Le secteur des domaines profite de la vente de drogues illégales en ligne et de la fraude liée à la COVID-19

LES CYBERCRIMINELS EXPLOITENT L'ÉTAT D'URGENCE SANITAIRE POUR FAIRE DU PROFIT

La pandémie a entraîné une flambée des cybercrimes qui visent une population désespérément à la recherche de sécurité et de réconfort. Ces activités criminelles nécessitent des noms de domaine afin de mettre en œuvre des campagnes d'hameçonnage, de pourriels et de logiciels malveillants ainsi que pour créer des sites Web frauduleux. [1]

- Au cours du mois de mars 2020, au moins **100 000 nouveaux noms de domaine** contenant des termes comme « covid », « corona » et « virus » [2] ont été enregistrés en plus des domaines enregistrés pour vendre des articles tels que des masques médicaux. [3] De plus, d'autres domaines ont été utilisés pour envoyer des pourriels d'annonces pour des fraudes sur le thème de la COVID-19.
- Depuis mars 2020, les noms de domaine malveillants liés à la COVID-19 confirmés se comptent par milliers.
- Environ **1000 nouveaux noms** de domaine correspondant à ces critères sont enregistrés au quotidien.[4]
  - Près de 6 500 de ces domaines sont en mesure d'envoyer et de recevoir des courriels; une indication claire qu'ils pourraient être utilisés dans le cadre d'attaques d'hameçonnage, de fraude ou de compromission de courriels d'affaires.
  - Parmi ces noms de domaines, 122 contiennent le mot « vaccin » et plus de 400 contiennent le mot « test ». Plus de 20 % de ces noms de domaine peuvent également envoyer et recevoir des courriels.
- Santé Canada a reconnu la menace que représentent ces plateformes en ligne et a diffusé une **alerte nationale rappelant que la vente de médicaments ou de vaccins contrefaits est une activité criminelle qui pose de graves risques pour la santé et la sécurité des Canadiens.** [5]
  - De plus, Santé Canada collabore avec des partenaires internationaux ainsi qu'avec d'autres départements et organismes gouvernementaux, tels que l'Agence des services frontaliers du Canada (ASFC), afin de protéger les Canadiens. L'Organisation internationale de police criminelle, INTERPOL, a publié une **alerte mondiale** adressée aux services chargés de l'application de la loi dans ses 196 pays membres afin de les mettre en garde. [6]

IL EXISTE TOUTEFOIS UNE SOLUTION : L'IMPUTABILITÉ DU SECTEUR DES DOMAINES

Les registres et registraires de noms de domaines doivent agir pour mettre un terme aux fraudes liées à la COVID-19 ainsi qu'à la vente en ligne d'opioïdes illicites et de médicaments d'ordonnance contrefaits ou non homologués.

- Les registres et les registraires ont le pouvoir de mettre un terme à l'énorme quantité de fraudes et de

préjudices à la santé publique en ligne.

- Les registres et les registraires devraient immédiatement bloquer et suspendre tout nom de domaine utilisé pour faciliter les fraudes liées à la COVID-19 et la vente illégale de médicaments illicites en ligne dès qu'il est signalé par un tiers crédible.
- Certains registres et registraires canadiens ferment (c.-à-d., bloquer et suspendre) les sites Web frauduleux selon les renseignements qui leur sont transmis par des déclarants de confiance tels que le Centre antifraude du Canada, Santé Canada et autres. Cependant, ils sont nombreux à ne pas le faire et ceux-ci servent souvent de refuge pour les activités illicites.
- Tous les acteurs, y compris les registres et les registraires, doivent faire leur possible pour mettre un terme aux fraudes liées à la COVID-19 et à la vente illégale de produits de santé en ligne, en particulier lors d'une urgence sanitaire.

EN QUOI CONSISTENT LES REGISTRAIRES ET LES REGISTRES DE NOMS DE DOMAINE?

- **Une entreprise de registre de noms de domaine crée, exploite et fait respecter les exigences en matière de suffixes de domaine, tels que .ca, .com, .edu, .org et .tech.** L'Autorité canadienne pour les enregistrements Internet (CIRA), Verisign, Radix et Neustar sont des exemples de registres.
- **Un registraire de noms de domaine est une entreprise accréditée qui vend des noms de domaine au public.**
  Rebel and Tucows (basé au Canada) et GoDaddy sont des exemples de registraires.

L'HISTORIQUE DE NÉGLIGENCE DES DANGERS POUR LA SANTÉ PUBLIQUE EN LIGNE

L'histoire a prouvé que, souvent, les registres et les registraires n'agissent pas pour éviter les préjudices en ligne à l'égard de la santé publique sans ordonnance du tribunal. Cela s'est avéré vrai même lorsque :

- les noms de domaines sous-entendent des activités illégales (p. ex., www.remèdescontrelacovid.com);
- le registre ou le registraire est mis au courant par un tiers de confiance que des noms de domaine sur leurs plateformes contreviennent aux conditions de leurs propres contrats (modalités);
- le registre ou le registraire est conscient qu'un nom de domaine est incontestablement utilisé pour vendre des opioïdes, offrir des « remèdes » contre la COVID-19 ou pour mettre en danger la santé et la sécurité publique.

LE RÉSULTAT : Les registres et les registraires profitent de l'octroi de noms de domaines qui créent ou aggravent les préjudices à la santé publique existants. Cette inaction met des vies en danger, en particulier lors d'une urgence sanitaire au cours de laquelle des millions de Canadiens confinés à leur domicile se fient à l'Internet pour avoir accès à des renseignements, des produits et des services de santé.

POURQUOI EST-IL SI DIFFICILE DE LUTTER CONTRE LES FRAUDES EN LIGNE DE NOS JOURS?

Auparavant, les cyberenquêteurs et les premiers répondants publics et privés pouvaient « trier » les attaques en obtenant des renseignements concernant des milliers de noms de domaine en temps quasi réel à l'aide d'un service appelé WHOIS.

- Ces parties sont responsables de la majorité des plus de deux milliards de requêtes envoyées de manière automatisée dans la plupart des cas à WHOIS au quotidien afin de faire un suivi ainsi que d'évaluer le bon fonctionnement des noms de domaine et les risques qu'ils présentent.
- Toutefois, au cours des deux dernières années, l'accès aux données de WHOIS a considérablement diminué en raison des politiques de l'ICANN, de la législation sur le respect des informations personnelles de l'UE et des pratiques optionnelles des registres et des registraires.

Les attaques sur le thème de la COVID-19 sont plus faciles à exécuter et plus difficiles à réduire, car les politiques du secteur des domaines et les intérêts commerciaux interfèrent avec l'acquisition d'informations essentielles aux enquêtes, à l'identification, à la réduction et à l'arrestation des criminels.

- Dans une lettre adressée aux registraires GoDaddy, NameCheap, Register.com et à d'autres, le bureau du procureur général de New York affirme que « la situation actuelle exige une grande vigilance » et demande aux registraires de prendre des mesures préventives visant à éviter, détecter et suspendre ces domaines malveillants.
- Le département américain de la justice a signalé à NemCheap que « des communications facilitées par [sa] propre entité et envoyées par [ses] clients directs ou partenaires d'affaires ont été associées à [de] telles activités criminelles » en faisant allusion aux manœuvres frauduleuses visant les citoyens américains et tirant profit de la pandémie de COVID-19.

LES DÉCIDEURS POLITIQUES PEUVENT OBLIGER LE SECTEUR CANADIEN DES DOMAINES À AGIR

Des actions immédiates sont nécessaires pour protéger les citoyens canadiens des préjudices constants et pour conserver la confiance des gens vis-à-vis de l'Internet ainsi que son intégrité au moment où la population en dépend le plus :

- Les registraires doivent bloquer et suspendre les noms de domaines suspects en lien avec la COVID-19 et lorsque les premiers répondants présentent des preuves qu'ils sont dangereux.
- Afin de préserver la sécurité et la transparence de l'Internet, des lois sont requises pour obliger les registres et les registraires à donner libre accès aux dossiers exacts, non anonymes et accessibles à grande échelle de WHOIS.

[1] *The Internet is drowning in COVID-19-related malware and phishing scams*, Ars Technica, 16 mars 2020, au : https://arstechnica.com/information-
Trend Micro, 20 mars 2020, au : https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

[2] *Don't Panic: COVID-19 Cyber Threats*, Palo Alto Networks Unit 42 blog, 24 mars 2020, au : https://unit42.paloaltonetworks.com/covid19-cyber-threats/

[3] *Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN,* Interisle Consulting Group, LLC, 31 mars 2021, page 18, au : http://bit.ly/DataCrossroads.

[4] Ibid.

[5]. *Santé Canada met en garde les Canadiens contre l'achat de vaccins contre la COVID-19 vendue en ligne ou provenant de sources non autorisées,* Avis de Santé Canada, 16 décembre 2020 au : https://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2020/74579a-eng.php

[6]. Ibid.