VERSION PRÉLIMINAIRE Mai 2023

Avis : Respect des Obligations en matière d’utilisation malveillante du DNS prévues dans le Contrat d'accréditation de bureau d'enregistrement et le Contrat de registre

Le présent Avis fournit des directives quant à l’interprétation et au respect des amendements, en date du [DATE], du Contrat d'accréditation de bureau d'enregistrement (RAA) et du Contrat de registre (RA) de base pour les domaines génériques de premier niveau (gTLD), relatifs aux obligations liées à l’atténuation de l’Utilisation malveillante du Système des noms de domaine (DNS) (les Amendements relatifs à l’Utilisation malveillante du DNS).

Sauf en cas de modification spécifique apportée par les Amendements relatifs à l’Utilisation malveillante du DNS, l’ensemble des obligations prévues dans le RAA et le RA avant que ces Amendements ne soient apportés restent applicables et en vigueur.

Tous les termes commençant par une majuscule qui ne sont pas définis dans le présent Avis ont la signification qui leur est attribuée dans le RAA et le RA.

Les bureaux d’enregistrement et les registres qui ont recours aux pratiques définis dans le présent Avis s’acquitteront probablement des obligations prévues dans les Amendements relatifs à l’Utilisation malveillante du DNS, mais même en cas de recours à une ou plusieurs de ces pratiques, il ne sera pas automatiquement déterminé que le bureau d’enregistrement ou l’opérateur de registre s’est acquitté de ses obligations. Les exemples ci-après sont uniquement illustratifs et ne visent pas à limiter les mesures d’atténuation envisageables. Dans tous les cas, dès que le Service de conformité contractuelle de l'ICANN lance une enquête, les bureaux d’enregistrement et les opérateurs de registre doivent fournir des preuves attestant de leur respect des exigences applicables prévues dans le RAA et le RA.

Contexte

L’organisation ICANN conclut des contrats (un RA) avec des registres à des fins d’exploitation de gTLD. Le RA définit les responsabilités de l’opérateur de registre, notamment le maintien à jour de la base de données faisant autorité de tous les noms

de domaine enregistrés dans le gTLD et la publication de la zone DNS pour le gTLD.

L'ICANN conclut également un RAA avec chaque bureau d'enregistrement, contrat qui permet au bureau d'enregistrement de proposer des services d'enregistrement de nom de domaine dans les gTLD. Le RAA définit les responsabilités du bureau d'enregistrement, telles que la vérification des informations du titulaire de nom de domaine (ou Titulaire de nom enregistré) et la tenue de registres exacts. Les rôles et obligations des bureaux d'enregistrement et des registres sont distincts et sont prévus dans leurs contrats respectifs, le RAA et le RA.

L'ICANN est habilitée à faire appliquer les règles relatives aux services d'enregistrement de nom de domaine et aux noms de domaine tel que prévu dans le RAA et le RA. Le présent Avis se concentre sur les noms de domaine (ou Noms enregistrés) dans les gTLD qui sont utilisés en tant qu'instruments ou mécanismes pour l'Utilisation malveillante du DNS. Les exigences posées par les Amendements relatifs à l'Utilisation malveillante du DNS dans le RAA et le RA sont fondées sur les mesures que les bureaux d'enregistrement et les opérateurs de registre peuvent prendre respectivement afin de minimiser la portée et l'intensité des dommages causés par l'Utilisation malveillante du DNS et donc le nombre de victimes. Ces exigences considèrent également que les bureaux d'enregistrement et les opérateurs de registre ne représentent qu'une partie de l'écosystème du DNS, qui est composé de nombreux acteurs[1]. L'acteur le plus à même de détecter, d'évaluer, de vérifier et de mettre un terme à l'activité abusive peut varier selon les circonstances spécifiques d'un cas d'Utilisation malveillante du DNS ; il peut parfois s'agir d'un acteur autre qu'un bureau d'enregistrement ou un opérateur de registre.

Utilisation malveillante du DNS

Aux fins du RAA, du RA et du présent Avis, l'*Utilisation malveillante du DNS* désigne les logiciels malveillants, les réseaux zombie, l'hameçonnage, le dévoiement et les courriers indésirables (lorsque les courriers indésirables servent de mécanisme de diffusion de l'un des quatre autres types d'Utilisation malveillante du DNS), tel que ces termes sont définis à la Section 2.1 du Rapport du Comité consultatif sur la sécurité et la stabilité relatif à une approche interopérable de la gestion de l'utilisation malveillante du DNS (SAC 115[2]) :

> Les **logiciels malveillants** sont des programmes malveillants installés et/ou exécutés sur un dispositif sans le consentement de l'utilisateur, qui interrompent les opérations du dispositif, collectent des informations sensibles et/ou accèdent à des systèmes informatiques privés. Les logiciels malveillants comprennent les virus, les logiciels espion, les rançonlogiciels et autres logiciels indésirables.

Les **réseaux zombie** sont des collections d'ordinateurs connectés à Internet qui ont été infectés par des logiciels malveillants et peuvent recevoir l'ordre d'effectuer des activités sous le contrôle d'un attaquant à distance.

[1] De plus amples informations sont disponibles dans le rapport élaboré par le Groupe d'intérêt particulier sur l'Utilisation malveillante du DNS lors du FIRST, rapport qui contient également des conseils destinés aux équipes de réponse aux incidents sur les organisations susceptibles d'être contactées lors des différentes phases de la réponse aux incidents du fait des différentes techniques d'utilisation malveillante du DNS. De plus, le Réseau politique Internet et juridiction (https://www.internetjurisdiction.net/) a fourni d'autres directives sur ces formes d'Utilisation malveillante du DNS dans son document intitulé « Approches opérationnelles, normes, critères et mécanismes ».

[2] Article 2.1, pages 12-13 du SAC 115 du Comité consultatif sur la sécurité et la stabilité de l'ICANN du 19 mars 2021.

L’**hameçonnage** se produit lorsqu’un attaquant trompe une victime de sorte à ce qu’elle révèle des informations personnelles, professionnelles ou financières sensibles (numéros de compte, identifiants de connexion, mots de passe, etc.), en envoyant des e-mails frauduleux ou similaires, ou en attirant les utilisateurs vers des sites web copieurs. Certaines campagnes d’hameçonnage visent à convaincre l’utilisateur d’installer un logiciel malveillant.

Le **dévoiement** est le redirectionnement des utilisateurs vers des sites ou des services frauduleux, en général par le biais d’un détournement ou d’un 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 et non pas le site initialement recherché. L’empoisonnement du DNS provoque la réponse d’un serveur DNS (ou résolveur) par une fausse adresse protocole Internet portant un logiciel malveillant. L’hameçonnage diffère du dévoiement en ce que ce dernier implique la modification des entrées DNS, tandis que le premier permet aux utilisateurs de saisir des informations personnelles.

Les **courriers indésirables** sont des e-mails en masse non sollicités, où le destinataire n’a pas autorisé l’envoi du message et où le message a été envoyé dans le cadre d’une plus grande collection de messages, tous ayant un contenu sensiblement identique. Les courriers indésirables sont uniquement considérés comme constituant une Utilisation malveillante du DNS lorsqu’ils sont utilisés comme mécanisme de diffusion d’au moins l’un des autres types d’utilisation malveillante du DNS décrits ci-dessus.

Obligations du bureau d’enregistrement

Article 3.18 du RAA

Avant l’entrée en vigueur des Amendements relatifs à l’Utilisation malveillante du DNS, l'Article 3.18 imposait aux bureaux d’enregistrement de tenir à jour et de publier des coordonnées à des fins de signalement de cas d’utilisation malveillante, notamment d’Activité illégale. Cette disposition posait également des exigences liées aux enquêtes et aux réponses au signalement de cas d’utilisation malveillante impliquant des Noms enregistrés parrainés par un bureau d’enregistrement, ainsi qu’aux registres connexes qu’un bureau d’enregistrement doit tenir. Les exigences prévues à l'Article 3.18 du RAA ont été amendées tel que suit :

Exigences relatives à la publication et au maintien à jour des contacts pour le signalement de cas d'utilisation malveillante (Article 3.18.1 du RAA)

Où signaler des cas d'utilisation malveillante[3]
Afin de faciliter le signalement par une partie d'un potentiel cas d'utilisation malveillante et/ou d'Activité illégale, le bureau d'enregistrement doit publier une adresse e-mail ou un formulaire web facilement accessible sur la page d'accueil du site web du bureau d'enregistrement[4]. Les formulaires web ne doivent pas imposer d'avoir un identifiant pour le signalement de cas d'utilisation malveillante.

Une page d'accueil d'un bureau d'enregistrement qui affiche clairement un lien vers une page « Signalement de cas d'utilisation malveillante » ou « Nous contacter » (qui indique clairement la personne à contacter pour le signalement de cas d'utilisation malveillante) et qui permet aux auteurs de signalement de rapporter facilement des cas d'utilisation malveillante à partir de la page contenant le lien sera jugée conforme.

Confirmation du reçu d'un signalement de cas d'utilisation malveillante
De plus, le bureau d'enregistrement doit fournir à l'auteur du signalement la confirmation que son signalement a bien été reçu. Cette confirmation peut être envoyée à l'auteur du signalement ou affichée sur l'écran après avoir procédé au signalement auprès du bureau d'enregistrement. Elle doit contenir suffisamment d'informations pour permettre à l'auteur du signalement de prouver qu'il a procédé au signalement d'un cas d'utilisation malveillante. La confirmation doit au moins identifier le bureau d'enregistrement, le ou les Noms enregistrés signalés ainsi que la date du signalement.

Contacts pour les organismes chargés de l'application de la loi
Les exigences liées aux contacts dédiés à la réception de signalements par des organismes chargés de l'application de la loi et autres autorités relevant de la juridiction du bureau d'enregistrement précédemment décrites à l'Article 3.18.2 du RAA figurent désormais à l'Article 3.18.3 du RAA ; ces exigences demeurent inchangées.

Exigences relatives à l'adoption de mesures d'atténuation suite à la réception de signalements concrets de cas d'Utilisation malveillante du DNS (Article 3.18.2 du RAA)

L'Article 3.18.2 du RAA, tel que modifié par les Amendements relatifs à l'Utilisation malveillante du DNS, est désormais le suivant :

> *Lorsqu'un Bureau d'enregistrement dispose de preuves concrètes de l'utilisation d'un Nom enregistré parrainé par un Bureau d'enregistrement à des fins d'Utilisation malveillante du DNS, le Bureau d'enregistrement doit prendre dans de brefs délais une ou des mesures d'atténuation adéquates nécessaires, dans*

la mesure du raisonnable, afin de mettre un terme à, ou d'interrompre, l'utilisation du Nom enregistré à des fins d'Utilisation malveillante du DNS. La ou les mesures prises peuvent varier en fonction des circonstances ; il convient de tenir compte de la cause et de la gravité des dommages causés par l'Utilisation malveillante du DNS et des éventuels dommages collatéraux associés.

[3] Dans un souci de clarté, les exigences relatives à la publication de l'adresse e-mail et du numéro de téléphone du contact du bureau d'enregistrement chargé de la réception des signalements de cas d'utilisation malveillante via le Service d'annuaire de données d'enregistrement (RDDS) demeurent inchangées.

[4] Ce site web doit être situé sur la même adresse universelle (URL) que celle saisie par le bureau d'enregistrement dans le champ « URL du bureau d'enregistrement » via son RDDS, fournie à l'ICANN et à l'opérateur de registre à des fins de publication dans le RDDS de l'opérateur de registre.

Preuves concrètes
Les preuves doivent être *concrètes*. Cela signifie que les informations auxquelles le bureau d'enregistrement peut facilement accéder doivent être suffisantes de sorte à permettre au bureau d'enregistrement de pouvoir déterminer, dans la mesure du raisonnable, si le Nom enregistré est utilisé ou non sous une ou plusieurs des formes d'Utilisation malveillante du DNS. Les bureaux d'enregistrement sont encouragés à assurer un suivi proactif des Noms enregistrés qu'ils parrainent afin d'identifier de potentiels cas d'utilisation malveillante du DNS. L'examen, par le bureau d'enregistrement, des preuves concrètes dépendra des circonstances de chaque cas.

Obtention des preuves concrètes auprès d'une partie externe
La Chambre des parties contractantes (CPH) a publié des directives visant à faciliter le signalement complet et concret aux bureaux d'enregistrement de cas d'utilisation malveillante (les Directives de la CPH). Les Directives de la CPH décrivent les preuves concrètes permettant de donner suite au signalement d'un cas d'utilisation malveillante. Par exemple, une capture d'écran montrant une tentative d'hameçonnage et indiquant contre qui est dirigé l'hameçonnage (par exemple, une institution financière) et l'URL complète où se situe l'utilisation malveillante (par exemple, example[.]tld/badpage[.]html)[5]. Les auteurs de signalements de cas d'utilisation malveillante sont encouragés à consulter et suivre les Directives de la CPH et à fournir autant d'informations que possible dans leurs signalements afin de permettre au bureau d'enregistrement de mener une enquête sur la potentielle Utilisation malveillante du DNS.

Dans les cas où un bureau d'enregistrement reçoit un signalement de cas d'utilisation malveillante ne contenant pas toutes les informations nécessaires et qu'il ne peut alors considérer être en possession de preuves concrètes d'Utilisation malveillante du DNS, le bureau d'enregistrement doit enquêter conformément à l'Article 3.18 du RAA. Dans certains cas, le bureau d'enregistrement peut avoir accès à des informations qui n'ont pas été fournies par l'auteur du signalement mais sont nécessaires ou utiles afin de déterminer que le Nom enregistré est utilisé à des fins d'Utilisation malveillante du DNS. Dans de tels cas, le bureau d'enregistrement doit privilégier les informations auxquelles il a raisonnablement accès et qui sont utiles à l'enquête (par exemple, les serveurs de noms, les informations et l'activité du compte, et le contenu d'au moins la principale page web ou l'URL spécifique fournie, le cas échéant, dans le signalement).

Après la fourniture de preuves concrètes, des mesures doivent être rapidement prises
Après avoir reçu des preuves concrètes, le bureau d'enregistrement *doit, dans de brefs délais, prendre une ou des mesures d'atténuation adéquates* raisonnablement nécessaires afin de mettre un terme à, ou d'interrompre,

[5] Cette URL est affichée sous un format connu sous le terme d’« URL inopérante ». Une URL inopérante est lisible à l'œil humain mais il n’est pas possible de cliquer dessus. Par conséquent, si vous ou la personne recevant le signalement cliquez accidentellement sur l’URL, vous ne serez pas dirigé vers un site potentiellement malveillant.

l'utilisation du Nom enregistré à des fins d'Utilisation malveillante du DNS. Afin de déterminer les mesures d'atténuation adéquates et pouvant être prises rapidement, le bureau d'enregistrement examinera les circonstances spécifiques du cas, et pourra notamment évaluer la portée et l'intensité des dommages causés par l'Utilisation malveillante du DNS au regard des éventuels dommages collatéraux associés.

Il est particulièrement important de tenir compte des dommages collatéraux lorsqu'un nom de domaine légitime ou bénin est utilisé en tant que vecteur de l'Utilisation malveillante du DNS sans que le titulaire de nom de domaine n'en ait connaissance ou n'y ait consenti. On parle souvent de « domaine compromis » et c'est parfois le fruit de l'exploitation d'un système de gestion de contenu de site web. Dans ces situations compromises, une suspension directe du domaine par le bureau d'enregistrement ou l'opérateur de registre peut ne pas s'avérer être l'atténuation adéquate, dans la mesure où une suspension pourrait empêcher l'accès à l'ensemble du contenu légitime et rendre inaccessibles tout e-mail associé ou autres services du domaine[6]. C'est également le cas lorsque l'Utilisation malveillante du DNS est associée à un domaine de troisième niveau ou sous-domaine. Les bureaux d'enregistrement et les registres peuvent uniquement agir au second niveau des domaines. Par conséquent, s'ils suspendent le domaine de second niveau, tous les domaines de troisième niveau seraient également suspendus, pas seulement le domaine associé à l'Utilisation malveillante du DNS. Dans ces situations, un bureau d'enregistrement peut choisir de prévenir le titulaire de nom de domaine, l'opérateur du site et/ou l'hébergeur.

Qu'est-ce qu'une mesure rapide ?
Tel qu'indiqué précédemment, la mesure d'atténuation adéquate visant à mettre un terme à ou à interrompre un cas d'Utilisation malveillante du DNS variera en fonction des circonstances spécifiques. De ce fait, le délai approprié pour enquêter et prendre des mesures variera lui aussi ; il est donc impossible de prescrire un délai fixe permettant de qualifier une mesure de « rapide ». Les bureaux d'enregistrement doivent donc faire preuve d'une vigilance de tous les instants quant aux allégations de noms parrainés utilisés à des fins d'Utilisation malveillante du DNS. Cette vigilance doit être proportionnelle aux dommages potentiels que l'Utilisation malveillante du DNS cause aux victimes.

Par conséquent, en réponse à une demande du Service de conformité contractuelle de l'ICANN, les bureaux d'enregistrement seront tenus d'expliquer comment les mesures ont été prises rapidement au vu des circonstances spécifiques. Le Service de conformité contractuelle de l'ICANN examinera ensuite l'explication et les circonstances du cas afin de déterminer, au cas par cas, si les mesures ont été raisonnablement rapides. Les délais des exemples fournis dans le présent Avis ne correspondent pas à des exigences contractuelles mais sont purement illustratifs. Si un bureau d'enregistrement prend davantage de temps pour enquêter et prendre des mesures

dans un cas similaire aux exemples, il ne s'agira pas forcément d'un cas de non-conformité. À l'inverse, d'autres circonstances peuvent imposer au bureau d'enregistrement d'agir plus rapidement, notamment dans les cas où l'Utilisation malveillante du DNS peut potentiellement causer

[6] De plus amples informations sur les dommages collatéraux et les considérations liées à la proportionnalité lorsque l'on agit au niveau du DNS sont disponibles dans la publication du Réseau politique Internet et juridiction intitulé « Boîte à outils pour l'adoption de mesures d'atténuation de l'utilisation malveillante au niveau du DNS ».

des dommages imminents aux utilisateurs finaux. Un bureau d'enregistrement est tenu d'enquêter et de prendre des mesures dès que possible après avoir tenté de manière raisonnable de confirmer un cas d'Utilisation malveillante du DNS.

Synthèse – Exemples de conformité de bureaux d'enregistrement
Les exemples ci-dessous illustrent les mesures d'atténuation raisonnables et rapides prises afin de mettre un terme à l'utilisation du Nom enregistré à des fins d'Utilisation malveillante du DNS (Scénario 1) et d'interrompre l'Utilisation malveillante du DNS en lien avec le Nom enregistré (Scénario 2). Ces scénarios contiennent des circonstances factuelles spécifiques. Selon les circonstances, des bureaux d'enregistrement individuels peuvent prendre différentes mesures et dans différents délais afin de mettre un terme à, ou d'interrompre, des cas individuels d'Utilisation malveillante du DNS. Dans tous les cas, les bureaux d'enregistrement doivent être en mesure de prouver que l'approche adoptée est conforme aux exigences applicables de l'Article 3.18 du RAA.

Scénario 1 : Un bureau d'enregistrement reçoit un signalement complet et concret de cas d'utilisation malveillante affirmant qu'un Nom enregistré parrainé par le bureau d'enregistrement est utilisé à des fins d'hameçonnage. Le signalement comprend des preuves qu'une URL contenant le Nom enregistré parrainé par le bureau d'enregistrement est envoyée via e-mail ou SMS, l'auteur du message se présentant comme une grande banque demandant aux destinataires de débloquer leurs comptes. Le bureau d'enregistrement lance une enquête en tenant compte de l'ensemble des informations pertinentes incluses dans le signalement. L'enquête menée par le bureau d'enregistrement révèle que le Nom enregistré ne dispose pas de site web accessible au public et affiche uniquement une URL directe avec ce qui ressemble à un écran de connexion d'une grande banque. C'est cette même URL qui est envoyée via e-mail ou SMS. Aussi, selon le bureau d'enregistrement, il s'agit d'un nouveau client et le Nom enregistré a été enregistré cinq jours auparavant.

Mesures d'atténuation adéquates : Le bureau d'enregistrement arrive logiquement à la conclusion que le Nom enregistré est utilisé à des fins d'Utilisation malveillante du DNS et met un terme à l'Utilisation malveillante du DNS en procédant à la suspension du Nom enregistré, en lui appliquant le statut de protocole d'avitaillement extensible (EPP) clientHold[7]. L'enquête est menée et la mesure d'atténuation est prise dans un délai de deux jours ouvrables à compter de la réception du signalement du cas d'utilisation malveillante. Le bureau d'enregistrement peut également décider d'appliquer un verrouillage du transfert au Nom enregistré afin d'empêcher le titulaire de nom de domaine de tenter de contourner la mesure d'atténuation et de réutiliser le nom de domaine à des fins d'Utilisation malveillante du DNS, à condition que le bureau d'enregistrement respecte les exigences applicables prévues dans la Politique de transfert de l'ICANN.

Scénario 2 : Un bureau d’enregistrement reçoit un signalement complet et concret de cas d’utilisation malveillante affirmant qu’un Nom enregistré parrainé par le bureau d’enregistrement, autobrand.tld, est utilisé à des fins d’hameçonnage. Le signalement comprend des preuves de l’utilisation d’une URL spécifique à des fins d’hameçonnage. Le bureau d’enregistrement mène une enquête en tenant compte de toutes les informations pertinentes incluses dans le signalement ainsi que des informations facilement et raisonnablement accessibles au bureau d’enregistrement.

[7] Cliquez ici pour en savoir plus, via l’ICANN, sur les statuts EPP.

L’enquête menée confirme que l’URL indiquée dans le signalement est utilisée à des fins d’hameçonnage. L’enquête révèle également que l’URL appartient à un sous-domaine (city.autobrand.tld) et semble être utilisée par un franchisé. Le bureau d’enregistrement reconnaît que le Nom enregistré autobrand.tld a été enregistré trois ans auparavant et dispose d’un solide ensemble de contenus pour une franchise de concessionnaire automobile. Le bureau d’enregistrement est en mesure de confirmer que le Nom enregistré est utilisé pour des e-mails d’entreprise d’Autobrand et des sous-domaines pour plusieurs franchisés.

Mesures d’atténuation adéquates : Le bureau d’enregistrement arrive logiquement à la conclusion que le Nom enregistré est utilisé à des fins d’Utilisation malveillante du DNS mais qu’il s’agit probablement du fruit d’un domaine compromis et que le titulaire de nom de domaine n’utilise pas sciemment le Nom enregistré à des fins d’Utilisation malveillante du DNS. Le bureau d’enregistrement évalue les potentiels dommages collatéraux que pourrait causer la suspension du nom de domaine et arrive logiquement à la conclusion qu’une telle mesure d’atténuation n’est, en l’état actuel des choses, pas appropriée. Le bureau d’enregistrement décide alors d’interrompre l’Utilisation malveillante du DNS et demande à Autobrand, le titulaire de nom de domaine d’autobrand.tld, de supprimer le contenu d’hameçonnage dans un délai spécifique déterminé, dans la mesure du raisonnable, par le bureau d’enregistrement. L’enquête est menée et la mesure d’atténuation est prise dans un délai de trois jours ouvrables à compter de la réception du signalement du cas d’utilisation malveillante.

Exigences relatives à la tenue et la fourniture à l’ICANN de registres

Les exigences relatives à la consignation et la fourniture de registres portant sur la réception de signalements de cas d’utilisation malveillante et les réponses apportées, précédemment décrites à l'Article 3.18.3 du RAA, figurent désormais à l’Article 3.18.4 du RAA ; ces exigences demeurent inchangées. Ces exigences s’appliquent également aux réponses apportées aux signalements de cas d’Utilisation malveillante du DNS en vertu de l'Article 3.18.2.

Obligations de l'opérateur de registre

Article 4 de la Spécification 6 du RA

L’Article 4 de la Spécification 6 du RA impose la publication et la fourniture à l’ICANN des coordonnées des personnes chargées du traitement des questions liées à des activités malveillantes dans le domaine de premier niveau (TLD). Il prévoit également des exigences relatives à la suppression des enregistrements orphelins de type glue lorsque de tels enregistrements ont fait l'objet d'une utilisation malveillante. Les exigences de cette Spécification ont été amendées tel que suit :

Exigences relatives à la publication et au maintien à jour des contacts pour le signalement de cas d'utilisation malveillante (Article 4.1 de la Spécification 6 du RA de base)

Où signaler un cas d'utilisation malveillante
Afin de faciliter le signalement d'une partie affirmant que le TLD a fait l'objet d'une activité malveillante, y compris une Utilisation malveillante du DNS, l'opérateur de registre doit publier une adresse e-mail ou un formulaire web, une adresse postale et un contact primaire chargé du traitement des signalements.

Une page d'accueil d'un opérateur de registre qui affiche clairement un lien vers une page « Signalement de cas d'utilisation malveillante » ou « Nous contacter » (qui indique clairement la personne à contacter pour le signalement de cas d'utilisation malveillante) permettant de procéder facilement à des signalements sera jugée conforme.

Confirmation du reçu d'un signalement de cas d'utilisation malveillante
Une fois le signalement reçu, l'opérateur de registre doit fournir à l'auteur du signalement la confirmation que son signalement a bien été reçu. Cette confirmation peut être envoyée à l'auteur du signalement ou affichée sur l'écran après avoir procédé au signalement auprès de l'opérateur de registre. Elle doit contenir suffisamment d'informations pour permettre à l'auteur du signalement de prouver qu'il a procédé au signalement d'un cas d'utilisation malveillante. La confirmation doit au moins identifier l'opérateur de registre, le ou les Noms enregistrés signalés ainsi que la date du signalement.

Exigences relatives à l'adoption de mesures d'atténuation suite à la réception de signalements concrets de cas d'Utilisation malveillante du DNS (Article 4.2 de la Spécification 6 du RA de base)

L'Article 4.2 de la Spécification 6, tel que modifié par les Amendements relatifs à l'Utilisation malveillante du DNS, est désormais le suivant :

> *Lorsqu'un Opérateur de registre détermine raisonnablement, sur la base de preuves concrètes, qu'un nom de domaine enregistré dans le TLD est utilisé à des fins d'Utilisation malveillante du DNS, l'Opérateur de registre doit prendre dans de brefs délais la ou les mesures d'atténuation adéquates nécessaires afin d'aider à mettre un terme à, ou à interrompre, l'utilisation du nom de domaine à des fins d'Utilisation malveillante du DNS. Cette ou ces mesures doivent comprendre au minimum : (i) le renvoi des domaines utilisés à des fins*

d'Utilisation malveillante du DNS, accompagnés des preuves pertinentes, au bureau d'enregistrement parrain ; ou (ii) l'adoption de mesures directes par l'Opérateur de registre lorsque ce dernier l'estime nécessaire. La ou les mesures prises peuvent varier en fonction des circonstances de chaque cas ; il convient de tenir compte de la gravité des dommages causés par l'Utilisation malveillante du DNS et des éventuels dommages collatéraux associés.

Preuves concrètes

Les preuves doivent être *concrètes*. Cela signifie que les informations auxquelles l'opérateur de registre peut facilement accéder doivent être suffisantes pour permettre à l'opérateur de registre de pouvoir déterminer, dans la mesure du raisonnable, si le Nom enregistré est utilisé ou non sous une ou plusieurs des formes d'Utilisation malveillante du DNS. Les opérateurs de registre peuvent obtenir des preuves concrètes en passant en revue les informations auxquelles ils peuvent accéder dans la mesure du raisonnable et en toute indépendance, conjointement à un signalement de cas d'utilisation malveillante ou dans le cadre de leurs propres initiatives en vertu de la Spécification 11(3)(b) du Contrat de registre en procédant à une analyse technique visant à identifier les domaines utilisés à des fins d'Utilisation malveillante du DNS. Les preuves concrètes peuvent également être présentées à l'opérateur de registre via une partie externe telle qu'un organisme chargé de l'application de la loi, des sources fiables ou reconnues de l'opérateur de registre, ou toute autre partie ou source. Les auteurs de signalements de cas d'utilisation malveillante sont encouragés à fournir autant d'informations que possible afin d'aider à s'assurer que l'opérateur de registre dispose de suffisamment d'informations pour mener une enquête sur la potentielle Utilisation malveillante du DNS. Dans un souci de clarté, un signalement jugé incomplet par l'opérateur de registre peut être considéré comme concret si l'opérateur de registre a accès à suffisamment d'informations afin de mener raisonnablement une enquête visant à déterminer si le Nom enregistré signalé est utilisé à des fins d'Utilisation malveillante du DNS.

Après la fourniture de preuves concrètes, des mesures doivent être rapidement prises

Après avoir reçu des preuves concrètes, l'opérateur de registre doit, dans de brefs délais, prendre une ou des mesures d'atténuation adéquates raisonnablement nécessaires afin d'aider à mettre un terme à, ou à interrompre, l'utilisation du nom de domaine à des fins d'Utilisation malveillante du DNS. Afin de déterminer les mesures d'atténuation adéquates, l'opérateur de registre examinera les circonstances spécifiques du cas, et pourra notamment évaluer la portée des dommages causés par l'Utilisation malveillante du DNS et le nombre de victimes au regard des éventuels dommages collatéraux associés. Dans le cas de domaines compromis tel que décrit ci-dessus pour les bureaux d'enregistrement, les dommages collatéraux revêtent la même importance pour les registres.

L'opérateur de registre déterminera également si lui, le bureau d'enregistrement parrain et/ou une autre partie sont les parties les plus à même d'examiner les éléments en présence et de prendre des mesures d'atténuation adéquates et proportionnelles. Par exemple, pour un Nom enregistré unique utilisé à des fins d'Utilisation malveillante du DNS, le bureau d'enregistrement peut être le mieux placé pour examiner le cas d'Utilisation malveillante du DNS et y remédier avec son client. De même, en cas de

systèmes compromis, le Titulaire de nom enregistré ou le fournisseur de solutions d’hébergement qui maintient l’accès administratif aux systèmes affectés peut être mieux placé pour régler les problèmes, et l’opérateur de registre doit dans un premier temps faire part au bureau d’enregistrement de ces problèmes, dans la mesure où la suspension du domaine via l’application du statut clientHold ou serverHold peut causer des dommages collatéraux sur des contenus bénins ou légitimes. D’un autre côté, l’opérateur de registre peut être le mieux placé pour répondre à des menaces à grande échelle qui touchent de nombreux Titulaires de noms enregistrés ou bureaux d’enregistrement, telles que des algorithmes de génération de domaine utilisés afin de propager des réseaux zombie.

Les mesures d'atténuation prises dans de brefs délais doivent être raisonnablement nécessaires afin d'obtenir l'un des résultats suivants : *aider à mettre un terme à ou à interrompre* l'utilisation du Nom enregistré à des fins d'Utilisation malveillante du DNS. L'opérateur de registre doit au minimum :

1) *Signaler* le ou les Noms enregistrés et *fournir* les preuves requises au(x) Bureau(x) d'enregistrement parrain(s) ; ou
2) *Prendre des mesures directes* à l'égard du ou des Noms enregistrés lorsque l'opérateur de registre juge de telles mesures directes adéquates.

Qu'est-ce qu'une mesure rapide ?

Tel qu'indiqué pour les bureaux d'enregistrement, la mesure adéquate devant être prise afin d'atténuer ou d'interrompre un cas d'Utilisation malveillante du DNS variera en fonction des circonstances spécifiques.

De ce fait, le délai approprié pour enquêter et prendre des mesures adéquates variera lui aussi ; il est donc impossible de prescrire un délai fixe permettant de qualifier une mesure de « rapide ». Les opérateurs de registre doivent donc faire preuve d'une vigilance de tous les instants quant aux allégations de noms parrainés utilisés à des fins d'Utilisation malveillante du DNS. Cette vigilance doit être proportionnelle aux dommages potentiels que l'Utilisation malveillante du DNS cause aux victimes.

Par conséquent, en réponse à une demande du Service de conformité contractuelle de l'ICANN, les opérateurs de registre seront tenus d'expliquer comment les mesures ont été prises rapidement au vu des circonstances spécifiques. Le Service de conformité contractuelle de l'ICANN examinera ensuite l'explication et les circonstances du cas afin de déterminer, au cas par cas, si les mesures ont été rapides. Les délais des exemples fournis dans le présent Avis ne correspondent pas à des exigences contractuelles mais sont purement illustratifs. Si un opérateur de registre prend davantage de temps dans un cas spécifique, il ne s'agira pas forcément d'un cas de non-conformité. À l'inverse, d'autres circonstances peuvent imposer à l'opérateur de registre d'agir plus rapidement, notamment dans les cas de menaces à grande échelle qui pourraient causer des dommages imminents à un grand nombre d'utilisateurs finaux. Un opérateur de registre est tenu d'enquêter et de prendre des mesures dès que possible après avoir tenté de manière raisonnable de confirmer un cas d'Utilisation malveillante du DNS.

Les exemples ci-dessous illustrent des mesures d'atténuation raisonnables et rapides prises afin d'aider à mettre un terme à l'utilisation du Nom enregistré à des fins d'Utilisation malveillante du DNS (Scénario 2) et d'aider à interrompre l'Utilisation malveillante du DNS en lien avec le Nom enregistré (Scénarios 1 et 3). Ces scénarios contiennent des circonstances factuelles spécifiques. Selon les circonstances, des opérateurs de registre individuels peuvent prendre différentes mesures et dans différents délais afin d'aider à mettre un terme à, ou à interrompre, des cas individuels

d’Utilisation malveillante du DNS. Dans tous les cas, les opérateurs de registre doivent être en mesure de prouver que l’approche adoptée est conforme aux exigences applicables de l'Article 4.2 de la Spécification 6 du RA.

Article 3(b) de la Spécification 11 du RA

Cet Article a été modifié afin de remplacer le terme de « menaces à la sécurité » par celui d'« Utilisation malveillante du DNS », tel que défini dans les amendements de l'Article 4 de la Spécification 6.

Synthèse – Exemples de conformité d'opérateurs de registre

Scénario 1 : Un opérateur de registre a reçu une notification d'une banque mutualiste (par exemple, Credit Union) via son formulaire web de signalement de cas d'utilisation malveillante indiquant qu'une entité avait enregistré le domaine <loginexamplecreditunion[.]TLD> six jours auparavant et la banque mutualiste affirme que le domaine est impliqué dans une opération d'hameçonnage. La banque mutualiste fournit une capture d'écran montrant une page web sur le domaine rassemblant des identifiants de connexion.

Mesures d'atténuation adéquates : Conformément à son processus interne, le signalement est traité et examiné par l'opérateur de registre dans un délai de deux jours ouvrables. À l'issue de l'enquête, l'opérateur de registre a raisonnablement déterminé que le Nom enregistré était utilisé à des fins d'Utilisation malveillante du DNS. Par conséquent, l'opérateur de registre interrompt le cas d'Utilisation malveillante du DNS, en informe le bureau d'enregistrement parrain et lui fournit toutes les informations pertinentes. L'opérateur de registre transmet au bureau d'enregistrement une demande assorti d'un délai afin qu'il mène une enquête et prenne les mesures d'atténuation raisonnablement nécessaires afin de mettre un terme à, ou d'interrompre, l'Utilisation malveillante du DNS. Dans le délai indiqué, l'opérateur de registre est en mesure de confirmer que le bureau d'enregistrement a suspendu le Nom enregistré via l'application du statut EPP clientHold.

Scénario 2 : Un opérateur de registre est contacté par un organisme chargé de l'application de la loi qui lui fournit des preuves indiquant qu'une série de domaines sont, ou seront, impliqués dans un algorithme de génération de domaine associé à un réseau zombie. Le réseau zombie utilise des Noms enregistrés existants, mais principalement des domaines qui n'ont pas encore été enregistrés.

Mesures d'atténuation adéquates : Dans les six heures suivant la conclusion de son enquête et la confirmation raisonnable de l'Utilisation malveillante du DNS, l'opérateur de registre aide à mettre un terme à l'Utilisation malveillante du DNS en prenant des mesures déterminées par l'organisme chargé de l'application de la loi ou convenues avec ce dernier. Dans ce cas, l'opérateur de registre a accepté que, pour les Noms enregistrés concernés, le registre délègue à différents serveurs de noms (par exemple, rediriger les serveurs de noms ou le gouffre) à la demande de l'organisme chargé de l'application de la loi. L'opérateur de registre crée aussi directement les domaines qui

n'avaient pas déjà été précédemment créés et qui sont associés au réseau zombie sur demande de l'organisme chargé de l'application de la loi. Il convient de noter que la création de domaines par l'opérateur de registre nécessite normalement une autorisation via le Processus de dérogation pour incident de sécurité (SRW) de l'ICANN[8]. L'opérateur de registre formulera également, en temps opportun, une demande d'obtention d'une dérogation contractuelle. Toutefois, il doit être précisé qu'une demande de SRW peut également être

[8] Des informations sur le Processus de dérogation pour incident de sécurité sont disponibles sur cette page.

formulée dès que raisonnablement possible après coup, et l'organisation ICANN peut répondre, le cas échéant, par une dérogation rétroactive, de sorte à ne pas retarder le soutien apportée à l'opération menée par l'organisme chargé de l'application de la loi[9].

Scénario 3 : Dans le cadre de son analyse technique visant à détecter un cas d'Utilisation malveillante du DNS en vertu de la Spécification 11(3)(b), un opérateur de registre découvre qu'une sous-page d'un domaine est utilisée à des fins de diffusion d'un logiciel malveillant alors que le reste du site sur le domaine semble constituer du contenu légitime ou bénin. Le nom de domaine est enregistré depuis trois ans.

Mesures d'atténuation adéquates : Trois heures après avoir déterminé que le Nom enregistré est utilisé à des fins d'Utilisation malveillante du DNS et est compromis, l'opérateur de registre aide à interrompre le cas d'Utilisation malveillante du DNS, en informe le bureau d'enregistrement parrain, lui fournit toutes les informations pertinentes, et lui transmet une demande assortie d'un délai afin qu'il prenne une mesure et qu'il en rende compte. Le bureau d'enregistrement en informe alors directement le titulaire de nom de domaine, qui règle le problème en mettant à jour son système de gestion de contenu de façon à supprimer le logiciel malveillant.

Enquêtes de l'organisation ICANN eu égard au respect du nouvel Article 3.18.2 du RAA et de l'article 4.2 de la Spécification 6 du RA

Qu'est-ce qui constituerait une réponse complète, bien documenté et conforme ?
Le Service de conformité contractuelle de l'ICANN fera respecter les exigences expliquées dans le présent Avis via le traitement de plaintes externes, un suivi proactif et des activités d'audit. Lorsque le Service de conformité contractuelle de l'ICANN reçoit une plainte, il examine toutes les preuves présentées par l'auteur du signalement ainsi que toutes les informations pertinentes disponibles afin de déterminer si un cas de conformité doit être ouvert avec le bureau d'enregistrement ou l'opérateur de registre concerné. En l'absence de preuves suffisantes venant appuyer une plainte pour Utilisation malveillante du DNS, le Service de conformité contractuelle de l'ICANN qualifiera le cas d'invalide et le clôturera. Entre autres, cet examen tâchera d'évaluer si les informations facilement accessibles au bureau d'enregistrement parrain directement ou via un revendeur, ou à l'opérateur de registre, selon le cas, sont suffisantes afin de déterminer, dans la mesure du raisonnable, que le Nom enregistré est utilisé sous une ou plusieurs des formes d'Utilisation malveillante du DNS. L'examen déterminera également s'il existe d'autres informations

[9] Pour en savoir plus sur la façon dont les registres peuvent collaborer avec les organismes chargés de l'application de la loi et l’ICANN afin de régler la question des algorithmes de génération de domaine, veuillez consulter le document intitulé « Cadre pour les algorithmes de génération de domaine associés aux logiciels malveillants et aux réseaux zombie », publié par le Groupe de travail sur la sécurité publique du Comité consultatif gouvernemental et le Groupe des représentants des opérateurs de registre gTLD.

fournies par la partie auteure du signalement en réponse aux demandes d’informations ou de preuves complémentaires du bureau d’enregistrement ou de l’opérateur de registre.

En outre, le cas échéant et si nécessaire dans un cas spécifique, le Service de conformité contractuelle de l'ICANN : (1) examinera les données pertinentes accessibles au public affichées via le Service d'annuaire de données d'enregistrement, telles que la date de création, le ou les statuts EPP ou les informations sur les serveurs de noms, et (2) effectuera des recherches sur le DNS afin de déterminer si les Noms enregistrés signalés sont résolus dans le DNS. Le Service de conformité contractuelle de l'ICANN peut également mener ses propres recherches et examiner d’autres informations pertinentes sur un Nom enregistré spécifique prétendument impliqué dans un cas d’Utilisation malveillante du DNS.

Lors de l’ouverture d’un cas de conformité avec un bureau d’enregistrement ou un opérateur de registre en vertu de l’Article
3.18.2 du RAA ou de l’Article 4.2 de la Spécification 6 du RA, respectivement, le Service de conformité contractuelle de l'ICANN fournira une liste détaillée de l’ensemble des informations et registres nécessaires afin d’évaluer la conformité en ce qui concerne le ou les Noms enregistrés signalés et les formes de la prétendue Utilisation malveillante du DNS. En réponse à un cas de conformité, le bureau d’enregistrement et l’opérateur de registre devront au minimum :

- Expliquer comment et pourquoi le bureau d’enregistrement ou l’opérateur de registre sont parvenus à la conclusion que les preuves obtenues n’étaient pas concrètes, le cas échéant. Par exemple, un bureau d’enregistrement peut expliquer que, après examen des informations et registres soumis par la partie auteure du signalement, et suite à son enquête, le bureau d’enregistrement n’a pas été en mesure de confirmer le cas d’Utilisation malveillante du DNS en lien avec le ou les Noms enregistrés signalés. Le Service de conformité contractuelle de l'ICANN peut demander au bureau d’enregistrement ou à l’opérateur de registre de clarifier certaines incohérences clairement identifiées entre l’explication fournie et les informations et données collectées par le Service de conformité contractuelle de l'ICANN lors du processus de validation des plaintes.
- Fournir une explication détaillée, étayée par des registres correspondants, des mesures d’atténuation spécifiques prises, du moment où les mesures ont été prises, et de la raison pour laquelle les mesures prises ont été jugées rapides et raisonnablement nécessaires afin de mettre un terme à ou d’interrompre ou d’aider à mettre un terme à ou à interrompre l’Utilisation malveillante du DNS, en ce qui concerne les circonstances spécifiques du cas d’espèce (notamment tout explication applicable relative au caractère disproportionné des mesures au niveau du DNS et aux dommages collatéraux). Les exigences imposant au bureau d’enregistrement de fournir ces informations continueront de s’appliquer

dans les cas dans lesquels le bureau d'enregistrement choisit de déléguer l'enquête sur le signalement d'un cas d'Utilisation malveillante du DNS à un revendeur. Dans de tels cas, le bureau d'enregistrement conserve l'obligation de prouver sa conformité à l'Article 3.18 du RAA[10] en expliquant les mesures qu'il a prises ainsi que les mesures prises par d'autres parties déléguées telles que des revendeurs et en fournissant les registres correspondants.

[10] Voir l'Article 3.12 du RAA.

Les politiques et exigences contractuelles de l’ICANN s’appliquent dans les limites des lois et réglementations applicables à chaque bureau d’enregistrement et opérateur de registre. Dans un souci de clarté, ni les bureaux d’enregistrement ni les opérateurs de registre ne seront tenus de prendre des mesures contraires aux lois et réglementions applicables.

Les informations répondant aux questions de savoir quand, comment et où déposer une plainte auprès du Service de conformité contractuelle de l'ICANN sont disponibles ici.