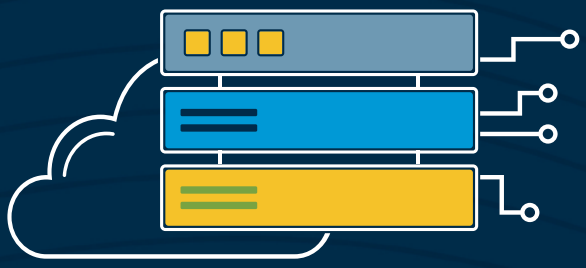
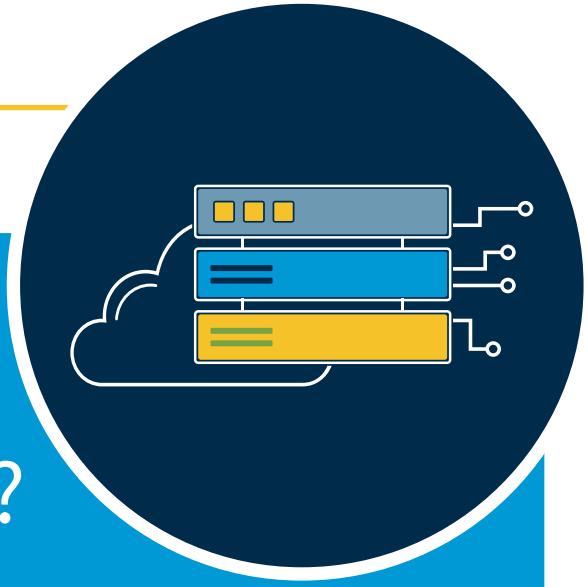


Signalement et collecte d'information sur des menaces à la sécurité des noms de domaine (DNSTICR)

Janvier 2022

Société pour l'attribution des noms de domaine
et des numéros sur Internet

ICANN



Que contient ce guide ?

2 Qu'est-ce que le système des noms de domaine (DNS) ?

2 Quelles sont les menaces à la sécurité du DNS ?

3 Signalement et collecte d'information sur des menaces à la sécurité des noms de domaine (DNSTICR).

4 Menaces non incluses dans le DNSTICR.

5 Origines du projet DNSTICR.

6 Comment vous pouvez nous aider.

7 Liens utiles et acronymes.

Qu’est-ce que le système des noms de domaine ?

Le système des noms de domaine (DNS) permet aux utilisateurs de se repérer plus facilement sur Internet. Chaque dispositif ou site Web sur Internet a une adresse unique, comparable à un numéro de téléphone. Cette adresse, qui consiste en une série complexe de chiffres, ou de chiffres et lettres, est appelée **adresse IP.** IP signifie Protocole Internet.

Les adresses IP sont difficiles à mémoriser. Le DNS facilite la navigation sur Internet.

Les adresses IP peuvent être difficiles à mémoriser. Le DNS facilite la navigation sur Internet en permettant aux utilisateurs de taper une chaîne alphabétique familière (le **nom de domaine**) au lieu de l’**adresse IP**. Ainsi, vous n’avez qu’à taper **https://icann.org** au lieu de l’**adresse IP 192.0.43.7** pour accéder au site web de l’ICANN.

Quelles menaces pour le DNS ?

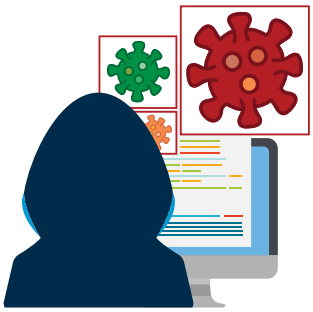
Il existe différentes formes d’**abus** associés à des contenus dans l’espace Internet. Parmi ces abus on retrouve des sites web qui servent de plate-forme à des activités illégales comme l’ exploitation des enfants et la traite de personnes. D’autres sites encouragent la cyberintimidation ou sont des paradis numériques pour la vente de produits inexistants ou contrefaits.

Or, le mandat de l’ICANN exclut la règlementation des contenus sur Internet.

L’organisation ICANN concentre ses efforts sur des **menaces à la sécurité du DNS** spécifiques dont la portée est plus limitée que celle des abus liés aux contenus. Alors, que considère-t-on des menaces à la sécurité du DNS ?

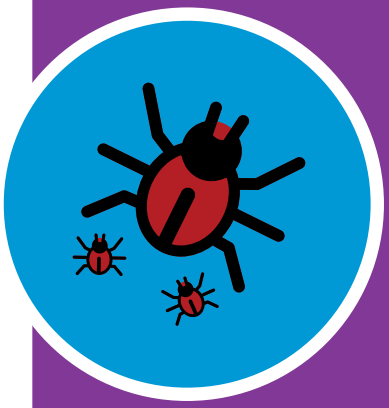
Par menaces à la sécurité du DNS, on entend toute activité malveillante visant à perturber l'infrastructure du DNS ou à faire fonctionner le DNS d'une manière non souhaitée.

Signalement et collecte d’information sur des menaces à la sécurité des noms de domaine (DNSTICR)



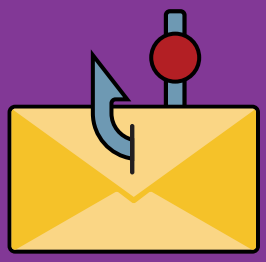
Le projet de **signalement et collecte d’information sur des menaces à la sécurité des noms de domaine (DNSTICR)** produit des rapports sur des enregistrements récents de domaines soupçonnés par l’organisation ICANN de profiter de la pandémie de COVID-19 pour des campagnes d’hameçonnage ou de distribution de logiciels malveillants.

Ces rapports contiennent les preuves qui conduisent l’organisation ICANN à croire que les domaines sont utilisés de manière malveillante. Associés à d’autres informations contextuelles, les rapports aident les bureaux d’enregistrement concernés à déterminer le plan d’action approprié.



Le projet DNSTICR vise à identifier des tentatives d’injection de code malveillant et d’hameçonnage.

Logiciel malveillant
Logiciel installé dans un dispositif sans le consentement de l’utilisateur pour perturber le fonctionnement du dispositif, collecter des informations sensibles ou accéder à des systèmes informatiques privés. Parmi les logiciels malveillants figurent les virus, les logiciels espions, les rançongiciels et autres logiciels indésirables.



Hameçonnage
Ce type de fraude se produit lorsqu'un attaquant manipule une victime pour lui faire révéler des informations personnelles, d'entreprise ou financières sensibles (numéros de compte, identifiants de connexion, mots de passe, etc.), à l'aide de courriers électroniques frauduleux ou ressemblant à ceux d' organismes familiers, ou bien en attirant les utilisateurs sur de faux sites Web.

Le projet DNSTICR n’est pas destiné à identifier les pratiques malveillantes suivantes :

Réseaux zombies

Groupes d'ordinateurs connectés à Internet qui ont été infectés par des logiciels malveillants et qui sont commandés pour effectuer des activités sous le contrôle d'un administrateur distant.

Dévoiement

Renvoi des utilisateurs vers des sites ou des services frauduleux, souvent par détournement ou empoisonnement du DNS.

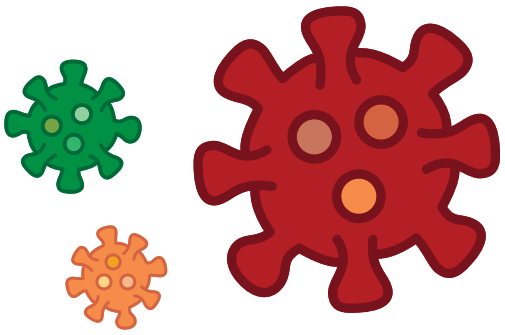
- Le détournement du DNS se produit lorsque des attaquants utilisent un logiciel malveillant pour rediriger les victimes vers le site de l’attaquant au lieu de celui demandé.
- L'empoisonnement du DNS force un serveur ou un résolveur DNS à répondre avec une fausse adresse IP portant un code malveillant. La différence entre le hameçonnage et le dévoiement réside dans le fait que ce dernier implique la modification des entrées DNS, tandis que le premier incite les utilisateurs à communiquer des informations personnelles.

Spam (utilisé pour propager d’autres menaces pour le DNS)

Envoi massif de courriels non sollicités, lorsque le destinataire n'a pas donné l'autorisation d'envoyer le message et lorsque le message a été envoyé dans le cadre d'une série plus vaste de messages présentant tous un contenu essentiellement identique. Un courriel générique non sollicité ne constitue pas à lui seul une menace pour la sécurité du DNS, mais il le serait si ce courriel faisait partie d'un plan d'hameçonnage.

Origines du projet DNSTICR

Lors de la **pandémie de COVID-19**, les fraudeurs ont escroqué les personnes vulnérables, les personnes peu vigilantes, les personnes âgées, les enfants et les moins fortunés. Ces criminels ciblent des victimes dans le monde entier et dans de nombreuses langues pour leur voler de l'argent et leur soutirer des renseignements personnels.



Les criminels et les escrocs téléphonent ou envoient des courriels ou des SMS aux victimes pour leur faire révéler des informations personnelles ou les inciter à acquérir de faux certificats de vaccination, de faux tests COVID-19 ou de faux traitements.

L'organisation ICANN a développé le **projet DNSTICR** afin de lutter contre l'hameçonnage et les logiciels malveillants sur Internet lors de la pandémie de COVID-19. Ce projet identifie et signale aux bureaux d'enregistrement des activités potentiellement malveillantes des noms de domaine ainsi que des informations de contexte utiles. Il apporte une autre dimension de défense au combat que mène l'organisation ICANN pour protéger les utilisateurs de l'Internet contre les menaces à la sécurité du DNS.

Les termes et les thèmes recherchés dans le cadre du projet DNSTICR sont mis à jour au fur et à mesure que la pandémie évolue. Cette mise à jour est un processus technique relativement simple. Parmi les termes ajoutés on retrouve « **passeport »,** en rapport avec le **passeport vaccinal** utilisé dans certains pays, et « **ivermectine »**, un médicament anti-parasitaire qui a été associé à la pandémie.

D'autres termes à inclure pourraient concerner le nom des principaux programmes gouvernementaux liés à la COVID-19 et destinés à aider les personnes en détresse. Des termes plus génériques comme « respirateurs », « masques N95 » et « désinfectants » ont également été incorporés.

Cependant, l'organisation ICANN ne dispose pas de ressources ou d'attributions pour vérifier si tous les sites proposant ce type de produits sont légitimes.

Aidez-nous à protéger l'Internet contre les logiciels malveillants et l'hameçonnage liés à la COVID-19 dans votre région du monde.

Vous êtes prestataire de soins de santé, gestionnaire financier, régulateur gouvernemental, décideur politique, responsable de la sécurité publique ou professionnel de la sécurité ?

Nous avons besoin de vous !

Voici comment nous pouvons travailler ensemble pour protéger les utilisateurs de l'Internet des menaces à la sécurité du DNS :

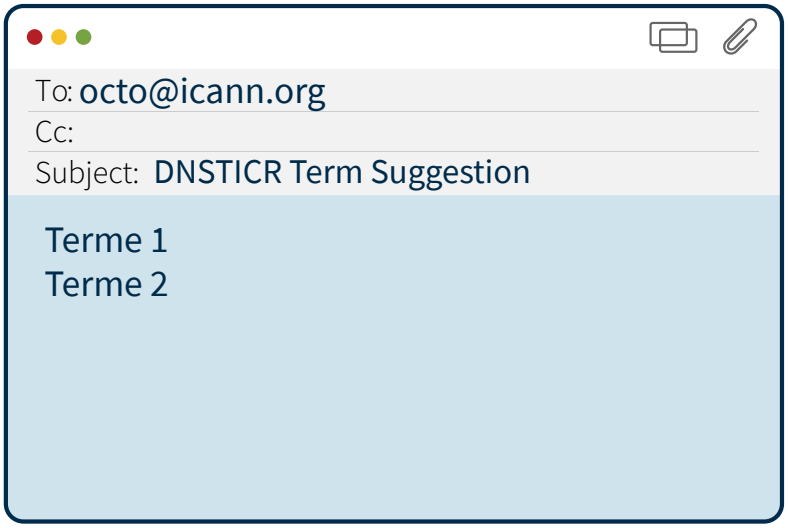
Étape 1
Dressez dans votre langue maternelle une liste de mots et de jeux de caractères liés à la pandémie de COVID-19 qui sont utilisés ou pourraient être utilisés dans votre région pour cibler des personnes ou des organisations.

Étape 2
Envoyez votre liste par email à **octo@icann.org** en mettant dans la ligne d'objet : **suggestion de termes pour DNSTICR.**

Les nouvelles suggestions doivent être soumises une par ligne dans le corps du courrier électronique.

Par exemple :
Terme 1
Terme 2

Si les termes nécessitent une explication, ajoutez-la après votre liste de termes.



Découvrez le projet de signalement et collecte d'information sur des menaces à la sécurité des noms de domaine (DNSTICR) et comment vous pouvez contribuer à rendre l'Internet plus sûr !

En savoir plus
Visitez notre page Web DNSTICR dédiée :
https://www.icann.org/dnsticr

Explorer
Découvrez les efforts déployés par l'ICANN à l'échelle de l'organisation pour atténuer les menaces à la sécurité du DNS :
https://www.icann.org/dnsabuse

Termes et acronymes
Cliquez sur les liens ci-dessous pour de plus amples informations sur les acronymes et les termes utilisés dans ce guide via la fonctionnalité Acronymes et termes de l'ICANN :
https://go.icann.org/acronyms

Nom de domaine
Étiquette de nom de domaine
Système des noms de domaine (DNS)
Protocole Internet (IP)
Adresse de Protocole Internet
Protocole Internet version 4 (IPv4)
Protocole Internet version 6 (IPv6)

NOUS CONTACTER

https://icann.org
flickr.com/icann
@icann
linkedin.com/company/icann
facebook.com/icannorg
soundcloud.com/icann
youtube.com/icannnews
instagram.com/icannorg

Ou visitez notre page dédiée aux réseaux sociaux :
https://go.icann.org/socialmedia