Rapport 2024 sur la sécurité des noms de domaine

INTRODUCTION

Au cours des cinq dernières années, CSC a été en tête du classement Forbes Global 2000 en matière de génération de rapports sur la stratégie de sécurité des noms de domaine. Pour cela, nous avons analysé l'adoption des mesures de sécurité des noms de domaine, celles mises en place pour atténuer les cyberrisques présents dans l'écosystème des noms de domaine 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.

Cette année, nous avons constaté que, bien que certaines entreprises aient 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 donc mieux sensibiliser les entreprises à ces menaces et partager les bonnes pratiques afin d'améliorer la stratégie de sécurité en matière de nom de domaine auprès des entreprises.

Alors que CSC s'apprête à célébrer le cinquième anniversaire de son « rapport sur la sécurité des noms de domaine » annuel, nous revenons sur notre engagement continu visant à analyser la stratégie de sécurité des noms de domaine des entreprises du classement Forbes Global 2000. Cette année, marquée par le 125e anniversaire de CSC, nous continuons à sensibiliser le public aux cyberrisques qui existent en dehors du périmètre de l'entreprise dans l'espace numérique, ainsi qu'à la nécessité de mettre en place des mesures de sécurité robustes au niveau des domaines.

RÉSUMÉ DES PRINCIPALES CONCLUSIONS

LE SECTEUR DES ÉQUIPEMENTS ET DES SERVICES DE SOINS DE SANTÉ A RECULÉ DANS LE CLASSEMENT DE LA SÉCURITÉ DES NOMS DE DOMAINE, MALGRÉ L'AUGMENTATION DES CYBERATTAQUES MAJEURES

Cette année, le changement le plus notable dans la sécurité des noms de domaine par secteur a été observé dans le secteur de l'équipement et des services de soins de santé, qui a perdu sept places, passant de la 5e place en 2023 à la 12e place en 2024. À l'inverse, le secteur de l'équipement et du matériel technologique a gagné huit places, passant de la 13e place en 2023 à la 5e en 2024.

80 % DES NOMS DE DOMAINE SIMILAIRES AUX MARQUES DU GLOBAL 2000 (HOMOGLYPHES) SONT DÉTENUS PAR DES TIERS ET N'APPARTIENNENT PAS À LA MARQUE CONCERNÉE

Parmi les 80 % de noms de domaine homoglyphes (faux noms ressemblant) détenus par des tiers autres que les propriétaires des marques du Global 2000, nous avons constaté que 42 % ont des enregistrements MX (enregistrements d'échange d'e-mails), contre 40 % en 2023. Les enregistrements MX (messagerie) permettent d'envoyer des e-mails de phishing ou d'intercepter des e-mails.

107 DES ENTREPRISES DU GLOBAL 2000 ONT UNE NOTE DE SÉCURITÉ DE NOM DE DOMAINE DE ZÉRO

5 % des entreprises du Global 2000 n'appliquent aucune des mesures de sécurité des noms de domaine recommandées et s'exposent ainsi aux risques les plus élevés. D'après notre analyse de l'adoption des principales mesures de sécurité des noms de domaine, une note de sécurité nulle indique qu'aucune mesure n'a été adoptée, ce qui expose les entreprises à un niveau de risque maximal vis-à-vis des menaces pour la sécurité des noms de domaine.

L'UTILISATION D'UN VERROU DE REGISTRE A AUGMENTÉ DE 7 POUR CENT DEPUIS 2020, MAIS L'ADOPTION GLOBALE RESTE FAIBLE (24 %)

Les verrous de registre permettent 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.

L'UTILISATION DU PROTOCOLE DMARC A AUGMENTÉ DE 32 POUR CENT DEPUIS 2020

En 2023, l'Anti-Phishing Working Group (APWG) a enregistré un nombre record de près de cinq millions d'attaques par hameçonnage, ce qui fait de 2023 la pire année pour ce qui est du hameçonnage. Une telle augmentation des attaques a contribué à accroître l'adoption 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 du spoofing et du hameçonnage.

LES SURFACES D'ATTAQUE EXTERNES ONT POUR CIBLE L'ÉCOSYSTÈME DES NOMS DE DOMAINE

Les cybermenaces étant de plus en plus assistées par l'IA, les attaques continuent d'augmenter. La sécurité des noms de domaine joue donc un rôle important dans l'évaluation des cyberrisques au plus haut niveau de l'entreprise, laquelle doit considérer l'écosystème des noms de domaine de l'entreprise comme une réelle vulnérabilité face aux attaques illustrées dans la figure 1. Les noms de domaine légitimes compromis ou détournés, ainsi que les enregistrements de noms de domaine malveillants, sont utilisés pour lancer toutes les attaques de la figure 1.

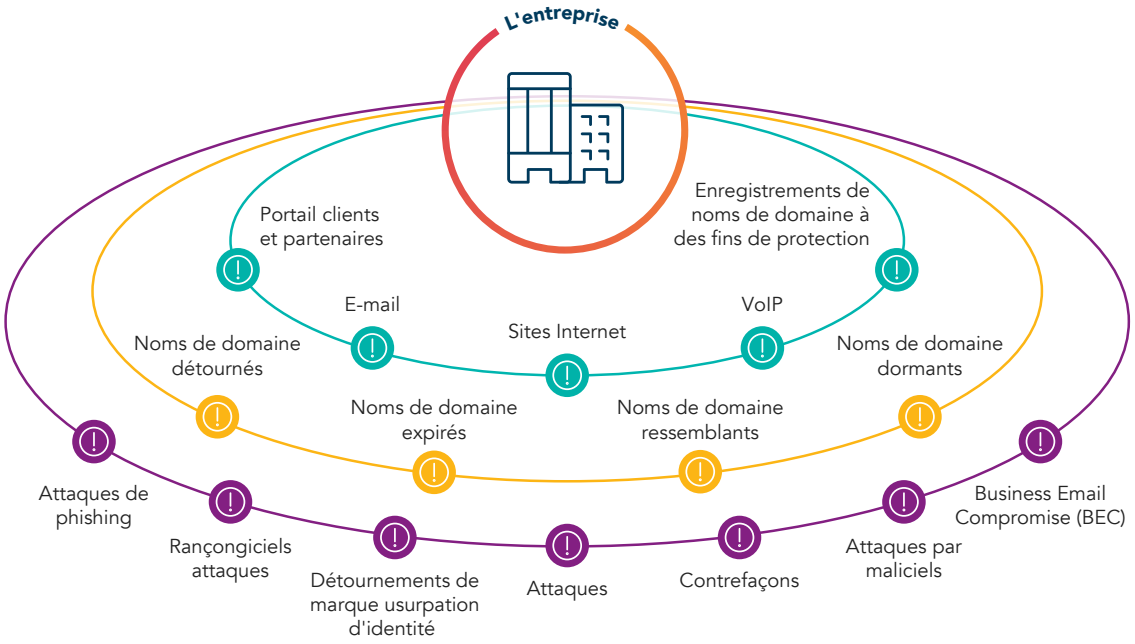
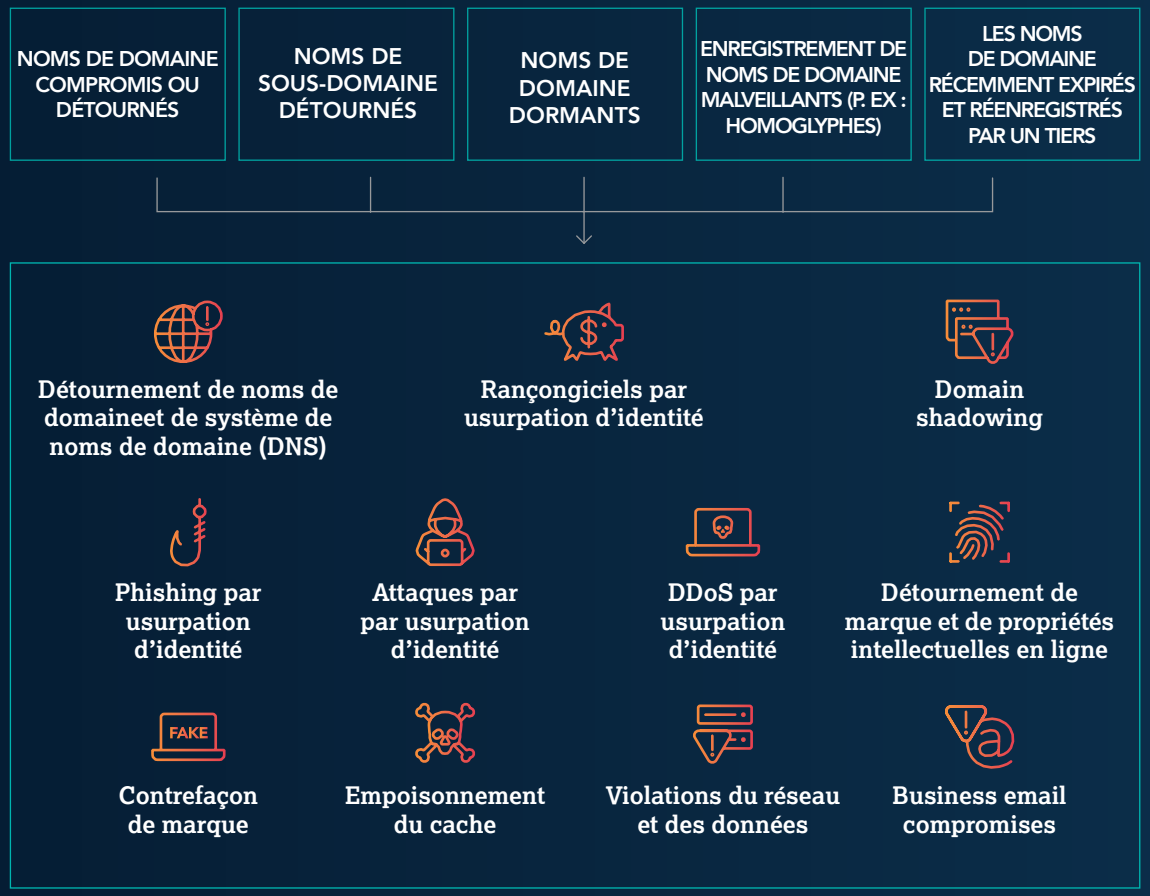


Figure 1 : La galaxie de l'écosystème des noms de domaine

DÉFINITION DE LA SÉCURITÉ DES NOMS DE DOMAINE

Les entreprises du monde entier utilisent Internet pour l'ensemble de leurs opérations : sites Internet, e-mails, authentification, communications VoIP, portails client, applications fournisseur 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 ne cessent d'augmenter, les entreprises et les cyberassureurs ont du mal à les quantifier et à estimer leur degré de nuisance. Cela montre que les noms de domaine sont des éléments cruciaux de la stratégie de cybersécurité d'une organisation, puisque l'Internet et les noms de domaine sont essentiels à l'infrastructure et à la poursuite des activités de l'entreprise.



NOMS DE DOMAINE COMPROMIS OU DÉTOURNÉS

Les cybercriminels compromettront tous les noms de domaine non sécurisés. Les entreprises doivent commencer par adopter une approche axée sur une protection aprofondie à plusieurs niveaux pour se prémunir contre les détournements.

NOMS DE SOUS-DOMAINE DÉTOURNÉS

Un détournement de nom de sous-domaine est une attaque par laquelle des cybercriminels prennent le contrôle d'un nom de sous-domaine légitime qui n'est plus utilisé pour héberger du contenu malveillant afin de cibler les entreprises par des attaques par hameçonnage ou maliciel. Ils y parviennent en exploitant des enregistrements oubliés du système de noms de domaine (DNS) (dangling DNS) pour renvoyer les utilisateurs vers leur propre contenu.

NOMS DE DOMAINE DORMANTS

Les cybercriminels peuvent enregistrer et conserver des noms de domaine de marque en les laissant inactifs jusqu'à ce qu'ils soient prêts à les utiliser dans le cadre d'une attaque par hameçonnage ou maliciel. Les noms de domaine inactifs échappent souvent à la détection initiale, parce qu'ils n'ont pas immédiatement à disposition l'un des indicateurs d'un nom de domaine enregistré pour lancer une attaque (par ex. un enregistrement MX actif), ce qui constituerait généralement un signal d'alarme.

ENREGISTREMENTS DE NOMS DE DOMAINE MALVEILLANTS

Il existe d'innombrables permutations d'usurpation des noms de domaine et d'homoglyphes pouvant être utilisées par les fraudeurs et les acteurs malveillants. L'objectif de ces enregistrements de faux noms de domaine est de profiter de la confiance des consommateurs dans la marque ciblée pour lancer des attaques par hameçonnage convaincantes ou d'autres formes de violation numérique de la marque.

LES DOMAINES DE MARQUE RÉCEMMENT EXPIRÉS RÉENREGISTRÉS PAR UN TIERS

Les entreprises peuvent choisir d'abandonner des noms de domaine précédemment enregistrés à des fins de protection, en raison de contraintes financières. Les cybercriminels n'attendent que cela et réenregistrent immédiatement ces noms de domaine à des fins malveillantes. Ils sont constamment à l'affût de noms de domaine de marque disponibles qu'ils peuvent utiliser pour lancer des attaques.

RÉSULTATS ET ANALYSE : ADOPTION DE MESURES DE SÉCURITÉ DU NOM DE DOMAINE PAR LES ENTREPRISES DU GLOBAL 2000

Dans cette analyse, CSC a examiné l'adoption de cinq mesures clés de sécurité des noms de domaine (à savoir DMARC, la redondance DNS, les verrous de registre, les enregistrements CAA [Certificate Authority Authorization] et les extensions de sécurité DNS (DNSSEC)) par tous les membres du Global 2000. Nous avons ensuite procédé à une analyse approfondie des niveaux d'adoption dans les différents groupes sectoriels et régions.

TENDANCES D'ADOPTION DES MESURES DE SÉCURITÉ DU NOM DE DOMAINE (2020-2024)

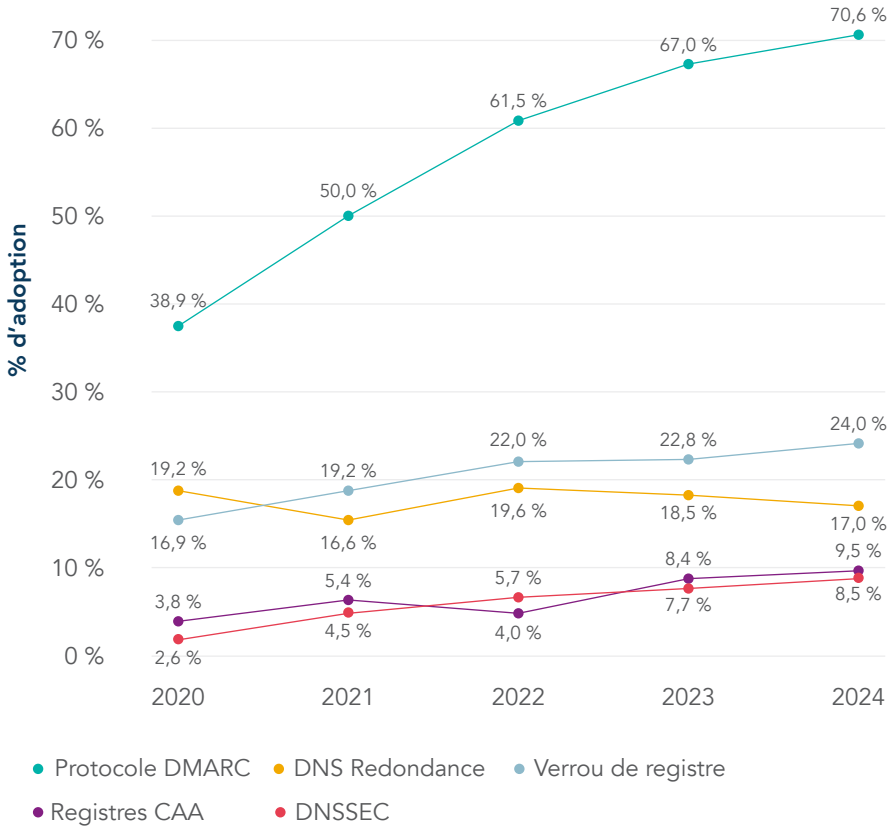


Figure 2 : Adoption des cinq mesures clés de sécurité du nom de domaine par les entreprises du Global 2000 entre 2020 et 2024

PROTOCOLE DMARC : UNE CROISSANCE MAJEURE

Au vu de l'actualité chargée concernant les attaques par hameçonnage, y compris leur augmentation en termes de volume et de complexité, il n'est pas surprenant que l'adoption du protocole DMARC ait connu une hausse rapide, passant de 39 % en 2020 à 71 % en 2024 (Figure 3).

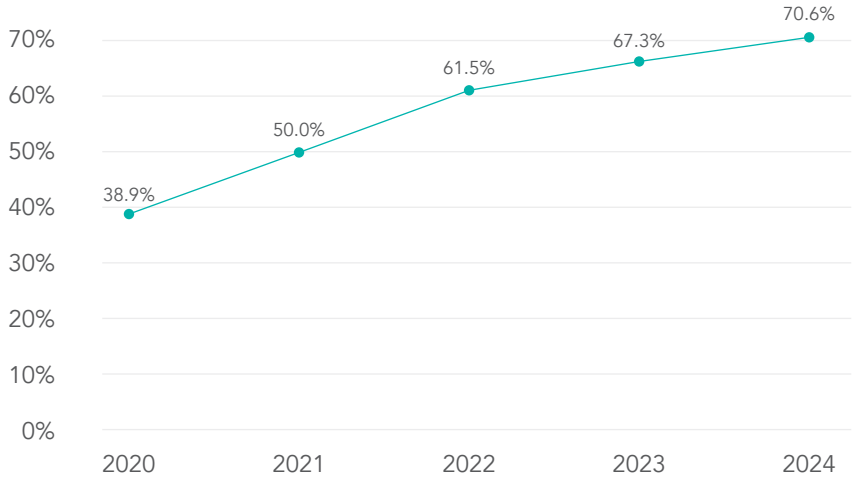


Figure 3 : Taux d'adoption du protocole DMARC entre 2020 et 2024

L'utilisation croissante d'indicateurs de marque pour l'identification des messages (BIMI) relative à la messagerie e-mail qui permettent d'afficher les logos des marques sur les e-mails authentifiés, pourrait également être un facteur de croissance de l'utilisation 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.

CROISSANCE CONSTANTE MAIS LENTE DE L'UTILISATION DES VERROUS DE REGISTRE

Le taux d'adoption des verrous de registre par les entreprises est passé de 17 % en 2020 à 24 % en 2024. Nous avons également constaté que les entreprises qui utilisent des registrars de corporate utilisent aussi plus fréquemment les verrous de registre (45 % en 2024). Face aux pressions croissantes en faveur du renforcement de la cybersécurité, de plus en plus de registres proposent des verrous sur leurs extensions de domaine afin d'assurer la sécurité des transactions de bout en bout, ce qui permet de limiter les erreurs humaines et les risques encourus par les tiers.

Compte tenu de l'évolution constante du portefeuille des noms de domaine des entreprises, CSC a recours à un algorithme de modélisation prédictif qui évalue plus de 20 attributs de noms de domaine afin de déterminer si le domaine en question joue un rôle essentiel pour les activités des entreprises et leur marque en ligne, et de recommander les domaines vitaux qui doivent être protégés.

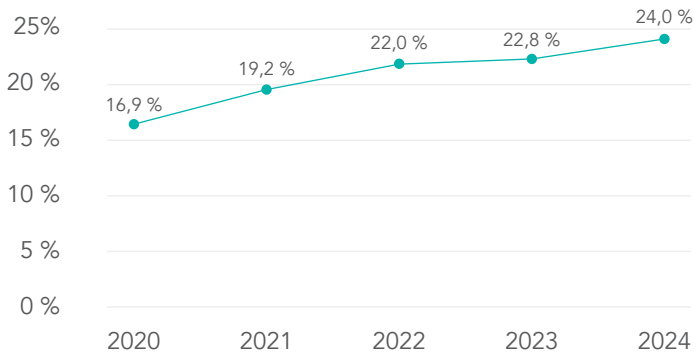


Figure 4 : Taux d'adoption des verrous de registre entre 2020 et 2024

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

Bien qu'encore peu nombreuses, le pourcentage d'entreprises déployant des extensions de sécurité du système de noms de domaine (Domain Name System Security Extension, DNSSEC) a triplé ont plus que doublé au cours des trois dernières années, passant de 3 % en 2020 à 9 % en 2024. Les extensions DNSSEC garantissent l'authentification et l'intégrité des données pour les requêtes et les réponses DNS, ce qui empêche les cybercriminels de rediriger le trafic Internet vers des sites Internet malveillants, tels que des sites d'hameçonnage.

Il est surprenant de constater que la redondance DNS a encore baissé de 1 % cette année ; ainsi, le pourcentage d'entreprises qui donnent la priorité à la redondance DNS est moins élevé cette année qu'en 2020. 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.

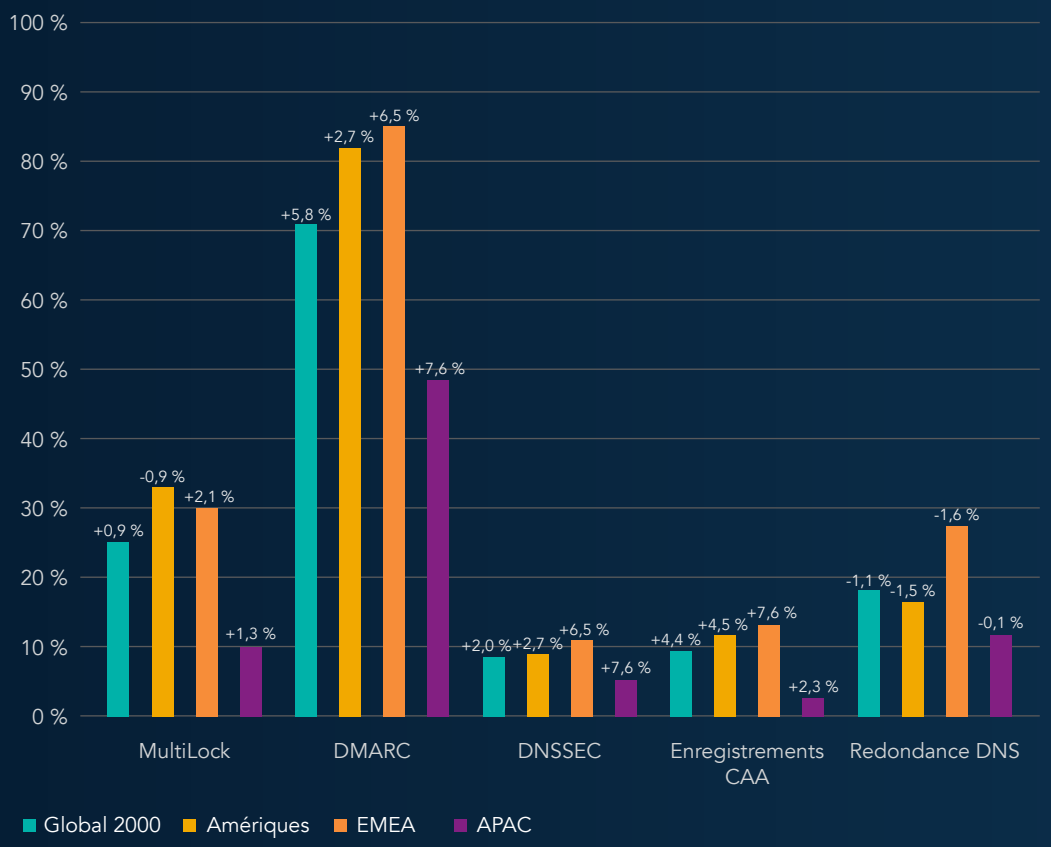
Enfin, l'utilisation des enregistrements CAA a augmenté cette année pour atteindre 10 % en 2024, contre 4 % en 2020. Les enregistrements CAA permettent aux entreprises de désigner une Autorité de certification (AC) spécifique en tant qu'émettrice unique des certificats numériques pour leurs noms de domaine. Agir ainsi empêche les cybercriminels de faire appel à une autorité de certification non validée pour obtenir un nouveau certificat numérique ; en effet, leur demande n'aboutira pas et l'entreprise recevra une alerte.

Nous avons également constaté que les entreprises qui utilisent des registrars de corporate utilisent aussi plus fréquemment les verrous de registre (45 % en 2024).

MESURES DE SÉCURITÉ DU NOM DE DOMAINE 2024

PAR RÉGION

La région EMEA a connu la plus forte croissance en matière de mise en œuvre de mesures de sécurité du nom de domaine entre 2023 et 2024.



+/- % par rapport à l'année précédente

Figure 5: Adoption des mesures de sécurité des noms de domaine par région

PAR SECTEUR

Le secteur des soins de santé perd sept places dans le classement de 2024.

Classement sectoriel	Place en 2024	Place en 2023	
Matériel et équipement technologique	5	13	↑
Équipement et services en matière de soins de santé	12	5	↓

Sur les 26 secteurs d'activité de Forbes Global 2000, **le secteur de l'équipement et des services en matière de soins de santé** a perdu sept places et n'occupe plus les cinq premières places du classement. Le recul de la 5e place en 2023 à la 12e place en 2024 fait contraste avec la forte augmentation des cyberattaques contre les hôpitaux et les systèmes de santé cette année, d'autant plus que le secteur des soins de santé est désormais devenu une cible privilégiée des attaques par rançongiciels.[1] Déjà en 2024, le secteur des soins de santé a recensé 280 cyberincidents. Cela représente « 24 % de tous les incidents cybernétiques aux États-Unis en 2024, ce qui place le secteur des soins de santé devant tous les autres secteurs. »[2]

Le secteur de l'équipement et du matériel technologique a gagné huit places et se hisse à la 5e place. Il est certain qu'il est avantageux pour les entreprises du secteur technologique de figurer dans les cinq premières places, et leur croissance peut être liée aux mesures de sécurité qu'elles ont mises en place depuis les attaques majeures contre la chaîne logistique qui ont commencé en 2020 avec Solar Winds.

↑ SECTEURS LES PLUS SÉCURISÉS

- Services et fournitures aux entreprises
- Logiciels et services IT
- Médias
- Vente au détail
- Matériel et équipement technologique

↓ SECTEURS LES MOINS SÉCURISÉS

- Construction
- Alimentation, boissons et tabac
- Marchés alimentaires
- Matériaux
- Opérations pétrolières et gazières

MESURES DE SÉCURISATION DES NOMS DE DOMAINE PAR TYPE DE REGISTRAR EN 2024

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.

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 ou ne pas avoir donné la priorité à celle-ci, 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.

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.

REGISTRARS GRAND PUBLIC :

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

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

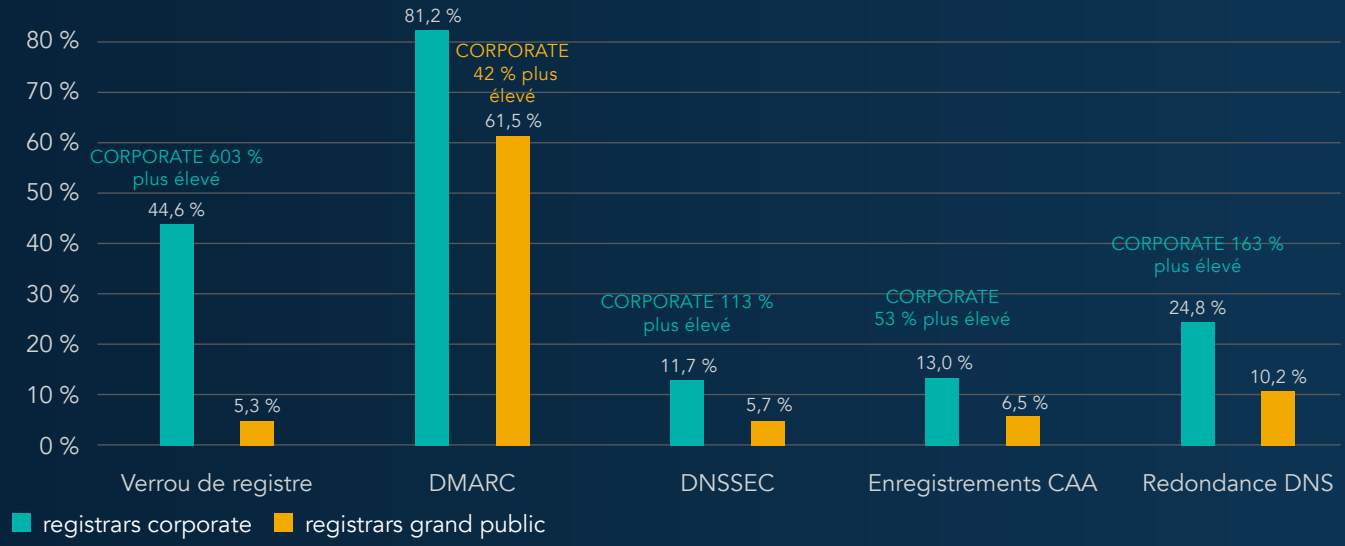


Figure 6 : Niveau de maturité des mesures de sécurité Registrars corporate (EC)/grand public (CG)

STRATÉGIE DE SÉCURITÉ DU NOM DE DOMAINE

En examinant l'importance d'une liste exhaustive de huit mesures de sécurité clés que nous avons regroupées en fonction du niveau de risque de sécurité du nom de domaine de l'entreprise, 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
- Verrou de registre (MultiLock)
- Enregistrements CAA
- Redondance DNS
- Extensions de sécurité DNS
- Cadre SPF (Sender policy framework)
- Norme DKIM (DomainKeys identified mail)
- DMARC

NIVEAU DE RISQUE DE SÉCURITÉ DU NOM DE DOMAINE

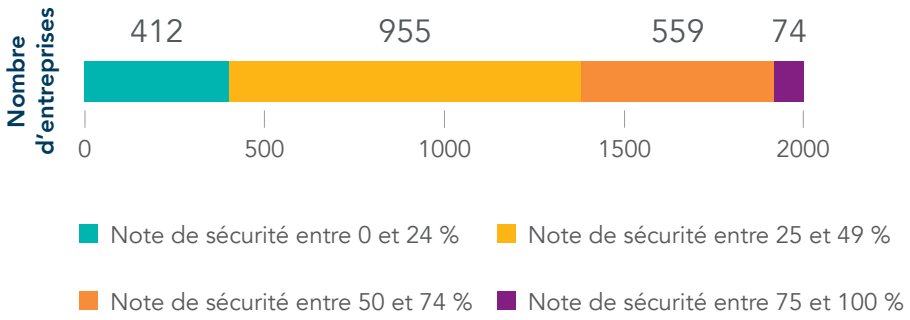


Figure 7 : notes de sécurité des noms de domaine et niveaux de risque associés pour les entreprises du Global 2000

68 % des entreprises du Global 2000 ont mis en place moins de la moitié des mesures de sécurité recommandées.

ENTREPRISES LES PLUS SÉCURISÉES

Une seule entreprise a une note de 100 % et a obtenu une note de 100 % l'année dernière. 12 entreprises ont une note de 7 sur 8.

ENTREPRISES LES MOINS SÉCURISÉES

107 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. Le but de ces noms de domaine tiers est de tirer parti de la confiance dont bénéficient les marques ciblées pour lancer des attaques par hameçonnage ou d'autres formes de détournements numériques de marque sur Internet, ainsi que des violations d'adresses IP. Cela entraîne des pertes de revenus, un détournement du trafic et une perte de 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 D'USURPATION DE NOMS DE DOMAINE POUR LES NOMS DE DOMAINE .COM

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

Figure 8 : Tactiques courantes d'usurpation de noms de domaine

HOMOGLYPHES COURANTS (CORRESPONDANCES FLOUES)

Sur la base de l'observation fréquente de l'utilisation de noms de domaine pour le hameçonnage, 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

c	→ e	0	→ 0	m	→ n	l	→ I	m	→ rn
g	→ q	E	→ 3	S	→ 5	B	→ 8	l	→ 1

Figure 9 : Homoglyphes courants (correspondances floues) pour les noms de domaine .COM

80 % DES NOMS DE DOMAINE HOMOGLYPHES SONT DÉTENUS PAR DES TIERS

Parmi les noms de domaine détenus par des tiers :

42% ont des enregistrements MX en 2024. Ce chiffre est de 40 % en 2023. Les enregistrements MX peuvent être utilisés pour envoyer des e-mails d'hameçonnage ou pour intercepter des e-mails.

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

48% redirigent les internautes vers du contenu publicitaire ou des liens sponsorisés, ou sont utilisés pour les services de parking de noms de domaine.

33% ont des sites Internet inactifs.

2% redirigent les utilisateurs vers un contenu malveillant, susceptible de nuire à la réputation d'une marque et de diminuer la confiance des clients envers cette dernière.

17% aboutissent à un site Internet actif qui n'a aucun lien avec le propriétaire de la marque.

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

- GoDaddy®
- Namecheap™
- Network Solutions

NOMS DE DOMAINE SUSPECTS OU MALVEILLANTS : QUI EST CIBLÉ ?

SECTEUR	POURCENTAGE DE RISQUE DE FAUX NOMS DE DOMAINE PAR RAPPORT AU TOTAL
Banque	19,9 %
Services financiers diversifiés	7,2 %
Logiciels et services IT	7,2 %
Construction	6,4 %
Assurance	6,3 %
Opérations pétrolières et gazières	6,2 %
Services publics	6,1 %
Biens d'équipement	5,5 %
Biens de consommation durables	5,3 %
Services et fournitures pour les entreprises	5,0 %
Transport	4,9 %
Matériaux	4,7 %
Vente au détail	4,6 %
Matériel et équipement technologique	4,2 %
Médicaments et biotechnologie	3,5 %
Alimentation, boissons et tabac	3,4 %
Équipement et services en matière de soins de santé	3,4 %
Services de télécommunication	3,0 %
Semi-conducteurs	2,9 %
Produits chimiques	2,6 %
Aérospatial et défense	2,0 %
Hôtellerie, restauration et loisirs	1,7 %
Articles ménagers et personnels.	1,7 %
Marchés alimentaires	1,5 %
Sociétés commerciales	1,2 %
Médias	1,1 %

DONNÉES SUR LA SÉCURITÉ DES NOMS DE DOMAINES : ENSEIGNEMENTS TIRÉS DE LA HAUSSE DU NOMBRE DE NOMS DE DOMAINE PENDANT LES JEUX OLYMPIQUES DE 2024

À l'instar d'autres grands événements mondiaux, les Jeux Olympiques de Paris, qui ont eu lieu en juillet 2024, ont dû faire face à des menaces numériques de la part d'escrocs cherchant à exploiter la portée mondiale de l'événement au moyen d'articles contrefaits, de faux billets, de sites de diffusion en continu frauduleux et d'attaques par hameçonnage. La surveillance des écosystèmes de noms de domaine à l'échelle mondiale, tels que les noms de domaine ressemblants, abandonnés, réenregistrés ou nouvellement enregistrés, doit être la priorité de toute approche en matière de sécurité d'entreprise et de la stratégie en ligne de la marque visant à atténuer ces menaces numériques. Les entreprises doivent être particulièrement vigilantes à l'égard des **noms de domaines dormants**, c'est-à-dire ceux qui n'ont pas encore été exploités, mais qui présentent des signes indiquant qu'une initiative d'attaque est en train de se former.

FAITS MARQUANTS

Nos recherches nous ont permis d'identifier 8 857 noms de domaine uniques de tiers contenant le terme « Jeux Olympiques » ou des mots-clés apparentés tels que « Paris 2024 » (voir figure 10). Notre analyse a étudié l'activité des noms de domaine, notamment les nouveaux enregistrements, les enregistrements abandonnés et les réenregistrements, au cours de la période allant du 1er août 2023 au 13 août 2024. Comme le montre la figure 10, nous avons observé une hausse significative du nombre de nouveaux enregistrements qui a coïncidé avec le début des Jeux Olympiques, le 26 juillet, et avec leur clôture, le 13 août. Parmi les noms de domaine encore enregistrés, 49 % étaient dormants et n'avaient pas de site Internet actif. En revanche, 25 % de ces noms de domaine disposaient d'un enregistrement MX et 8 % d'un certificat SSL.

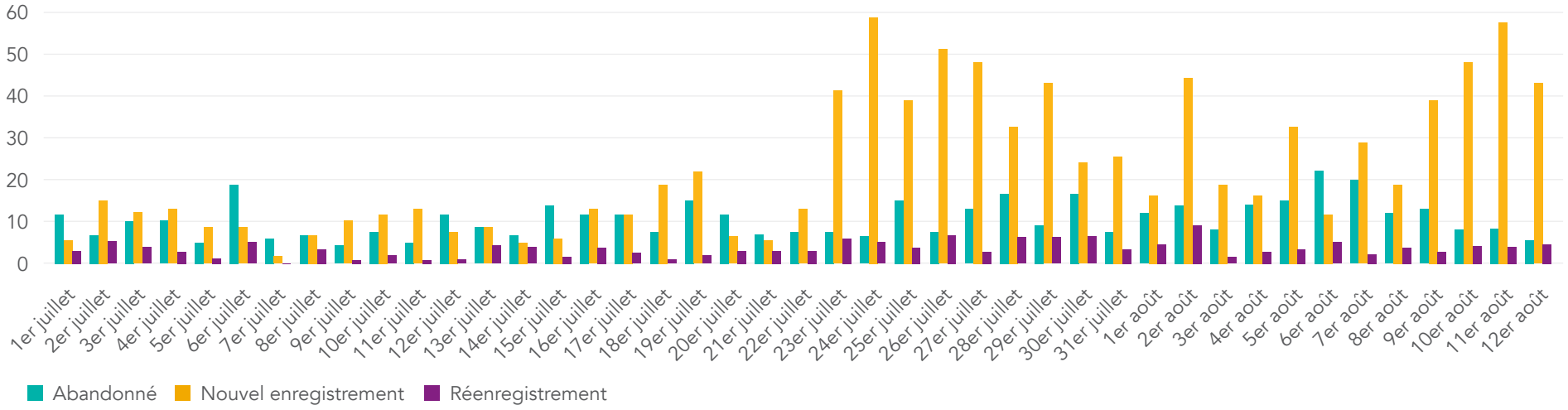


Figure 10 : Tendances des enregistrements de noms de domaines entre le 1er juillet 2024 et le 1er août 2024 (60 jours)

POINT À RETENIR

La surveillance continue en temps réel de ces noms de domaine est cruciale, car l'exploitation des noms de domaine dormants peut survenir à n'importe quel moment. En suivant les noms de domaine malveillants, les organisations peuvent mieux identifier les facteurs de risque potentiels avant qu'ils ne deviennent actifs.

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 la stratégie de cybersécurité, la protection des données, la sécurité des consommateurs, la propriété intellectuelle, les chaînes logistiques, le chiffre d'affaires et la réputation des entreprises.

Si les entreprises n'ont pas déjà mis en place des mesures de protection, elles doivent effectuer des recherches dans l'ensemble de l'écosystème mondial des noms de domaine, y compris les noms de domaine génériques de premier niveau et les noms de domaine de premier niveau des codes de pays. Les services de surveillance avancés tels que la solution 3D Domain Security and Enforcement de CSC permettent de détecter un éventail plus large de variations de noms de domaine au-delà des correspondances exactes de base, des caractères génériques et des fautes de frappe. De plus, les entreprises doivent s'associer à un fournisseur capable de neutraliser diverses menaces, notamment les sites d'hameçonnage, les téléchargeurs de maliciels, les domaines de typosquattage, les sites de référencement trompeurs, les portails de médias sociaux, les boutiques d'applications mobiles et les places de marché vendant des produits contrefaits.

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.

CSC est le partenaire de confiance des entreprises du classement Forbes Global 2000 (Interbrand®) et 100 Best Global Brands en matière de sécurité et de veille sur les menaces et propose des solutions de gestion de la sécurité des domaines et, de protection des marques en ligne et contre la fraude. Les entreprises internationales investissent considérablement dans leur stratégie de sécurité. C'est la raison pour laquelle notre plateforme DomainSec℠ peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leur marque en ligne. En s'appuyant sur la technologie exclusive 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 catastrophiques et les atteintes à la réputation de leur marque. CSC propose également une protection de la marque en ligne (une combinaison de la surveillance de la marque en ligne et des activités de mise en œuvre) et une vue multidimensionnelle des différentes menaces à l'extérieur du pare-feu ciblant des noms de domaine spécifiques. Des services de protection contre la fraude, qui luttent contre l'hameçonnage dès les premiers stades de l'attaque, viennent compléter nos solutions. 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.

Contactez-nous

cscdbs.com/fr

[1]npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-ransomware-health-care-federal-response

[2]tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024

DBS10222024