PRAGUE – Forum on DNS Abuse
Monday, June 25, 2012 – 16:30 to 17:30
ICANN - Prague, Czech Republic

Margie Milam: Bien, bonjour, nous allons commencer le forum sur les abus de DNS.

Je suis Margie Milam et je vais présenter le modérateur: Ondrej Filip de CZ.NIC va être le modérateur de cette session et vous donnera davantage d'informations sur ce que nous attendons.

Ondrej Filip, vous avez la parole.

Ondrej Filip: Bien, alors, bienvenue à tous. Je pense que nous avons entendu beaucoup de choses très intéressantes sur la façon de créer un Internet, un nouveau domaine. Maintenant, nous devons comprendre que l'Internet, ce n'est pas seulement pour les personnes honnêtes mais aussi pour d'autres personnes.

Donc cette session va être sur les abus de DNS, le côté sombre de l'Internet et du cyberespace. Nous avons eu une discussion sur cette question.

À côté de moi, nous avons quatre personnes qui s'y connaissent dans ce domaine, qui sont expertes dans ce domaine et nous allons voir trois présentations.

La première va être faite par Martin Peterka, la deuxième par Branko Stamenkovic, et ensuite par Christopher Malone et par Christopher Landi.

La première présentation va être faite par Martin Peterka qui est un collègue à moi, qui travaille dans la compagnie. C'est le président d'un organisme, et il va vous parler un petit peu de son expérience, organisme d'une nationale tchèque, SRT national tchèque, il va nous parler de son expérience dans la région, et ça va être très intéressant, donc nous lui donnons la parole.

Martin, vous avez la parole.

Martin Peterka: Bonjour à tous. Merci de me présenter. Martin Peterka.

Bien. Aujourd'hui, je vais vous parler un petit peu de notre association, CZ.NIC. Je vais vous présenter notre équipe de sécurité, comment nous travaillons. Et je vais décrire quelques incidents que nous avons résolus.

Et à la fin de ma présentation, je voudrais vous présenter notre directeur du secteur de fraude et les outils que nous utilisons.

Commençons donc par CZ.NIC qui est une association qui a été fondée en 1998 par douze ISP importantes en République Tchèque, et nous avons une adhésion ouverte pour les membres, différents groupes de membres et nous avons plus d'une centaine de membres actuellement. Aujourd'hui, nous avons plus de 50 employés et notre secteur d'activité principal est donc l'opération du registre du domaine CZ. Nous avons signé un mémoire avec les agences de sécurité nationales tchèques

focalisé sur tout ce qui concerne la République tchèque et la sécurité dans ce domaine. Nous sommes une organisation à but non-lucratif et nous avons une série d'activités. Par exemple, nous avons un centre de formation. Nous avons un département qui travaille sur le développement de logiciels. Nous avons, bien sur, une équipe de sécurité et chez CZ.NIC, nous avons deux équipes de sécurité. La première est une équipe interne, CZ.NIC interne et CSIRT, qui travaillent sur notre système interne.

Comme nous n'avons pas de système de clientèle autonome, nous avons un réseau, et normalement nous n'avons pas beaucoup de problème. Mais le deuxième rôle de notre équipe est beaucoup plus important de notre point de vue parce qu'il est directement lié aux questions de registre. Notre équipe est capable de travailler sur les domaines qui ont un contenu dangereux, virus, spam, etc. Si nous trouvons donc un site dont le contenu peut être dangereux, nous pouvons désactiver ce domaine pendant un mois. Si c'est nécessaire, on peut le faire pendant un peu plus de temps.

La deuxième équipe de sécurité opère au niveau national, c'est l'équipe CSIRT national. Nous travaillons donc depuis l'année 2011. Jusqu'à la fin de l'année 2010, on travaillait avec une association académique de CESNET qui dépendait du ministère de l'Intérieur, et cet accord a conclu a la fin de l'année 2011 et CZ.NIC était d'accord pour continuer l'opération de cette équipe et donc nous avons commencé en 2011, et nous avons commencé à transférer l'agenda de l'association CESNET. Ce transfert s'est achevé a la fin de l'année. Donc depuis juin 2011 nous opérons complètement et nous travaillons bien sur encore avec des collègues de CESNET. Notre principal rôle est le rapport des incidents et

la maîtrise de ces incidents. Nous travaillons bien dans ce domaine mais nous avons différentes expériences. Par exemple, l'année dernière nous avons analysé les données de serveurs DNS autoritatives qui étaient considérées comme non surs au niveau des resolvers de DNS. Et donc, on a envoyé des lettres aux administrateurs, aux gestionnaires de ces domaines en expliquant comment on pouvait les aider. Comme certains resolvers étaient au niveau du réseau gouvernemental, on a coopéré dans ce projet avec le service de sécurité tchèque.

Mon équipe organise des activités comme des réunions, des ateliers pour la communauté. Et nous avons des cours spéciaux qui sont focalisés sur la sécurité, qui sont donnés au niveau de notre centre de formation.

Nous coopérons avec des organisations internationales. Par exemple, peut-être que vous connaissez TERENA et d'autres. Et ENISA par exemple. CESERT est accrédité depuis le mois d'octobre 2011.

Donc voilà, certaines statistiques de notre équipe que vous pouvez trouver sur notre page web, si ça vous intéresse.

Et vous pouvez voir ici les principaux incidents que nous avons dû résoudre à travers notre système de détection. La plupart du temps, c'était un problème de phishing.

Je voudrais parler de deux incidents qui ont eu lieu que nous avons résolus pendant le passé. Le premier était un incident que l'équipe de CESERT a résolu au début du mois de juin 2012. C'était une amplification du DNS.

L'autre était un peu plus ancien. Je vais parler d'un cas de phishing que nous avons résolu au niveau du CSIRT.CZ en 2010.

Commençons donc par l'amplification du DNS. L'objectif ici était une banque. Cette attaque a eu lieu contre les services du DNS du monde entier. La plupart était située aux États-Unis mais certains étaient en Europe aussi et 172 se trouvaient en République tchèque. Donc notre équipe a résolu ce problème grâce à notre équipe, on nous a envoyé des données que nous avons analysées. Nous avons trouvé des informations sur les gestionnaires, nous les avons contactés, nous leur avons demandé de corriger certains aspects. Les attaques se sont conclues au bout de quelques jours, comme d'habitude. Mais pour nous, c'est un progrès parce que nous sommes encore en contact avec les gestionnaires et nous essayons de les aider à continuer à résoudre les problèmes. Aujourd'hui, apparemment 50% des problèmes de DNS ont été réglés.

Les noms de services qui étaient concernés par ces attaques étaient des noms de service que nous avons communiqué l'année dernière au cours d'une présentation de statistiques. Et donc nous avons comparé ces données, et nous avons constaté qu'il y en avait 5 ou 6 qui figuraient dans les deux listes.

À l'attaque de phishing en 2010. Et qui avait enregistré plusieurs domaines pour des titulaires étrangers et tous étaient payés par des cartes de crédit volées.

Nous avons fait une enquête et nous avons constaté qu'il y avait des Troyan horse qui attaquaient des organisations gouvernementales pour par exemple les impôts et ces troyans ressemblaient à des applications

qu'il faut utiliser si on veut résoudre certains problèmes dans la présentation des impôts.

Pendant cinq jours nous avons enregistré 150 domaines et avec les experts d'IRS et les registraires, notre équipe a pu contrôler ces domaines et les situer, et La plupart de ces domaines ont été désactivés rapidement une heure après l'enregistrement, ce qui est un bon moment. Le résultat c'était que Cinq jours plus tard, les enregistrements se sont arrêtés. Et donc on peut dire que nous avons eu du succès dans notre travail mais lorsque nous avons discuté de ce problème, nous avons décidé que ça ne suffisait pas d'être préparé pour affronter certains incidents et que nous devions être plus proactifs, essayer de situer les problèmes avant que l'incident est lieu, donc avec notre laboratoire de CZ.NIC, nous avons organisé un système qui s'appelle gestion de domaines frauduleux ce sont des logiciels qui viennent de sources publiques et qui stockent les données concernant le problème de contenu frauduleux, nous utilisons différents outils et différentes ressources pour ces applications et avec des données sélectionnées sur certains sources et des données de contact pour ces domaines et comme notre application est contactée avec un système de ticket et nous pouvons communiquer avec les gestionnaires avec ces contacts et contrôler pour voir comment résoudre ce problème sur ce site. On a commencé avec des applications au mois de juin et voila nous avons ici quelques résultats. Pendant cette année là, nous sommes orgueilleux de pouvoir dire que nous avons pu supprimer 11,000 et quelques pages, donc plus de 2,000 domaines qui ont été nettoyés, sur ce tableau vous voyez les problèmes de phishing, nous un pourcentage de pages, de phishing entre juin et décembre 2011 qui ont été désactivés. Vous

pouvez voir qu'il y a eu une baisse importante de 6% en juin, à 2% en décembre, et ce tableau n'a pas été complété parce que le problème de phishing doit être analysé au niveau de tout le pays mais je suis sûr que le gestionnaire de domaines frauduleux a été par ce travail que nous avons réalisé et cette application est de source ouverte, donc si vous êtes intéressés, vous pouvez l'utiliser et vous avez ici un lien sur ce projet.

Merci pour votre attention.

ONDREJ FILIP: Merci, Martin.

Donc, nous allons maintenant entendre la présentation des registres de ccTLD, et vous aurez le temps de poser vos questions quand tout le monde aura fini. Maintenant je vais demander au prochain narrateur de faire ça présentation ; Branko Stamenkovic va faire ça présentation, il a travaillé dans des projets de cybercriminalité au niveau européen et international et il a travaillé pour le procureur en Serbie.

BRANKO STAMENKOVIC: Merci monsieur la président.

Comme le président l'a dit, BRANKO STAMENKOVIC travaille au bureau du procureur pour le cyber-délit, oui je dépends du gouvernement et j'appartiens au secteur de la justice et je pense que c'est ma première réunion d'ICANN et je dois remercier l'invitation qui m'a été faite, elle est d'un grand intérêt pour moi, mais soyez bon parce que je dois partager dans ma présentation 3 niveaux de ce qui se fait actuellement,

lorsque il s'agit de problèmes de cybercrime au niveau local à la racine et au niveau des tierces parties, dans certains cas que nous avons trouvé en Serbie.

Au niveau mondial, nous avons un outil lorsqu'il s'agit de lutter contre le cybercrime et c'est un outil qui est la convention sur la cybercriminalité du conseil de l'Europe et ETS 185 qu'on appelle aussi la convention de Budapest qui a été signée ratifiée 2001, et 47 pays ont ratifié cette convention et nous pensons qu'il y aura beaucoup d'autres pays encore qui vont se joindre à cette convention contre le cybercrime.

Ce qui est intéressant dans cette convention c'est qu'elle dépend du conseil de l'Europe donc organisation des états européens dès qu'elle est ouverte pour sa ratification et pour tous les pays du monde.

Comme vous le voyez la Serbie a ratifié cette convention en 2005 – signé en 2005- l'a ratifié en 2009 et elle a commencé à l'appliquer en 2009 et les États-Unis l'ont signé en 2001, ratifié en 2006 et l'ont mis en vigueur en 2007.

Donc cet outil implique les autorités des États-Unis et de la Serbie dans une force conjointe qui travaille dans le monde entier.

C'est le premier traité international sur le crime et à travers donc internet, et il l'a donc une série de domaines.

Ici vous voyez sur l'écran que le cyberespace est conduit donc à différents travaux qui sont divisés en cinq groupes, d'abord la défense de la confidentialité ensuite la lutte contre la fraude informatique, ensuite la pornographie des enfants…etc., ensuite la combinaison de différents problèmes tels que spam, phishing…etc. lorsqu'il s'agit des

délits contre la confidentialité du système d'internet, les abus du DNS…etc.

Nous avons un accès légal pour le système d'informatique avec une interférence de données et dans la portée des outils de la convention de Budapest et dans le secteur de la loi, je dirais que nous avons un accès légal, une interception contrôle les problèmes d'illégalité, la fraude, la pornographie infantile, et interception de données informatiques. Donc, tous les pays qui ont ratifié aussi cette convention doivent avoir au sein de leur cadre local légal dans chaque pays tous ces outils légaux dans leur droit. Et finalement cela va permettre de toutes les autorités criminelles et lorsqu'il s'agit de cybercrime dans le monde, vont travailler sur une seule et même page avec les mêmes outils ce qu'il va faciliter notre travail pour lutter contre le cybercrime dans le monde entier.

Ensuite au niveau local, nous avons l'exemple Serbe qui a commencé dans les années 90, une tâche importante qui a été faite et que nous devions réaliser, était au niveau national, heureusement que le gouvernement de la république de Serbie et le ministre du programme numérique a adopté un système qui est un document clé lorsqu'il s'agit de l'organisation de cette protection et de la protection de l'internet et du cyberespace de la Serbie au niveau de l'état.

Comme vous voyez, la stratégie nationale pour le développement inclut la confiance des citoyens, des utilisateurs et la sécurité des données personnelles, et nous travaillons sur le besoin d'utiliser des mesures de sécurité protection des données personnelles.

Et donc, ce qui est spécifique dans mon pays, c'est que très tôt nous avons compris qu'il fallait avoir des outils et les autorités spéciales au niveau du gouvernement pour combattre le cybercrime et même au niveau de l'union européenne ce type de spécialisation est rare actuellement.

Une des raisons pour lesquelles nous avons décidé d'être spécialisé dans mon pays dans ce domaine, c'est que la portée et le poids du cybercrime était très élevé pendant les années 90 et au début de l'année 2000, et donc une ignorance des poursuites et du système judicaire dans mon pays faisait qu'on avait pensé qu'une autorité spéciale pourrait résoudre ce nouveau défit qui existe au niveau national et pourrait nous permettre de lutter contre le cybercrime et qui a affecté notre pays la Serbie et qui affecte le monde entier par les délinquants de notre pays.

Donc on a commencé en 2000. En 2004 le projet de loi était proposé à l'assemblée nationale.

2005 la loi a été adoptée par l'assemblée nationale et à partir de 2005 jusqu'à aujourd'hui nous avons donc cette loi spéciale sur l'organisation et sur la compétence des autorités spéciales du gouvernement pour lutter contre le cybercrime en Serbie.

Et cette loi comprend l'organisation, c'est une loi de procédure, ce n'est pas une loi substantielle ; elle inclut l'organisation à trois niveaux, et pour les autorités gouvernementales d'abord il y a un service spécial au niveau du ministère de l'intérieur, ensuite il y a un bureau du procureur et une cour spéciale pour le cybercrime à Belgrade.

Il est clair qu'avec ces autorités gouvernementales nous sommes maintenant au début d'une formation, d'une recherche au niveau national, nous avons le SIRT académique mais pas donc gouvernemental, donc nous voulons mettre en place cet organe pour protéger la Serbie du cybercrime.

Et rapidement, je voudrais vous monter ici que nous avons ici trois groupes de la loi criminelle qui sont différentes selon l'exécution du délit en lui-même et selon la façon dont les délinquants agissent et ici il faut souligner que tous ces délits sont en ligne avec la convention de Budapest. Comme je l'ai dit, nous avons un bureau du procureur spécial, nous avons aussi un service spécial pour la suppression du cybercrime au niveau du ministère de l'intérieur et nous avons une organisation avec le tribunal (cour), comme je l'ai dit, chambre spéciale. À nous d'avoir un tribunal spécial à Belgrade qui traite donc ces questions. Vous voyez ici les coordonnées pour le bureau du procureur, nous traitons actuellement plus de 2600 affaires. Et ici quelque chose à propos de ces affaires, si vous voyez cette image avec le masque, ce fameux masque, cette affaire est assez récente, c'est la première affaire au cours de laquelle on a trouvé une organisation qui s'appelle Anonymous en Serbie, qui a attiré notre attention par leurs tentatives pour entrer dans certains serveurs du gouvernement, et le defacing du ministère de la justice, le bureau du procureur et d'autres autorités gouvernementales, les sites de ces autorités où cela a eu lieu.

Certains proxying et DNSing étaient utilisés par ce groupe Anonymous, le proxying a été utilisé et à la fin de la journée lorsque l'on a fait des recherches et des saisies, on a constaté que cela avait été réalisé pendant les six derniers mois et qu'ils étaient parvenus à mettre en

place 776,590 opérations de phishing dans le monde entier et en Serbie, donc une seule personne a pu entrer à ce moment-là à 50% de ISP Serbienne et il a pris le contrôle du service de ces ISP, et cela veut dire qu'il pouvait contrôler le flux de données sur les serveurs de certains principaux ISP de la Serbie.

Une des principales menaces, est les abus des cartes de crédit, et ces cartes de crédit concernent toujours les identités volées sur internet et l'utilisation de la carte de crédit donne lieu à beaucoup de proxys dans le monde mais aussi en Serbie. Donc finalement à la fin de l'exécution de cette affaire criminelle, on a des compagnies des fois mais la plupart du temps des citoyens qui constatent un vol de leur propriété sur la carte de crédit ; donc on comprend que ce type de crime est dangereux pour le public en général et pour tout le monde disant.

Une des affaires criminelles que nous avons aussi rencontrée, c'est la pornographie infantile sur internet et par définition il s'agit toujours des personnes qui réalisent ces crimes vont utiliser des proxys anonymes et des faux DNS ou des serveurs dans des sous-réseaux ou dans d'autres branches d'internet sur lesquelles ils vont contrôler des espaces de l'ISP ou du gouvernement. Donc lorsque l'on cherche des délinquants, il faut avoir beaucoup de patience, beaucoup de connaissances et beaucoup de coopération internationale. À certain moment nous avons rencontré une coopération qui n'était pas vraiment très bonne au niveau des ISP étrangers mais je dois admettre que nous avons une coopération impeccable avec les autorités américaines dans ce domaine, et je pense que le danger de la pornographie infantile sur internet peut réveiller tous ceux qui sont un petit peu endormis dans ce domaine parce que c'est un danger important.

Voila quelques cas intéressants sur les abus des domaines d'internet, qui est le cas de EscrowEurope.com, un DNS faux et un site faux qui ont été détruits par les responsables de Serbie, qui ont demandé au système de surveillance de direction en ligne des États-Unis et lorsque ce type d'exécutions ont eu lieu, ils ont accéléré leur conduite. Vous allez voir maintenant certains articles achetés sur internet, envoyer une guitare, et des objets dont les prix allant de 2000 $ à 20 000 $, et nous avons même vu saisir une moto de course par exemple, un peu de n'importe quoi donc c'est très intéressant. Donc actuellement ce que les délinquants sont prêts à faire au cours de l'exécution des actes criminels pour avoir des gains financiers et pour envoyer cette moto des États-Unis à Belgrade en utilisant un avion cargo. Et le reste des attaques de DNS qui ont lieu souvent et qui peuvent donner lieu à des graves dommages préjudices, non seulement pour les ISP mais aussi pour les utilisateurs des ISP c'est-à-dire les compagnies et pour les citoyens aussi de ces pays. Par exemple dans le cas de cette attaque de DDOS qui avait eu lieu en Serbie et qui a vraiment annulé l'accès à internet en Serbie pendant 12 heures, donc le réseau central de la communication de fournisseurs à l'extérieur de la Serbie et le principal fournisseur en Serbie a été en danger, et pendant 12 heures nous avons eu aucun trafic qui pouvait sortir ou entrer en Serbie sur internet.

En résumé, je dirais que je suis membre du gouvernement et j'appartiens au système de justice, mais vous pouvez voir ma présentation que nous avons une spécialisation au niveau des autorités gouvernementales et nous pensons que cette spécialisation va devoir augmenter auprès des fonctionnaires et surtout au niveau des organisations gouvernementales légales, et nous allons voir de plus en

plus de procureurs spécialisés, de juges spécialisés dans ce domaine et ils seront donc les personnes qui vont devoir gérer ces problèmes, demander davantage d'informations et qui vont devoir demander des informations à l'étranger, nous allons plus pouvoir rester à l'intérieur des frontières de notre pays parce que nous savons qu'il s'agit de crime transnational, et donc nous allons devoir utiliser les outils qui sont en notre possession comme la convention de Budapest pour demander des preuves, des informations et nous allons le faire en coopération avec nos collègues des agences de mise en vigueur des décisions légales ou de la loi, heureusement nous pensons que c'est la protection de notre société en général et des sociétés du monde entier.

Si vous avez des questions, je suis à votre disposition. Merci.

ONDREJ FILIP: Merci pour ta présentation.

Nous avons une autre présentation qui va montrer la méthodologie des recherches et l'appropriation de noms de domaine qui va être présentée par deux personnes du département de la sécurité intérieure du gouvernement des États-Unis, c'est le centre d'investigation sur les cybercrime. Nous avons alors, Christopher Malone et Christopher Landi.

CHRISTOPHER MALONE: Merci monsieur le président et merci Margie.

Je suis CHRISTOPHER MALONE, je suis agent spécial pour le département de recherche sur la sécurité intérieure du département de

sécurité interne, et je travaille au centre du cybercrime à Washington D.C., ce que l'on appelle le C3.

Avec mon collègue ici présent, ancien membres d'ad hoc du GAC pour le groupe consultatif de l'application de la loi, et comme vous le savez, nous avons défendu l'idée d'avoir un organisme qui défend les affaires de gouvernance d'internet, pour ce qui est des intérêts de l'application de la loi, on travaille donc sur la transition d'IPv6 et les périodes de rétention standardisées et la précision des enregistrements, mais on a déjà discuté de ceci les dernières 48 heures, je suis ici au nom de la précision et de l'importance des données WHOIS pour nos activités de recherche.

Lors de nos discussions avec ce groupe, on a les membres ici présents ; le FBI, la DEA, et les services secrets de mon pays et on a aussi des collègues du Royaume-Uni et du RCMP, des gens de l'Europe, et on partage cette vision de l'importance des données WHOIS et comment cela est important pour nos activités de recherche.

Et dans mon échange avec eux, on a discuté le fait que les gens pensent que nos activités de recherche sont peu conventionnelles, ceci semble évident mais peut-être parfois les gens ne connaissent pas les méthodologies dont on se sert pour faire nos recherches, donc vu ces commentaires j'ai préparé une présentation sur les aspects un peu peut-être anodins de notre nature, et qui traite sur l'importance de la précision des données pour initier nos activités.

Aujourd'hui je me présente comme l'enquêteur sur le terrain et n'en pas du point de vue politique ni comme défenseur, même si l'on défend

les bonnes politique du gouvernement, mais je défends la conduite dans le terrain.

Donc pour préciser la valeur de cette précision de données, un agent de notre organisation acquière des informations d'adresses IP de n'importe quelle façon à travers de différents moyens, peut-être à travers des contenus sur des sites web et peut-être que ce sont d'adresses IP associées à des échanges d'emails ou des emails qui révèlent des activités qui peuvent être criminelles, et peut-être comme information IP que l'argent donc acquière.

Pour initier la réponse, il doit se rendre sur les ressources ouvertes et libres et suivre le titulaire de ce registre pour identifier qui est le délinquant, et donc il doit se servir d'outils du WHOIS pour voir quand le site web se sert des outils et des méthodologies pour se connecter, on espère à un fournisseur d'internet, et l'agent cherchera à suivre les processus légaux sous une investigation d'un tribunal dans mon pays, et potentiellement on cherchera le titulaire de ce registre pour identifier la personne qui a fait cette contrefaçon.

On ne parle pas ici d'outils d'autorité parce que sont déjà mis en place, et ma discussion avec mes collègues et que l'on se dit, il y a des outils et des autorités en fait, et peut-être quand on identifie des modifications qu'on voudrait faire aux autorités ou aux outils mais ici il ne s'agit pas d'extension d'élargissement mais il s'agit de processus légaux qui sont en train d'être utilisés de façon légale, ne sont pas à la discrétion de l'investigateur, et à moment donné le processus devra passer pas cette évaluation judicaire et les membres de notre groupe de pairs devra être évalué par un juré.

Et on ne cherche pas à élargir ces outils comme je l'ai dit, ce que l'on dit est que ça serait une étape qui devrait être critique pour commencer à voir ces registres de façon précise, et lorsque l'on génère ces subpoenas on ne pourrait pas espérer que la personne répond immédiatement, on a entre 14 et 30 jours pour répondre.

Les données qui ne sont pas précises à la fin de cette période de 30 jours sans réponse du fournisseur d'internet mènent à une nouvelle demande, un nouveau fournisseur d'internet que ce soit par la non-réponse ou parce que la réponse n'a pas été précise, quant aux données transférées. Alors vous imaginez le plus des obstacles que nous avons, d'élargir ce processus, et vous savez peut-être que ces données ont une date d'échéance, on ne retient pas toutes des données, dans mon pays on a discuté et je sais que l'on est en train de discuter toujours quel est le délai de temps pendant lequel on pourrait retenir les informations.

Mais collègues de RCMP vont traiter ce sujet dans leur propre pays mais tout délai nécessaire pour acquérir les informations précisément, bien sûr font que la recherche prend davantage de temps, et donc pour obtenir un processus légal, les informations dont on a besoin pour présenter les demandes aux fournisseurs d'internet; l'adresse IP même n'est pas une panacée. Ceci c'est un pas qui déclenche une série de d'autres mesures et qui requière d'autres outils d'investigation pour connecter la personne qui paye les factures avec le potentiel délinquant, qui n'est peut-être pas le délinquant ou la personne qui commet des délits et qui est incluse sur cette diapo. La due diligence inclut l'identification de l'individu cible et obtenir l'évidence numérique et d'autres sortes d'évidences qui peuvent être utiles pour le procureur. Pendant que l'on fait des efforts pour commencer à travailler, pour

pouvoir identifier les délinquants, pour pouvoir faire davantage de recherches et qui peuvent être nécessaires ; c'est ça que l'on voudrait préciser. Mais d'habitude on entend parler de ces ressources qui devraient être limitées et je défends l'agent dans le terrain qui doit gérer 5, 10, 20 cas, et qui doit prendre ces mesures et suivre ces étapes et ces mécanismes, faire mesure qu'il avance dans sa recherche pour découvrir le potentiel crime en ligne et ces évidences dans les périodes élargies que nous devrions permettre qu'ils reçoivent des réponses précises de la part des fournisseurs internet pour la précision des données WHOIS.

Président, si vous le permettez, je passe la parole directement à mon collègue !

CHRISTOPHER LANDI: Bonsoir tout le monde, comme Ondrej a dit je m'appelle Christopher Landi, je travaille dans le centre d'investigation de recherche de crime du département de sécurité interne. Je voudrais féliciter mon collègue de parler d'une panacée pour se servir de ce terme (panacée), on a parié qu'il ne réussirait pas à le faire. Mais je vais discuter brièvement, ce qui se passe après l'identification d'un nom de domaine que ce soit un nom de domaine qui héberge de la pornographie enfantine ou alors d'un viol, droit d'une propriété intellectuelle… l'un des outils dont on pourrait s'en servir pour avoir les informations qui portent atteinte sur internet, sont les appropriations des noms de domaine à travers un processus léga. Ceci pourrait vous faire peur mais en fait on veut être compréhensif et d'aborder ce sujet sérieusement. On ne va jamais interrompre d'activités légales, donc en fait on cherche à avoir des

personnes très malhonnêtes c'est-à-dire des personnes qui sont titulaire d'un domaine avec des images de pornographie enfantine, avec des images d'enfants de 2 ans qui sont en train d'être violés, c'est ça que l'on cherche, et donc l'une des premières étapes, c'est d'identifier l'URL complet. On veut être sûr que tous les caractères ou toutes les erreurs typographiques soient exactes, parce que si l'on fait une petite erreur de frappe, on peut avoir un autre domaine qui n'a rien à avoir. Et puis on veut savoir qui haute ces informations ou ces données illégales?, où est-il? S'il se trouve sous un dossier et où est-ce que ce dossier est hébergé?

Et puis on va vérifier le contenu, on pourrait acquérir des informations sur l'URL de la part d'un citoyen privé, d'une agence d'application de la loi ou même d'un des titulaires d'un registre. On va d'abord vérifier le contenu, est-ce qu'il s'agit d'abus enfantin ou alors de matériels IPR qui ont changé? Ou alors, est-ce qu'il faudrait capturer le contenu du site web parce que si la personne le change pour des propos légaux, on devra savoir quand est-ce que l'on a trouvé ces informations sur ce site. C'est là que les informations sont importantes parce qu'on peut déterminer qui est le titulaire de ce site web, qui l'a enregistré, qui est le registrant. Ceci pourrait conclure la recherche et pour certains cas ceci veut dire que les victimes enfantines sont téléchargées en temps réel qui sont en train d'être violées, et tous ces crimes peuvent être identifiés. Une fois que l'on les a identifiées, on vérifie le contenu et on cherche où se trouve ce contenu illégal, et on devra voir s'il y a des activités illégales parce que des fois il n'y en a pas. Ce que l'on fait d'habitude, c'est de passer un processus légal pour faire que ce site soit fermé, on n'a pas à appeler la titulaire du registre pour qu'il ferme ce

nom de domaine. On doit le modifier du fait qu'il y a des contenus illégaux mais on doit toujours traverser le processus légal pour qu'il fasse les démarches légales pour fermer son site web, donc on devra passer par ces démarches.

On va voir un peu plus sur les différentes locations où ceci peut être contenu. Mais je voudrai m'assurer que tout le monde comprenne que nous ne faisons pas de suivi, ni nous fermons des sites où on a une image avec copyright, ce que l'on cherche, c'est des personnes qui gagnent des milliers de dollars ou des millions de dollars avec des images de pornographie enfantine ou des producteurs de pornographie enfantine, ce sont les sites qu'on est en train d'arrêter.

Avec ceci. Ondrej vous avez la parole encore une fois.

ONDREJ FILIP: Merci CHRISTOPHER pour cette intéressante présentation, on ce moment vous pouvez poser vos questions. Est-ce que quelqu'un a des questions?

Bien, nous avons une question.

Dites votre nom s'il vous paît avec de poser votre.

FRANK SCHILLING: Bonjour, je suis FRANK SCHILLING, et je suis un candidat connu ou surnommé l'Uniregistry, c'est un registrant de nom de domaine, lorsque je vous entendais parler, je trouve que cette fin de la session très intéressante et le consommateur internet et l'opérateur du registre prend le risque de vivre dans un monde où tout le monde pense à la

vengeance, avant on avait un processus à suivre, une due diligence et le gouvernement nous protégeait, le risque est de continuer à vivre dans un monde où même si les intentions que vous avez sont bonnes, on fait des erreurs, on le lit tous les jours sur internet et finalement on arrive à des endroits où l'on ne voulait pas en arriver. On a des intentions pures et respectables ; personne ne veut voir la pornographie enfantine bien sûr. En fait lorsque l'on devient le victimaire, le juge ou le juré où on a l'application de la loi, on passe un jugement. Peut-être il s'agit d'une évolution naturelle de la technologie, et une partie de ceci nous fait penser au monde avant internet, ça nous énerve vous savez. Est-ce que vous avez des discussions internes? Est-ce que ceci est un peu trop? Qu'est-ce que l'on peut faire au lieu de vieillir dans cet embarras, de vous avoir trompé? Est-ce que vous avez des mécanismes de contrôle interne? Qu'est-ce qu'il vous vient à l'esprit lorsque l'on parle de contre-mesure? Est-ce que vous avez des systèmes de contrôle, c'est ça? Est-ce que l'on peut parler de cet aspect?

CHRISTOPHER LANDI: Oui bien sûr, nous avons des mécanismes de contrôle. Moi-même je ne pourrais pas compléter une recherche moi-même, sur plusieurs niveaux on a un agent sur le terrain, des superviseurs, on a des dispositions de première ligne, de deuxième ligne, un cas peut être amené chez un procureur, un juge ou n'importe quelle personne qui doit réviser. Donc on a des mécanismes de contrôle.

Je vous ai entendu dire des extras limitations, est-ce le gouvernement s'extra limite ! Je ne veux pas parler de trop et je ne vais rien dire là-dessus, mais je peux vous dire que la raison pour laquelle l'application

de la loi vient dans ces réunions parce que l'on console la communauté en tant que communauté, et dons on vient pour chercher des réponses ici. On ne veut pas que nous dise qu'on doit légiférer, on cherche à nous faire entendre, c'est qu'on voit, autant que communauté technique qui gère internet, comment peut-on résoudre ce problème, comment permettre à internet de continuer à être aussi libre quelle est actuellement sans ces gens malhonnêtes qui gâchent tout pour tout le monde malheureusement. De toute façon pour certaines personnes le viol des enfants n'est pas un problème. Mais bon.

FRANK SCHILLING: Je pense que personne ne veut penser ainsi et c'est pour cela qu'on a des agences pour l'application de la loi mais puisque vous avez des mécanismes de contrôle, on se réunit trois fois par mois, non pas récemment mais on entend parler tous les mois de ce type de délit mais on s'intègre là-dessus, on ne sait pas quelle est la limite et jusqu'où on peut arriver ! Et si personne ne dit rien, peut-être qu'on se demande est-ce que on s'est extra limité, est-ce qu'on devrait chercher une limite et donc de passer le pouvoir des États-Unis aux registres étrangers. Je ne suis pas un américain mais j'habite aux États-Unis, j'adore les États-Unis, mais je pense qu'il y a un risque appliqué, qui pourra être de s'extra limité, de surpasser la conclusion logique d'arriver au point où l'équilibre du pouvoir passe d'un environnement centré, et c'est cela qui ne me laisse pas dormir le soir.

On a besoin d'un mécanisme de contrôle, c'est pour cela qu'on vient à ces réunions, pour parler de ce problème et le résoudre.

CHRISTOPHER MALONE: Je voudrais élargir ce que l'on a mentionné du mécanisme de contrôle, oui le mécanisme de contrôle, le principal des enquêteurs, sont les instruments du pouvoir judicaire de tous les pays qui représentent, par exemple moi j'ai un procureur dans ma juridiction qui est ici présent, je ne sais pas où, mais lui-même est un contrôle, et je ne vais pas présenter un cas qui ne veut pas gagner à un juré supérieur, c'est un juré de 12 personnes potentiellement, donc ce sont des élargissements à futur qu'on doit considérer.

C'est une zone de crise d'activité, ce sont des investigations légales, qui sont approuvées et ce sont des outils judiciaires honnêtes pour obtenir ce genre d'information qui couvrent les couches qu'on devrait inclure aux niveaux les plus basiques où un investigateur ne va pas chercher des informations non pertinentes pour sa recherche. Et c'est pour cela qu'on un mécanisme de contrôle.

NANCY LUPIANO: Margie, c'est NANCY qui parle. C'est la fin de la session, on a plus le temps.

MARGIE MILAM: Avons-nous assez de temps pour terminer la file d'attente?

NANCY LUPIANO: Vous avez cinq minutes.

ELLIOT NOSS: Merci, je suis ELLIOT et je vais parler de la langue dans ce dialogue.

Christopher, tu as fait une référence à la pornographie enfantine et à la propriété intellectuelle une fois, et la pornographie enfantine cinq fois et vous avez dit: ce n'était pas une image isolée, c'était des gens qui gagnaient des milliers de dollars ou même des milliards de dollars. Je voudrais vraiment vous mettre au défi d'identifier une propriété qui se soit rapprochée à des milliards de dollars et je répète ceci parce que les données publiques disponibles suggèrent que la large majorité de ces références impliquent des problèmes de propriété intellectuelle, et que l'élargissement des délits, des propriétés intellectuelles se sont multipliées ces cinq dernières années disant, donc lorsque l'on parle de ces problèmes, je trouve incroyable de n'avoir personne ici dans la salle qui soit pour la pornographie enfantine, on va pas y parvenir à trouver une personne mais y a d'autres problèmes plus polémiques autour des extensions des droits de propriété intellectuelle et c'est de là que les problèmes viennent. C'est là qu'on a notre réponse. Dans le Royaume-Uni nous avons non seulement l'élargissement des crimes de propriété intellectuelle dans un pays, mais c'est en fait même l'application extraterritoriale de ces lois, et ceci est une portion significative son seulement pour la communauté internet mais pour toute la communauté d'utilisateurs d'internet, et je suggère puisque nous allons revenir armés contre la pornographie enfantine et contre d'autres problèmes qui constituent des délits sérieux, qu'on puisse avancer dans cette voie et continuer à travailler pour élargir les droits de propriété intellectuelle. Si on pourrait battre les problèmes de délits les plus sérieux et certains des problèmes qui sont plus significatifs pour la communauté, si on pouvait appliquer les droits commerciaux privés. Merci.

CHRISTOPHER LANDI: Je te remercie de faire ce commentaire, c'est plutôt une question législative, je peux parler aux politiques de mon agence mais je ne peux pas dire si je suis d'accord ou pas, mais je peux dire qu'on a des crimes financiers qui font des profils de milliards de dollars, et dans certains cas nous avons les liens avec IPR et parfois on voit des violations de IPR, est ce que c'est la seule coopération qui est impliquée, non mais peut-être c'est la seule coopération qui gagne des milliards de dollars, et donc on recherche ce type de délit, et quant à l'IPR c'est plus facile pour moi, il s'agit d'un problème d'investigation politique, et le public sait ce qu'il sait, il veut qu'on applique la loi, il faudrait voir comment ils veulent qu'on change les lois, je ne vois pas que tout le monde fasse du lobbying. Pour qu'on leur permettre de violer des enfants de 2 mois. Donc violations d'IPR, oui je comprends ce que tu veux dire, on a un conflit là-dessus, et je comprends ce que tu veux dire.

ONDREJ FILIP: C'est une question?

ZAHID JAMIL: Oui ça prendra qu'une minute, d'habitude on parle très vite pour décrire nos problèmes, je voudrais parler sur l'IPR et je parle de mon propre nom, je ne représente personne, je viens d'une zone du monde ou l'IPR est un aliment pour le crime organisé. Peut-être dans les États-Unis vous avez d'autres aspects là-dessus. Je voudrais soutenir votre travail dans cet aspect, par rapport à l'approche centrée sur les États-Unis, pour moi on a un problème que le reste du monde n'a pas jusqu'à

présent dans l'application sur internet et ceci porte sur ce que Branko a dit du crime organisé. Comment vous considérez ceci en tant que crime organisé global ou régional, on dit parfois il s'agit d'une organisation régional, Il me semble étrange, je ne vois pas les États-Unis, le Canada et l'Union européenne ou le japon, comment voyez-vous ceci par rapport à la permission de parties à travers les frontières, et d'accéder dans la convention. Est-ce que ceci serait utile? Je voudrais aussi des copies de votre présentation parce que je ne la vois en ligne.

MARGIE MILAM: Oui, ils doivent être en ligne en ce moment, je pense que l'on n'a plus le temps maintenant.

BRANKO STAMENKOVIC: Bon, je réponds rapidement.

Oui, je vois que la convention du cybercrime est un outil global parce qu'il a été soutenu par tous les membres du conseil d'Europe conjointement avec les États-Unis comme vous l'avez dit, et le Japon va ratifier cette convention et la dans la dernière conférence d'octobre y a quelques semaines, on a maintenu cette conférence et le conseil d'Europe et plusieurs pays d'Amérique du sud et du Moyen-Orient vont mettre en place la convention du cybercrime et pour la ratifier. Et donc les outils légaux ont été mis en place par la convention de Budapest et ces dispositions ont été mises en place dans les cadres légaux de chaque pays, donc c'est un grand outil que l'on se sert de lui directement ou indirectement et on aura davantage de pays qui vont rejoindre ce processus.

ONDREJ FILIP: Merci à tous les orateurs, et merci pour la discussion, et merci à Margie d'avoir organisé cette session aussi intéressante. Merci.

[Applaudissements]

[Fin de la transcription]