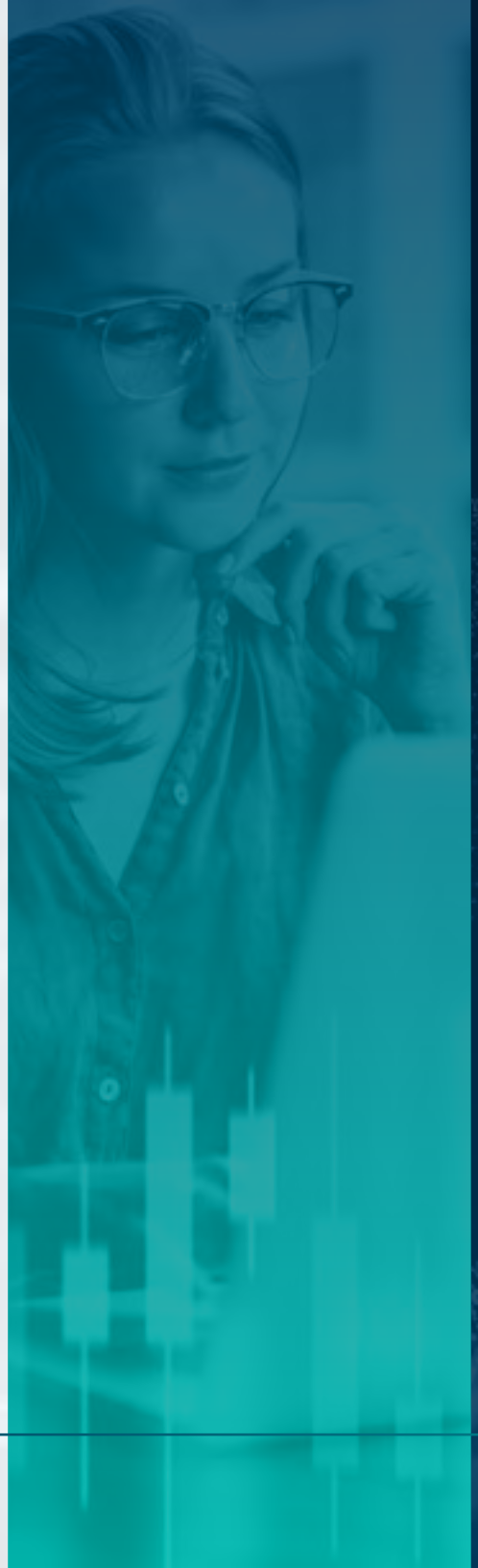


2023

RAPPORT SUR LA SÉCURITÉ DES NOMS DE DOMAINE

Au cours des quatre dernières années, CSC a renforcé son positionnement cyber avec notamment ses rapports sur la stratégie de sécurité des noms de domaine des entreprises du classement Forbes Global 2000. Cette année, nous avons constaté que bien que certaines entreprises ont mis fortement l'accent sur la sécurité, une grande partie d'entre elles présentent encore des risques élevés en matière de sécurité des noms de domaine. Nous souhaitons sensibiliser les entreprises à ces menaces et partager les bonnes pratiques de sécurité en matière de nom de domaine.

Pour cela, nous avons analysé l'adoption des mesures de sécurité des noms de domaine mises en place pour atténuer les cyberrisques présents dans l'écosystème des noms de domaines appartenant aux entreprises du Global 2000 qui échappent à la vigilance du pare-feu de l'entreprise, ainsi que les cas d'abus et de potentielles violations de marques en ligne par des tiers.

RÉSUMÉ DES PRINCIPALES CONCLUSIONS

43 % DES NOMS DE DOMAINES .AI SONT ENREGISTRÉS PAR DES TIERS

Certaines entreprises ont négligé l'achat de leurs noms de domaine .AI, ou découvrent aujourd'hui que de nombreux fraudeurs ont acheté ces domaines à leur place, comme en témoigne l'augmentation de 350 % en une année, des litiges relatifs à un nom de domaine impliquant l'extension .AI en 2023.

21 % DES ENREGISTREMENTS DNS DE SOUS-DOMAINES POINTENT VERS UN CONTENU QUI NE RÉSOUT PAS, CE QUI REND LES ENTREPRISES VULNÉRABLES AU DÉTOURNEMENT DE SOUS-DOMAINE

CSC a analysé plus de 6 millions d'enregistrements système de noms de domaine (Domain Name System, DNS) issus de notre base de données, puis a filtré cet ensemble de manière à obtenir environ 440 000 enregistrements DNS correspondant à des enregistrements d'alias et CNAME qui pointent vers une infrastructure cloud, où il existe un risque de détournement de sous-domaine.

79 % DES NOMS DE DOMAINE ENREGISTRÉS SIMILAIRES AUX MARQUES DU GLOBAL 2000 (HOMOGLYPHES) ÉTAIENT DÉTENUS PAR DES TIERS

Parmi les 79 % de (faux) noms de domaine homoglyphes détenus par des tiers autres que les propriétaires de marques du Global 2000, 40 % disposent d'enregistrements MX qui pourraient être utilisés dans le cadre d'une attaque de phishing.

46 % DES ENTREPRISES QUI FONT APPEL À DES REGISTRARS CORPORATE UTILISENT AUSSI LE VERROU DE REGISTRE

Le verrou de registre permet de sécuriser de bout en bout les transactions associées au nom de domaine afin de limiter les erreurs humaines et les risques externes. C'est un moyen très économique de protéger les noms de domaine contre les modifications ou les suppressions accidentelles ou non autorisées. Seuls 7 % des entreprises qui recourent à des registrars grand public ont déployé le verrou de registre. (Voir la section registrars corporates vs registrars grand public.)

112 ENTREPRISES AFFICHENT UNE NOTE DE SÉCURITÉ DES NOMS DE DOMAINE DE **0 %**

6 % des entreprises du Global 2000 n'appliquent aucune des mesures de sécurité des noms de domaine recommandées et s'exposent à des risques plus élevés. D'après notre analyse de l'adoption des principales mesures de sécurité des noms de domaine, un score de 0 % indique qu'aucune mesure n'a été adoptée, ce qui expose l'entreprise à un niveau de risque maximal vis-à-vis des menaces pour la sécurité des noms de domaine.

6 % DE CROISSANCE DU PROTOCOLE DMARC SOIT LE TAUX LE PLUS ÉLEVÉ DEPUIS CES QUATRE DERNIÈRES ANNÉES

Lors de ces quatre dernières années, nous avons pu constater une croissance cumulée de 28 % concernant la mise en place du DMARC (Domain-based Message Authentication Reporting and Conformance), un système de validation des e-mails conçu pour protéger le domaine de messagerie d'une entreprise contre le spoofing et le phishing.

2023 : UNE ÉTUDE DE CAS CONVAINCANTE EN FAVEUR DE LA SÉCURITÉ DES NOMS DE DOMAINE

Alors que la cybersécurité s'appuie de plus en plus sur l'intelligence artificielle (IA, ou AI en anglais), les attaques n'ont toujours de cesse de se multiplier, faisant de la sécurité des noms de domaine un critère majeur de l'évaluation des cyberrisques au plus haut niveau d'une entreprise. Les trois menaces suivantes sur la sécurité des noms de domaine servent à faciliter les attaques présentées ci-dessous.

NOMS DE DOMAINE COMPROMIS OU DÉTOURNÉS

ENREGISTREMENT DE NOMS DE DOMAINE MALVEILLANTS (P. EX. : HOMOGLYPHE)

SOUS-DOMAINE DÉTOURNÉS

Détournement de nom de domaine/système de noms de domaine (DNS)

Attaques par rançongiciel

Domain-shadowing

Attaques de phishing

Attaques par usurpation d'identité

Attaques DDoS

Détournement de marque et de propriétés intellectuelles en ligne

Contrefaçon d'articles de marque

Empoisonnement du cache

Violations du réseau et des données

Business Email Compromise

DÉFINITION DE LA SÉCURITÉ DES NOMS DE DOMAINE

Les entreprises du monde entier utilisent Internet pour l'ensemble de leurs opérations : sites web, e-mails, authentification, communications VoIP, et plus encore. Cela fait partie intégrante du périmètre d'attaque externe d'une entreprise. Il doit donc être surveillé en permanence pour lutter contre la cybercriminalité et la fraude.. Alors que les cyberrisques sont en augmentation constante, les organisations et les assureurs cyber ont de grandes difficultés à les quantifier et à gérer leur capacité de nuisance. Et de fait, chaque jour, nous découvrons de nouveaux développements concernant des attaques de la chaîne logistique, des rançongiciels et des attaques de phishing, ainsi que des niveaux de complexité supplémentaires qu'il est nécessaire d'adopter pour s'en protéger et les contrer.

Grâce à sa technologie propriétaire, CSC assure la sécurité des noms de domaine avec une approche à plusieurs niveaux. Tout d'abord, nous sécurisons la présence en ligne d'une marque en sécurisant son portefeuille de noms de domaine, qui peut contenir diverses marques obtenues via des acquisitions, et son empreinte DNS en ligne. Ensuite, nous surveillons, analysons et intervenons lorsque nous détectons des vecteurs de menace qui ciblent des marques en ligne.

QU'EST-CE QUE LE DÉTOURNEMENT DE SOUS-DOMAINE ?

Le détournement de sous-domaine est une attaque au cours de laquelle un cybercriminel prend le contrôle d'un sous-domaine légitime qui n'est plus utilisé, afin d'y charger du contenu malveillant visant à cibler les entreprises par des campagnes de phishing ou l'envoi de "malware". Pour ce faire, il exploite intelligemment les enregistrements DNS « oubliés » afin qu'ils renvoient vers son propre contenu.

MENACE ÉMERGENTE : DÉTOURNEMENT DE SOUS-DOMAINE

21 % des enregistrements DNS de sous-domaine actifs pointent vers un contenu qui ne résout pas, ce qui rend les entreprises vulnérables au détournement de sous-domaine.

CSC a analysé plus de 6 millions d'enregistrements DNS issus de notre base de données, en s'intéressant aux enregistrements d'alias et CNAME pointant vers une infrastructure cloud majeure, et a ainsi identifié plus de 440 000 enregistrements de sous-domaine. Or, cette situation soulève des risques de détournement de sous-domaine par des tiers malveillants. Cette recherche avait pour but de comprendre la gestion de sous-domaine actuelle dans une grande entreprise, ainsi que son impact sur la stratégie de sécurité globale.

COMMENT DÉTECTER UN DÉTOURNEMENT DE SOUS-DOMAINE DE MANIÈRE PROACTIVE ?

1. Procédez à un audit complet des fichiers de zone DNS existants et interrogez chaque enregistrement.
2. Identifiez les noms de domaine et les noms de sous-domaine correspondants qui doivent être actifs.
3. Maintenez une surveillance en continu grâce à des analyses périodiques des enregistrements DNS actifs, afin de repérer toute modification d'état et de générer des alertes immédiates à l'équipe SOC, 24 h/24, 7 j/7 et 365 jours par an.
4. Prenez des mesures d'intervention immédiates contre tout site lancé illégalement et utilisez une fonctionnalité de blocage sur Internet pour contrer le contenu en ligne nuisible.

COMMENT VOS SOUS-DOMAINES PEUVENT-ILS ÊTRE DÉTOURNÉS SANS POUR AUTANT ÊTRE PIRATÉS ?

Il n'est pas rare que les grandes entreprises avec des portefeuilles de marque variés et opérant à l'international n'aient pas conscience de l'ampleur de leur empreinte numérique mondiale. Au fil du temps, les enregistrements numériques s'accumulent, compliquant le maintien de bonnes habitudes en matière d'informatique. Si les entreprises ont fait appel à des fournisseurs de cloud pour accéder à de nouvelles technologies, cette multiplication toujours croissante des enregistrements DNS, associée à des environnements de plus en plus complexes, les expose à des risques accrus. Sans un suivi quotidien approprié des enregistrements numériques, les entreprises accumulent le « bruit » qui complique l'application d'un bonne hygiène cybernétique, ouvrant des failles faciles à exploiter pour les cybercriminels.

En effet, les cybercriminels scrutent les infrastructures, notamment le cloud et les services mis à la disposition du public. Ils recherchent en particulier les enregistrements de zone DNS qui renvoient vers des services Web qui ne sont plus utilisés par une marque. En hébergeant leur contenu chez des fournisseurs de service cloud qui n'exécutent pas de vérifications, les criminels peuvent récupérer une zone de destination précédemment utilisée. Ils peuvent ainsi rediriger les internautes vers des sous-domaines sur lesquels ils ont chargé leur propre contenu illégitime, sans avoir à infiltrer l'infrastructure d'une entreprise ou le compte d'un service tiers. Par exemple, ZDNet a rapporté que Microsoft® avait été victime d'un détournement mené par des tiers malveillants afin de présenter des jeux de casinos et de poker sur leurs sous-domaines.

Appelée « Dangling DNS », cette accumulation de zones inactives qui ne renvoient pas vers du contenu expose les entreprises au risque de détournement de sous-domaine.

Cela ouvre également une passerelle pour d'autres cyberattaques ciblant des marques, notamment le phishing et les programmes malveillants, ce qui peut entraîner des pertes de revenus, l'exfiltration de données, la perte de la confiance des consommateurs et une atteinte à la réputation d'une entreprise induite par des failles de sécurité. Une étude réalisée par la société viennoise de conseil en sécurité informatique Certitude Consulting et récemment publiée sur Security Week tire la sonnette d'alarme : des milliers d'entités sont vulnérables à ces attaques.

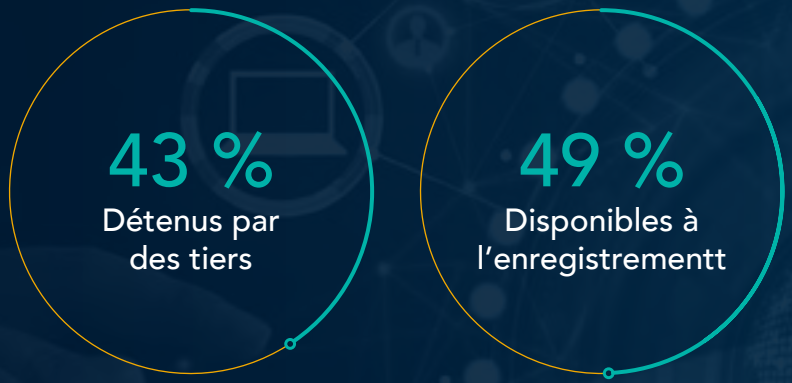
Parmi les bonnes habitudes informatiques, il est impératif d'intégrer la gestion des enregistrements DNS. Depuis plus de 20 ans, les entreprises s'exposent à un risque de mauvaise gestion en s'appuyant sur une multiplicité de propriétaires, de stratégies et de fournisseurs pour assurer la gestion DNS. Par surcroît, la tâche se complique encore en cas de fusions et acquisitions. D'autre part, les propriétaires en proie au doute ont profondément peur de supprimer des éléments.

Le détournement de sous-domaine fait partie des nombreuses menaces qui pèsent actuellement sur la sécurité des noms de domaine, comme le « DNS hijacking », le « domain-shadowing » ou encore le « cache poisoning ». Ces menaces servent souvent de levier pour lancer des attaques plus répandues par rançongiciel, par phishing, par compromission de la messagerie d'une entreprise ou par exfiltration de données.

Consultez notre rapport sur les vulnérabilités au détournement de sous-domaine ou contactez CSC pour en savoir plus !

43 % DES NOMS DE DOMAINES .AI SONT ENREGISTRÉS PAR DES TIERS

Certaines entreprises ont négligé l'achat de leurs noms de domaine .AI, ou découvrent aujourd'hui que de nombreux fraudeurs en ligne astucieux ont acheté ces domaines à leur place.



Avec le développement de l'intelligence artificielle (IA), l'environnement technologique a connu une évolution majeure. Cette évolution a d'ailleurs eu un impact considérable, notamment sur l'augmentation des enregistrements de noms de domaine .AI, témoignant ainsi d'une adoption massive et d'un enthousiasme à l'égard de l'IA. Suivant cette tendance, CSC a joué un rôle majeur, conseillant proactivement ses clients sur l'importance d'avoir une stratégie d'enregistrement et d'intervention pour les domaines .AI[1].

De plus, l'année 2023 a été marquée par une augmentation significative des litiges relatifs à des noms de domaine impliquant les extensions .AI. En effet, le mois de septembre 2023 a connu une augmentation importante par rapport aux années précédentes. Cette augmentation de 350 % en une année, associée au nombre total de cas qui a déjà dépassé le total combiné des quatre dernières années, souligne le besoin croissant de faire preuve de vigilance et d'appliquer une réglementation[2].

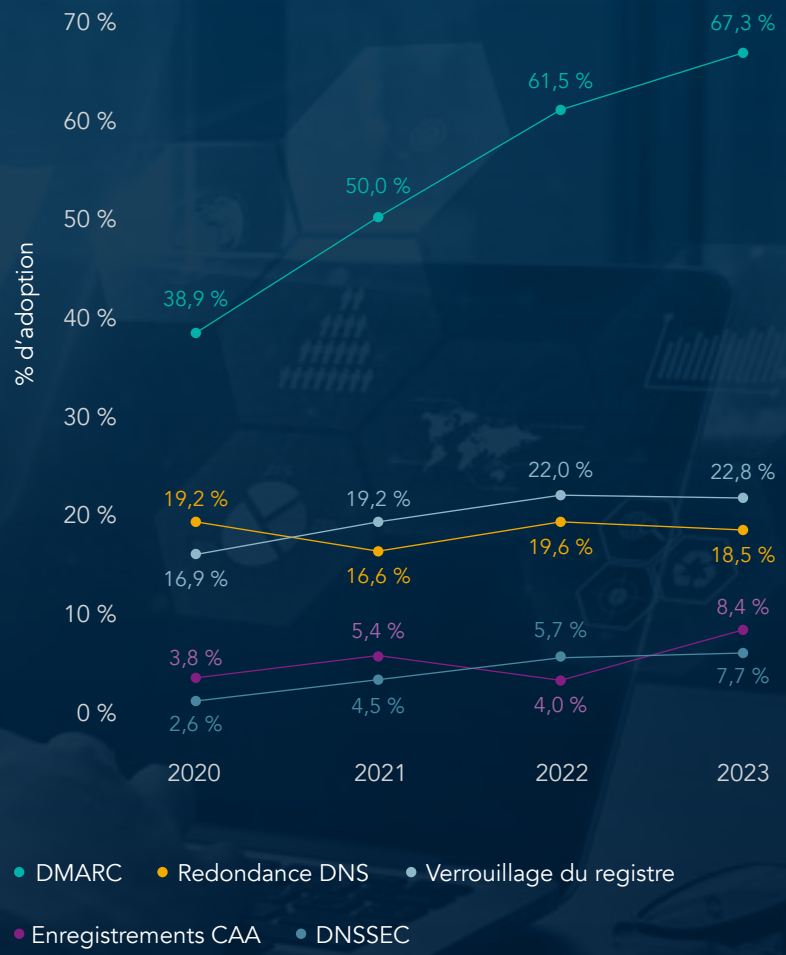
Le taux global d'enregistrements ou de violations par des tiers s'élève à 43 % au sein des entreprises du Global 2000. De fait, 84 % des noms de domaine .AI enregistrés sont détenus par des tiers. De plus, 49 % sont disponibles à l'enregistrement. Certains secteurs, tels que celui de la banque, des services financiers divers ainsi que des logiciels et des services informatiques, comptent le plus grand nombre de domaines .AI enregistrés.

Dans le même temps, les gouvernements renforcent la réglementation relative aux outils d'IA, tandis que les entreprises continuent de développer et d'appliquer des systèmes ainsi que des processus d'IA. Une tendance qui laisse présager une augmentation continue de la demande à l'égard des domaines .AI. À cela vient s'ajouter la récente décision de Google® de traiter les domaines .AI comme des noms de domaine génériques de premier niveau plutôt que comme un nom de domaine sous une extension pays, témoignant de la reconnaissance de l'importance de l'IA à l'échelle mondiale[3].

L'augmentation du nombre d'enregistrements de noms de domaine .AI est représentative du paysage technologique dans son ensemble. Alors que l'IA continue de se faire une place de plus en plus importante dans notre quotidien, les responsabilités et les défis qui en découlent doivent être relevés avec diligence et vigilance.

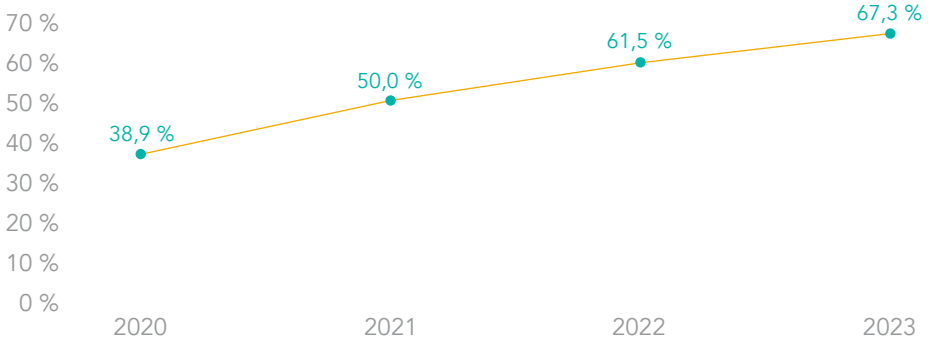
Cette année, les cas de litige concernant un nom de domaine impliquant des extensions .AI ont augmenté de 350 %.

TENDANCES D'ADOPTION DES MESURES DE SÉCURITÉ DU NOM DE DOMAINE (2020-2023)



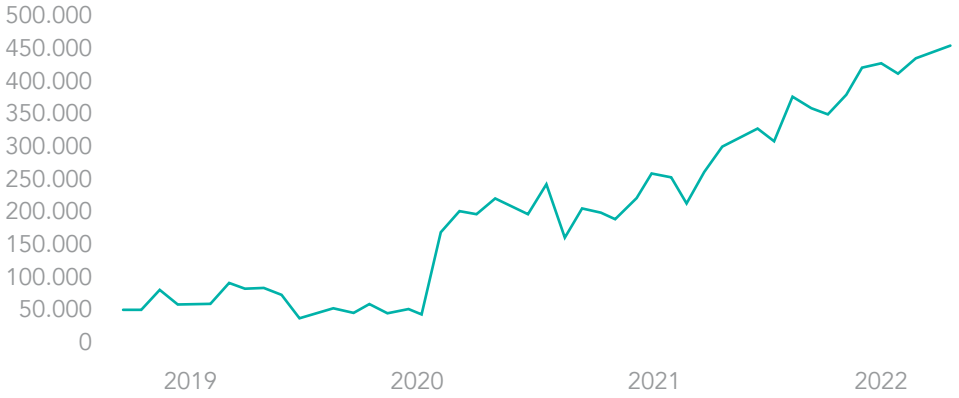
PROTOCOLE DMARC : UNE CROISSANCE MAJEURE

Au vu de l'actualité chargée concernant les attaques de phishing, y compris leur augmentation en termes de volume et de complexité, il n'est pas surprenant que l'utilisation du protocole DMARC ait connu une hausse rapide, passant de 39 % en 2020 à 67 % en 2023.



Les chiffres les plus récents de l'APWG montrent que 2022 a été une année record pour le phishing avec plus de 4,7 millions d'attaques enregistrées et une moyenne de 132 559 dollars pour les attaques de type BEC pendant le quatrième trimestre 2022. Depuis le début de 2019, le nombre d'attaques de phishing a augmenté de plus de 150 % par an, avec plus d'un million d'attaques de phishing par trimestre ces dernières années, ciblant environ 600 marques distinctes chaque mois.

TOTAL MENSUEL DES ATTAQUES DE PHISHING UNIQUES (APWG)



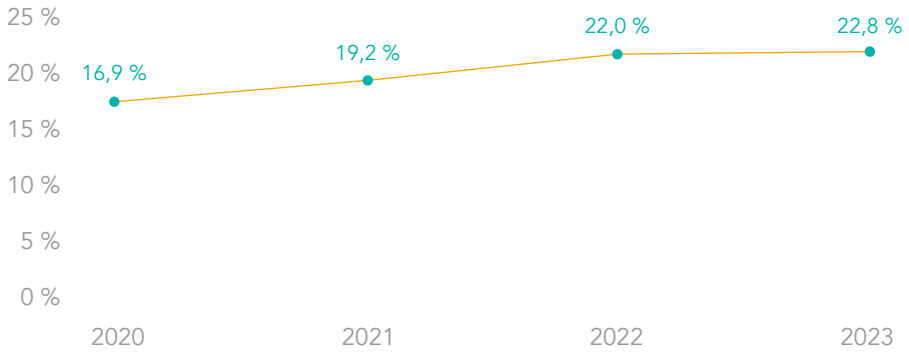
L'utilisation croissante d'indicateurs de marque pour l'identification des messages (BIMI) au sein d'un e-mail, qui permettent d'afficher les logos des marques sur les courriels authentifiés, est également un moyen efficace pour stimuler l'adoption du protocole DMARC. À noter toutefois : le protocole DMARC est une condition préalable à la mise en place de BIMI, et les deux fonctionnent en tandem pour vérifier l'authenticité de l'identité d'une entreprise sur un domaine de messagerie.

UN RISQUE ÉLEVÉ PERSISTANT POUR LES ENTREPRISES DU GLOBAL 2000 MALGRÉ UNE LÉGÈRE AUGMENTATION DU NOMBRE DE VERROUS DE REGISTRES

Le pourcentage d'entreprises ayant activé le verrou de registre est passé de 17 % en 2020, à 23 % en 2023. Dans le cadre de notre étude, nous avons également observé une évolution plus conséquente avec 46 % des entreprises qui utilisent des registrars corporates ayant également recours au verrou de registre. Les agences gouvernementales incitant toujours plus les entreprises à renforcer leur cybersécurité et à éliminer les risques d'abus de DNS, et pour répondre à la réglementation ainsi qu'à la pression du secteur, de plus en plus de registres proposent des options de verrouillages sur leurs extensions de domaine. Le verrou de registre permet de sécuriser de bout en bout les transactions associées au nom de domaine afin de limiter les erreurs humaines et les risques externes. C'est un moyen très économique de protéger les noms de domaine contre les modifications ou les suppressions accidentelles ou non autorisées. Il arrive toutefois que certains noms de domaine restent non verrouillés, certains registres ne proposant pas de services de verrouillage.

Le portefeuille de noms de domaine d'une entreprise évoluant constamment, CSC propose un algorithme de modélisation prédictive permettant d'évaluer plus de 20 attributs d'un nom de domaine afin d'identifier si ce dernier réalise une tâche essentielle pour les opérations de l'entreprise et la marque en ligne, et de recommander les domaines essentiels à verrouiller.

VERROUILLAGE DU REGISTRE

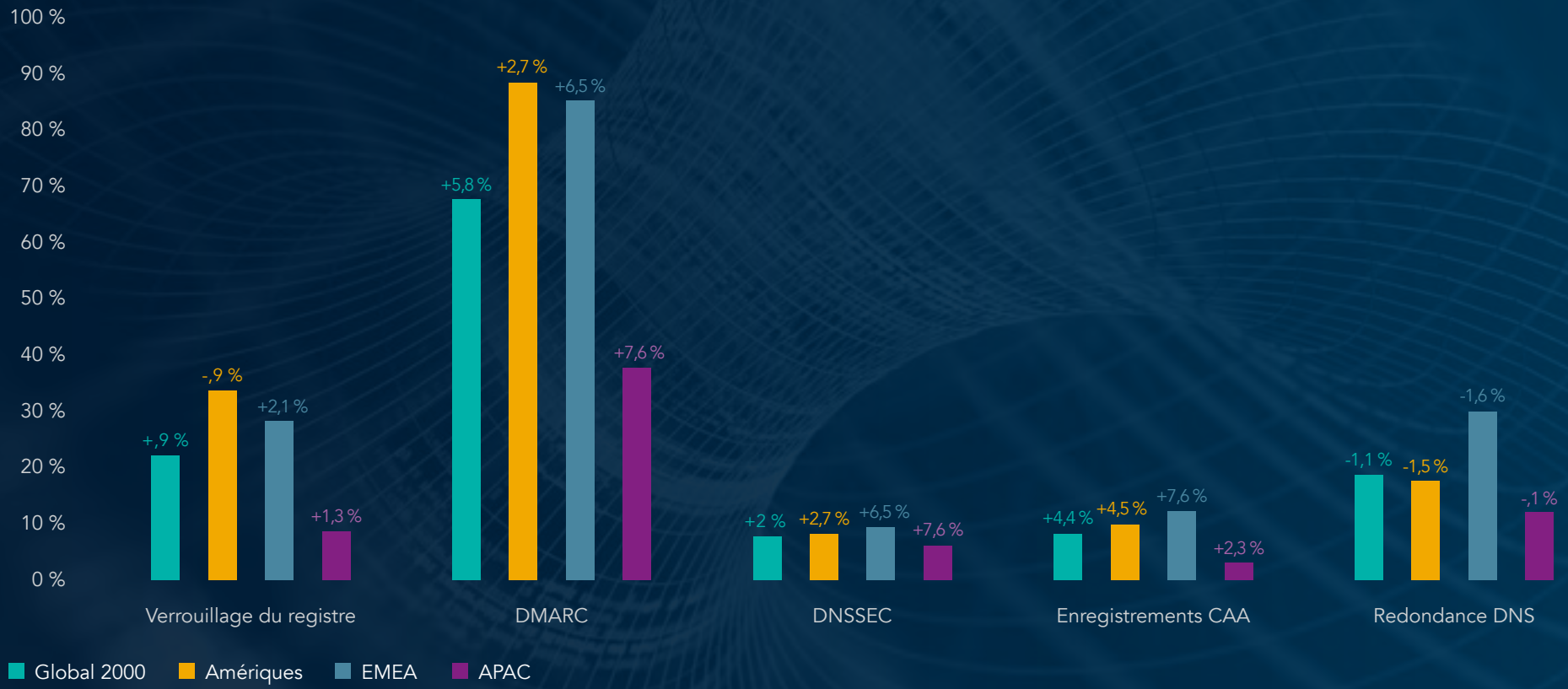


DES MESURES DE SÉCURITÉ TELLES QUE LA REDONDANCE DU DNS, DNSSEC ET LES ENREGISTREMENTS CAA

Bien qu'encore peu nombreuses, les entreprises déployant des extensions de sécurité du système de noms de domaine (Domain Name System Security Extension, DNSSEC) ont plus que doublé au cours des trois dernières années, passant de 3 % en 2020 à 8 % en 2023. Curieusement, alors même que de plus en plus d'organismes gouvernementaux insistent sur l'importance de la résilience du DNS, la redondance de ce système a quant à elle baissé de 1 % par rapport à l'année dernière pour atteindre 19 %. Malgré l'importance de cette redondance pour l'infrastructure centrale de toute organisation, nous constatons que l'adoption de cette mesure de sécurité diminue, et ce probablement car les entreprises doivent planifier l'augmentation de leurs coûts et l'allocation de leurs ressources en conséquence.

Enfin, l'utilisation des enregistrements certificate authority authorization (CAA) a considérablement augmenté cette année, passant de 3,8 % en 2020 à 8,4 % en 2023. Les enregistrements CAA permettent aux entreprises de désigner une Autorité de certification (AC) spécifique en tant qu'émettrice unique des certificats pour les noms de domaine de votre entreprise. Agir ainsi empêche les cybercriminels de faire appel à une autorité de certification non validée pour obtenir un nouveau certificat. Cependant, de nombreuses entreprises continuent de n'utiliser que partiellement ce contrôle de sécurité, souvent en raison de la complexité des exigences, notamment lorsqu'elles recourent à différents fournisseurs pour la gestion de leurs noms de domaine, de leurs services DNS et de leurs certificats SSL (Secure Sockets Layer).

MESURES DE SÉCURISATION DES NOMS DE DOMAINE PAR RÉGION EN 2023



+/- % par rapport à l'année précédente

MESURES DE SÉCURISATION DES NOMS DE DOMAINE PAR TYPE DE REGISTRAR EN 2023

Pour les besoins de ce rapport, nous avons analysé la tendance d'adoption des dispositifs de sécurité des noms de domaine en fonction du type de registrar de noms de domaine auquel font appel les entreprises du Global 2000.

Registrars grand public :

un registrar grand public propose des services liés aux noms de domaine, aux sites web et aux messageries qui peuvent convenir aux particuliers, aux indépendants et aux petites entreprises qui démarrent.

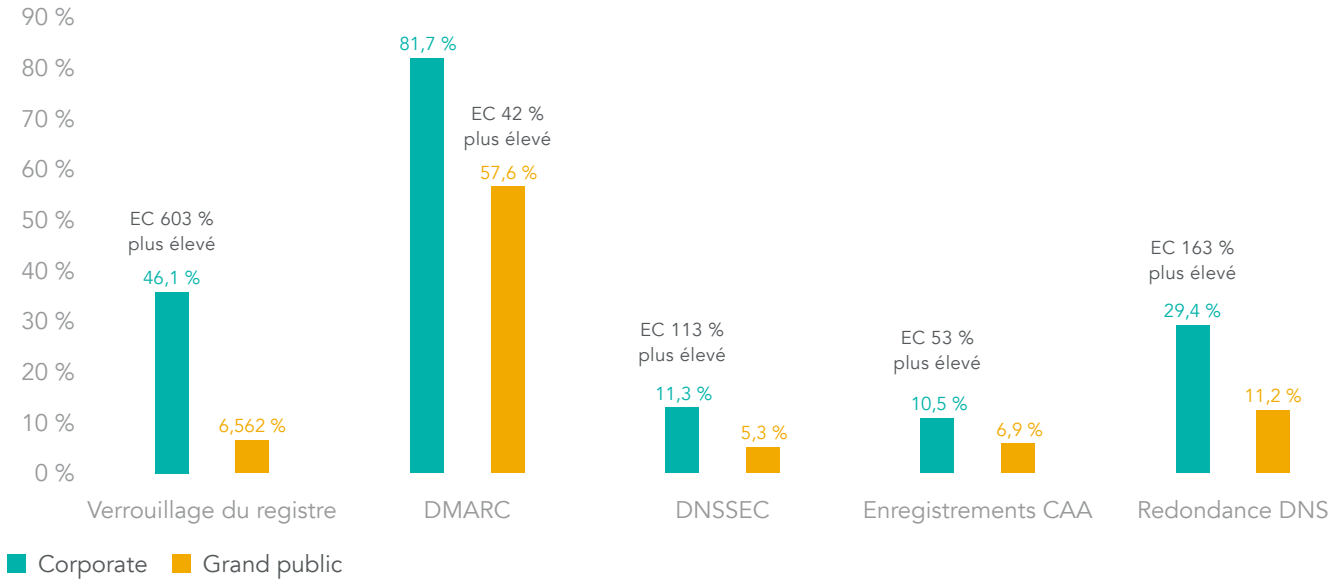
Registrars corporate :

un registrar corporate se spécialise dans la prestation de services aux entreprises et aux propriétaires de marques qui ont besoin de niveaux avancés de pratiques commerciales, de capacités, d'expertise et de personnel d'assistance en matière de gestion de domaine et de DNS ainsi qu'en termes de sécurité, de protection de la marque et de lutte contre la fraude, de gouvernance des données et de cybersécurité.

De nombreuses entreprises considèrent que tous les registrars se valent. Une confiance injustifiée envers des registrars grand public, qui peuvent ne pas avoir prévu de mesure de sécurisation des noms de domaine, est susceptible de nuire à la stratégie de sécurité globale d'une entreprise. Cette distinction est particulièrement évidente concernant l'adoption du verrouillage du registre, car la plupart des registrars grand public ne prennent pas en charge ce dispositif.

LES ENTREPRISES QUI ONT BESOIN DE FONCTIONNALITÉS DESTINÉES AUX PROFESSIONNELS AFFICHENT UN PLUS HAUT NIVEAU D'ADOPTION DE MESURES DE SÉCURITÉ DU NOM DE DOMAINE

Niveau de maturité des mesures de sécurité, Registrars corporate (EC)/grand public (CG)



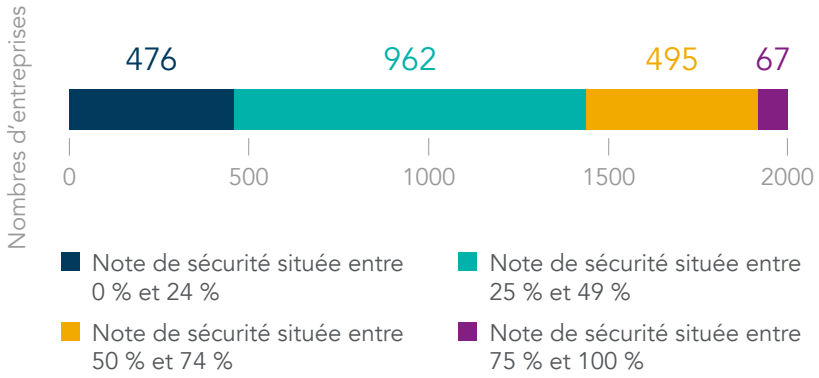
STRATÉGIE GLOBALE DE SÉCURITÉ DU NOM DE DOMAINE

En examinant l'importance de huit mesures de sécurité essentielles regroupées en fonction du niveau de risque de sécurité du nom de domaine, CSC a obtenu une note moyenne pour chaque entreprise. Cette moyenne constitue la note de sécurité de l'entreprise, une note plus élevée témoignant d'une stratégie de sécurité plus efficace, ce qui signifie que l'entreprise est moins exposée aux menaces de sécurité liées au nom de domaine.

FONCTIONNALITÉS AVANCÉES DE LA SÉCURITÉ DU NOM DE DOMAINE :

- Registrar corporate
- Verrouillage du registre
- Enregistrements CAA
- Redondance DNS
- DNSSEC
- Sender policy framework (SPF)
- DomainKeys identified mail (DKIM)
- DMARC

NIVEAU DE RISQUE DE SÉCURITÉ DU NOM DE DOMAINE



72 % des entreprises ont implémenté moins de la moitié de l'ensemble des mesures de sécurisation du nom de domaine

SECTEURS LES PLUS SÉCURISÉS

- Logiciels et services IT
- Médias
- Services et fournitures pour les entreprises
- Hôtellerie, restauration et loisirs
- Équipement et services en matière de soins de santé

ENTREPRISES LES PLUS SÉCURISÉES

- Seules deux entreprises affichaient la note de sécurité la plus élevée avec le plus fort taux d'adoption de mesures de sécurité.

SECTEURS LES MOINS SÉCURISÉS

- Services publics
- Sociétés commerciales
- Marchés alimentaires
- Construction
- Matériaux

ENTREPRISES LES MOINS SÉCURISÉES

- 112 entreprises affichent une note de sécurité des noms de domaine de zéro.
- Ces entreprises sont principalement situées dans la région Asie-Pacifique et représentent 87 % des entreprises avec la note de zéro.

ACTIVITÉS SUSPECTES OU MALVEILLANTES CIBLANT LES NOMS DE DOMAINE DES ENTREPRISES DU GLOBAL 2000

Nous avons identifié et analysé les noms de domaine contenant les noms de marque à plus de six caractères des entreprises du classement Global 2000, mais qui n'étaient pas détenus par les marques elles-mêmes. Ces enregistrements abusifs de noms de domaine visent à tirer parti de la confiance accordée à la marque ciblée pour lancer des attaques de phishing ou d'autres formes d'abus de marque numérique ou encore de violations de la propriété intellectuelle, qui entraînent une perte de revenus et un détournement du trafic web, et entachent la réputation de la marque.

Il existe d'innombrables permutations et tactiques d'usurpation des noms de domaine pouvant être utilisées par les fraudeurs et les acteurs malveillants.

NOUS NOUS SOMMES VOLONTAIREMENT CONCENTRÉS SUR LES HOMOGLYPHES, CAR ILS CONSTITUENT L'UNE DES MÉTHODES D'ATTAQUE LES PLUS RÉPANDUES UTILISÉES PAR LES CYBERCRIMINELS

Tactiques de spoofing de noms de domaine

Correspondances floues	cscg1obal.com | cscgl0bal.com
Homoglyphes : noms de domaine internationalisés (IDN)	ćscglobal.com | csçglobal.com
Noms de domaine similaires	cscglobal.jp | cscglobal.ec
Correspondance de mots clés	cscglobalcovid.com | covidcscglobal.ar | covid19.com
Homophones (soundex)	siesiglobal.com | cscclobol.com

Homoglyphes courants (correspondances floues) dans les noms de domaine .COM

Sur la base de l'observation fréquente de l'utilisation de noms de domaine pour le phishing, notre analyse a porté sur les substitutions courantes de caractères latins, par exemple l'utilisation de C0rnpanyNarne.com au lieu de CompanyName.com.

C0rnpanyNarne.com

Substitutions de caractères les plus courantes

i → l	m → rn	i → 1	s → 5	o → 0
e → 3	l → 1	l → i	w → vv	

PLUS DE 79 % DES NOMS DE DOMAINES HOMOGLYPHES SONT DÉTENUS PAR DES TIERS

Parmi les noms de domaine détenus par des tiers :

87 % ont leurs coordonnées WHOIS ou les informations liées à la propriété du site masquées en 2023 contre 82 % en 2022. Une augmentation qui pourrait être intentionnelle ou due à des politiques de confidentialité telles que le Règlement général sur la protection des données (RGPD). Cependant, ces tentatives de masquer ou de dissimuler la propriété et l'identité, notamment en ce qui concerne les noms de domaine de tiers, s'expliquent principalement par des intentions malveillantes de la part de ces derniers.

40 % d'entre eux disposent d'enregistrements MX en 2023, contre 48 % en 2022. Les enregistrements MX (messagerie) permettent d'envoyer des e-mails de phishing ou d'intercepter des e-mails.

COMMENT CES NOMS DE DOMAINE DE TIERS SONT-ILS UTILISÉS ?

36 % redirigent les internautes vers du contenu publicitaire ou des liens sponsorisés, ou sont utilisés pour les services de parking de noms de domaine.

49 % détenaient des sites web inactifs.

1 % redirigeaient les utilisateurs vers un contenu malveillant. Susceptible de nuire à la réputation d'une marque et diminuer.

14 % se résolvent en un site web actif qui n'a aucun lien avec le propriétaire de marque.

Suite au récent lancement de Threads par Instagram en juillet 2023, les marques constatent d'ores et déjà les effets des enregistrements de nom de domaines tiers, certains étant utilisés pour revendiquer une affiliation, utiliser des logos de manière frauduleuse, usurper l'identité de marque et plus encore.

En savoir plus : Une nouvelle étude de CSC indique que le lancement de Threads par Instagram constitue déjà une cible pour la fraude et le détournement de marque

NOMS DE DOMAINE SUSPECTS OU MALVEILLANTS QUI SONT LES CIBLES ?

Secteur	Pourcentage de risque de faux noms de domaine par rapport au total
Banque	13,1 %
Construction	5,4 %
Opérations pétrolières et gazières	4,5 %
Services financiers diversifiés	4,2 %
Matériaux	4,2 %
Logiciels et services IT	4,1 %
Services publics	3,6 %
Services et fournitures pour les entreprises	3,5 %
Assurance	3,5 %
Biens d'équipement	3,4 %
Biens de consommation durables	3,3 %
Vente au détail	3,2 %
Produits chimiques	2,8 %
Médicaments et biotechnologie	2,6 %
Transport	2,4 %
Matériel et équipement technologique	2,2 %
Alimentation, boissons et tabac	2,1 %
Services de télécommunication	1,9 %
Équipement et services en matière de soins de santé	1,9 %
Semi-conducteurs	1,7 %
Hôtellerie, restauration et loisirs	1,2 %
Aérospatial et défense	1,1 %
Articles ménagers et personnels	1,0 %
Sociétés commerciales	0,9 %
Médias	0,9 %
Marchés alimentaires	0,8 %

REGISTRARS DE NOMS DE DOMAINE LES PLUS ASSOCIÉS AUX ENREGISTREMENTS ABUSIFS DE NOMS DE DOMAINE PAR DES TIERS :

- GoDaddy®
- Namecheap™
- Network Solutions

CONCLUSION

Pour une entreprise, négliger la sécurité de ses noms de domaine peut avoir des conséquences catastrophiques. Les noms de domaine non protégés constituent une menace importante pour votre stratégie de cybersécurité, mais aussi pour la protection des données, la sécurité des consommateurs, la propriété intellectuelle, les chaînes d'approvisionnement, le chiffre d'affaires et la réputation de votre entreprise.

Nos recherches ont démontré que 43 % des domaines .AI associés aux entreprises du Global 2000 sont enregistrés par des tiers. Les entreprises qui n'ont pas sécurisé leurs domaines .AI découvrent aujourd'hui que de nombreux fraudeurs en ligne astucieux ont acheté ces domaines à leur place, comme en témoigne l'augmentation de 350 % des litiges relatifs à un nom de domaine impliquant des extensions .AI en 2023 par rapport à l'année précédente.

Pour compléter les enregistrements de noms de domaine stratégiques, les entreprises doivent également garantir la sécurité des noms de domaine à l'aide d'un modèle de sécurité à plusieurs niveaux dans le cadre d'une structure Zero Trust afin de mettre en œuvre une stratégie de sécurité renforcée qui protège au maximum leur activité. Un partenariat avec un registrar corporate est primordial non seulement pour obtenir un aperçu des surfaces exposées (qui comprennent les noms de domaine et les DNS), et la capacité d'analyser les vecteurs de menace ciblant la présence en ligne d'une entreprise, mais aussi pour disposer des ressources nécessaires pour offrir des solutions d'atténuation et des mesures d'intervention.

Consultez la liste des mesures de sécurité défensives et proactives proposée par CSC pour protéger vos noms de domaine et vos marques grâce à une approche de défense multicouche en profondeur de la sécurité des noms de domaine.

Télécharger notre checklist concernant la sécurité des noms de domaine.

À PROPOS DE LA PLATEFORME DOMAINSEC DE CSC

La solution 3D Domain Security and Enforcement de CSC a été conçue pour exploiter la puissance de la plateforme DomainSec℠ de CSC. DomainSec est une plateforme de cybersécurité Software-as-a-Service (SAAS) créée par CSC. Elle propose la première approche holistique du secteur en matière de sécurisation et de défense des écosystèmes de domaine des marques. Elle utilise la technologie propriétaire de recherche approfondie reposant sur le machine learning qui allie cette technologie, l'intelligence artificielle et une technologie de mise en cluster pour identifier les principaux indicateurs de compromission.

DomainSec réunit dans une plateforme unique les solutions de sécurité et de gestion de domaine et les solutions de protection des marques et de lutte contre la fraude de CSC. Cela signifie que nous sommes en mesure de vous proposer une protection exponentielle et de vous aider à affiner votre modèle de sécurité Zero Trust en allant au-delà de la simple défense des périmètres.

CSC est le fournisseur de choix en matière de sécurité et de renseignements sur les menaces qui offre des solutions de sécurité des domaines pour les entreprises du classement Forbes Global 2000 ainsi qu'aux marques du classement 100 Best Global Brands. Il propose notamment la gestion de portefeuilles de domaines sécurisés, un système de noms de domaine (DNS), la gestion de certificats numériques, ainsi que la protection des marques en ligne et la protection contre la fraude. Alors que les entreprises internationales investissent considérablement dans leur stratégie de sécurité et poursuivent leurs efforts pour protéger leur surface d'attaque externe, CSC est la solution idéale pour les aider à comprendre les risques liés à la sécurité des noms de domaine et leur lien avec leur modèle Zero Trust. En s'appuyant sur la technologie propriétaire de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type Règlement général sur la protection des données (RGPD). Nous fournissons également des services de protection des marques en ligne, qui combinent la surveillance de marque et des interventions ciblées. Nous proposons une approche holistique des actifs numériques et des services de protection contre la fraude pour contrer les tentatives de phishing. Basée à Wilmington (Delaware) aux États-Unis depuis 1899, CSC possède des bureaux sur tout le territoire des États-Unis, mais également au Canada, en Europe et dans la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités. Consultez notre site à l'adresse suivante : cscdbs.com/fr.

[1] Blog CSC, « Êtes-vous prêts pour l'IA ? .AI : un nom de domaine à intégrer à votre portefeuille…avant que d'autres ne le fassent » cscdbs.com/blog/ai-you-ready-a-domain-to-add-to-your-portfoliobefore-someone-else-does/

[2] DNDisputes.com, « IA : litige relatif à un nom de domaine impliquant des extensions .AI » dndisputes.com/case/domain/extension/ai/

[3] Search Engine Land, « Les domaines .AI désormais considérés comme des noms de domaine génériques de premier niveau par Google » searchengineland.com/google-now-treats-ai-domains-as-generic-top-level-domains-427770

CSC10192023