ICANN69 | Réunion générale annuelle virtuelle – Changements du WHOIS sous le RGPD : impact sur les utilisateurs finaux et la sécurité publique
Mercredi 21 octobre 2020 – 10h30 à 12h00 CEST

OZAN SAHIN: La séance va commencer, veuillez commencer l'enregistrement s'il vous plait.

Bonjour et bienvenue à cette session changement de WHOIS conformément au RGDP, impact sur les utilisateurs finaux et la sécurité publique.

Je m'appelle Ozan Sahin et je vais administrer cette réunion à distance. Veuillez noter que cette séance est enregistrée et est conforme au code de conduite attendu à l'ICANN.

Pendant cette séance, les questions et commentaires ne seront lus que s'ils sont soumis en langue anglaise dans l'onglet correspondant Q&A. Vous pourrez y accéder dans la barre d'outils de Zoom. Je vais lire les questions et commentaires à haute voix pendant le temps alloué par le modérateur de cette séance.

La séance inclut la transcription en temps réel et l'interprétation. Pour accéder à la transcription en temps réel, cliquer sur « closed caption » dans la barre d'outils de Zoom. L'interprétation pour cette séance va inclure l'arabe, le chinois, l'anglais, le français, le russe et l'espagnol. Vous pourrez y accéder par l'intermédiaire de Zoom et de la

plateforme d'interprétation simultanée à distance opérée par Congress Rental Network. Les participants sont encouragés à télécharger l'appli de CRW en suivant les instructions dans le chat de zoom ou sur la page web de la réunion.

Si vous voulez intervenir, veuillez lever la main sur la salle Zoom et une fois que le modérateur vous appelle, nos techniciens vous permettront d'activer votre micro. Veuillez alors indiquer votre nom pour la transcription et la langue dans laquelle vous allez intervenir si c'est dans une autre langue que l'anglais. Lorsque vous interviendrez, assurez-vous de mettre sur muet tous les autres dispositifs, y compris l'application de Congress Rental Network. Veuillez parler distinctement et à un rythme raisonnable pour permettre une interprétation exacte.

J'aimerais insister sur le fait que les participants à distance ne peuvent pas cliquer sur le bouton micro et activer leur micro pendant cette réunion sans l'assistance du technicien.

Sachez que les participants de cette séance peuvent faire des commentaires sur le chat. Pour ce faire, vous pouvez utiliser dans le menu déroulant du chat l'icône répondre à tous les panélistes et participants. Veuillez noter que les chats privés ne sont possibles qu'entre panélistes et dans ce format de webinaire Zoom. Tout message envoyé par un panéliste ou un participant standard sera également vu par les hôtes, co-hôtes et autres panélistes.

Sur ce je vous cède la parole. Jonathan Zuck c'est à vous.

JONATHAN ZUCK : Merci. Je suis vice-président de l'ALAC. Comme vous le savez, At-Large a pris l'utilisation malveillante du DNS et les questions annexes comme questions prioritaires cette année.

Mais on a l'impression qu'on en parle sans arrêt et qu'on n'est pas arrivés bien loin finalement en l'absence de données. Il y a beaucoup de discours, d'un côté comme de l'autre, des discussions rationnelles qui portent sur cette question, une question très complexe du reste. Et, très souvent, on voit dans le contexte de l'ICANN que parfois les prévisions qui sont faites dans le feu de l'action, par rapport à de nouvelles politiques, ne se transposent pas dans les faits finalement.

Par exemple, lorsque le nouveau programme des gTLD a d'abord été proposé, il a été suggéré que nous allions investir 12 millions de dollars dans la défense des enregistrements. C'est ce qu'ils prétendaient faire, et finalement ils ne l'ont pas fait. Ils ont trouvé un moyen pour protéger leur marque.

Et, de même, par rapport à l'entrée en vigueur du RGPD et la sonnette d'alarme qui a été tirée à la suite de cela par la communauté ICANN pour la mise en œuvre des spécifications temporaires, la constitution d'un groupe de travail sur les politiques accélérées, et la manière dont nous allions pouvoir être conforme au RGPD. Et donc tout cela a engendré un changement dramatique par rapport à la disponibilité des données publiques dans le système WHOIS. Et un nouveau système a été mis en place par lequel les gens devaient remplacer des informations des parties contractantes.

Donc, tout au long du processus EPDP il y a eu les gestionnaires de données et les demandeurs de données qui sont devenus des parties prépondérantes de ce processus. Et ça, ça nous a permis de voir qu'on a des conversations mais on ne se rend pas bien compte du niveau de requête qui est fait et comment ces requêtes sont gérées. Très souvent on est surpris par le fait que ces chiffres ne sont pas si élevés qu'on pourrait s'y attendre.

Et tout ça, ça commence par des chiffres, des faits, qui peuvent rassurer ou pas. Il faut voir quelles sont ces données. Il se peut que les parties qui sont en premier lieu concernées par l'accès aux données d'enregistrement ont trouvé des solutions alternatives pour obtenir ces données afin d'assurer l'application de la loi, la protection des consommateurs, etc.

Donc, il s'agit de faire un état des lieux d'où on en est actuellement, quelques années après, en termes de disponibilité des données, efficacité, les requêtes qui sont faites par les parties contractantes, etc. Et voilà donc l'idée de cette séance et de l'organisation de cette séance et de la conversation que j'aimerais avoir avec vous aujourd'hui.

J'espère qu'on va pouvoir avoir le moins possible une discussion idéologique, mais plutôt une discussion factuelle et pragmatique.

Pour lancer un petit peu cette conversation, on va demander à l'une des parties prenantes de la communauté, à savoir les forces de l'ordre, de nous donner leur point de vue.

Laureen Kapin, de la Fédéral Trade Commission, FTC, va nous parler de la perspective des forces de l'ordre, du besoin de trouver des solutions alternatives, savoir ce à quoi ressemble le processus depuis ces deux dernières années.

Donc Laureen, sans plus attendre, je vous cède la parole. Il faut que vous activiez votre micro Laureen.

LAUREEN KAPIN : Merci, excusez-moi c'est un peu tôt encore pour moi, vous savez le fuseau horaire n'est pas très avantageux pour moi. Je m'appelle Laureen Kaplin, et je suis ici pour vous donner la perspective des forces de l'ordre et de la protection des consommateurs.

Diapo suivante s'il vous plait.

Je suis avocate à la FTC et je travaille aux affaires et à la protection du consommateur. Et cette question préoccupe mon agence depuis un certain nombre d'années. Et ce que je vais vous dire reflète mon avis personnel et non pas l'avis de la FTC pour laquelle je travaille, c'est mon avis personnel en tant qu'avocate. Et je suis également co-présidente du groupe de travail sur la sécurité publique qui fait un plaidoyer dans ce sens depuis un certain nombre d'années maintenant.

Donc la FTC a une ressource extraordinaire où les consommateurs et le public, non seulement aux États-Unis mais dans le monde entier, peuvent déposer des plaintes lorsqu'ils ont été victimes ou sont préoccupés par des pratiques trompeuses ou des fraudes. C'est ce qu'on appelle la base de données des consommateurs qui collecte des

dizaines de milliers de plaintes par an et beaucoup de personnes contribuent à cette base de données de par le monde.

Et ce n'est pas surprenant de voir que lorsqu'on analyse ces plaintes, on peut avoir un instantané de la manière dont le public, le public qui veut acheter des choses, obtenir des informations, retrouver des amis, comment le public utilise WHOIS, parce que la référence à WHOIS se trouve au cœur de leur plainte.

Donc qu'est-ce que j'ai fait ? Je me suis penchée sur une partie de ces plaintes, en particulier après les changements au système WHOIS, et lorsque je parle de changements du système WHOIS, je parle des changements qui masquent certaines informations, en particulier les données de contact des titulaires de noms de domaine.

Et voilà ce que j'ai trouvé : les utilisateurs utilisent WHOIS pour toute une série de choses, mais essentiellement ils cherchent des informations fiables. Ils veulent chercher dans WHOIS un moyen d'effectuer une recherche avec diligence raisonnable, ils veulent savoir qui est responsable, donc ils veulent prendre contact avec cette personne. Et, parfois, c'est ce que j'ai vu dans ces plaintes, ils enquêtent eux-mêmes sur une fraude lorsque quelqu'un essaye de découvrir quel est le nom de domaine qui peut les avoir fourvoyés.

Et les consommateurs ont noté dans ces changements WHOIS qu'il y a des informations expurgées ou qui manquent. Et ils pensent que ça, c'est malhonnête parce qu'il y a un manque d'information. Et c'est

vrai ou pas puisque la manière dont le FTC reçoit ces requêtes fait qu'il ne vérifie pas ces informations. Il reçoit simplement ces plaintes.

Donc ça, ça interfère un petit peu avec les efforts de diligence raisonnable. Par exemple une personne se plaint qu'il n'y a pas de données par rapport à telle ou telle chose. Donc vous voyez qu'il y a toute une série de manière dont les gens utilisent cela. Et voilà les termes que j'ai retrouvés le plus dans les plaintes que j'ai examinées.

Pour vous donner une idée, parce que je n'ai plus que quelques minutes d'intervention, pour vous donner une idée donc du type de fraude sur lesquels on enquête, des biens contrefaits, des fraudes par rapport aux animaux de compagnie, vous seriez impressionnés de voir le nombre de fraudes par rapport aux animaux de compagnies, inventions techniques, également des choses liées au coronavirus, le hameçonnage, des fraudes gouvernementales, il y a toute une variété de fraudes et d'escroquerie.

Et j'aimerais insisté sur le fait que les gens n'utilisent pas simplement les données de contact de WHOIS, et là on a de la chance parce qu'il y a encore des informations utiles là, parce qu'on sait lorsque le domaine a été créé, donc lorsque l'utilisateur final utilise les données WHOIS pour se protéger et qu'il y a un certain niveau de frustration qu'on peut noter dans ces plaintes, c'est parce que ces informations ne sont pas disponibles à cet effet.

Et sans plus attendre, je vais céder la parole à mon collègue Gabriel.

GABRIEL ANDREWS: Alors, je vais parler au nom des forces de l'ordre et de manière anecdotique. C'est difficile d'avoir des chiffres réels et précis de la part des forces de l'ordre.

Il y a plusieurs questions qui se posent, que ce soit le RGPD ou la loi californienne sur la vie privée du consommateur, en fin de compte ce qui est important pour l'enquêteur, c'est qu'il essaye d'avoir accès aux données et les données ne sont pas là. Donc pour parler d'une de ces questions, il faut finalement parler de toutes ces questions.

Diapo suivante s'il vous plait.

Et j'aimerais voir combien de temps ça prend pour avoir accès aux données. C'est important parce qu'il y a différentes durées en fonctions des conditions et des situations.

Avant, vous pouviez faire une recherche et revenir vers la personne qui faisait la requête en 10 secondes. Ça c'était par le passé. S'ils n'obtiennent pas ces données, ils ne vont pas forcément se tourner vers le bureau d'enregistrement pour obtenir des données expurgées, s'il n'y a pas de service d'anonymisation et d'enregistrement fiduciaire, alors il y aura une réponse aux forces de l'ordre, il s'agira d'informations expurgées. Et certains répondront aux forces de l'ordre locales. Et si vous n'êtes pas cet agent, alors on va peut-être vous demander une procédure juridique. Alors là il s'agit d'une demande d'instruction ou ce genre de chose, bref quelque chose d'officiel au niveau juridique. Donc si le bureau d'enregistrement le fait de manière volontaire, si vous parlez d'une procédure juridique alors il faut

envisager une à deux semaines d'attente. Donc vous avez besoin d'un processus juridique théoriquement, si vous êtes signataire du traité d'entraide judiciaire, vous pouvez obtenir peut-être en 6 mois les données.

Diapo suivante.

Donc lorsque l'on parle de l'impact, j'aimerais vous parler un petit peu des processus et des responsabilités que nous avons concernant les notifications. Par exemple ici, vous avez une compromission d'un courriel commercial - et ça arrive souvent sur l'internet aujourd'hui, nous avons 23 milliards de dollars qui ont été perdus et le chiffre double pratiquement chaque année. Donc je ne sais pas ce que ça va être en 2020 - Donc vous voyez ce mauvais acteur dit qu'il est PDG d'EXEMPLE.COM et c'est un homoglyphe, c'est un domaine qui ressemble à véritable nom de domaine, un nom de domaine commun, donc il fait transférer et gagne ainsi des centaines de millions de dollars. Donc nous devons faire une recherche inversée du DNS pour remonter à ces noms de domaine, voir comment il a été enregistré et on peut retrouver les victimes de cette manière également. Donc si on va rapidement, si on est rapide à ce niveau et bien on sera en mesure de faire beaucoup de requêtes DNS sur ces victimes et nous aurons des contacts et en temps réel nous pourrons leur dire : vous avez un mauvais acteur qui essaye de vous contacter pour vous soutirer de l'argent.

Donc il y a différentes requêtes, différentes demandes, et vous avez un impact négatif au niveau des notifications.

Maintenant nous essayons d'obtenir plus d'informations sur ces victimes potentielles, mais on a besoin d'un système juridique à ce niveau. Ça peut prendre des semaines, ça peut prendre des mois.

Donc ça c'est une répercussion dans le monde réel du travail que nous faisons. Si on perd du temps, si on perd des jours et des mois, ça a des conséquences réelles sur le gens, les victimes de fraude. Le temps est très précieux.

Je donne la parole au prochain panéliste.

JONATHAN ZUCK : Merci Gabriel. Donc nous allons entendre parler de recherches en cybersécurité d'un groupe de consultants, de Greg Aaron et Lyman Chapin.

GREG AARON: Donc nous allons passer à la diapositive de notre présentation. Donc avec Lyman nous avons fait des recherches récemment sur l'hameçonnage et nous avons essayé de capturer beaucoup d'informations sur le nombre d'hameçonnages d'URL, si c'est très fréquent ou quoi que ce soit.

[L'interprète s'excuse, nous n'entendons plus l'intervenant]

[L'interprète vous présente ses excuses, nous n'entendons plus l'intervenant, nous avons eu une coupure. L'interprète vous présente ses excuses, nous n'avons pas actuellement le son et nous connaissons des problèmes techniques, merci de votre patience].

Donc cela dépend de ce que nous mesurons et de la manière dont nous le mesurons.

Donc Google par exemple, s'intéresse à ces mesures parce qu'ils sont en mesure de voir combien d'hameçonnage et de listes noires, de listes de blocages sont utilisés donc c'est très intéressant ces indicateurs. Vous avez d'ailleurs cela qui provient de Google, que vous avez à l'écran, qui montre les blocages et les listes noires, donc ça c'est sur une longue période de temps ce que vous voyez. C'est des logiciels malveillants qui sont retirés.

Et donc la cybercriminalité change avec le temps, et une des raisons pour laquelle les logiciels malveillants n'existent plus c'est parce qu'il y a des botnets, des robots, qui les retirent et il y a d'autres types de criminalité. Par exemple compromettre les courriels d'entreprises, comme Gabriel en a parlé tout à l'heure.

Donc nous essayons de comprendre à quel point il y a de la cybercriminalité, on essaye de mesurer cela. Comment le mesurer véritablement ? Comment voir cela d'une manière plus large ? Parce que si vous ne mesurez pas quelque chose, et bien vous avez tendance à l'ignorer.

Donc pourquoi avons-nous besoin des informations WHOIS ? Nous en avons besoin parce que nous voulons découvrir quand un domaine a été enregistré, la date d'enregistrement, le bureau d'enregistrement également qui a effectué cela. Ce sont des données qui ne sont pas sensibles, qui sont publiques et qui comptent beaucoup. Le problème que nous avons ici, c'est que nous sommes limités quelque part. Donc les opérateurs ne vous permettent de faire un certain nombre de requêtes. Donc vous savez, SSAC, ce document est tout à fait

intéressant à ce sujet, il y a des informations non sensibles qui nous seraient très utiles pour lutter contre l'hameçonnage mais auxquelles on n'a pas toujours accès.

Donc les personnes qui essayent de se battre contre cela, essayer de trouver les informations de contact et ç'est important parce que les criminels, très souvent, les délinquants, ne donnent pas leur nom réel, ne donnent pas leur adresse et contacts et coordonnées. Donc si ce n'est pas exact, ça montre bien qu'il y a de la mauvaise foi au niveau du bureau d'enregistrement et que le bureau d'enregistrement en lui-même peut faire de l'hameçonnage.

Donc nous devons comparer les informations, c'est ce que nous faisons, mais c'est de plus en plus difficile de faire cela à la suite du RGPDP. Ce que nous avons vu dans notre rapport, et ça nous le savions depuis longtemps, lorsque les criminels enregistrent un nom de domaine, et bien ils en font plusieurs à la fois, il y a un ensemble, il y a un groupement de tous ces noms de domaines enregistrés, il y a une séquence de noms de domaine. Et certains sont mis sur une liste noire, mais il y en a d'autres qui passent à travers, donc ce que l'on regarde, c'est la durée de ces attaques d'hameçonnage.

Et ça c'est des données que vous voyez à l'écran qui proviennent de personnes de PayPal, de Google et de l'université de l'État d'Arizona, une étude qui a été faite cette année d'ailleurs. Et ils sont très au courant parce qu'ils voient sur quoi les personnes cliquent et ils peuvent voir, dès la première visite, quand l'hameçonnage se fait et s'il y a un hameçon sur PayPal, et bien ils voient comment ils sont

victimes et s'ils ont perdu beaucoup d'argent sur leur compte avec PayPal. Et donc cette étude est cohérente avec d'autres études que nous avons effectuées. Et ça montre bien que les attaques d'hameçonnage sont courtes et rapides. Vous recevez votre première visite et une fois que l'hameçonnage est détecté et bien c'est environ 8 heures. En tout c'est à peu près 17 heures une attaque d'Hameçonnage. Donc en général c'est détecté, mais les dégâts sont déjà faits, la victime a déjà été sur le site et a perdu de l'argent, a été sur un faux site et donc devient victime. Cet utilisateur de l'internet devient victime.

Ce que nous avons noté c'est qu'environ 60 % des domaines utilisés par les attaques de hameçonnage sont enregistrés par les hameçonneurs.

Il y a deux catégories vous savez. Il y a des hameçonneurs qui achètent des noms de domaine et qui ont des faux sites web et ils utilisent parfois des noms de domaine qu'ils cachent au niveau de l'hébergement. Donc ils font de l'hameçonnage avec un autre nom de domaine. Ils usurpent un site web. Donc ce que l'on veut, lorsque l'on répond contre cela, c'est que ces sites soient bien gérés au niveau de l'hôte et de l'hébergement, et qu'il n'y ait pas de dommage collatéraux, pour qu'on ne puisse pas utiliser un bon nom de domaine pour faire de l'hameçonnage. Donc il peut y avoir une suspension, sans aucun problème, sans dommage collatéraux.

Mais nous avons noté avec notre méthodologie qu'environ 60 % des noms de domaine sont enregistrés d'une manière malhonnête, donc

SIDN et AFNIC, donc c'est .NL et .FR, AFNIC pour la France, ont un autre système, il y a eu un autre projet, une autre méthodologie, mais relativement similaire, c'est un système relativement élaboré qui a estimé qu'il y a 50 % des domaines utilisant ces attaques d'hameçonnages qui sont enregistrés par les hameçonneurs. C'est tout à fait intéressant.

Nous passons à la diapositive suivante.

Pour conclure, qu'est-ce qu'on peut retenir de tout cela ? Et bien nous notons que beaucoup de ces enregistrements, on a parfois du mal à les retrouver. Une des raisons pour cela est que nous n'avons pas les données qui étaient autrefois disponibles, avant le RGPD. Et, la conclusion est claire : les données de contact, c'est quelque chose qui distingue un nom de domaine d'un autre, ça indique la bonne ou la mauvaise fois, ça indique qui l'a enregistré ou qui dit l'avoir enregistré. Donc ce sont des informations importantes.

La bonne nouvelle, s'il y a une bonne nouvelle, c'est que les bureaux d'enregistrement et les opérateurs de registre ont toujours accès à ces données et ils peuvent voir ce qu'il se passe, même si personne d'autre ne peut le voir. Donc étant donné que l'hameçonnage est fait par des hameçonneurs qui enregistrent ces noms de domaine, et bien il y a une possibilité à ce niveau pour les bureaux d'enregistrement et les opérateurs de registre de continuer à utiliser ces données.

Ce que l'on voit, néanmoins, c'est qu'il y a toujours du hameçonnage qui se fait sur certains TLD et avec certains bureaux d'enregistrement. Ça, cela pose problème.

Et en ce qui concerne l'EPDP, un des résultats c'est que nous allons donc avoir des délais, on va avoir un temps d'attente et de rotation, la cybersécurité, les demandes de données dans le cadre du RGPD, quand c'est légitime, dans un intérêt légitime pour une demande de données, cela prend quelque temps, cela prend 5 jours, et ça peut même être 10 jours. Donc ça, ce n'est pas efficace parce que, comme je vous l'ai montré, les attaques durent moins de 24 h, moins d'un jour. Donc les données dans le système normalisé d'accès et de divulgation SSAD vont arriver lentement.

Donc je pense que l'hameçonnage est un excellent candidat pour l'automatisation dans le cadre du SSAD pour que ça ailler rapidement. Je crois qu'il faut véritablement réfléchir à cela, et que ce soit un travail de routine, que SSAD, ce système d'accès et de divulgation, soit utiliser et nous permettre d'obtenir plus de données pour répondre à ce problème d'hameçonnage et à toutes ces victimes pour pouvoir les aider.

Merci beaucoup.

JONATHAN ZUCK : Merci, merci beaucoup Greg. Je crois que Mark n'est pas sur cet appel. Est-ce que Mark est avec nous ?

NON IDENTIFIE : Non, effectivement, il n'est pas là.

JONATHAN ZUCK : Bon, alors on va passer au suivant. Milton pour ensuite passer à la discussion que j'espère très active après ces présentations, donc qu'on puisse avoir tous ensemble une conversation. Milton allez-y.

MILTON MUELLER: Bonjour. Je suis professeur de l'Institut de Technologie de Georgie aux États-Unis. Et d'ailleurs sur ce panel tous les intervenants viennent des États-Unis, c'est intéressant, n'est-ce pas ?

Et, de fait, WHOIS se concentre sur ces différences entre l'Europe et les États-Unis en termes de législation relative à la vie privée.

Alors, quelque chose dont on n'a pas entendu parler encore, et raison pour laquelle je fais partie de ce panel, c'est que je vais vous parler des droits et intérêts des titulaires de nom de domaine, de la personne qui enregistre un nom de domaine. Et il est aisé de comprendre pourquoi les gens qui enregistrent un nom de domaine ont un intérêt vis-à-vis de ce nom de domaine pour expurger certaines informations personnelles, certaines données personnelles identifiables. Et, conformément à certaines législations relatives à la vie privée, ils ont ces droits pour protéger ces données et, de fait, la Féderal Trade Commision, pour laquelle Laureen travaille, a beaucoup d'informations par rapport au fait de savoir pourquoi est-ce que vous ne devriez pas rendre publiques certaines informations, ou facilement disponibles en ligne, par rapport à votre adresse postale, votre courriel, etc.

Et, avec la mise en œuvre et l'application du RGPD sur le WHOIS, l'idée c'est d'utiliser ce sens commun pour réitérer que ce n'est pas une

bonne idée de rendre disponible de manière totalement aléatoire, sur internet, ce genre d'information, donc données personnelles.

Et WHOIS contient beaucoup d'informations, le nom du titulaire de nom de domaine, le pays, parfois l'État, la ville, et nous espérons que nous avons mis en œuvre une nouvelle méthode efficace pour divulguer les données expurgées, le SSAD, donc système normalisé d'accès et de divulgation.

Il est intéressant de voir pourquoi l'At-Large ne s'est pas plus intéressé aux droits des titulaires de nom de domaine. Je sais qu'ils sont supposés représenter les utilisateurs finaux, mais j'aimerais savoir quelle était la position des structures européennes d'At-Large par rapport à WHOIS. Parce que ce qui est sûr c'est qu'on n'a pas entendu de soutien vis-à-vis de la conformité au RGPD de la part de l'ALAC pendant le processus EPDP.

Diapo suivante s'il vous plait.

J'ai beaucoup apprécié l'introduction de Jonathan pour présenter ce panel en disant est-ce qu'on a des faits pour étayer cette discussion. Ce n'est pas facile de trouver des informations précises, concrètes, puisqu'on se concentre sur le fait qu'on ne parle pas du fait de savoir si le hameçonnage est mauvais ou comment ça fonctionne, mais plutôt de voir comment ces choses fonctionnaient avant et après que les données soient expurgées et après la mise en œuvre ou l'application du RGPD.

Donc si vous regardez ce qu'il s'est passé entre décembre 2015 ou plutôt mai 2008 et décembre 2015, donc 18 mois avant l'entrée en vigueur du RGPD et les 17 mois qui ont suivi la mise en œuvre du RGPD, et le taux de délits avant et après, vous voyez les chiffres à l'écran, si vous voyez ce qu'il se passe du côté du hameçonnage, vous voyez une forte augmentation avant et après l'entrée en vigueur de ces données expurgées.

Et, grâce à ces données, vous voyez qu'il n'y a pas de lien entre les données expurgées en 2018 et l'ampleur et la portée du problème. Il y a une corrélation statistique entre les données expurgées et les types de changements survenus dans le problème.

Donc je pense que l'argument qui se fonde sur les données entre les données expurgées et le problème en termes de cyberdélinquance est extrêmement faible.

Ce n'est parce qu'évidemment c'est très utile dans certains cas pour les forces de l'ordre d'avoir un accès rapide à ces données, c'est évidemment le cas, mais cet accès rapide, c'est aussi un vecteur et une cause de ce problème.

Mais le fait est que les enregistrements abusifs font que les délinquants ont appris à contrefaire ces informations et il y a des références croisées qui sont faites sans qu'on puisse facilement les détecter, en tout cas de la part des gens qui regardent les données WHOIS.

Et, dernier commentaire par rapport au hameçonnage, nous à l'université, on fait un exercice où on demande à un groupe de 5 étudiants de développer, d'élaborer un mail de hameçonnage, et ce qu'on s'est aperçu c'est que les domaines hameçonnés sont très souvent détectés par des algorithmes, par des entreprises d'hébergement, par également les entreprises de navigateurs. Et la moitié des étudiants découvre que le nom de domaine hameçonné est bloqué avant même qu'il ne soit réellement détecté.

Donc là encore, il ne s'agit pas de dire qu'on a totalement bloqué l'accès à ces informations, on ne l'a pas fait, mais il faut voir quels sont les processus politiques et trouver un moyen normalisé de faire une requête.

Et ce qu'il faut comprendre, c'est qu'il s'agit finalement de conformité, ce n'est pas quelque chose d'optionnel, il faut s'y conformer. Il faut se conformer à la loi. Et ce que l'on a fait dans le cadre des efforts de l'EPDP c'est de proposer un mécanisme pour que les requêtes soient examinées, qu'on vérifie s'il y a un intérêt légitime, voir si la requête est légitime, etc.

Voilà pour ce qui est de ma présentation, et j'attends maintenant avec impatience des échanges qui vont suivre. Merci.

JONATHAN ZUCK : Merci beaucoup Milton. Et je voulais réitérer ce qui a déjà été dit, effectivement il s'agit de se conformer à la loi.

À mesure qu'on avance, il est important de voir où on en est par rapport à cette loi. Et il ne s'agit plus de revenir sur le fait de savoir si

cette loi était bonne ou pas, il faut voir le lien entre le demandeur et celui qui administre les données. Il ne s'agit pas de revenir sur ce qui a occupé l'EPDP et le groupe de travail sur l'EPDP pendant 2 ans, ce n'est pas la peine.

Et, pour parler de cela, je pense qu'Owen, qui va nous parler d'un rapport sur les requêtes récentes – je crois qu'il y a eu un webinaire récemment fait sur cette thématique – et Owen va nous parler donc du détenteur des données et de ce qu'il s'est passé de ce côté-là depuis la mise en œuvre des spécifications temporaires.

Owen, c'est à vous.

OWEN SMIGELSKI: Merci Jonathan. Alors… Je vois que ma vidéo est activée, mais je ne suis pas sûr que vous me voyez à l'écran.

JONATHAN ZUCK : Si, si on vous voit.

OWEN SMIGELSKI: Diapo suivante. Je suis Owen, je travaille à Namecheap, je suis aussi vice-président du groupe des représentants des bureaux d'enregistrement.

Ce que je vais vous présenter maintenant c'est une version condensée d'un webinaire que les opérateurs de registre et les bureaux d'enregistrement ont élaboré en septembre dernier. D'ailleurs vous avez un lien vers le webinaire, enregistrement présentation sur la diapo pour que vous puissiez vous y référer. Je vous invite à le consulter parce que vous trouverez beaucoup plus d'informations que celles que je vais vous présenter maintenant.

Donc j'ai présenté ce webinaire avec 3 autres collègues pour présenter des informations que je ne vais pas détailler maintenant, Alan Woods de l'opérateur de registre Donuts, Beth Bacon représentant de .ORG et un autre représentant des bureaux d'enregistrement. Donc j'aimerais les remercier parce que je vais présenter certaines des informations qu'ils ont présentées lors de ce webinaire aujourd'hui.

Ce qui est important dans cette discussion c'est de dire que le RGPD et la protection des données à caractère personnel, ça n'a rien de nouveau, ça remonte à la fin de la Deuxième Guerre mondiale. Et, pendant cette période, les données à caractère personnel des gens étaient utilisées pour établir des profils et pour cibler différents groupes, comme la religion, l'orientation sexuelle, l'origine ethnique, etc. Et donc, à l'époque, l'intérêt de protéger les données à caractère personnel ont pris une importance toute particulière. C'est pourquoi la protection des données à caractère personnel c'est quelque chose de très important qu'il ne faut pas négliger, parce que certains perçoivent qu'on peut le négliger de temps en temps, mais sachez que ça figure dans la déclaration universelle des droits de l'homme en 1948, ça fait l'objet de différents traités, il y a une loi suédoise qui date de 73 qui fait référence à la protection des données à caractère personnel.

Diapo suivante s'il vous plait.

Donc il y a 7 principes présents dans toute législation européenne relative à la protection des données à caractère personnel. D'abord l'objet ou l'individu qui est objet de cette protection, je ne vais les

passer en revue ici, mais certains de ces principes sont très intéressants, très important. Il ne faut pas, par exemple, prendre plus de données que nécessaire, il faut s'assurer que les données sont stockées pendant un certain temps, il faut que cela soit fait de manière sûre et il faut être redevable de ces données.

Et, avant l'entrée en vigueur du RGPD il y avait un accès restreint aux données. Et le WHOIS violait d'ailleurs bon nombre de ces principes.

Diapo suivante s'il vous plait.

Donc j'aimerais vous donner un aperçu un petit peu des problèmes dont nous parlons aujourd'hui, de notre thématique. Donc le RGPD ce n'est pas nouveau. Il y a eu quelques changements au niveau de la responsabilité civile par exemple, mais c'était déjà présent en Europe et dans d'autres pays et traités de nombreuses années avant. Et le WHOIS existe toujours, maintenant il se conforme tout simplement à la loi. Et je sais que ça a été répété, les données WHOIS ne représentent pas le meilleur chemin pour arrêter les abus. Donc je crois qu'il faut travailler plus facilement avec les prestataires de services, d'hébergement par exemple, l'analyse doit être pour savoir qui fait quoi.

Et, on l'a vu, le hameçonnage va très rapidement, donc il faut véritablement agir rapidement si on veut prendre des mesures. Et, une nouvelle fois, toutes, CCPA en Californie, la loi qui protège le respect à la vie privée en Californie et tout cela, ça ne fournit pas le droit aux

parties tierces d'avoir accès aux données et ce n'est pas une obligation non plus de divulguer les données.

Donc nous avons les données qui sont expurgées, qui ne sont pas expurgées, et le hameçonnage, le problème des pourriels, des spams, tous ces problèmes, tous ces détournements de domaine également, ce sont des choses qui peuvent être gérées en ayant les données d'enregistrement et en donnant un accès total à tout le monde.

Donc l'abus des noms de domaine est en baisse en fait. Et on a noté pas d'augmentation durant le Covid 19, durant la pandémie.

Donc je mets cela, ces informations et si cela vous intéresse. Ça, c'est le minimum c'est les informations que vous pouvez fournir à un bureau d'enregistrement ou un registre et ça c'est basé sur l'EPDP phase 2, rapport final, ainsi que les meilleures pratiques que nous avons. Il y a un lien hypertexte à l'écran si cela vous intéresse. Donc les parties contractantes, c'est le minimum qu'ils doivent fournir. Et se pose la question de la divulgation ou non de ces données.

Donc oui, les bureaux d'enregistrement et les registres reçoivent des plaintes sur des noms de domaine et il y a donc des demandes qui sont nombreuses et il y a des retards en effet. Il faut donc une meilleure collaboration avec les bureaux d'enregistrement, les registres, il faut que les choses aillent plus vite si on veut régler les problèmes.

Donc maintenant quelques informations que nous avons sur le nombre de demandes. Il y a eu des bureaux d'enregistrement et

registres qui nous ont donné des informations, et cela représente les bureaux d'enregistrement qui sont relativement petits ou un petit peu plus grands dans certaines régions et dans plusieurs régions, il y a une large gamme de bureaux d'enregistrement. Certains nous ont dit une trentaine de demandes, et des registres c'était parfois un petit peu moins. Il y a eu beaucoup de demandes et de requêtes à la suite du RGPD, et un petit peu moins maintenant depuis 2020.

Donc cela dépend un petit peu des règles d'expurgation et comment ils peuvent donc ajuster un petit peu cela.

Donc avec SSAD nous aurons plus d'indicateurs, beaucoup plus de mesures pour l'ICANN et l'ICANN sera mise au courant. Donc la communauté comprendra beaucoup mieux le processus et comment fonctionne ce système normalisé d'accès et de normalisation et quels sont les résultats que l'on obtient avec cela.

Maintenant, quelques résultats que nous avons vus au niveau des bureaux d'enregistrement et des registres. Dans la majorité des cas, c'est divulgué, il y a moins de cas où c'est redirigé, où c'est refusé. Parfois il n'y a pas d'aspect juridique suffisant pour divulguer les données. Il y a d'autres raisons, il y a un système d'anonymisation, ou bien le registre n'était pas en mesure donc de divulguer ces données.

Donc quel type de données sont fournies ? La plupart du temps, les données du titulaire du nom de domaine, ou bien des données plus techniques. Il y a un raisonnement qui est donné lorsqu'il n'y a pas de divulgation et lorsqu'un système d'anonymisation et d'enregistrement

fiduciaire qui n'est pas en place, la pratique en général c'est de ne pas révéler toutes les données sous-jacentes, mais donc de donner d'autres informations.

Quelques bureaux d'enregistrement ont eu des appels, des personnes qui ont fait appel après avoir eu un déni, après un refus donc, mais ça c'est très bas comme chiffre. Ce n'était pas toujours les bons mécanismes qui étaient utilisés. Donc on a besoin de faire beaucoup d'éducation et d'information à ce niveau. Et aucun des appels sont revenus sur les décisions de divulgation.

Donc là nous avons des informations sur le type de demande et de personnes faisant la demande. Donc les demandes au niveau de protocole internet, vous avez 15 % pour les forces de l'ordre et le reste c'était des recherches sécurités, différents noms de domaine.

Donc en ce qui concerne les demandeurs que nous avons eus, et bien il y a beaucoup de répétition, il y a une personne qui a demandé en général au moins 4 informations. Vous voyez que ça, ça représente un nombre important. Il y a des personnes qui font une majorité de demandes.

Le temps de réponse moyen, en jours, c'est moins de 3 jours en général pour les registres c'est un peu plus rapide, parce que c'est plus facile pour eux par rapport aux données qui doivent être divulguées.

Donc c'est ma présentation. J'espère qu'on aura assez de temps pour répondre à des questions et parler un petit peu de tout cela.

JONATHAN ZUCK : Oui, vous aviez très peu de temps, merci d'avoir été aussi vite, c'est des données extrêmement importantes.

OWEN SMIGELSKI: Oui, il y a eu un webinaire en septembre qui vous donne beaucoup plus d'information. Il a duré 1 h 30, donc c'est très utile pour obtenir plus de détails.

JONATHAN ZUCK : Très bien, merci. Donc vous avez un enregistrement sur Zoom de cela, c'est très bien. Merci beaucoup c'est des informations de base tout à fait intéressantes et utiles pour nous. Donc voilà.

J'aimerais que… Mark est avec nous, Mark Svancarek, nous voulons lui donner la possibilité de s'exprimer. Il est de Microsoft et de la prévention des fraudes au niveau des entreprises.

MARK SVANCAREK: Oui, j'espère que vous m'entendez bien.

JONATHAN ZUCK : Oui c'est bon, on vous entend.

MARK SVANCAREK: Désolé, j'ai eu un petit problème de réveil, il n'a pas sonné, parce que l'heure est un petit tôt le matin.

Donc j'aimerais donner ma perspective sur ce que nous faisons à Microsoft par rapport au RGPD. Et je serai rapide pour que l'on passe très rapidement à la discussion qui va suivre.

Alors, donc je mets quelque chose dans le chat, c'est de Microsoft. Nous avons un rapport sur les défenses numériques et cela nous indique comment nous voyons la cybercriminalité.

Donc il y a beaucoup de débats au sujet de la cybercriminalité, est-ce que ça monte ou ça descend, en augmentation ou pas. Moi, je dirais que ça monte, c'est en augmentation, et qu'on a besoin de se défendre. C'est une priorité pour nous à Microsoft, et on fait beaucoup d'effort.

Donc nous avons des techniques que nous utilisons à Microsoft avec nos sites pour lutter contre la criminalité qui va à l'encontre des entreprises et des consommateurs, le piratage parfois que nous observons, et il y a beaucoup, beaucoup de problèmes qui se posent.

Vraiment désolé et je n'ai pas non plus donné de diapositives, donc je pense que ça va être plus une conversation qu'une présentation sur PowerPoint, donc je n'ai pas de diapositive à vous présenter. Et désolé, je me réveille.

Donc ce que vous voyez au niveau du RGPD c'est que nous n'avons pas encore développé un système qui nous permettra d'avoir accès aux données, autant que cela soit possible dans le cadre des règlementations. Et donc je pense qu'il serait intéressant de débattre de cela et je crois qu'à la base, nous recevons des informations juridiques et dans le groupe il n'y avait pas de consensus sur la signification véritablement de ces informations juridiques. Donc la nécessité pour avoir ces informations, la précision de ces informations également.

Donc, si vous observez ce webinaire de septembre, si vous allez l'écouter, nous donnons beaucoup plus d'informations sur les

processus que nous utilisons pour faire des tests, et cela diffère beaucoup du feedback que nous avions reçu de [inaudible] concernant ce que veut dire, ce que signifie « nécessaire ».

Donc j'ai ces informations quelque part. Si vous regardez… Où est-ce que c'est… Désolé mon lien hypertexte n'est pas prêt.

Oui, à la base, et je suis désolé une nouvelle fois… Je vous présente vraiment mes excuses. Je mettrai cela sur le chat d'ici quelques minutes…

Vraiment il faut que je retrouve ce lien et cette citation… Ha la la…

Donc je cherche toujours ce lien hypertexte. Donc il y a la résolution des litiges qui nous indiquait que ce ne serait jamais possible de divulguer des données, donc ce n'est pas le cas…

Je vais revenir d'ici une minute, je suis vraiment désolé.

JONATHAN ZUCK : Vous n'avez pas besoin d'avoir le lien, c'est simplement des points généraux que nous vous demandions de faire. Donc je crois que nous allons bientôt passer aux débats.

GREG AARRON: Oui, mais je trouverai ces liens d'ici peu. Il y a eu beaucoup de suppositions, vous savez que le système normalisé d'accès et de divulgation SSAD aurait existé que d'une seule manière, et on avait beaucoup plus de possibilités pour SSAD et on a décidé de ne pas développer le SSAD de cette manière.

JONATHAN ZUCK : Merci beaucoup Mark. Vraiment ce qu'on essaye d'analyser ici c'est les demandes qui nous arrivent et le temps qu'il faut pour traiter ces demandes. Nous avons vu des demandes par rapport aux personnes qui font des demandes et effectuent des demandes.

Ce que j'essaye de voir c'est que le RGPD est une réalité, et vraiment faire respecter ces règles c'est une réalité également. Et il y a des canaux de communication, est-ce qu'ils fonctionnent, telle est la question. Et ensuite, ce qu'il en est des personnes qui détiennent les données. Voilà un petit peu comment est-ce que cet échange a eu lieu, c'est ça qu'il est réellement utile de savoir.

Parce que vous savez, par exemple, l'une des choses qui ont été évoquées auparavant dans les présentations, je crois que c'est Gabriel qui en a parlé, c'est qu'une fois que la fraude est détectée, c'est déjà fini, c'est trop tard pour agir. Donc c'est un délai trop court pour que les parties contractantes puissent porter plainte par exemple.

Donc il faudrait avoir une réelle conversation par rapport à ce qui est réaliste et par rapport à ce à quoi devrait ressembler l'échange de données.

Alors, voyons. Donc je vous le disais, ce qui est revenu une fois et encore, c'est que les données montrent bien que l'utilisation malveillante du DNS a reculé. Et j'aimerais revenir sur la question de Luc qui demande pourquoi est-ce qu'il y a une dichotonomie entre ces deux séries de données, pourquoi est-ce qu'on n'a pas une réponse

toute faite par rapport à la tendance vis-à-vis de l'utilisation malveillante du DNS.

GREG AARON: Alors là je peux répondre, parce que j'ai participé à la conception du DAAR. Alors que fait le DAAR ?

Il examine les données à partir de différentes listes de catégories, qui contiennent des noms de domaine, et examine les catégories mises sur liste noire, comme les catégories de hameçonnage etc. Et on pourrait s'attendre à ce qu'il y ait des fluctuations au fil du temps.

Donc le DAAR mesure des choses très spécifiques à partir de sources très spécifiques. Et ce qu'on a vu, c'est qu'il y a des nouvelles techniques d'évasion qui peuvent faire réduire le nombre de domaines affectés. On ne sait pas quel est l'effet sur le fait d'avoir moins de données disponibles dans WHOIS et quel effet ça peut avoir sur le hameçonnage.

Il y a également eu des publications qui nous montrent que s'il est plus difficile de trouver les mauvais acteurs, alors vous pouvez plus facilement faire une liste noire des noms de domaine. C'est l'effet possible. Ce qui ne veut pas dire que la cyberdélinquance a reculé parce qu'il y aurait moins de noms sur cette liste noire.

Donc d'une manière générale le nombre de noms de domaine affecté qui recule, ça peut être une mesure, mais quelle que soit la manière dont vous le mesurez, les chiffres sont élevés.

Autre chose, le nombre de noms de domaine sur une liste données, ça ne vous donne pas une idée des risques impliqués ou des dommages engendrés. Mais l'argent perdu dans ce genre de fraude a augmenté. Si vous avez le même nombre de noms de domaine affectés, les dommages pour les victimes, eux, ont augmenté.

Donc tout dépend de la manière dont vous mesurez et ce que vous mesurez. Certains indicateurs disent que ces chiffres augmentent. Donc le DAAR fait une chose d'une manière particulière, mais ça n'est pas forcement représentatif de tout ce qu'il se passe dans l'écosystème.

JONATHAN ZUCK : Merci Greg.

Oui, et par rapport aux données expurgées, est-ce que c'est utilisable de la part des forces de l'ordre ? Parce qu'on a entendu qu'il y avait un manque d'exactitude et qu'il y avait également les services d'anonymisation et d'enregistrement fiduciaires. Alors est-ce que vous pouvez réellement attribuer les difficultés auxquelles vous êtes confrontés aux changements qui découlent de la conformité au RGPD ? Ça c'est une question qui s'adresse peut-être aux représentants des forces de l'ordre et de la recherche en cybersécurité.

GABRIEL ANDREWS: Je réponds brièvement à cela. Je pense que la qualité de la réponse dépend beaucoup des services d'anonymisation et d'enregistrement fiduciaires. Et on s'aperçoit que même si les délinquants mentent par rapport à leurs données d'enregistrement ou ont utilisé de faux

identifiants, c'est très difficile de trouver le point d'entrée pour une enquête.

Donc moi, je préfèrerais utiliser des données frauduleuses plutôt que de ne pas avoir de données du tout.

JONATHAN ZUCK : Merci Gabriel. Stéphanie Perrin a posé une question : est-ce qu'on a des statistiques sur la fréquence de validité des données qui sont volées et substituées par des données criminelles. Des données historiques ont d'ores et déjà été chiffrées, mais bon nombre d'entre elles sont encore valides.

GREG AARON: Je peux y répondre. Merci Stéphanie de cette question. Vous savez, j'ai analysé les données de contact pour des millions de noms de domaine qui ont été affectés. Et ce que je vois, c'est que les délinquants n'ont pas tendance à prendre les données d'autres et à les utiliser. Ils les inventent tout simplement.

Alors, certains sont meilleurs pour faire cela que d'autres, mais d'après mon expérience personnelle, ce ne sont pas des données qui sont volées.

JONATHAN ZUCK : Merci. Alors, je voulais vous demander, est-ce que vous pourriez activer votre caméra pour qu'on puisse vous voir et que ça ressemble plus à des réunions présentielles, surtout lorsqu'on vous pose des questions, ce serait bien de vous voir en direct y répondre.

Alors Volker dit : Greg semble dire qu'il n'y a pas de bénéfice à supprimer les noms de domaine lorsqu'un rapport est reçu.

GREG AARON: Non, je pense que Volker a mal compris. En fait ce que vous avez vu dans mon graphe c'est que si vous désactivez un domaine, vous allez avoir un bénéfice supplémentaire. Et, également, c'est l'un des cybercrimes qui est le plus court en termes de temps.

Donc lorsque vous effectuez une suspension du nom de domaine d'un délinquant, ça peut être utile, mais la question est la suivante : il y a une différence entre administrer un médicament ou faire de la prévention. Et, ce que l'on a vu c'est qu'il y a certains endroits où les délinquants vont et enregistrent un nom de domaine, ensuite le domaine est suspendu et ils en enregistrent un autre. Donc on a un problème par rapport à ces activités réitérées et il serait bon que toutes ces activités réitérées soient arrêtées en amont, qu'il y ait un travail de prévention à ce niveau-là.

Ensuite, suspendre les noms de domaine, est-ce que ça ne vaut pas la peine ? Non, pas du tout, ça vaut la peine de suspendre les noms de domaine en question, mais la question qui se pose alors c'est protéger les individus.

MILTON MUELLER: Puis-je intervenir ?

JONATHAN ZUCK : Oui, allez-y.

MILTON MUELLER: Bon, je pense que là il faut se concentrer sur la période avant et après les données expurgées. Alors dire que le hameçonnage est un problème, on le sait tous, c'est clair.

La question est : est-ce que le hameçonnage ou d'autres types de cybercrimes utilisent les données et de quelle manière ? Je pense que les délinquants ont trouvé des manières assez robustes d'éviter, de contourner la détection. Et la plupart des hameçonnages proviennent de suspensions et d'algorithmes qui détectent des modèles et qui les bloquent rapidement et je ne pense pas que les données WHOIS aient quoi que ce soit à voir avec ça.

Parce que là encore, on n'a vu aucune corrélation statistique entre l'avant et l'après. Donc concentrons-nous là-dessus. On peut simplement dire qu'on appréciait quand on avait cet accès, mais lorsqu'on avait cet accès indiscriminé, ouvert, aux données, on avait un problème croissant et ce problème augmentait et à un rythme beaucoup plus rapide que maintenant. Donc la question reste entière.

JONATHAN ZUCK : Excellente question Milton. Est-ce que quelqu'un veut y répondre ? Du Côté je ne sais pas, cybersécurité ou forces de l'ordre ?

GABRIEL ANDREWS: Oui, je peux commenter. Les enquêtes sont affectées de manière négative par cette absence de données. Et ça se produit de différentes manières, on pourrait avoir une conversation là-dessus, mais nos responsabilités n'impliquent pas seulement les attributions, mais aussi les notifications rapides des victimes potentielles.

Et c'est un exemple de la manière dont on est totalement désemparé face à ce système. Parce que des données qui sont supposément valides sont disponibles et, ensuite, il y a une prise de contact par

téléphone, le lendemain, ou le jour même, et parfois on peut avoir cette conversation, parfois on ne peut pas l'avoir.

JONATHAN ZUCK : Alors Gabriel, est-ce que vous êtes en train de suggérer que l'utilisation des données est plus valable pour contacter les victimes plutôt que pour trouver les délinquants ?

GABRIEL ANDREWS: Non, je pense qu'on les utilise dans les deux cas. Moi, j'ai un problème pour dire clairement ce qu'il se place parce que j'essaye de collecter des données et je vois à quel point c'est difficile de le faire parce qu'on n'arrive pas à assurer un suivi de ce qui ne marche pas. Mais ce que je peux dire avec certitude c'est que, d'après mon expérience – c'est ça qui m'a frappé le plus – la frustration ressentie par les enquêteurs pour pouvoir notifier les victimes potentielles et leurs difficultés à contacter ces personnes.

Donc dire que c'était la méthode la plus simple pour eux de trouver ces données de contact et contacter les victimes potentielles, et maintenant ils n'ont plus cette possibilité.

JONATHAN ZUCK : Merci Gabriel. Alors, Owen, je sais qu'une partie de la présentation qui a eu lieu récemment par les parties contractantes par rapport a l'accès aux données a jeté les bases de la meilleure manière de formater des requêtes et le faire de manière accélérée, etc. Est-ce qu'on a un autre exemple de données ou de personnes qui feraient de cette manière et est-ce qu'il y a un lien avec la plus grande probabilité des données fournies et de manière plus rapide peut-être ?

OWEN SMIGELSKI: Je n'ai pas de conclusion à ce niveau, donc notre étude et nos données ne sont pas complètes et exhaustives. Les différentes parties contractantes, lorsqu'ils ont des demandes, ont été en mesure de les gérer et de faire les tests nécessaires.

Mais lorsque vous fournissez toutes les informations, ça ne veut pas dire que ça va passer ce test d'équilibre. Et c'est assez complexe, ça va plus loin que de simplement obtenir les données, il y a beaucoup de facteurs qui rentrent en ligne de compte. Mais c'est un processus plus rapide, on arrive à une conclusion, et la plupart des données demandées par des requêtes c'est pour des marques commerciales qui sont enfreintes. Donc peut-être il y a des problèmes avec des robots sur l'internet qu'il faudrait retirer.

Il y a beaucoup, beaucoup de points qui rentrent en ligne de compte donc.

JONATHAN ZUCK : Owen est-ce que vous pensez que ces problèmes qui existent parfois avoir des réseaux zombie ça va être réglé au cas par cas ? Ou est-ce qu'il y a un cadre de référence pour l'utilisation malveillante du DNS ? Est-ce que c'est vraiment un petit peu difficile pour les parties contractantes d'obtenir les données ?

OWEN SMIGELSKI: Je ne sais pas ce qu'il va arriver à l'avenir. Il y a beaucoup d'ambiguïté et d'incertitude. Qu'est-ce qui sera admis, accepté ou pas ? On ne le sait pas encore. Au niveau de l'automatisation et au niveau des divulgations il y a beaucoup d'incertitudes et d'inconnus.

Comme je l'ai vu, que va faire le Congrès américain par exemple par rapport à un WHOIS disponible publiquement ? Nous avons des millions de consommateurs dans le monde entier, c'est très difficile à gérer, on ne peut le dire à 100 %, ça dépend les personnes ; Il y a des personnes qui sont en dehors des juridictions, il y a différentes lois et textes sur le respect de la vie privée. Il y a beaucoup de points juridiques et de responsabilités civiles qui sont engagées. Donc il y a des petits bureaux d'enregistrement qui sont uniquement sur une petite région, qui n'ont pas beaucoup de moyens. Donc je crois que ça va évoluer avec le temps.

Et nous allons voir cela avec SSAC, avec notre groupe également, et nous allons voir où tout cela nous mène.

JONATHAN ZUCK : Merci beaucoup. Oui, Lori nous demandait : est-ce que vous voulez parler d'expériences précises et spécifiques et des résultats de divulgations peut-être ?

OWEN SMIGELSKI: Je ne suis pas en mesure de parler de cela, je n'ai pas accès à ces données actuellement.

JONATHAN ZUCK : Merci. Alors, je sais qu'il y a une conversation, j'essayais de regarder tout ce qui passait sur le chat pour essayer de comprendre ce que dit la communauté.

Je sais que Mike Graham, vous avez une question précise je crois sur une modification au niveau de l'expurgation, vous pouvez ouvrir votre micro et nous parler Mike.

Je ne veux pas vous mettre sur la sellette de cette manière mais… Mickaël Graham, vous avez la parole. Nous laissons s'exprimer Mickaël Graham, je dis cela au personnel pour qu'ils allument votre micro.

MICKAËL GRAHAM: Ça marche ? Vous m'entendez ?

JONATHAN ZUCK : Parfait.

MICKAËL GRAHAM: Vraiment rapidement, je peux seulement donner quelques informations en ce qui concerne les efforts et les coûts. Il y a deux différentes manières et impacts. Donc découvrir les informations pour que nous puissions déterminer si un domaine a été enregistré frauduleusement et utilisé frauduleusement ou bien enregistré par quelqu'un qui a un rapport avec une entreprise et, sans le savoir se trouve victime et un peu piraté.

Donc il y a des personnes qui ne sont pas très sophistiquées et qui font beaucoup de dégâts au niveau de certaines entreprises. Et ça ne nous permet pas toujours d'atteindre tous les consommateurs et d'informer les citoyens du net.

Et, donc cela revient très cher aux entreprises pour trouver toutes ces informations. Et les véritables abus et utilisations malveillantes, pas seulement le hameçonnage, mais la contrefaçon également qui est très fréquente sur l'internet, les enquêtes coûtent très cher. Le Cybersquattage est un problème également.

Nous en souffrons, les consommateurs en souffrent, les institutions financières en souffrent. Et la confiance qu'on a dans l'internet est

impactée négativement. Donc parfois c'est un jeu de dupes et on risque de se faire avoir sur l'internet.

JONATHAN ZUCK : Oui, merci beaucoup. Oui c'est complexe, parce que les demandes de données et ces requêtes ne sont pas toujours sensibles par rapport au coût que cela représente. Donc on demande beaucoup aux entreprises pour être en conformité avec la loi, et aux bureaux d'enregistrement. C'est une question d'équilibre, une nouvelle fois.

MILTON MUELLER: Je peux rebondir là-dessus ?

JONATHAN ZUCK : Oui.

MILTON MUELLER: Les coûts c'est essentiel. C'est au centre de tout cela. Pendant 20 ans, les demandeurs n'avaient pas de problème c'était facile pour eux, ils étaient subventionnés par le régime de l'ICANN et ils présentaient… Il y avait un contrat d'adhésion, un nom de domaine, et on leur demandait sans consentement, on vous oblige à donner vos données personnelles identifiables qui vont être accessibles pour tout le monde dans le monde entier. Ça c'était quelque chose qui coûtait cher aussi pour les bureaux d'enregistrement et c'était subventionné cet accès. Il y a des personnes qui gagnaient beaucoup d'argent grâce à cela.

Et je crois que ce que nous avons fait avec SSAD, avec ce système normalisé d'accès et de divulgation, et bien les coûts vont être équilibrés, plus équitables. Et si vous êtes un demandeur important, il y a des entreprises qui font beaucoup de demandes sur le WHOIS. Et bien ils génèrent des coûts pour le système, et bien ils causent des

coûts, il faut qu'ils payent plus. Il faut être équitable, il faut qu'il y ait des frais. Il faut qu'il y ait des coûts d'accréditation qui vont couvrir les coûts de disponibilité de ces données.

Et la rapidité, on a parlé de la rapidité, aussi rapidement que possible, ça coûte cher aussi pour les parties. On évalue ces demandes qui arrivent et, une nouvelle fois on peut éviter ces coûts en automatisant tout cela. Mais l'automatisation, ça peut être illégal si vous n'avez pas de contrôle sur la nature de la requête.

Donc l'équilibre en effet est très complexe. Mais je crois que ce panel, cette table ronde, devrait avoir plus conscience du fait que les coûts doivent distribués d'une manière équilibrée entre les différentes parties prenantes.

JONATHAN ZUCK : Merci Milton. Oui, la plupart des registres européens ont un service pour être en conformité avec le RGPD par rapport aux marques commerciales également, donc il y a beaucoup de gTLD et ccTLD qui pensent à adopter un modèle similaire. Cela aiderait beaucoup à la possibilité de faire respecter les règles par rapport à ces registres européens qui offrent ces services de divulgation de données et en conformité avec le RGPD.

OWEN SMIGELSKI: C'était quelle question ?

JONATHAN ZUCK : C'est de Nathalie Leroy, c'est en bas de l'écran et du chat.

OWEN SMIGELSKI: Je ne suis pas sûr. Je ne sais pas s'il y a d'autres ccTLD ou gTLD qui adoptent des modèles similaires, mais nous commençons simplement

avec ce système normalisé d'accès et de divulgation SSAD, donc nous allons voir si certains gTLD auront des services de ce type. Je ne sais pas exactement, nous aurons le rapport final de la phase 2 de l'EPDP, et on a dû aller très vite, on avait beaucoup de pression au niveau du temps.

Je crois qu'ils sont allés plus vite que le travail que nous effectuons, c'est peut-être une possibilité, c'est une suggestion peut-être à l'avenir.

Mais je pense que le modèle de SSAD va évoluer de toute façon. Et tant que c'est en conformité avec la loi, c'est possible.

JONATHAN ZUCK : Merci beaucoup Oxen. J'espère qu'on a répondu à la question de Nathalie.

Laureen nous a demandé de répondre à… Laureen..

LAUREEN KAPIN : Oui, par rapport à ce qu'a dit Milton Mueller, ces informations c'est une épée à double tranchant. Et véritablement Milton je suis d'accord, nous le voyons dans les plaintes qui arrivent.

Mais d'un autre côté, le DNS est une ressource publique. Milton nous a mis l'accent sur ce qui était caché et qui est illégal et va à l'encontre des lois et règlements. Mais le RGPD travaille à cela.

Et je pense qu'il va y avoir un développement de politique et des efforts de développement de politique par rapport au RGPD. Parce que le public a le droit de savoir comment on gère ses informations, notamment au niveau juridique, et les utilisateurs doivent savoir qui

est derrière ces noms de domaine, quelles sont ces entités. Ça, ça aide le public et les forces de l'ordre dans leurs enquêtes, et pour la diligence raisonnée également.

Donc on requiert certaines informations pour utiliser des ressources publiques, que ce soit un permis de conduire ou une licence commerciale. C'est public tout cela. Ça doit être la même chose pour les informations juridiques associées avec ces entités juridiques.

JONATHAN ZUCK : Merci beaucoup Laureen. Il y a plus de questions, nous allons les collecter, nous allons nous assurer de répondre à vos questions, si possible.

Excellent débat, excellentes conversations. On doit toujours se concentrer évidemment sur ces points, ce qui n'est pas toujours facile. Mais pour répondre à Jeff, nous sommes en séance plénière et nous avons une situation de fait avant et après les changements de politique de l'ICANN. Et il y a des mesures qui doivent être prises, différentes actions, pour avancer. Donc il faut changer le statu quo et, par rapport à la disponibilité des données, par rapport à la protection des consommateurs. Donc on essaye de trouver des faits, d'obtenir des informations aujourd'hui.

Il reste encore beaucoup de questions auxquelles nous devons répondre, mais nous n'avons pas le temps de faire aujourd'hui. Il est 3 h du matin pour moi, donc je n'ai plus grand-chose à dire. Je voudrais simplement vous remercier, remercier les présentateurs de

cette table ronde et toutes les personnes qui ont participé, participé aux débats. Ils sont nombreux nous l'avons vu sur le chat.

Merci beaucoup de votre attention, merci à tous, la séance est levée et l'enregistrement terminé.

[FIN DE LA TRANSCRIPTION]