicites et plus violentes. Parmi les auteurs de crimes sur enfants identifiés dans une étude récente aux États-Unis, 39% ont obtenu des images d'enfants de moins de six ans, 19% ont eu des images d'enfants de moins de 3 ans.
- Le centre d'appel CyberTipline reçoit également des signalements des membres de l'Association Internationale des Fournisseurs de Ligne directe pour l'Internet (INHOPE). Jusqu'ici, les membres ont envoyé près de 50.000 signalements de pornographie mettant en scène des enfants

au CyberTipline. Il y a 33 lignes directes membres d'INHOPE dans 29 pays s'efforçant de retirer le contenu illégal d'Internet.

C'est dans ce plus large contexte qu'est observée la croissance de la pédo-pornographie à caractère commerciale, c'est à dire le fait de tirer profit d'images d'enfants et d'adolescents sexuellement abusés par des organisations criminelles ou autres. La pédo-pornographie à caractère commerciale est devenue une industrie de plusieurs milliards de dollars et des enfants du monde entier sont vendus ou achetés comme des biens marchands.

Pour faire marcher ces entreprises, les organisations criminelles doivent accéder à l'infrastructure des industries établies. En conséquence, il y a des compagnies de services financiers et les sociétés de prestations de services d'Internet qui ont, sciemment ou à leur insu, été impliquées dans ces affaires odieuses. En conséquence, il est impératif que le secteur privé rejoigne la police et les O.N.G. dans leurs efforts de lutte contre la pornographie mettant en scène des enfants dans un but commercial.

Coalition financière contre la pédo-pornographie

La CFPMSE est une initiative unique qui allie les ressources des secteurs public et privé pour perturber significativement et démanteler les entreprises commerciales de pédo-pornographie.

La CFPMSE se compose d'importantes banques, de compagnies de carte de crédit, de sociétés de portage et de prestations de service sur Internet. Elle représente 95% de l'industrie des paiements aux États-Unis. Son but est de supprimer la rentabilité de la pornographie mettant en scène des enfants en suivant les flux de transactions et en fermant les comptes de paiement qui sont utilisés par ces entreprises illégales.

Avant que la CFPMSE n'ait été lancée en 2006, plusieurs sociétés de paiement et de prestations de services sur Internet combattaient des sites web de pédo-pornographie de leur propre chef. Mais les différents efforts individuels se sont avérés insuffisants face à l'étendue du problème. La CFPMSE constitue un espace où elles peuvent associer des ressources, l'expertise et les capacités d'analyse afin de progresser dans cette lutte.

Les membres de la CFPMSE sont :

AmericaOnline	Global Payments Inc.
American Express Company	Google
Authorize.Net	HSBC - North America
Bank of America	JP Morgan Chase
New YorkThe Bank of Mellon	Mastercard
Capital One	Microsoft
Chase Paymentech Solutions	North American Bancard
CheckFree	PayPal
Citigroup	ProPay Inc.
Deutsche Bank Americas	Premier Bankcard, LLC
Discover Financial Services	Standard Chartered Bank
Elavon	Visa
First Data Corporation	WashingtonMutual
First National Bank of Omaha	Wells Fargo

Western Union

Yahoo! Inc.

La CFPMSE bénéficie également du conseil et de l'assistance de cabinets juridiques, d'associations financières, d'experts en matière de cyber-sécurité et d'organismes de contrôle.

La coalition reconnaît que le simple nombre des individus impliqués dans cette industrie commerciale mondiale interdit de les poursuivre tous, peu importe la volonté des autorités policières. La CFPMSE, qui est fondamentalement une initiative civile, a proposé une approche différente : en se fondant sur des informations de CyberTipline, le CNEDE identifie des sites Web contenant des images illégales en même temps que des informations des modalités de paiement. Cette information est expédiée aux agents de la police fédérale américaine, qui procèdent ensuite à des investigations sur des sites particuliers afin de recueillir les preuves et de déterminer le contenu et les actes illégaux. Si la police n'engage pas de poursuite, la compagnie financière est avertie et prendra les mesures appropriées sur le compte concerné en accord avec les termes du contrat de service.

Accomplissements

De nombreuses tendances positives montrent que les efforts de la CFPMSE et de la police ont un impact sur la filière de la pédo-pornographie.

Par exemple, il est devenu plus difficile d'utiliser sa carte de crédit dans les transactions clandestines. Si la police est gênée pour effectuer ces transactions, il est raisonnable de penser que le consommateur l'est aussi. Et le prix d'achat des images d'enfants sexuellement exploités a nettement augmenté - une indication que les efforts de la CFPMSE peuvent affecter la rentabilité de ces sites.

La CFPMSE s'est efforcée de comprendre comment les marchands de pédo-pornographie sont entrés dans le système de paiement dans le passé, afin d'éviter des situations semblables dans le futur. Le résultat de ce travail fut la publication du rapport « L'achat sur Internet et les meilleures pratiques de surveillance pour la prévention et la détection de la pornographie mettant en scène des enfants à des fins commerciales ». Le *Comptroller of the Currency* (OCC ; Office de contrôle des devises) américain et le *Federal Deposit Insurance Corporation* (organisme destiné à assurer les dépôts effectués dans les banques commerciales) ont distribué ce document aux cadres des banques à travers le pays et à d'autres groupes d'intérêt et, à titre d'information, au CNEDE et à la CFPMSE. En outre, l'OCC a publié un communiqué de presse annonçant cette initiative.

La CFPMSE a publié la deuxième édition de son livre blanc des bonnes pratiques en 2008, qui est en référence ci-dessous.

Défis à venir

La CFPMSE accomplit de grands progrès aux Etats-Unis. Dans une prochaine étape, il est fondamental que le modèle soit étendu à d'autres pays pour traiter ce problème mondial. Le but de la CFPMSE est de mettre un frein aux transactions de la filière de la pédo-pornographie par des alliances avec les entreprises financières et de services sur Internet, les O.N.G., les experts légaux et la police, et de

proposer des solutions conformes aux lois et aux coutumes locales. Les régions cibles comprennent l'Europe, l'Asie et le Pacifique.

Régulièrement, les compagnies contactent le CNEDE et le CIEDE pour rejoindre la coalition. Certains de ces établissements sont notoires et fonctionnent sous l'examen minutieux d'organismes de contrôle. D'autres sont moins bien connus, mais sont des acteurs potentiellement importants dans les nouvelles méthodes de paiement émergentes. Il est important de contrôler les nouveaux demandeurs pour être sûr que leur modèle économique, leur éthique d'entreprise et leur réputation soient compatibles avec les buts de la CFPMSE. Un système de filtrage développé récemment est actuellement testé.

Alors qu'on exerce de la pression sur des sites Web commerciaux de pédo-pornographie, les entreprises qui les gèrent évoluent. C'est particulièrement vrai dans les secteurs de l'hébergement de pages Web et des outils alternatifs de paiement. Le Groupe de Travail sur les Défis Technologiques de la CFPMSE a récemment publié un article sur le sujet. Cet article est ajouté en supplément étant donné la valeur de son contenu et parce qu'il constitue une démonstration substantielle des bienfaits de la collaboration qui caractérise la CFPMSE.

Addendum: Rapport du Groupe de Travail sur les Défis Technologiques . « Tendances de l'hébergement et des modes de paiement pour des sites Web commerciaux de pornographie mettant en scène des enfants. »

**RAPPORT DU GROUPE DE TRAVAIL SUR LES DEFIS TECHNOLOGIQUES :
« TENDANCES DE L'HEBERGEMENT ET DES MODES DE PAIEMENT
POUR DES SITES WEB COMMERCIAUX DE PORNOGRAPHIE METTANT EN SCENE DES ENFANTS. »**

La coalition financière contre la pornographie mettant en scène des enfants ("la coalition") a été formée en 2006 pour répondre à la croissance alarmante de la pédo-pornographie à but commerciale sur Internet. Ses membres comprennent des banques leaders et d'importantes compagnies de paiement, ainsi que des sociétés de prestations de services en ligne. Un des objectifs statutaires de la coalition est de dépister et de prévoir comment les mécanismes de la pédo-pornographie à but commercial évoluent. À cet effet, le Groupe de Travail sur les Défis Technologiques (GTDT) de la coalition présente les résultats qui suivent.

Remarques préalables

Ce rapport a été créé et rédigé par des volontaires au nom du GTDT et représente la position du GTDT sur les questions abordées au moment de sa publication. Le contenu est fondé sur la contribution individuelle des auteurs et ne reflète pas nécessairement les opinions ou les politiques des compagnies dans lesquelles ils travaillent. Depuis la parution du rapport, il est possible qu'il contienne désormais des inexactitudes ou de l'information devenue obsolète.

Ce rapport a été écrit à titre d'information seulement et ne prétend pas fournir spécifiquement des conseils légaux, financiers ou de management. Si vous avez besoin de services de conseil ou d'avis spécifiques, vous devez vous adresser à un professionnel. Le GTDT NE DONNE AUCUNE GARANTIE, EXPLICITE, IMPLICITE OU STATUTAIRE, QUANT À L'INFORMATION DE CE RAPPORT. La mention d'une organisation ou d'une entité ci-dessous n'implique en aucune manière l'approbation par une telle organisation ou entité.

Le respect des lois sur les Droits d'Auteur applicables est de votre responsabilité. Ce rapport peut être librement et gratuitement redistribué dans son intégralité à condition qu'aucune notification légale, y compris toutes les notes sur la propriété intellectuelle, n'en soit retirée. Il ne peut être vendu pour le profit ou être employé dans des documents commerciaux sans l'autorisation écrite du GTDT, délivrée à sa seule discrétion.

Tendances

Le problème central pour des gouvernements et des autorités policières essayant de traiter la pédo-pornographie à but commercial (PPC) sur Internet est l'anonymat. Les criminels ont de façon innovante

protégé leurs opérations en ligne, permises par l'anonymat de leurs transactions et de l'hébergement du contenu.

À savoir:

- ❖ Le contenu de la PPC peut être hébergé dans des pays où la loi ne s'applique pas, n'ayant pas accès au recours légal direct, ou il peut être hébergé involontairement sur un système de plates-formes informatiques qui elles-mêmes ont été récupérées par des fournisseurs de PPC techniquement habiles.
- ❖ Le paiement en ligne pour de la PPC est, en pratique, anonyme. Bien que les fournisseurs traditionnels de service de paiement soient des banques ou des établissements de type bancaire observent la réglementation nationale, le GTDT observe l'émergence de services de paiement 'alternatifs' et d'entités financières, dont le statut non-bancaire les autorise à contourner les règles exigeant de connaître l'identité du payeur et du receveur.

Le problème fondamental de la détection et de la prévention de la PPC en ligne est qu'Internet fournit un espace anonyme dans lequel les cybercriminels peuvent opérer impunément et réaliser toute sorte de crimes, en plus de la vente de PPC. L'anonymat facilite des opérations en ligne de PPC de trois manières : facilité de cacher le contenu stocké ; criminels de créer rapidement des sites dynamiques de paiement (« existe aujourd'hui, disparaît demain, recréé le jour suivant ») pour éviter la détection ; l'absence de règlement des méthodes alternatives émergentes de paiement.

En règle générale, l'Internet est truffé de liens vers de la pédo-pornographie. Certains sites d'annonceurs ont de nombreux liens de renvoi qui réorientent le client potentiel vers un domaine sans rapport. Quand un consommateur potentiel ouvre une page qui offre une adhésion moyennant une cotisation, plusieurs cas de figures peuvent se présenter. Le site d'hébergement peut proposer un paiement par carte de crédit pour le compte du site. À ce moment-là, une page Web non codée peut être utilisée pour enregistrer le nom, l'adresse, le téléphone et les données de la carte de crédit. La majorité des sites d'annonceurs qui offrent des adhésions traitent les paiements par carte de crédit sans utiliser la technologie https, exposant ainsi grandement le consommateur. L'information est susceptible d'être exploitée par des cybercriminels. Le GTDT peut seulement supposer que les sites d'annonceurs choisissent de ne pas obtenir de certificat SSL parce qu'ils devraient alors sacrifier une partie de leur anonymat.

Quelques sites offrent des produits de PPC à vendre via confirmation par email. Le client envoie un email à un individu inconnu pour accomplir la transaction, utilisant parfois des transferts de fonds en ligne ou en envoyant simplement l'argent comptant par courrier. D'autres sites de PPC offrent une adhésion, mais réorientent le client à un site regroupant de sites de paiement par carte de crédit. Certains de ces sites de regroupement offrent à la fois des transactions sûres et peu sûres. Ces sites de regroupement, en générale : ne chiffrent pas les transactions par carte ; et contreferont ou imiteront les pages de transaction par carte pour se faire passer pour un tiers payeur légitime ou semi-légitime. Le GTDT n'a pas constaté une baisse significative du nombre de paiements pour des sites de PPC, mais a observé un déclin dans l'identification des sites de PPC probablement dû à une application plus stricte, incitant ainsi ceux qui profitent de la PPC à se rendre plus difficiles à identifier.

Hébergement¹

Hébergement des entreprises

Beaucoup de compagnies d'hébergement sont devenues des intermédiaires pour le stockage de la PPC. À cette fin, dans la plupart des cas, les URL catalogués ou les sites de contenu tourneront en fonction des résultats des clients potentiels et des méthodes de paiement jusqu'à ce que chacun soit fermé. Les sites catalogués établiront alors de nouveaux comptes et méthodes de paiement. De cette façon, il est possible qu'un site individuel se fasse retirer son contenu et ses moyens de paiement à plusieurs reprises pour réapparaître ensuite avec un nouvel hébergeur et de nouveaux clients. L'observateur occasionnel, il s'avère que ces sites ont continué à fonctionner sans interruption. Pour un œil entraîné et averti, il est clair que ces sites ont été en réalité désactivés à plusieurs reprises pour mieux réapparaître. Le caractère vain de ce processus peut être comparé au jeu pour enfant « tape-taupe » dans les fêtes foraines.

Chose intéressante, les sites et les URL « label blanc » (apparemment inoffensif) ont un cycle de vie entièrement différent. En général, ces URL sont utilisés simplement pour mener les consommateurs vers des contenus "label blanc" provisoire ou vers un site provisoire de contenu de marque. À cet égard, ces URL sont la « chair à canon » dans la bataille pour la viabilité commerciale. En fait, il est possible de voir 10 à 20 différents URL apparaître à quelques jours d'intervalle dans des campagnes de masse de *spam*, où tous les URL finissent par héberger le même contenu catalogué.

Actuellement, beaucoup d'entreprises d'hébergement se focalisent essentiellement sur la rentabilité et n'ont plus aucune politique écrite en ce qui concerne les contenus illégaux. Dans certains cas, les conditions générales d'utilisation déclarent que l'hébergement de contenu illégal par leurs clients pourrait avoir comme conséquence l'arrêt du service. Cependant, la question reste de savoir dans quelle mesure ils imposent ces clauses de manière proactive. D'une façon générale, les hébergeurs ne filtrent pas le contenu et comptent sur le signalement de PPC avant qu'ils ne soient disposés à agir. Le GTDT a appris par un expert juridique que les hébergeurs qui n'ont pas consulté un avocat ou quelqu'un de bien informé sur la question répondent souvent aux plaintes au sujet de ce type de contenu en menant leur propre enquête en interne ; le même expert affirme que c'est une pratique risquée et peu judicieuse pour les raisons suivantes : a) ce ne devrait pas être le rôle de l'hébergeur « de maintenir l'ordre » dans le contenu ; b) des hôtes ne sont pas qualifiés pour déterminer ce qui constitue de la PPC ; c) les hébergeurs peuvent violer les lois concernant la possession de PPC. Ceux qui ont cherché un avis juridique ont des procédures institutionnelles en place pour isoler le contenu et pour le signaler au CNEDE.

La première étape serait d'obliger les compagnies d'hébergement à adopter les meilleures pratiques. Les études du GTDT ont prouvé qu'il n'existe pas d'organisation commerciale pour les hébergeurs équivalente à l'Association Américaine des Prestataires de Service d'Internet. Une telle organisation serait utile pour établir des standards et pourrait servir de mécanisme pour régler les questions soulevées par le GTDT.

¹ Un service d'hébergement est un type de service sur Internet qui permet à des particuliers ou à des organisations de donner accès à leur site via la World Wide Web. Les fournisseurs d'hébergement sont des entreprises qui offrent un espace sur un serveur qui leur appartient pour le compte de leur client en plus du service de connexion à Internet, en général dans un centre de données. Voir (définition en anglais) : http://en.wikipedia.org/wiki/Web_hosting

La brève liste qui suit sert à recommander et mettre en avant un niveau minimum de réactivité des entreprises d'hébergement en vue de supprimer le stockage de PPC.

- Politique concernant la pornographie mettant en scène des enfants : maintenir une politique sur la façon de détecter et de réagir à l'hébergement et au stockage de la PPC. Le site web suivant a été suggéré par un expert juridique comme en ce qui concerne la question de la PPC : <http://www.peakinternet.com/legal/aup/>. Bien que le GTDT n'approuve pas ce document comme modèle, ce dernier a le mérite d'essayer de traiter le problème.
- Surveillance : les changements fréquents des méthodes, de la technologie, des URL, etc. sont clairement des efforts délibérés employés par les criminels pour échapper à la détection. Ils se donnent aussi beaucoup de peine pour maintenir leur anonymat. Le GTDT recommande donc que les hébergeurs recherchent les sites connus de PPC trimestriellement avec l'objectif à terme d'une surveillance hebdomadaire de tous les sites actifs connus. La technologie "Spider" et les moteurs automatiques existent pour aider à localiser facilement le lexique lié à la PPC et les images. Une fois trouvés, ces sites doivent être retirés par l'hébergeur.
- Filtrage WRT : tout comme des fournisseurs d'accès Internet le font actuellement lorsqu'ils recourent à la technologie pour débarrasser leurs systèmes du contenu illégal, les hébergeurs devraient supprimer tout le contenu illicite de leurs serveurs.
- Partage d'informations avec le CNEDE sur les hôtes délinquants (les hôtes qui stockent du contenu illicite) : en accord avec leurs politiques, les hébergeurs sont encouragés à partager l'information qu'ils possèdent avec le CNEDE concernant des personnes ou des prestataires censés être impliqués dans la distribution de PPC.
- Diligence à l'égard de la clientèle : de la même manière que les banques ont été requises d'adopter des politiques pour « connaître leurs clients » pour éviter de blanchir l'argent de trafiquants de drogue et de terroristes, les hôtes devraient être encouragés, sinon obligés, à pratiquer la diligence normale à l'égard de leurs sur les clients et de leur contenu.

En conclusion, il appartiendrait à la coalition de créer une « liste noire » d'hébergement les compagnies à qui sont connus pour héberger de la PPC ou pratiquent un laxisme volontaire, et d'autres qui sont peu disposés à suivre les cinq étapes de la diligence mis en relief ci-dessus.

Serveurs d'entreprises compromis dans l'hébergement de PPC

Des failles dans la sécurité d'un réseau d'entreprise sont ouvertes par les groupes criminels avec des logiciels malveillants, qui prennent la commande de n'importe quel utilisateur connecté à un réseau et, à leur tour, compromettent la totalité du réseau rendant la propriété intellectuelle et les données financières vulnérables à l'exploitation par le crime organisé ou, dans le cas de la PPC, permettent à des groupes de déposer ou de distribuer du contenu par le biais de ces réseaux².

Imaginer que le contrôle du serveur d'une société importante, d'une université ou d'une institution financière soit pris et que celui-ci serve de relai à la vente de PPC. L'existence avérée de manquements

² Voir <http://www.securityfocus.com/brief/691>.

majeurs aux règles de sécurité rend une telle hypothèse non seulement possible, mais probable. La liste des meilleures pratiques en annexe devrait être distribuée aux responsables technologiques et de l'information des organisations membres de la Coalition.

Systèmes de paiement en ligne

Dans l'introduction de "l'Evaluation des menaces nationales de blanchiment d'argent aux États-Unis"³ ("EMNBA"), de décembre 2005, le gouvernement des États-Unis déclara que « les criminels jouissent de nouveaux avantages avec la globalisation et l'arrivée de nouveaux services financiers tels que les porte-monnaie électroniques et les services de paiement en ligne. » L'EMNBA a identifié et a évalué treize menaces financières contre les États-Unis et, parmi elles, deux - les systèmes de paiement en ligne et les porte-monnaie électroniques - constituent de nouveaux chapitres qui ne seraient pas apparus dans une évaluation similaire quelques années plus tôt. Ces nouvelles et changeantes menaces dans le système financier, supposées être en partie la conséquence aux besoins de services financiers hors-banques et, en partie, issues de la globalisation des systèmes financiers et de leurs réactions à la réalité de l'Internet, posent des menaces potentielles de criminels et autre utilisation illicite non seulement pour l'économie américaine, mais aussi pour l'économie mondiale.

Comme l'affirme l'EMNBA, « des services de paiement en ligne nouveaux et innovateurs émergent en réponse à la demande du marché de la part des particuliers et des commerçants en ligne... Les commerçants en ligne, notamment ceux des secteurs où les taux de rejet de débit sont élevés, nourrissent la demande de nouvelles méthodes de paiement. Il existe des centaines de ces systèmes de paiement en ligne. Ces marchés comprennent les systèmes de paiement en ligne qui placent leurs propres conditions de transactions en l'absence de toute protection des consommateurs. En général, des transactions par ces prestataires de service sont finalisées sans recours possible pour les individus qui pensent avoir été victimes de fraude. En conséquence, selon les agences de police fédérales, ces systèmes sont devenus les mécanismes préférés de paiement pour les malfaiteurs en ligne responsables de montages d'investissements frauduleux et autres activités illégales. »

L'EMNBA a permis d'avoir une vue d'ensemble des « services de monnaie électronique » comme e-gold, Ltd. récemment mise en examen, et d'autres systèmes de paiement en ligne. L'EMNBA a évalué les faiblesses de ces technologies en évolution notant que les transmetteurs d'argent sont obligés de s'inscrire auprès du FinCEN⁴ et sont soumis à la tenue d'archives et au signalement d'actes frauduleux selon les termes la loi anti-blanchiment d'argent ("ABA"), de même qu'ils sont, en général, tenus de déclarer les conditions d'autorisation. Les termes de l'ABA pour un système de paiement en ligne ou pour une monnaie électronique varient selon « leur domiciliation et les méthodes de transaction employées. »

Ces nouveaux et changeants moyens de paiement, y compris deux techniques qui n'ont pas été abordées dans l'EMNBA - à savoir les jeux sur Internet tels que l'Univers d'Entropia, qui ont leurs propres devises convertibles reliées à des capacités réelles de débit, ainsi que les opérations bancaires par téléphone mobile - montrent le nouveau paysage radicalement différent des méthodes traditionnelles d'argent comptant, de contrôle, et par carte de crédit. Ces nouveaux mécanismes de paiement, en particulier quand ils sont associés à Internet, peuvent favoriser le crime conventionnel de nouvelles manières ou

³ Voir <http://www.treas.gov/press/releases/docs/nmls.pdf>.

⁴ U.S. Treasury Financial Center.

peuvent générer de nouvelles activités criminelles qui ne seraient pas apparues sans cela. Le flux financier peut être l'origine de l'acte criminel, ou le mécanisme de blanchir pour déplacer le montant, une fois que produit.

Internationalement, le Groupe de Travail sur l'Action Financière (GTAF), comprenant 34 nations membres⁵, a publié un rapport, en octobre 2006, 6 étudiant la manière dont de l'argent peut être blanchi par l'exploitation de nouvelles technologies de paiement (cartes payées d'avance, systèmes de paiement en ligne, des paiements par téléphones mobiles et les métaux précieux électroniques). Le rapport a établi que, alors qu'il y a une demande légitime du marché de ces méthodes de paiement, ils sont fortement vulnérables aux montages financement de blanchiment ou aux activités terroristes. En particulier, les fournisseurs internationaux de nouvelles méthodes de paiement peuvent poser plus de risques que des fournisseurs fonctionnant exclusivement dans un pays donné. Le rapport du GTAF recommander la vigilance continue de tous les pays pour évaluer davantage l'impact des technologies en évolution dans les cadres de normalisation internationales et nationales. Cependant, étant donné le niveau de la corruption ou de la connivence de certains gouvernements étrangers avec divers types d'activités criminelles, la surveillance et l'application stricte des transactions financières sont peu probables.

PayPal a fait preuve d'un extraordinaire niveau de vigilance en tant que système de paiement en ligne et peut être un modèle pour d'autres entreprises du secteur. Par des politiques saines, des modèles déposés, des moyens d'audit et d'investigation et des partenariats public/privé, PayPal démontre une rigueur dont d'autres systèmes de paiement en ligne devraient s'inspirer afin de contrecarrer des paiements pour la pornographie mettant en scène des enfants. Les politiques et les procédures de PayPal en termes de vigilance sont décrites ci-dessous :

Politique

- PayPal a une politique de tolérance zéro pour l'usage de son système pour tout contenu et services illégaux.
- Les conditions générales d'utilisation de PayPal déclarent clairement que tout compte offrant du matériel ou des services illégaux viole la politique d'usage et sera sujet à une fermeture immédiate.

Modèles et autres outils de détection

- PayPal possède des modèles déposés qui sont spécifiquement conçus pour la question de l'exploitation des enfants.
- PayPal a plus de 1700 mots clés dans des langues multiples intégrés dans ses outils.
- PayPal investit fortement dans des outils de surveillance et de détection dans le domaine de l'exploitation d'enfant.
- PayPal utilise les outils qui parcourent et scrutent ("*crawlers*" et "*spiders*") son système interne et sur le Web à la recherche d'infractions.

⁵ Depuis sa création, the GTAF a mené l'effort international pour l'adoption and la mise en place des mesures pour contrecarrer l'utilisation du système financier international par des criminels. Il a proposé une série de 40 Recommandations en 1990, révisées en 1996 et en 2003, afin d'en maintenir l'actualité et la pertinence face aux nouvelles menaces de blanchiment d'argent.

⁶ http://www.fatfgafi.org/document/17/0,3343,en_32250379_32237217_37627409_1_1_1_1,00.html

- Les mots clés et les techniques de modélisation sont mis à jour hebdomadairement.
- PayPal encourage quiconque possède des informations sur l'utilisation illégale potentielle de PayPal à contacter la compagnie.

Audit

PayPal emploie plusieurs prestataires qui parcourent le Web à la recherche d'infractions potentielles liées à sa marque.

Agents investigateurs, analystes et une équipe pour les opérations de police internationales

- PayPal a une équipe de près de 100 agents dans le monde qui recherche et étudie les infractions à haut risque, y compris celles liées à l'exploitation des enfants.
- En outre, PayPal a une équipe d'agents spécialisés dédiée à la lutte contre l'exploitation des enfants. Ils ont été formés pendant plusieurs années par le CNEDE et dont l'expertise est régulièrement évaluée.
- PayPal investit fortement dans des programmes de formation et d'orientation pour son équipe d'investigations et ses analystes, et notamment dans la formation interne et externe, les bibliothèques en ligne et d'autres ressources pour s'assurer que PayPal ait en sa possession la documentation de référence la plus récente.
- PayPal a un programme de recherche qui étudie les tendances du secteur, les nouvelles et des événements, et fait de la veille technologique.

Partenariats publics et privés

- PayPal travaille étroitement avec l'office des douanes aux États-Unis, le FBI et d'autres organismes de contrôle pour s'assurer qu'il reste pointu sur les problèmes de contenu illégal.
- PayPal a invité divers représentants de la police en tant que conférencier pour son programme de formation.
- En tant que membres de leur équipe mondiale d'opérations d'application de la loi, PayPal compte des anciens policiers, des avocats, des professionnels du monde industriel qui travaillent étroitement avec leurs contreparties dans la police, les organismes de contrôle et les O.N.G. pour favoriser les échanges et pour coopérer sur les enquêtes.

Conclusion

L'évolution du paiement de la PPC et de l'hébergement de sites Web depuis des modes financiers et d'hébergement traditionnels vers des formes plus complexes est un défi majeur qui nécessite une attention particulière et une compréhension approfondie, de même que, comme pour d'autres aspects du commerce en ligne, une régulation accrue. L'économie souterraine de la PPC et sa distribution sont dynamiques et résilientes face aux initiatives de la coalition pour la combattre. Comme diverses industries liées à Internet mûrissent et deviennent plus citoyennes, il sera essentiel pour la coalition de les

-12-

Tendances dans l'hébergement et le paiement pour des sites Web commerciaux de pornographie mettant en scène des enfants.

Mai 2008

© 2008 Coalition Financière Contre la Pornographie Mettant en Scène des Enfants. Tous droits réservés.

ANNEXE : PRATIQUE EN MATIERE DE SECURITE DES SERVEURS

intégrer au mouvement et de les encourager à adopter des politiques adéquates, telles qu'une plus grande vigilance et un certain degré de filtrage et de surveillance des sites qu'elles hébergent.

Sécurité des serveurs Web
1. Se rappeler que l'installation par défaut du HTTP peut mener aux attaques du DDoS et à l'exposition des informations confidentielles rendant le serveur vulnérable à une attaque.
2. Utiliser le SSL ou le SSH.
3. Ne pas ouvrir d'autres applications sur le système. Se limiter au HTTP et aux autres services requis.
4. Installer les dernières offres de services, mises à jour et patches.
5. Contrôle d'accès : limiter la liste des utilisateurs du serveur en utilisant l'authentification à deux facteurs.
6. Effectuer un test de pénétration avec des scans de vulnérabilité appropriés pour évaluer les failles critiques exploitables.
7. Le contrôle de l'évolution du système permet-il de réduire le risque global? Est -ce que les changements de système sont répertoriés et surveillés ?
8. Enlever tous les échantillons de programmes sur le serveur.
9. Ouvrir les applications Web de scan pour simuler une attaque du site Web et pour déterminer son niveau de sécurité. Procéder ainsi souvent pendant la phase de conception et scanner chaque semaine pour identifier les nouvelles vulnérabilités.
10. Passer les logs en revue fréquemment. L'utilisation des logs doit être systématique. Si cela est possible, centraliser tous les logs pour analyser les tendances ou déterminer des similitudes avec d'autres serveurs.
11. Plannifier avec soin et traiter les aspects de la sécurité du déploiement de n'importe quel serveur Web public.
12. Mettre en place les pratiques de gestion de la sécurité pour maintenir et faire fonctionner une présence sans risque sur le Web.
13. Pour assurer la sécurité du serveur Web et de l'infrastructure du réseau, les pratiques suivantes devraient être mises en œuvre : <ul style="list-style-type: none">▪ Une politique de sécurité du système d'information pour l'ensemble de l'organisation.▪ Contrôle de configuration et gestion du changement.▪ Évaluation et gestion des risques.▪ Standards de configuration de logiciel qui satisfassent la politique de sécurité du système d'information.▪ Sensibilisation et formation à la sécurité.▪ Planification d'urgence, continuité des opérations et réparation des dommages.