ICANN82 | Forum de la communauté – Séance conjointe : ALAC et SSAC
Dimanche 9 mars 2025 – 13h15 à 14h30 PST

JONATHAN ZUCK

Je voudrais répéter ce que Michelle vient de nous dire. C'est un groupe plein d'énergie. Je vous conseille de vous préparer, de préparer vos appareils pour l'interprétariat afin d'être prêts à écouter les interventions dans d'autres langues que l'anglais.

Et maintenant, je vais parler de l'ALAC et du SSAC. Donc nous sommes en train de recevoir des réponses sur les thématiques qui nous intéressent. Nous travaillons en ce moment à la campagne d'éducation sur l'hameçonnage au sein du DNS et nous sommes en cours de finaliser les traductions des différents cours.

Nous sommes très intéressés donc des deux côtés de l'utilisation malveillante du DNS. Je ne sais pas si vous avez les mêmes frustrations que nous en ce qui concerne le webinaire INFERMAL concernant les problèmes qui sont détectés. Nous vous remercions de votre présence. Vous, vous remplacez Ram. Donc veuillez vous présenter.

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

JEFFREY BEDSER Donc moi, je remplace Ram Mohan. Je m'appelle Jeff Bedser et j'appartiens à l'équipe dirigeante du SSAC. Nous nous intéressons principalement à tout ce qui a trait à l'usage malveillant du DNS.

JONATHAN ZUCK Dans notre ordre du jour, nous avions prévu donc d'examiner un peu en quoi consiste ce cours, l'état d'avancement. Et je vais partager mon écran. Donc voici à quoi cela ressemble. Normalement, il devrait y avoir un peu plus de couleur, mais je crois que cela ira.

Alors nous avons des chiffres généraux. Ce problème continue de progresser. Nous parlons des différents types de cybercriminalité. Nous nous concentrons principalement sur l'hameçonnage. Nous examinons la définition de l'hameçonnage, nous identifions les tentatives d'hameçonnage et ensuite nous parlons de la façon de prévenir l'hameçonnage.

Nous parlons de ce qu'est l'hameçonnage, les étapes – il s'agit de cibler un utilisateur. Ensuite, on met en place un site, un site de dévoiement. Et ensuite, il y a un email qui est envoyé à la victime.

Donc là, vous avez l'impression que ça provient de Bank of America. Vous cliquez et le lien vous emmène directement sur le site web que vous pensez être de Bank of America. Et si le pirate est intelligent, il va envoyer cela à Bank of America et vous ne le saurez pas, mais toutes vos données auront été saisies.

Nous allons parler des différents types d'hameçonnage. J'ai proposé donc un cours pour les organisations de l'Amérique du Nord. On a parlé donc de l'hameçonnage ciblé et on a fait donc une simulation avec le président de l'organisation et on lui a envoyé une lettre demandant des fonds. Et en fait, donc il a été le cobaye et il a été surpris de voir à quel point nous avions des informations.

Ensuite, nous avons ajouté l'hameçonnage par SMS, le smishing. Moi, j'en reçois de plus en plus. Cela a donc toute sa pertinence. Nous avons parlé des emails à proprement parler et la façon dont ils sont construits. Il y a un envoyeur, un expéditeur qui est tout à fait suspect. Et il y a un texte. Et on montre des emails réels pour donner l'exemple de ce à quoi ils ressemblent. Et nous allons proposer cette formation en différentes langues.

Nous avons parlé donc des logiciels malveillants qui peuvent être réalisés à la place d'un site web malveillant. Et il y a aussi les personnes qui se prétendent être des représentants de support informatique ou support technique. On voit des liens qui sont malveillants. On donne des exemples, des conseils.

Et vous savez peut-être que Google avait mis en place un petit test sur l'hameçonnage disponible en plusieurs langues et donc nous pouvons diriger notre public vers ce site. Voilà les différents types d'hameçonnage et les différentes possibilités que l'on a pour éviter de se faire attraper et comment signaler les cas. Je serai ravi de partager ces informations avec vous. Il y avait une version

préliminaire et je crois que nous arrivons donc à bout de la nouvelle version.

Il y a des URL et les QR codes pour vous permettre de signaler les cas. Donc bon, il s'agit de signaler les cas aux autorités compétentes. Si vous êtes en France, vous n'allez pas contacter les autorités américaines, bien entendu. Donc il y a les organisations At-Large et il y a les structures At-Large. Et il y a des organisations aussi qui s'intéressent aux activités de l'ICANN et qui s'intéressent à participer aux choses que nous faisons, par exemple autour de l'acceptation universelle.

Et il y a aussi une relation avec l'Association internationale des bibliothèques, car à ce niveau là, il y a de la sensibilisation qui est faite sur le terrain. Et donc ces acteurs-là ont été heureux de voir qu'il y avait donc ces outils disponibles en plusieurs langues.

BARRY LEIBA Vous avez parlé donc des emails personnalisés rédigés dans un langage adapté au niveau local. Donc moi, j'ai fait partie du groupe de travail anti-usage malveillant et il a été dit que l'on voit de plus en plus des emails, des messages hyper personnalisés et des informations sont recueillies par le biais de l'IA sur tout le monde.

Et auparavant, on ne pouvait envoyer des messages que, par exemple, au dirigeant de l'entreprise. Mais maintenant, on peut envoyer des informations à tous les échelons avec des informations très précises : où vous habitez, ce que vous faites. Et

donc il s'agit d'un problème qui est vraiment très grave, et même des gens éclairés peuvent se faire avoir.

JONATHAN ZUCK

Si vous avez des exemples que vous pouvez partager, ça serait très bien. Moi, je n'ai pas reçu de message hyper personnalisé et je suis désolé. J'en suis désolé, car je ne sais pas pourquoi je suis négligé. Je pourrais acheter des bitcoins. Je ne fais qu'entendre parler de ce type de message, mais j'aimerais bien pouvoir voir ces messages.

MATTHIAS HUDOBNIK

Deux choses. Tout d'abord, ça a l'air très bien. Ma première question, c'est est-ce qu'il y a un plan pour faire des interrogations, des tests à l'issue de la formation, juste pour tester les connaissances acquises. Et ensuite, je voudrais savoir si ça sera disponible sur le site de l'ICANN. Ainsi, un public plus élargi pourrait avoir accès à ces informations.

JONATHAN ZUCK

Donc très bonne idée. Merci. J'avais des quiz, des petits tests auparavant, mais je me suis dit que ce serait mieux d'avoir un test oral, mais je pourrais donc revenir sur ces tests écrits. Donc sur ICANN Learn… Je ne sais pas si c'est une bonne idée. Normalement, les supports sur ICANN Learn ressemblent à des ouvrages pédagogiques des années 70. Il y a des gens qui disent voilà, moi je suis dyslexique et 30 pages de texte va compromettre

ma capacité d'apprendre. Mais la suggestion est bonne. Je ne sais pas dans quel ordre les gens doivent prendre la parole.

LAYAL JEBRAN Donc, vous avez introduit les MFA. Donc, l'authentification est très difficile. Est-ce que vous pensez introduire les pass keys?

JONATHAN ZUCK Je ne sais pas de quels pass keys vous parlez. Est-ce que c'est les applications d'authentification? Peut-être. Donc ici, il s'agit vraiment d'identifier le public que l'on cible. Donc il y a par exemple un extrême. Sébastien a fait un essai avec les versions antérieures avec des femmes retraitées et elles ont trouvé que l'information était un petit peu complexe. Donc il faudrait peut-être simplifier le message. Donc voilà, ce n'est pas vraiment une objection, mais il faut pouvoir répondre aux attentes de notre public.

LAYAL JEBRAN Donc pour rebondir là-dessus, étant donné que les pass keys sont mis en œuvre par défaut par exemple avec Google, donc il y a l'authentification qui existe à ce niveau.

JONATHAN ZUCK Très bien. Vous vouliez intervenir?

TARA WHALEN

Oui, je suis tout à fait d'accord avec cela. Donc je pense que vous êtes préoccupé par cela également. C'est indiquer aux personnes quelles sont les attentes et ce qu'ils peuvent reconnaître au niveau des URL qui ne sont pas les bonnes adresses et ainsi de suite. Tout ce qui permet donc de prendre des décisions pour savoir si c'est une escroquerie ou pas. Donc il y a les identifications multi-facteur. Voilà les options que vous avez avec les différents mots de passe. Il y a différents niveaux également pour atténuer les risques. Donc voir s'il y a une compromission des sites web également. Donc rien n'est parfait, mais il y a quand même des mesures qui permettent de se protéger et de diffuser des informations pour mieux comprendre comment l'hameçonnage se réalise.

JONATHAN ZUCK

La plupart des mots de passe dans les années 90, c'était carrément des personnes qui vous appelaient au téléphone. Quel est le mot de passe? Tout simplement.

BARRY LEIBA

Donc, j'aimerais terminer là-dessus. Je crois que le public voit déjà des demandes de sites web qui sont envoyés et on me demande d'utiliser des pass keys. Donc, ce qui est important, c'est de former les personnes à ces pass keys et de savoir exactement ce que c'est et comment cela fonctionne.

SÉBASTIEN BACHOLLET

Merci. Oui, effectivement, j'ai utilisé une des premières versions de Jonathan pour la mettre en français et la localiser aussi, trouver des exemples qui m'étaient tombés dessus moi et essayer de l'exprimer et de le présenter essentiellement à des dames à la retraite. Et je comprends qu'on veuille – et c'est normal puisque c'est votre job – essayer d'être le plus complet possible. Mais ça veut dire qu'il faut savoir comment est-ce qu'on va le présenter? Quels sont les exemples qu'on va prendre dans chacune des langues et dans chacun des pays où on va aller? Et ça prend beaucoup de temps et ça va être une grande partie de la chose. Est-ce qu'on peut avoir une présentation qui soit à plusieurs étages? Là, on rentre à l'école et puis on va à la classe suivante, puis à la classe suivante. Mais là, ça demande aussi beaucoup de temps et beaucoup de travail. Donc je pense qu'il faut d'abord…

Et merci Jonathan d'avoir fait ce travail-là. N'en rajoutons pas trop pour l'instant. Faisons déjà, utilisons ça. Et puis voyons quels sont les retours que l'on peut avoir qui nous permettront d'améliorer, qui ne seront pas faits par des spécialistes, mais par les gens qui ont effectivement besoin de ça. Dans le fin fond de ma province en France, pour l'instant, même expliquer ce genre de choses est compliqué et quand on doit expliquer ce qui se passe sur un téléphone, ce qui se passe sur une tablette, ce qui se passe sur un ordinateur et quelle marque d'ordinateur, etc., on prend déjà beaucoup de temps. Et donc voilà, je crois qu'il faut prendre tout ça en compte à un moment ou à un autre. Encore une fois, c'est super ce qui a déjà été fait.

JONATHAN ZUCK

Oui, merci beaucoup. Sébastien. Donc je crois que nous avons une liste, en effet, pour encourager les personnes à s'engager là-dedans, pour les aider, et ce qu'ils ont besoin d'apprendre et de savoir au niveau de la technologie, au niveau des problèmes qu'ils peuvent rencontrer. Donc en effet, il faut se limiter. Donc je n'ai pas la liste de participants devant moi, mais nous avons Robert, je crois. Vous avez 10 minutes, environ 12 minutes.

JEFFREY BEDSER

Donc, je crois qu'il faut considérer, c'est qu'il y a une tendance pour atténuer les risques. On a des fake shops et c'est la perception des résultats. C'est de l'hameçonnage également. Mais ça c'est avec les réseaux sociaux. Lorsque je dis fake shop, ça c'est à l'ICANN. C'est vraiment quelque chose qui est faux. Ce n'est pas une véritable boutique où on croit acheter des biens, mais en fait on vole vos cartes de crédit, vos numéros de carte de crédit, vos informations.

C'est la même fraude que l'hameçonnage, mais c'est un autre mécanisme avec les réseaux sociaux. Donc si le prix n'est pas le bon dans cette boutique sur l'Internet, eh bien c'est un problème. Cela peut vous envoyer vers un nouveau nom de domaine. Et ça, c'est de l'hameçonnage.

JONATHAN ZUCK

Oui, donc n'allez plus en ligne. Voilà ce qu'on pourrait dire. Ce serait plus simple.

Ça fait très peur d'aller en ligne. Il y a beaucoup de problèmes qui existent en effet. Merci.

NABIL BENAMAR

Moi, j'aimerais dire qu'avec l'intelligence artificielle, tout a changé véritablement, tout particulièrement les attaques d'hameçonnage avec les courriels. Il y a de nombreuses attaques. On en a parlé. On y travaille à SSAC et moi j'ai demandé à un de mes étudiants de faire une enquête à ce sujet. Il y a différentes approches pour lutter contre ces attaques. Et nous avons trouvé un grand nombre de personnes qui ont été attaqués de cette manière. Donc c'est urgent à cause de l'intelligence artificielle qui est utilisée. Donc, on doit repenser notre approche pour combattre les attaques d'hameçonnage utilisant l'intelligence artificielle. Heureusement, avec l'intelligence artificielle, on peut détecter ce type d'attaques et c'est donc un outil, l'intelligence artificielle, qu'on peut utiliser pour lutter contre aussi.

JONATHAN ZUCK

Oui, c'est vraiment une course aux armements. Robert.

ROBERT GUERRA

Robert Guerra du SSAC. Je crois améliorer le cours, avoir différents tests de marché. Mais je crois que c'est important. Ce que je n'entends pas, c'est que les besoins pour cela, c'est de plus en plus important. Et il y a des activistes qui se retrouvent aux États-Unis. Il y a des menaces qui sont très importantes, plus importantes que

jamais. Donc on n'a pas besoin que ce soit parfait. Il faut que les personnes soient informées, il faut que ça soit traduit aussi. Il y a des besoins énormes dans d'autres parties du monde, et tout particulièrement pour l'hameçonnage. Ce n'est pas un seul marché, ça doit être sur un maximum de marchés. Voilà ce que je voulais dire.

JONATHAN ZUCK Merci Robert. Je donne la parole à Hadia.

HADIA EL MINIAWI Oui, j'ai levé la main pour rebondir sur ce qu'a dit Sébastien. Pendant le COVID, j'ai effectué des webinaires sur la sécurité en ligne et sur les fraudes en ligne. C'était en arabe et j'ai inclus les SMS également et j'ai inclus l'authentification à double facteur et donc comment se protéger. Et les webinaires, c'était pour un réseau de femmes non professionnelles et la plupart étaient à la retraite. Elles avaient plus de 70 ans et ça a été très bien reçu. Et elles ont bien compris, ces dames âgées, ce qui leur était présenté et elles étaient très intéressées par en savoir plus.

Et la perception, je pense que si vous êtes un senior plus âgé, vous n'avez pas eu une carrière professionnelle peut-être, on pourrait penser que vous n'allez pas être en mesure de comprendre ce qui est présenté, mais en fait, ce n'est pas juste parce que si vous êtes en ligne, vous appréciez beaucoup les informations qui vous

permettent de vous protéger, pour les SMS aussi, pour les textos et pour éventuellement l'hameçonnage avec les noms de domaine.

JONATHAN ZUCK Oui. Allez-y.

MATTHIAS HUDOBNIK Oui, c'est ce que je voulais dire, c'est qu'il y a des lignes de conduite qui existent avec Privacy International, par exemple, qui offre beaucoup de ressources en ligne. Vous en avez d'autres et vous pouvez vraiment voir pour différents auditoires ce qui se trouve en ligne, comment avoir l'authentification, comment avoir des mots de passe solides, comment se défendre dans le monde numérique, comment bloquer différents sites pour enlever les cookies et pour ne pas avoir de publicités intempestives. Donc c'est beaucoup testé. Donc il y a beaucoup de choses qui existent déjà, de ressources qui existent sur l'Internet que l'on peut trouver.

ADRIAN SCHMIDT Moi, professionnellement, à moins que vous êtes à la retraite professionnellement. Moi, je travaille pour une organisation à but non lucratif et nous avons eu une campagne. Cette année, nous allons lancer cette campagne sur la cybersécurité, le mois de la cybersécurité. Ce devait être octobre et on a eu une très bonne réception concernant ce mois de la cybersécurité.

Alors ce que je veux dire, c'est que c'est important de communiquer en effet et de travailler avec les plus âgés. Mon père

est mort il y a de cela quelques mois, à 92 ans. Comment je pouvais l'aider avec ces nouvelles technologies pour m'assurer qu'on ne lui vole pas son argent ou quoi que ce soit? Je crois qu'il faut repenser tout cela. Il faut lutter contre l'hameçonnage et également voir comment nous pouvons communiquer là-dessus.

Et les plus âgés ont l'impression que c'est ma banque, je vais les appeler. Mais les jeunes aussi qui sont nés avec la technologie font plus confiance à la technologie et parfois se font donc avoir de cette manière. Donc je ne pense pas que les gouvernements vont être en mesure de chiffrer tout, de tout sécuriser. Il faut trouver une différente manière au niveau technologique pour que les maillons les plus faibles soient renforcés. Merci.

JONATHAN ZUCK Oui, l'ingénierie sociale, c'est quelque chose qui est très nécessaire. Je donne la parole à Amrita Choudhury.

AMRITA CHOUDHURY Comme l'a dit Roberto, l'hameçonnage, c'est dans le monde entier que cela se passe. Et ce que nous devons voir à l'ICANN, nos cadres de référence, notre mandat, c'est les noms de domaine. Mais comment est-ce que l'on peut donc prendre en compte… Est-ce que nous allons aliéner une partie de notre auditoire?

Il y a beaucoup de messages qui existent, mais si vous voyez les pays en développement notamment, ils ne parlent peut-être pas en anglais. Donc les messages vidéo, en Inde, il y a des personnes

qui sont analphabètes et il faut faire des vidéos parce que ces personnes vont mieux comprendre avec des vidéos. Il y a beaucoup de problèmes et on a besoin de faire des vidéos d'information pour les personnes qui ne savent pas lire. Il faut que ça soit très interactif. Il faut protéger les gens parce qu'il y a beaucoup d'abus au niveau financier de personnes qui perdent donc des fonds de cette manière à cause de l'hameçonnage.

Donc ce n'est pas seulement au niveau du nom de domaine, mais c'est au niveau du contenu. On sait que l'ICANN ne gère pas le contenu, mais c'est important de savoir également les problèmes qui peuvent exister avec les différents contenus.

JONATHAN ZUCK

Oui, vous avez absolument raison, c'est un problème grave. C'est pour cela que on travaille avec les parties contractantes à l'ICANN. On essaye de faire en sorte qu'ils fassent un maximum de travail à ce sujet et nous essayons de faire ce que nous pouvons pour atténuer les risques d'abus. Donc, je pense que nous avons passé en revue toutes les personnes, non?

NATÁLIE TERČOVÁ

Natalie Tercova au micro. Je voudrais faire un commentaire rapide. Au cours des quatre dernières années, dans le cadre de mon doctorat, j'ai donc étudié la question des enfants, des jeunes. Mais les personnes âgées sont aussi un groupe vulnérable. Et il y a par exemple un groupe qui est jeune, qui possède toutes les

compétences nécessaires, car ils sont nés à l'ère numérique, mais je crois qu'ils sont vulnérables, ces gens-là.

Dans ma région, l'Europe, très souvent ces jeunes donc surestiment leurs compétences. Il leur manque des connaissances critiques et ils ont aussi besoin d'aide. Je voudrais souligner qu'il y a donc des publics qui ont besoin d'acquérir davantage de compétences et il y a les publics âgés qui ont la possibilité de transférer leurs compétences de vie vers les compétences nécessaires lorsqu'ils sont en ligne. Mais justement, il ne faut pas oublier les jeunes.

Dans le cadre de mon travail, on dit toujours que s'il y a des erreurs dans un texte, c'est parce qu'il y a des erreurs, alors que maintenant c'est l'inverse. S'il n'y a plus d'erreurs du tout, on considère que c'est le produit de l'intelligence artificielle. Alors comment détecter que quelque chose est donc une arnaque ou de l'hameçonnage s'il n'y a pas d'erreur?

JONATHAN ZUCK

Vous avez tout à fait raison. Les jeunes, d'après ce que je sais, ne savent même pas faire bouillir un œuf, faire cuire un œuf dur. Je me souviens qu'à l'époque où c'était les Nigérians, donc ces princes nigérians qui envoyaient ces hameçons, c'était truffé d'erreurs. Leurs textes étaient truffés d'erreurs. Et donc vous n'accordiez peut-être pas davantage d'attention. Maintenant, ça n'est plus le cas. L'intelligence artificielle a changé la donne pour le pire.

EMILIA ZALEWSKA-CZAJCZYŃSKA Désolée, j'ai oublié ma carte, mon petit carton avec mon nom.

JONATHAN ZUCK Voilà les jeunes.

EMILIA ZALEWSKA-CZAJCZYŃSKA Je voulais rebondir sur ce que disait Natalia et parler d'autres groupes vulnérables. En Europe, il y a des groupes qui sont maintenant désignés comme étant vulnérables aux manipulations : les personnes âgées, les enfants, les personnes handicapées et les personnes en situation économique difficile, en situation socio-économique difficile, les diverses minorités.

Ce sont des groupes dont on ne parle pas. On parle d'alphabétisation numérique d'enfants, mais par exemple, les personnes handicapées sont aussi vulnérables. Leurs besoins sont probablement différents et il leur faut renforcer leurs capacités, non seulement en raison de leur handicap, mais aussi pour vraiment leur expliquer comment ils peuvent être vulnérables à l'hameçonnage.

Et ici, nous avons parlé donc de l'IA qui recueille des données sur ce type de personnes. En Pologne par exemple, il y a quelques années, il y a eu des cas similaires et une publication a été rédigée par des personnes qui rénovent des appartements pour les revendre ensuite. Il y avait donc un lien qui a été créé pour vendre

un appartement. Donc vous cliquez sur le lien pour acheter un appartement et des renseignements vous concernant seront envoyés aux personnes qui vont utiliser ces données. On voit donc que les personnes qui ont cliqué sur le lien ont contracté des emprunts, ont des dettes et des données sur ces personnes sont recueillies.

Ainsi, il est possible de classer les personnes dans les différents groupes de personnes vulnérables et il faudrait tenir compte de ces choses quand on parle de personnes vulnérables ou de groupes vulnérables. Il y a donc différentes nouvelles façons de cibler ces publics vulnérables.

JONATHAN ZUCK

Merci, c'est très déprimant tout cela, mais c'est toujours intéressant de débattre de tout cela. Je crois que, comme Robert nous l'a dit, il faut poursuivre le travail et examiner les différents besoins dans les différents environnements.

A ce stade, je pense qu'il faut promettre de n'exclure personne. Il faut tendre la main et il faut trouver les différentes alliances. Moi, je suis très enthousiaste par rapport aux bibliothèques, donc voyons comment les choses avancent. Alors donnez-nous de bonnes nouvelles sur vos derniers travaux, car je crois que nous avons terminé le sujet précédent clairement maintenant.

JEFFREY BEDSER

Désolé, je ne sais pas si ce sera de bonnes nouvelles, mais ce sera une conversation intéressante. Je voudrais donc vous donner des informations sur INFERMAL. Ici, c'est un rapport mis en place par OCTO et c'est une étude effectuée sur des questions clés basées sur l'hameçonnage et l'usage malveillant du DNS.

La conclusion du rapport, c'est qu'il y a donc des incitations. Il y a donc une concentration de l'usage malveillant du DNS. Donc il n'y a pas encore de solution. Nous validons les notions qui prévalent depuis plusieurs années. Donc est-ce que le prix faible facilite l'hameçonnage? Est-ce que la facilité d'accès favorise l'hameçonnage? Est-ce que la possibilité d'avoir des domaines plus facilement augmente l'usage malveillant?

Donc les frais d'enregistrement plus faibles, les restrictions, la gratuité. Donc la gratuité, ce n'est pas bon. Les restrictions rigoureuses, ce sont des mesures progressives et donc l'accès API, une interface de programmation donc, et les pratiques de vérification peuvent être une mesure proactive pour la vérification des informations des titulaires.

Les mesures réactives, la durée d'atténuation. Donc il y aura un message à la fin que je livrerai. Donc on parle rarement de l'hameçonnage ciblé, mais Jonathan nous en a parlé. Donc ça c'est une question de nombre de victimes qui peuvent être ciblées en dix secondes plutôt qu'en 48 h. Donc il s'agit de mesurer. Les pratiques des bureaux d'enregistrement. Les bureaux d'enregistrement qui offrent des prix plus bas ou des services gratuits.

Le prix et la facilité d'accès. Ce sont des questions économiques. Les gens vont se diriger vers les prix les plus bas. C'est le cas en Amérique du Nord. Nous le voyons chez les grands distributeurs, les discounteurs. Ils offrent la possibilité d'acheter en gros. Et personne ne sera surpris que la concentration des activités malveillantes se trouveront là où les prix sont bas.

Mais nous avons vu les chiffres, donc de 1 trillion à 3 trillions. De toute façon, ces trillions, ce sont des chiffres qu'on ne peut pas s'imaginer, des milliers de milliards. La perte par victime au niveau mondial est considérable : 136 trillions. Et donc aux États-Unis, c'est 3 520. Donc au niveau mondial 136, au niveau des États-Unis, 3520.

Donc, quel est le prix auquel les criminels n'achèteront pas de domaine à des fins malveillantes? La réalité des choses, c'est que les activités malveillantes se concentrent là où les prix sont les plus bas. Il serait évidemment difficile de fixer des prix, car de toute façon, ce n'est pas la solution. Il y aura toujours le prix le plus bas qui va émerger.

Ensuite, parlons des processus de vérification. Il y a des ccTLD qui ont des processus de vérification très stricts, mais ce n'est pas imparable car il est possible de créer un personnage fictif ou utiliser votre identité pour créer une identité tierce et ces fausses identités générées par l'intelligence artificielle sont rendues plus efficaces. Donc quand on veut créer un permis de conduire dans un autre État, c'est beaucoup plus facile avec l'intelligence artificielle.

Donc, il faut améliorer les processus de vérification. Il y a donc le facteur d'intelligence artificielle qui entre en jeu. On n'est plus dans une situation où on aura chaque fois affaire à un être humain.

Les taux de détection de la délégation à l'atténuation. Est-ce que c'est une mesure valide? Je pense que, en ce qui concerne l'abus du DNS, c'est probant. Donc il y a ces indicateurs que nous devons utiliser. Il y a des données publiques, et je crois que c'est le sommet de l'iceberg.

Tous les publics ciblés par ces usages malveillants sont sur des listes. Donc quand un usage malveillant est détecté, il doit être signalé. Qui a été victime sans l'avoir signalé? Je crois que cela s'applique à beaucoup de gens.

La majorité des cas ne sont pas signalés. Donc le temps, le laps de temps entre la délégation et l'atténuation, si ce laps de temps est de quelques secondes, il y aura peut-être 10 victimes. Mais le but, c'est de réduire le nombre de victimes. Il s'agit donc de tuer ce domaine malveillant et les cyberpirates trouveront toujours un moyen donc d'agir.

Et donc, je pense que l'autre question, c'est également mesurer le nombre de victimes par domaine. On a besoin d'indicateurs à ce niveau pour que nous puissions mieux comprendre la taille, les pertes également, le nombre de pertes. Diapo suivante, s'il vous plaît.

Donc un des points, je vois qu'il y avait une augmentation de 400 % lorsqu'il y avait un API de disponible pour l'enregistrement d'un nom de domaine. Mais les algorithmes de génération de domaine – les DGA – pouvaient avoir des logiciels malveillants qui étaient diffusés. Donc le volume allait être très différent par rapport aux API avec les DGA. Donc à quel niveau est-il approprié de restreindre l'achat de beaucoup de domaines à la fois en vrac? Donc lorsque l'on lance une nouvelle marque, on essaye d'avoir beaucoup de TLD Lorsqu'il y a des milliers, par exemple, de marques qui achètent en même temps des TLD. Donc il faut véritablement que l'on soit plus sérieux à ce niveau et que l'on comprenne mieux comment la situation peut être problématique.

Ça, c'était la dernière diapo. Donc ça c'est des questions techniques sur lesquelles on doit se concentrer. Donc on a des indicateurs sur les noms de domaine, on voit qu'il y a une concentration autour des achats aux prix les plus bas et également pour les criminels, ils ont tout intérêt à utiliser un nom de domaine parce qu'ils peuvent gagner beaucoup d'argent. Donc est-ce que l'on peut avoir un prix beaucoup plus élevé pour les noms de domaine? Et bien là, à ce moment-là, les noms de domaine ne seront plus atteignables pour des personnes qui ne sont pas des criminels.

Donc il faut qu'on fasse des rapports, de la détection et il faut qu'on fasse de l'atténuation rapide des problèmes pour que les cybercriminels ne soient pas en mesure d'agir. Et pour qu'il y ait

une fenêtre très étroite pour des abus éventuels, il ne faut pas qu'ils puissent gagner tant d'argent avec ces fraudes.

RAM MOHAN Donc nous avons Robert, puis Satish. Robert? Ah non! Satish, alors?

SATISH BABU Oui, merci beaucoup. Donc c'était sur la section précédente. Je crois que c'est pertinent néanmoins. Ce mois-ci, la Banque centrale d'Inde a envoyé une circulaire introduisant des sous-domaines exclusifs : .bank.in et .fin.in. Et donc les banques et les institutions financières d'Inde vont utiliser ces extensions. Donc je voulais le mentionner. Je ne sais pas si ça va être couronné de succès, mais en tout cas, c'est un point de contrôle où on ne pourrait pas acheter des noms de domaine en vrac et avec un grand nombre de noms de domaine, comme on l'a vu précédemment.

RAM MOHAN Merci Satish. Jonathan?

JONATHAN ZUCK Oui, oui, c'est similaire. Plus de restrictions avec ces noms de domaine, moins de concentration, d'abus. Peut-être que c'est au niveau du GAC. Le GAC a également travaillé là-dessus. Ils le font, je crois, et ils essayent de faire une régulation par exemple pour les institutions financières, pour les médecins, les TLD enregistrés.

C'est très important pour qu'il y ait donc une homologation de certains gTLD dans le secteur bancaire et médical notamment.

Mais que devrions-nous faire? Comment pourrions-nous encourager les parties contractantes, en particulièrement les bureaux d'enregistrement à être plus rationnels? Il doit y avoir des négociations avec ces bureaux d'enregistrement par rapport à ce qu'ils doivent faire au niveau de la vérification. Donc, est-ce que ça vaut la peine de travailler avec les bureaux d'enregistrement? Donc, que pouvons-nous faire sinon notre conversation, ça va être tout simplement de l'espoir plutôt que des actions?

JEFFREY BEDSER Je pense que c'est un problème. Et ça on l'a dans SAC 115. Les besoins pour les parties contractantes de vérifier tous les rapports malfaisants, c'est un point de friction et c'est pour cela que les nouvelles obligations indiquent que s'il y a un rapport qui envoie des preuves, ce sera plus facile de prendre des actions, des mesures. Parce qu'on parle de volumes très élevés, de rapports d'hameçonnage, ça pourrait prendre des mois avec des milliers de personnes qui travailleraient à tous ces rapports sur des hameçonnages. Donc il faut vraiment qu'il y ait des preuves très solides.

Il faut s'assurer qu'il y ait des rapports. Lorsqu'il y a de l'hameçonnage, il faut qu'il y ait des processus en place pour faire des rapports. Ça existait il y a six sept ans. Il y avait des rapports qui étaient faits et rien ne se passait parce qu'il y avait beaucoup

d'efforts de validation et rien ne se passait. Il n'y a pas de mesures prises. Donc je crois que c'est très important au niveau des gTLD et je vois qu'il y a besoin d'obligation et je crois qu'on a besoin d'avoir en effet un impact sur l'information.

Et il faut savoir comment effectuer des rapports. Et avec Net Beacon par exemple, on a des standards et des normes pour effectuer des rapports concernant l'hameçonnage.

JONATHAN ZUCK Oui, on a travaillé là-dessus. On a fait de la sensibilisation sur ces outils dans notre communauté, mais j'ai été un petit peu frustré avec NetBeacon parce que ça requiert d'avoir une partie du courriel dans le rapport et donc ça exclut la plupart des personnes qui pourraient faire des rapports. Ce serait bien d'avoir un outil. Donc on pourrait simplement renvoyer l'email plutôt que de faire du copier-coller et ainsi de suite.

JEFFREY BEDSER Donc on peut travailler là-dessus avec le DNSClean, avec des logiciels qui pourraient travailler sur cela. Et s'il y a un point de friction, je pense que on pourrait faire des rapports plus faciles sur l'hameçonnage et je vais parler avec les personnes responsables pour essayer de remédier à cette situation par rapport à NetBeacon.

RAM MOHAN Nous avons Olivier.

JEFFREY BEDSER Je crois qu'il y a une autre personne qui parle sur Zoom et nous avons de l'écho.

OLIVIER CREPIN-LEBLOND Nous avons un écho. Vous m'entendez maintenant? Olivier Crépin-Leblond au micro. Merci beaucoup et je vois le rapport INFERMAL sur l'hameçonnage qui date de novembre de l'année dernière, je crois comprendre. Nous avons une nouvelle administration aux États-Unis et le monde n'est plus le même depuis ce nouveau gouvernement américain. Tout change donc. Qu'en est-il?

Ça fait quatre mois qu'on a eu ce rapport INFERMAL. Est-ce qu'il y a des actions qui vont être prises pour la formation des personnes? Est-ce qu'il va y avoir donc un aspect disruptif dans cet espace? Est-ce que nous allons avoir des mesures plus solides pour lutter contre ces hameçonnages? Ou bien est-ce qu'on se rend compte que la situation est grave et que l'on fait juste des rapports sur à quel point la situation est désastreuse? Donc que pouvons-nous faire?

RAM MOHAN Si on peut revenir sur la diapo précédente, je pense que nous pourrons le voir et peut-être qu'il y aura une conclusion à ce niveau de la part de mon collègue.

JEFFERY BEDSER

Vous avez raison, Olivier, et dans un forum public, je ne pourrai pas répondre à cela. On pourra en parler de manière privée, mais le plus grand problème que nous avons, c'est que c'est le haut de l'iceberg que nous gérons. Il faut vraiment qu'on se rende compte à quel point l'iceberg est géant et nous devons faire plus. Nous devons agir en effet, mais cela va être facilité par plus de rapports. On a besoin de plus de rapports qui nous proviennent pour pouvoir prendre des mesures.

Je ne sais pas exactement quels sont les mécanismes pour voir les abus. Je crois que les victimes doivent effectuer des rapports et je crois qu'il y a déjà eu des pertes à ce moment-là s'il y a eu des victimes, Donc, en effet, c'est un rapport minoritaire. C'est le crime qui doit être arrêté avant d'être commis.

Donc, y a-t-il un besoin d'infrastructures? Comment est-ce que l'on peut déterminer si les noms de domaine vont être malveillants ou utilisés d'une manière malveillante? Et est-ce que l'on va éviter la délégation de ce domaine ou interdire la délégation de ce domaine? Est-ce qu'il y a un processus qui nous permettra de gérer cela en amont? Je suis d'accord. Je suis frustré aussi. Donc nous avons beaucoup de rapports qui existent et on ne se préoccupe que du haut de l'iceberg parce qu'on ne se rend pas compte à quel point cet iceberg est grand.

RAM MOHAN Alan, vous avez la parole.

ALAN GREENBERG Donc moi j'ai reçu un SMS d'hameçonnage et j'ai fait mon rapport. C'est toujours actif quelques jours plus tard. J'étais dans le même vol que Graeme et je lui ai demandé combien de temps ça prend pour avoir une réponse. Il y a des bureaux d'enregistrement qui sont très lents, donc il y a des obligations qui existent, mais elles ne sont pas obligatoirement honorées.

Et je pense que notre seul choix à ce moment-là, c'est de voir ce que l'on peut faire de plus facile. Et donc les enregistrements en vrac, de grand nombre de noms de domaine, on doit lutter contre cela. Ce serait un bon processus, voir qui peut utiliser le système API d'interface et également si nous avons des domaines qui sont retirés en cas d'abus, qu'on ne puisse plus les utiliser. C'est facile, ça à mettre en œuvre, c'est la mise en œuvre qui est difficile.

RAM MOHAN Vous avez raison, Alan. Dans notre environnement, je crois que la première chose que nous pourrions faire, c'est publier les meilleures pratiques, ce qui fait sens, les pratiques qui font sens et qui peuvent être considérées dans le cadre du développement des politiques. Parce que si vous commencez un PDP sur quelque chose comme cela, avec tout le temps qu'il faudra pour avoir des résultats, toutes les recommandations seront obsolètes parce que les choses auront évolué.

Mais comme l'a dit Jeff, de plus en plus de parties dans cet environnement veulent faire plus et font plus pour atténuer et réduire l'incidence de ces problèmes. Ce n'est pas uniforme. Mais ce que l'on doit observer, c'est des instruments de mesure. Ce n'est pas l'uniformité, c'est obtenir assez de parties prenantes pour qu'elles puissent se conformer à ces obligations.

Et l'ALAC d'un autre côté et le SSAC pourront collaborer avec vous. Vraiment, nous devons avoir plus de formations qui soient effectuées. Pas seulement comment on reconnaît cet hameçonnage, mais qu'est-ce que l'on peut faire? Comment on fait les rapports? Comment est-ce que l'on peut indiquer qu'il y a cet hameçonnage qui est effectué? Donc peut-être que ça pourrait être automatisé et on pourrait avoir beaucoup de données à ce niveau-là et que nous pourrions ainsi pointer vers les personnes qui doivent prendre des mesures et dire : Vous avez une incidence très forte de cas d'hameçonnage et il y a des rapports qui vont être effectués. Et ensuite, là, on pourra agir et mettre la pression sur les personnes qui doivent agir et prendre des mesures. Pour le moment, c'est un petit peu faire un devoir moral, mais on ne peut pas uniquement se reposer sur un devoir moral.

ALAN GREEBERG Vous avez un devoir économique aussi et obtenir donc des revenus et ne pas se préoccuper de l'impact que cela a. Donc, je crois que si on avait des personnes du département de la conformité qui

veuillent bien avoir des interactions avec nous plutôt que de donner la ligne du parti.

JEFFREY BEDSER

Au niveau économique, ce que j'ai noté, c'est que ni les registres ni les bureaux d'enregistrement ne gagnent pas d'argent lors de la première année. Dès qu'ils passent de l'argent sur l'utilisation malveillante, ils commencent à perdre des fonds sur les noms de domaine.

Et, il n'y a que quelques exceptions, mais après 365 jours beaucoup de noms de domaine donc n'existent plus, mais il y a la fraude aux cartes de crédit également. Donc, je crois qu'il faut s'améliorer. Il faut améliorer la situation avec certaines étapes, étape par étape.

Et, j'aimerais vous rappeler, et nous prêchons auprès de la chorale. Je crois que l'on en parle dans ce forum public. Je crois que tout cela est observé, donc il se demande ce que l'on va faire. Il y a des bureaux d'enregistrement qui ont un problème avec des clients légitimes, qui achètent des comptes, qui les financent ces noms de domaine et qui les vendent avec leurs informations.

Elles peuvent utiliser ensuite ces noms de domaine d'une manière malveillante et frauduleuse. Donc, ça, c'est véritablement un problème. C'est revendre des comptes alors que ce ne sont pas des revendeurs, donc on ne peut pas restreindre l'accès au nom de domaine, mais il faut arrêter l'utilisation malveillante de ces

domaines parce que les criminels, ils sont bien en avance par rapport à nous.

JONATHAN ZUCK Informal a raison.

RAM MOHAN Bien, alors tout n'est pas sombre ici. Donc, nous avons notre fil conducteur ici. Il s'agit de lancer un dialogue avec vous. Il faut partager avec vous les cinq points qui sont les axes de concentration du SSAC. J'avais un acronyme auparavant qui n'a pas été vraiment bien accepté. Donc, nous appelons cela les sujets Keystone.

Ici, sur ces cinq éléments que nous avons partagés avec vous, nous nous impliquons principalement dans l'usage malveillant du DNS, qui a un impact fondamental sur les utilisateurs finaux et c'est quelque chose de tangible et que l'on peut exprimer. Nous souhaitons continuer de travailler avec vous et un Internet plus sûr, c'est quelque chose qui est en cours de progrès. Nous avons 125 documents que nous avons rédigé avec des conclusions et des recommandations qui pourraient pour la plupart, avoir des implications concrètes. Il y en a qui ont été écrits peut-être dans un but ludique? Pas forcément, non.

Nous souhaitons travailler avec vous sur ces aspects et ce que nous demandons... Et, nous pourrions donc prévoir une séance spécifique avec vous à ce sujet. Mais, pour le moment, quels sont

les sujets qui représentent le plus fort besoin pour vos publics? C'est une chose d'avoir une pléthore d'informations, mais le véritable objectif, c'est de façonner les informations afin qu'elles puissent être utilisées à bon escient.

En ce qui concerne l'usage malveillant du DNS en particulier, nous avons en tout cas 30 à 40 documents rédigés dans ce domaine. Il y a une mine d'informations disponibles pour les nouveaux gTLD. À titre de rappel, nous avons examiné, fourni des avis et des conseils sur les nouveaux gTLD depuis longtemps, mais plus récemment, nous avons donc fait des recommandations concernant la collision de noms et comment éviter la confusion, mais aussi la collision avec les noms qui ont déjà été résolus.

Aujourd'hui, sur Internet, par exemple, lors de la série précédente, les candidats qui avaient fait une demande pour .home, .corp ce qu'ils n'ont pas réalisé, ce qu'ils ne savaient pas, c'est que c'est TLD avaient déjà été utilisés pendant des décennies. Il y avait déjà énormément de trafic qui utilisait donc .home, .corp, et nous avons fourni à l'ICANN et au conseil d'administration de l'ICANN des recommandations sur la façon d'éviter ou tout du moins, atténuer ces collisions dans la prochaine série.

Concernant le DNSSEC, il y a déjà maintenant deux décennies qu'il a été mis en œuvre et au cours de ce laps de temps, au fil donc des mesures opérationnelles que nous avons pu observer. Il y a donc des observations empiriques. Il y a des fragilités qui ont été introduites lorsqu'on essaye de déployer les clés DNSSEC. Il y a

donc les petits TLD, les gros TLD, les TLD d'opérateurs qui ont beaucoup de ressources ou ceux qui ont peu de ressources, il y a des problèmes. Nous sommes en cours d'examen de la possibilité de travailler dans ce domaine. Voilà, vers quoi nous souhaitons nous orienter.

En ce qui concerne les espaces de noms alternatifs au sein de l'ICANN, cela est exprimé par les nombreuses initiatives qui sont disponibles relatives à la blockchain, des espaces de noms et l'intégration des espaces de noms du DNS. Nous avons essayé d'examiner qu'est-ce que c'est que des espaces de noms, donc avec une intégration responsable. Comment assurer l'intégration responsable afin que les paramètres de stabilité et de sécurité ne soient pas affectés de façon négative? Nous reviendrons vers vous avec un rapport sur ce que cela pourrait être.

Ensuite, au sein du SSAC, l'approche pour la blockchain et les autres espaces de noms. Cette approche n'est pas de dire que c'est mauvais et qu'il faut l'empêcher. Nous examinons rarement quelles sont les intentions de quelqu'un qui propose une innovation. Nous examinons surtout les interactions entre les différentes technologies qui existent déjà.

Et, enfin, Olivier parlait des changements qui se déroulent dans le monde. Nous ne nous concentrons pas trop sur les aspects géopolitiques, mais nous accordons notre attention aux aspects SSR et notre approche générale dans ce secteur, c'est de procurer des indices réels. Comment est-ce que le DNS fonctionne si vous

êtes un décideur politique, un décideur? Vous vous dites Nous allons adopter une loi sur l'approche, donc il faudrait bloquer donc le DNS. Nous ne souhaitons pas formuler une opinion sur le fait qu'il faut bloquer ou pas. Nous apportons des éclaircissements sur les conséquences éventuelles d'un cours d'action. Si vous prenez donc un trop gros marteau pour enfoncer un clou, ça ne serait pas utile. Donc, hier, par exemple, on m'a informé qu'apparemment, il y a un travail qui est en cours au sein de l'Union européenne. Notamment suite à un échec de résolveur DNS au sein de l'Europe et je me dis face à ça ce n'est pas de l'ingénierie, c'est de l'hallucination, véritablement.

Je ne dirai pas cela à un décideur politique, mais nous dirions peut-être alors donnez-nous les détails techniques sur la façon dont la résolution fonctionne. Tout cela pour dire que SSAC d'une manière générale est composée de personnes sceptiques sur la direction à prendre à l'avenir, mais ce sont des personnes qui sont réalistes sur le fait qu'il y a beaucoup de forces en présence et beaucoup de personnes qui cherchent à tirer profit d'une culture qui dit qu'on peut faire confiance à l'interlocuteur que l'on a en face de nous dans une transaction.

Les membres du SSAC en général ont cet état d'esprit, mais ils se rendent compte que c'est exactement ce que les interlocuteurs malveillants souhaitent exploiter. Voilà, les principaux axes de concentration pour nous. Je souhaite donner la parole à d'autres collègues du SSAC.

JONATHAN ZUCK Malheureusement, nous arrivons à court de temps et nous nous réjouissons de la prochaine réunion de l'ICANN pour poursuivre cette conversation. Peut-être que nous mettrons en place de petites équipes pour continuer la discussion et peut-être que nous pourrions voir comment tout cela se rapporte à notre mandat et quel est l'impact sur notre public élargi.

Nous arrivons à la fin de notre réunion, nous allons permettre à nos interprètes de prendre une pause. N'attendons pas trois mois. La prochaine réunion, en réalité, se déroulera dans quatorze jours, mais réunissons-nous sur Zoom et prenons ces éléments un par un pour les approfondir. En tout cas, il semblerait que nous n'ayons jamais suffisamment de temps. Nous avons énormément de choses en commun dans notre vue du monde. Continuons ces échanges. Merci à tout le monde, et merci aux interprètes.

[FIN DE LA TRANSCRIPTION]