
CSC
Rapport 2026 sur la sécurité des noms de domaine

Introduction

Pour la sixième année consécutive, CSC a passé en revue le niveau de sécurité des noms de domaine en évaluant la stratégie de sécurité des entreprises figurant dans le classement Forbes Global 2000. 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 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 comparé les pratiques en matière de sécurité des noms de domaine des entreprises du Global 2000 à celles des 100 premières licornes mondiales. Bien qu'il existe certaines similitudes, l'une de nos principales interrogations était de savoir si ces jeunes entreprises, dont beaucoup évoluent dans les secteurs de la technologie et de l'IA, avaient adopté une approche plus stricte en matière de sécurité des noms de domaine. Ce rapport présente nos conclusions.

Avec la recrudescence des cyberattaques contre les multinationales telles que celles du Global 2000, CSC continue de sensibiliser ses clients aux enjeux liés à la sécurité des noms de domaine. Les menaces peuvent survenir à tous les niveaux de l'infrastructure informatique d'une entreprise, même si la plupart des attaques exploitent un nom de domaine pour infiltrer les systèmes. Plus que jamais, il est essentiel de vous assurer de disposer d'une stratégie de sécurité solide.

Résumé des principales conclusions

Les licornes appliquent rigoureusement les mesures de sécurité essentielles des noms de domaine relatives aux enregistrements DNS, mais accusent un retard dans d'autres secteurs, ce qui risque de constituer un danger à mesure qu'elles gagnent en maturité

En ce qui concerne les mesures de sécurité des noms de domaine qui s'appuient sur les enregistrements du système de noms de domaine (DNS), telles que l'authentification, le rapport et la conformité des messages basés sur le nom de domaine (DMARC), le cadre de politique de l'expéditeur (SPF), la messagerie identifiée par DomainKeys (DKIM), les extensions de sécurité DNS (DNSSEC) et les enregistrements d'autorisation de l'autorité de certification (CAA), nous avons observé une adhésion plus importante parmi les licornes, avec un taux d'utilisation atteignant même 100 % pour le SPF dans leurs protocoles d'authentification des e-mails. Pourtant, seulement 1 % d'entre elles utilisent la redondance DNS et près de 90 % des licornes reposent sur une infrastructure unique dans le cloud.

Les licornes ont adopté cinq des huit mesures de sécurité des noms de domaines dans une proportion plus élevée que les entreprises du Global 2000

Les licornes ont davantage mis en œuvre les mesures liées aux enregistrements DNS que les entreprises du Global 2000, notamment les protocoles DMARC (96,0 % contre 79,8 %), DNSSEC (16,8 % contre 10,8 %) et les enregistrements CAA (33,0 % contre 11,4 %). Cela semble indiquer que les équipes qui gèrent les noms de domaine des licornes sont probablement composées de professionnels de l'informatique maîtrisant les protocoles de sécurité disponibles dans le DNS, dont le coût pour l'entreprise est relativement faible. Il s'agit là d'une tendance encourageante pour les entreprises qui stimulent l'innovation (technologique) et que les plus matures pourraient imiter.

La disparité dans le recours au verrou de registre entre les entreprises du Global 2000 utilisant des registrars corporate et celles utilisant des registrars grand public est plus de 6 fois supérieure

Les verrous de registre constituent l'une des défenses les plus efficaces contre le détournement, car ils empêchent toute modification non autorisée de vos noms de domaine et de votre DNS, même si votre compte de registrar est compromis. En raison des ressources nécessaires pour prendre en charge ce service, la plupart des registrars grand public ne sont pas en mesure de le proposer, comme le confirment les données selon lesquelles les entreprises qui utilisent des registrars corporate affichent un taux d'adoption six fois supérieur et des mesures de sécurité plus strictes. Nous avons également constaté dans notre récent rapport intitulé « Le paysage du SSL» que 60 % des grandes entreprises utilisaient au moins trois fournisseurs SSL (Secure Sockets Layer), augmentant ainsi leur niveau de risque. Les fournisseurs corporate permettent aux entreprises de mieux maîtriser leur environnement numérique et de garantir que leur chaîne d'approvisionnement bénéficie du même niveau de sécurité élevé, car nous avons pu constater à quel point cela a causé des dommages aux entreprises au cours de l'année écoulée.[1]

La région APAC a enregistré la plus forte croissance entre 2024 et 2025, mais reste à la traîne derrière la région EMEA et le continent américain en termes d'adoption globale

Les deux ont progressé de cinq places respectivement au cours de l'année dernière. La croissance rapide de ces deux secteurs, alimentée par l'essor de l'intelligence artificielle (IA) et des technologies financières (FinTech), associée à des exigences plus strictes en matière de cybersécurité, pourrait expliquer l'amélioration des mesures de sécurité observée.

Les secteurs des semi-conducteurs et des services bancaires affichent la plus forte hausse des scores globaux au cours de l'année écoulée

Les deux ont progressé de cinq places respectivement au cours de l'année dernière. La croissance rapide de ces deux secteurs, alimentée par l'essor de l'intelligence artificielle (IA) et des technologies financières (FinTech), associée à des exigences plus strictes en matière de cybersécurité, pourrait expliquer l'amélioration des mesures de sécurité observée.

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.

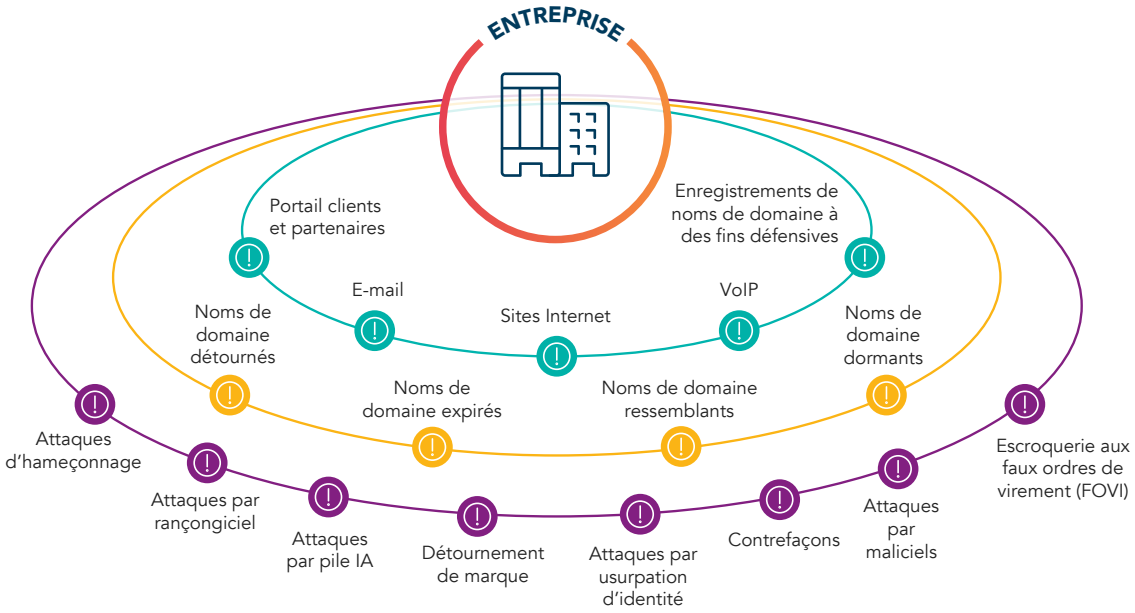
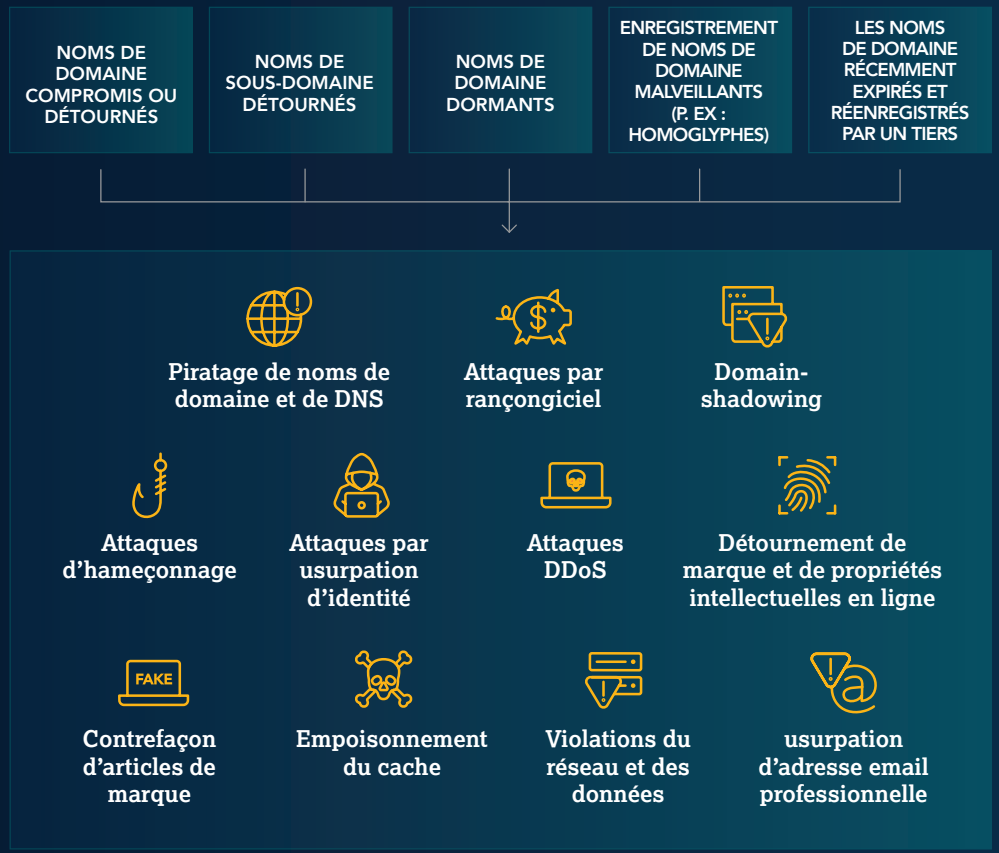


Figure 1: La galaxie de l'écosystème des noms de domaine

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 fournisseurs, ainsi que la gestion de leurs chaînes d'approvisionnement. Internet 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 légitimes, 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 approfondie 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 dormants échappent souvent à la détection initiale, car ils ne présentent pas immédiatement les indicateurs caractéristiques d'un nom de domaine enregistré dans le but de lancer une attaque, par exemple un enregistrement MX (e-mail) actif, qui déclencherait généralement une alerte.

→ 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 noms de domaine de marques 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 le 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 (2020-2025)

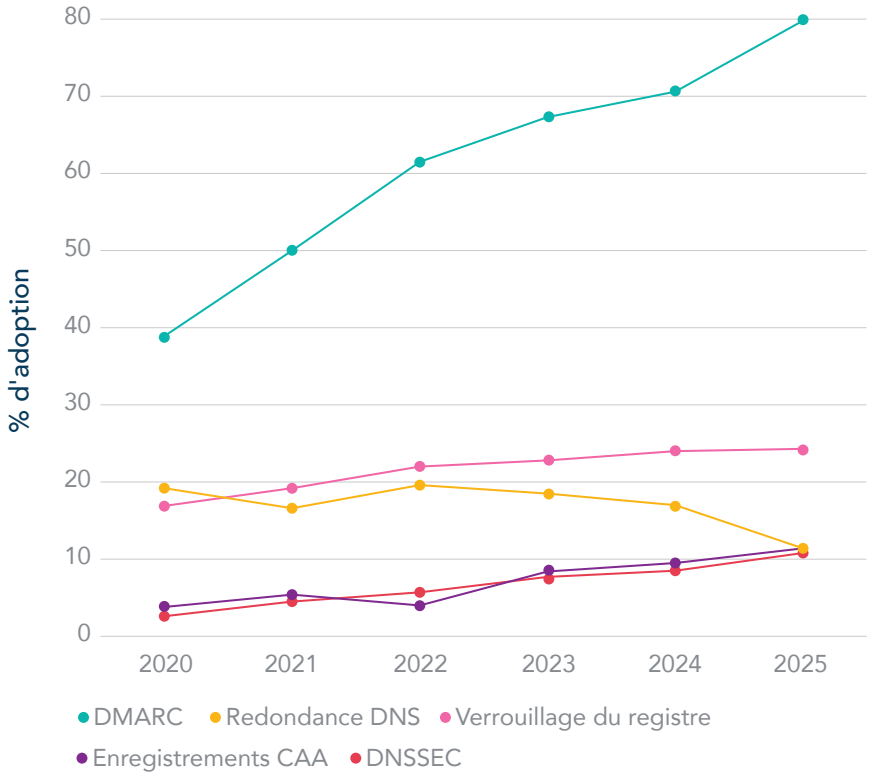


Figure 2: Adoption des cinq mesures clés de sécurité du nom de domaine par les entreprises du Global 2000 entre 2020 et 2025

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 80 % en 2025 (Figure 3). Nous avons également constaté une accélération de l'adoption du protocole DMARC en raison de l'entrée en vigueur de la directive NIS2 en octobre 2024, qui met davantage l'accent sur la cybersécurité pour les entreprises exerçant leurs activités au sein de l'Union européenne. Parmi les 20 % restants qui accusent encore un retard en matière d'adoption, 85 % proviennent de la région APAC, tous secteurs confondus, ce qui correspond à nos observations relatives à l'adoption par région.

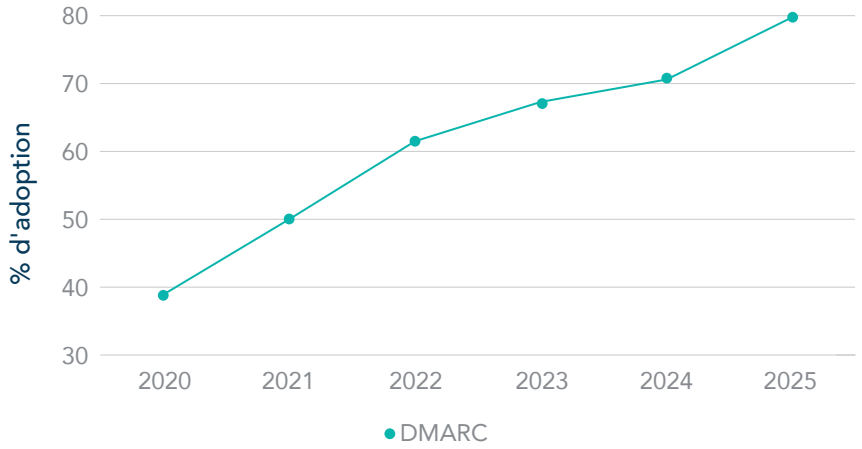


Figure 3 : Taux d'adoption du protocole DMARC entre 2020 et 2025

Qu'est-ce que la directive NIS2 ?

La directive NIS2 (Network and Information Security) est la nouvelle loi de l'Union européenne en matière de cybersécurité (directive (UE) 2022/2555) adoptée le 14 décembre 2022. Elle fixe des exigences plus strictes que les directives précédentes afin de garantir un niveau commun plus élevé de cybersécurité dans tous les États membres de l'UE. Cette directive définit les obligations, en particulier pour les entités essentielles relevant de la directive sur la résilience des entités essentielles (CER) (directive (UE) 2022/2557), notamment les entreprises des secteurs de l'énergie, des transports, de la santé, bancaire, financier, des infrastructures de commercialisation, des infrastructures numériques et de l'administration publique. Ces entreprises doivent prendre des mesures concrètes pour maîtriser les cyberrisques, protéger leurs systèmes, réagir rapidement aux incidents et se conformer aux stratégies nationales en matière de cybersécurité. Le signalement des incidents est obligatoire, tandis que le partage des renseignements sur les menaces est encouragé. Les organismes de réglementation sont également habilités à effectuer des audits, à faire respecter la conformité et à infliger des amendes aux entreprises en cas d'infraction.

Cette attention portée à la cybersécurité au niveau national trouve un écho dans les gouvernements du monde entier, qui ont également adopté des directives similaires pour les secteur clés dans leurs pays respectifs. En Australie par exemple, la Stratégie australienne en matière de cybersécurité 2023-2030, qui comprend une nouvelle loi sur la cybersécurité 2024, ainsi que des amendements à la loi sur la sécurité des infrastructures critiques (SOCI Act) qui impose des normes minimales de sécurité, introduit une obligation de signalement et clarifie les réglementations et obligations en matière de gestion des risques et de sécurité des données. Les entreprises qui opèrent à l'échelle internationale devront aligner leurs pratiques en matière de sécurité sur ces normes internationales de plus en plus strictes.

Déclin de la redondance DNS

La redondance DNS a légèrement diminué par rapport à l'année dernière, ce qui s'explique en partie par le changement de méthodologie de CSC au cours de l'année précédente, même si les données sous-jacentes montrent toujours une légère baisse. Il en a résulté une évolution globale de 6 % en glissement annuel, les entreprises accordant la priorité à la redondance DNS. Malgré l'importance de cette redondance pour l'infrastructure centrale de toute organisation, nous constatons que l'adoption de cette mesure de sécurité diminue, probablement parce que les entreprises doivent planifier l'augmentation de leurs coûts et l'allocation de leurs ressources en conséquence. De nombreuses entreprises se tournent également vers une infrastructure unique basée sur le cloud, pour réaliser des économies, bénéficier d'une meilleure évolutivité, d'une plus grande accessibilité des données, etc. D'une part, le cloud offre un système distribué à l'échelle mondiale, mais il présente toujours les mêmes risques potentiels si certaines parties du système sont mises hors ligne. La seule façon de vraiment réduire les risques liés au DNS, c'est de mettre en place deux réseaux indépendants et solides pour assurer la redondance (double infrastructure).

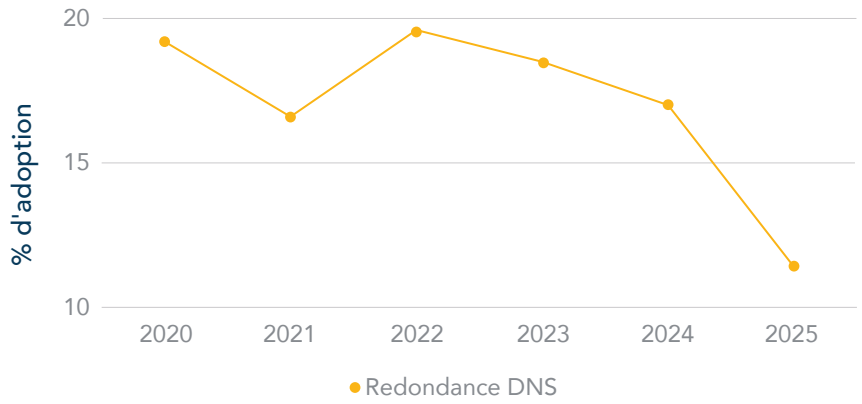


Figure 4 : Taux d'adoption de la redondance DNS entre 2020 et 2025

Regardez notre webinaire pour découvrir pourquoi le DNS est devenu le principal point de défaillance dans l'écosystème numérique actuel.

Des mesures de sécurité telles que le verrou de registre, le DNSSEC et les enregistrements CAA se développent constamment mais lentement

Le taux d'adoption des verrous de registre a légèrement augmenté pour atteindre 24 % en 2025. Nous avons également constaté que les entreprises utilisant des registrars corporate font aussi plus fréquemment appel aux verrous de registre (53 % en 2025). 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.

Comme le portefeuille de noms de domaine d'une entreprise est en constante évolution, 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. Avec l'essor de l'IA, nous continuons à préconiser une posture de sécurité solide de vos noms de domaine comme gage de confiance. Ce positionnement est particulièrement pertinent dans la mesure où la pile IA d'une entreprise utilisant des interfaces de programmation d'applications (API) et des plugins repose entièrement sur les noms de domaine et le DNS pour fonctionner.

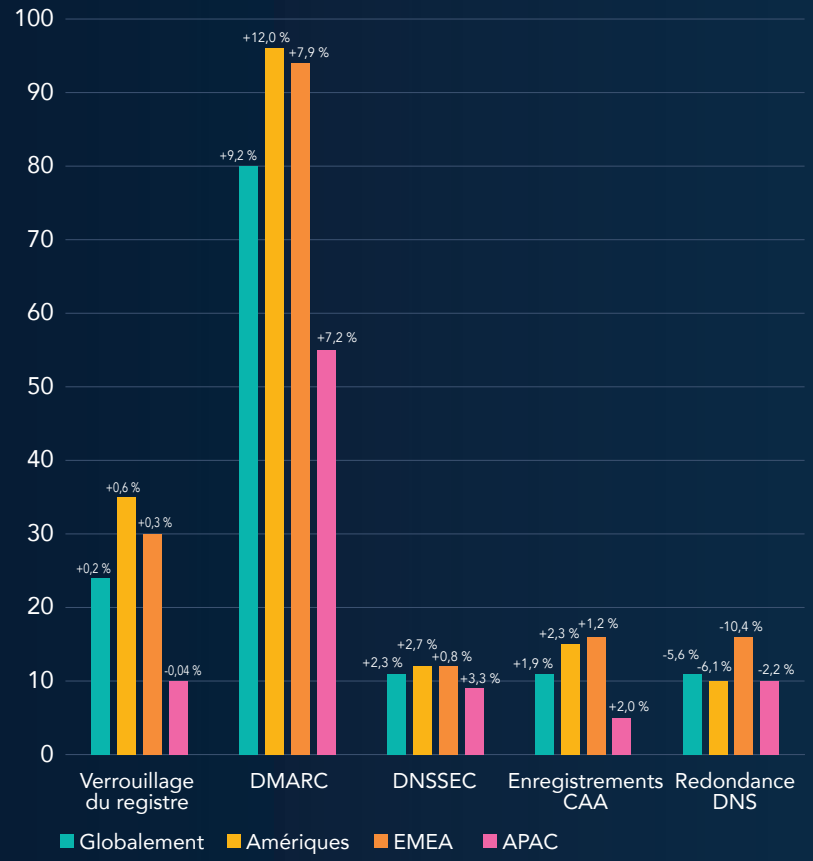
Bien qu'encore peu nombreuses, le pourcentage d'entreprises déployant des extensions de sécurité du système de noms de domaine (Domain Name System Security Extension, DNSSEC) a quadruplé ces six dernières années pour atteindre 11 % en 2025. Les extensions DNSSEC garantissent l'authentification et l'intégrité 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. Dans certains pays, l'adoption des extensions DNSSEC est supérieure à 67 %. Cependant, elle reste plus faible dans les grandes entreprises. Cela s'explique en partie par la nécessité de mettre à jour les clés dans une structure organisationnelle plus complexe, mais cela reste une mesure de sécurité que tous les noms de domaine stratégiques devraient adopter.

Enfin, l'utilisation des enregistrements CAA a encore augmenté pour atteindre 11 % en 2025. Les enregistrements CAA permettent aux entreprises de désigner une Autorité de certification (AC) spécifique en tant qu'émettrice 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. Les enregistrements CAA présentent l'avantage supplémentaire de permettre aux entreprises de garantir la conformité, afin que leur personnel n'utilise que des fournisseurs autorisés. Nous avons également constaté dans notre récent rapport intitulé « Le paysage du SSL », que plus de 60 % des grandes entreprises utilisaient plus de trois fournisseurs. L'une d'entre elles en utilisait même 13. Le rapport souligne également que les fournisseurs les plus utilisés par les sites Internet frauduleux sont également ceux qui sont les plus populaires. Une surveillance accrue de la gestion du protocole SSL est nécessaire, en particulier à mesure que les piles IA deviennent plus autonomes.

Fonctionnalités de la sécurité du nom de domaine

Par région

La région APAC a enregistré la plus forte croissance en matière d'adoption de sécurité des noms de domaine entre 2024 et 2025, mais reste à la traîne derrière la région EMEA et le continent américain en termes d'adoption globale.



+/- % par rapport à l'année précédente

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

Par secteur

Les logiciels et services informatiques demeurent le secteur le plus performant en 2025.

Classement sectoriel	Place en 2025	Place en 2024
Semi-conducteurs	6	11
Banque	11	16
Matériel et équipement technologique	13	5
Aérospatial et défense	16	8

Les secteurs les plus performants restent ceux qui dépendent fortement d'Internet pour leurs activités commerciales, tels que les logiciels et services informatiques et les médias. Nous avons également constaté que les secteurs bancaire et des semi-conducteurs continuaient de progresser au cours de l'année dernière. La croissance rapide de ces deux secteurs, alimentée par l'essor de l'intelligence artificielle (IA) et des technologies financières (FinTech), associée à des exigences plus strictes en matière de cybersécurité, pourrait expliquer l'amélioration des mesures de sécurité observée. Parmi les secteurs les moins performants, on retrouve toujours ceux de la construction, des mines et des services publics. Il est intéressant de noter que bon nombre des secteurs peu performants sont également considérés comme des secteurs sensibles, en particulier au sens de la directive NIS2. Cela pourrait se traduire, au cours de l'année à venir, par une prise en compte plus sérieuse de la sécurité des noms de domaine par ces secteurs, en particulier compte tenu de la recrudescence des attaques visant précisément ces secteurs.

↑ SECTEURS LES PLUS SÉCURISÉS

- Logiciels et services IT
- Médias
- Vente au détail
- Services et fournitures pour les entreprises
- Services de télécommunication

↓ SECTEURS LES MOINS SÉCURISÉS

- Construction
- Matériaux
- Marchés alimentaires
- Services publics
- Alimentation, boissons et tabac

Mesures de sécurisation des noms de domaine par type de registrar

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. Pour en savoir plus sur la manière dont l'utilisation d'un registrar corporate permet de réduire les risques de détournement de noms de domaine, de DNS dangling et d'usurpation de noms de domaine, téléchargez notre « Liste récapitulative sur la sécurité des noms de domaines. »

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. Bon nombre d'entre eux ne proposent pas de services de sécurité des noms de domaine, ce qui réduit également leur adoption.

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

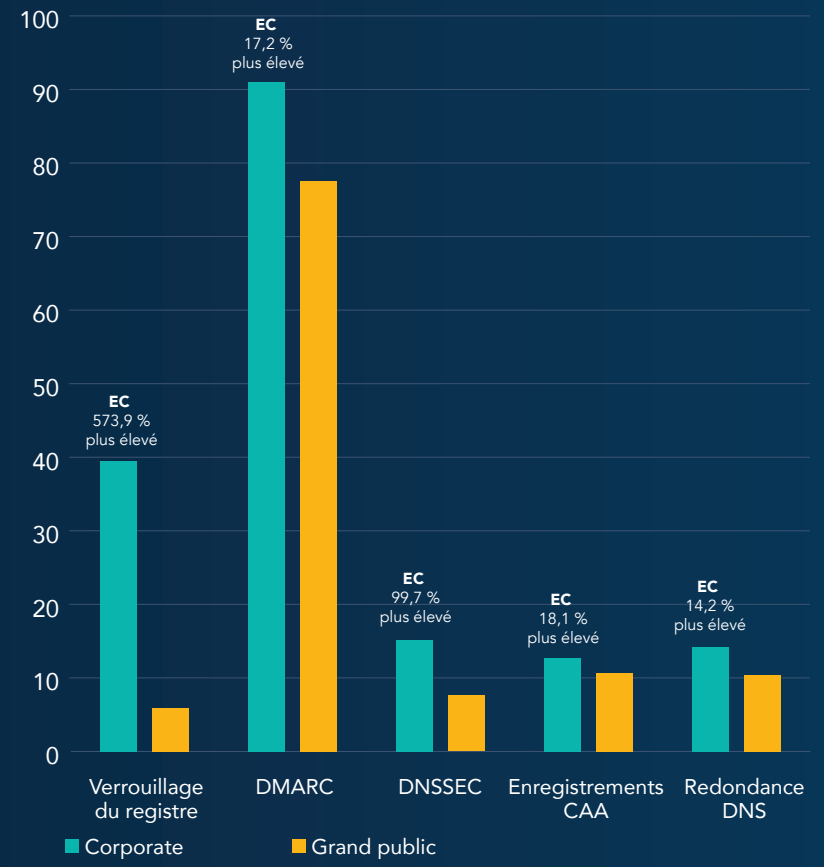


Figure 6 : Niveau de maturité des mesures de sécurité Registrars corporate (EC)/grand public (CG)

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 de noms de domaine corporate
- Verrouillage du registre (MultiLock)
- Enregistrements CAA
- Redondance DNS
- Norme DKIM (DomainKeys identified mail)
- Cadre SPF (Sender policy framework)
- DNSSEC
- DMARC

Niveau de risque de sécurité du nom de domaine

Nombre d'entreprises

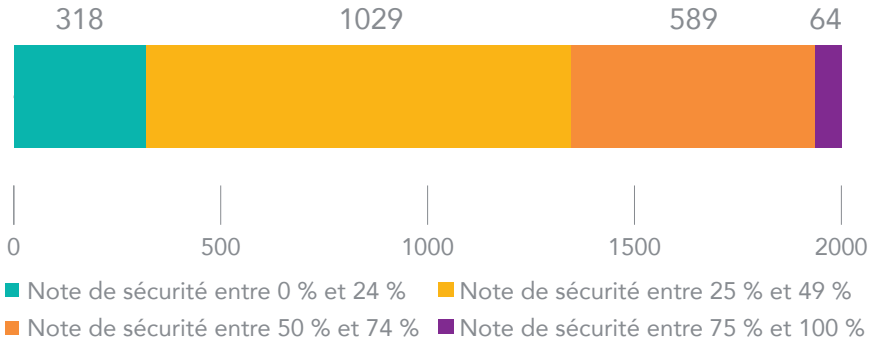


Figure 7 : notes de sécurité des noms de domaine et niveaux de risque associés pour les entreprises du Global 2000

> 67 % 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 obtenu une note de 100 % tout comme l'année dernière. Seules huit entreprises ont obtenu un score de sept sur huit, soit un tiers de moins que l'année dernière.

↓ ENTREPRISES LES MOINS SÉCURISÉES

Quatre-vingt-sept entreprises ont obtenu un score de sécurité de noms de domaine égal à zéro, soit une amélioration par rapport aux 107 entreprises concernées l'année dernière. 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.

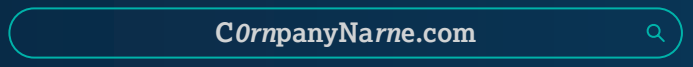
NOUS NOUS SOMMES VOLONTAIREMENT CONCENTRÉS SUR LES HOMOGLYPHES, CAR ILS CONSTITUENT L'UNE DES MÉTHODES D'ATTAQUE LES PLUS RÉPANDUES UTILISÉES PAR LES CYBERCRIMINELS.

Tactiques d'usurpation de noms de domaine

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

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 l'hameçonnage, notre analyse a porté sur les substitutions courantes de caractères latins, par exemple l'utilisation de N0rnD'Entreprise.com au lieu de NomD'Entreprise.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) dans les noms de domaine .com

88 % DES NOMS DE DOMAINE HOMOGLYPHES SONT DÉTENUS PAR DES TIERS

Parmi les noms de domaine détenus par des tiers :

40 % ont des enregistrements MX en 2025 contre 42 % en 2024. Les enregistrements MX (messagerie) permettent d'envoyer des e-mails de phishing ou d'intercepter des e-mails. C'est l'une des principales raisons de l'augmentation du nombre d'enregistrements DMARC ajoutés.

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

40 % redirigent les internautes vers du contenu publicitaire ou des liens sponsorisés, ou sont utilisés pour les services de parking de noms de domaine.

39 % ont des sites Internet inactifs..

32 % de tous les noms de domaine inactifs possèdent des enregistrements de messagerie actifs, ce qui signifie que même les noms de domaine qui ne renvoient pas vers du contenu actif peuvent toujours être utilisés à des fins de messagerie électronique.

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.

19 % aboutissent à un site Internet actif qui n'a aucun lien avec le propriétaire de la marque.

L'un des aspects dont les entreprises doivent être conscientes est l'utilisation de noms de domaine dormants, où des tiers procèdent à des enregistrements massifs et maintiennent les noms dormants parfois pendant une longue période. Comme le montrent les résultats, 32 % des domaines tiers sont inactifs, mais contiennent des enregistrements MX, qui pourraient facilement être activés.

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	16,3 %
Logiciels et services IT	6,6 %
Services financiers diversifiés	5,8 %
Services publics	5,4 %
Assurance	5,4 %
Construction	5.2%
Opérations pétrolières et gazières	5,1 %
Services et fournitures pour les entreprises	4,3 %
Biens d'équipement	4,3 %
Transport	4,3 %
Biens de consommation durables	4,0 %
Vente au détail	3,6 %
Matériel et équipement technologique	3,6 %
Matériaux	3,5 %
Alimentation, boissons et tabac	2,8 %
Services de télécommunication	2,7 %
Médicaments et biotechnologie	2,4 %
Équipement et services en matière de soins de santé	2,4 %
Semi-conducteurs	2,3 %
Aérospatial et défense	1,9 %
Sociétés commerciales	1,7 %
Produits chimiques	1,7 %
Marchés alimentaires	1,5 %
Hôtellerie, restauration et loisirs	1,3 %
Articles ménagers et personnels	1,0 %
Médias	0,9 %

Perspectives en matière de sécurité des noms de domaine : les licornes sont-elles les défenderesses rêvées de la sécurité des noms de domaine ?

CSC a décidé cette année de comparer les entreprises du Global 2000, dont beaucoup évoluent dans des secteurs établis de longue date, aux 100 premières licornes. La majorité des entreprises figurant dans le classement des 100 premières licornes sont des sociétés informatiques, dont beaucoup appartiennent au secteur de l'IA. Pour simplifier les choses, nous avons examiné les mêmes caractéristiques de sécurité des noms de domaine pour ces entreprises que pour celles du Global 2000. Notre objectif principal dans cette analyse était de déterminer si les petites start-ups sont plus sensibles aux risques liés à la sécurité des noms de domaine et ont la capacité de mettre en œuvre des mesures de sécurité, comparativement aux grandes entreprises bien établies. La plupart des licornes du secteur de l'IA sont conscientes de la nécessité de mettre en place des protocoles de sécurité concernant leurs infrastructures sensibles (noms de domaine et DNS) et ont largement adopté ces protocoles dans certains secteurs, mais pas dans d'autres. De plus, la pile IA que bon nombre de ces entreprises sont en train de mettre en place contribuera à accroître les risques dans la chaîne d'approvisionnement des entreprises qui y ont recours.

Qu'est-ce qu'une licorne ?

Une licorne est une entreprise privée dont la valeur est estimée à plus d'un milliard de dollars. Il s'agit généralement de start-ups ou d'entreprises relativement récentes, souvent innovantes dans leur secteur d'activité.

Faits marquants

Figure 10 : Adoption de la sécurité des noms de domaine : Les 100 premières licornes comparées aux entreprises du Global 2000

Par rapport aux entreprises du Global 2000, sur huit attributs de sécurité des noms de domaine, les licornes obtiennent un score plus élevé dans cinq catégories. Les domaines clés dans lesquels elles sont plus performantes sont la sécurité des e-mails, avec une adoption plus importante des protocoles SPF, DKIM et DMARC, ainsi que des enregistrements DNSSEC et CAA. Le point commun entre tous ces éléments est qu'ils sont gérés via des enregistrements DNS. Cela semble indiquer que les équipes qui gèrent les noms de domaine des licornes sont probablement composées de professionnels de l'informatique maîtrisant les protocoles de sécurité disponibles dans le DNS, dont le coût pour l'entreprise est relativement faible.

La différence entre les entreprises du Global 2000 adoptant une approche plus stricte en matière de sécurité commence avant tout par le fait qu'elles sont plus nombreuses à utiliser un registrar corporate. Pourquoi est-ce important ? Les registrars corporate ont mis en place des mesures de sécurité rigoureuses, telles que la formation du personnel à la lutte contre l'ingénierie sociale et l'authentification à deux facteurs. Les entreprises qui utilisent des registrars grand public ont été confrontées à des situations telles que le « doppleganging de domaine », où des comptes sont piratés et des sous-domaines sont créés à partir de noms de domaine légitimes.

Autre différence : les verrous de registre ont été moins utilisés, car de nombreux registrars grand public ne proposent pas ce service. Étant donné que les entreprises du Global 2000 utilisent des registrars corporate, les chances d'adoption du verrou de registre s'en trouvent accrues.

Dans la mesure où les licornes en sont encore à leurs débuts et se concentrent sur la croissance du marché, le choix du registrar pourrait ne pas figurer parmi leurs priorités commerciales ou elles pourraient ne pas connaître les différences entre les registrars et leur impact sur leur sécurité. La nature du registrar a une influence directe sur l'adoption et la sécurité des verrous de registre. Ces verrous ne sont pas pris en charge par les registrars grand public, ce qui rend les licornes vulnérables à des attaques telles que le détournement de DNS, le détournement de noms de domaine, l'usurpation d'adresse e-mail, etc., lorsque leur registrar est plus facilement compromis sans niveaux de défense supplémentaires. Même avec une équipe informatique expérimentée et maîtrisant les bases du protocole DNS, à mesure que les licornes développent leurs activités avec des portefeuilles de noms de domaine plus volumineux et plus complexes, un manque de vigilance concernant la sécurité de leurs noms de domaine confiés à un registrar tiers peut comporter des risques considérables, car tout incident ou interruption de service a un impact direct sur la plupart de ces entreprises opèrant en ligne.

L'IA et la technologie dominent

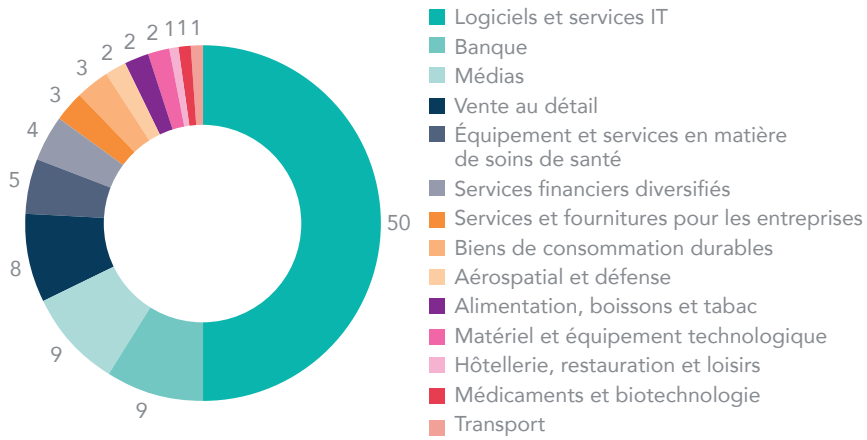


Figure 11 : Représentation sectorielle parmi les 100 premières licornes

La moitié des entreprises figurant dans le classement des 100 premières licornes sont des prestataires de services informatiques, suivies par des entreprises du secteur bancaire, occupant la deuxième place. De nombreuses entreprises spécialisées dans les services informatiques sont des sociétés exclusivement axées sur l'IA et la plupart des entreprises du secteur bancaire sont des start-ups FinTech (technologie financière). Dans les deux cas, elles dépendent fortement d'Internet pour mener à bien leurs activités.

Qui est le plus en sécurité ?

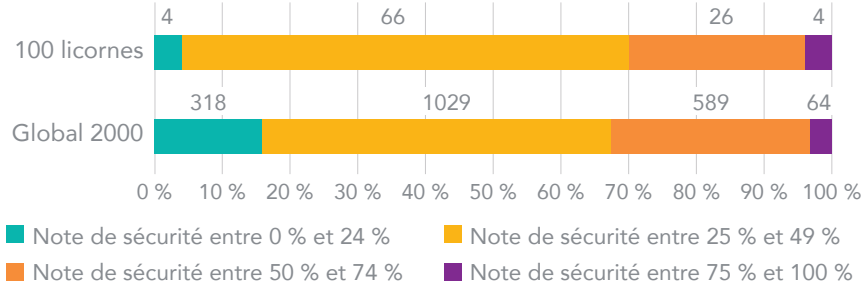


Figure 12 : Niveaux de sécurité des noms de domaine : Les 100 premières licornes comparées aux entreprises du Global 2000

La comparaison entre les scores de risque des noms de domaine des entreprises du Global 2000 et ceux des licornes ne révèle pas de différences significatives. Il est évident que moins de licornes (4 %) se situent dans la fourchette des scores faibles, contre 15 % parmi les entreprises du Global 2000. Cependant, un nombre nettement plus important de licornes se situe dans la moyenne, preuve qu'elles accordent une grande importance à certains éléments, tels que la sécurité des e-mails, mais qu'elles ne disposent pas de certains protocoles de sécurité parmi les plus avancés, tels que le verrou de registre et la redondance DNS.

Conclusion

Les entreprises continuent de renforcer progressivement la sécurité de leurs noms de domaine. Toutefois, les plus grandes entreprises internationales ont encore beaucoup à faire pour améliorer leur système de sécurité. Nous pensons que les interventions gouvernementales via des législations telles que la directive NIS2 inciteront davantage à accélérer ces changements, d'autant plus que nous assistons à une augmentation constante des cyberattaques contre les multinationales.

Les licornes ont rapidement adopté des protocoles de sécurité des noms de domaine axés sur la sécurité DNS, souvent sous l'impulsion d'une sous-direction de services informatiques plus petite et plus agile, capable de prendre des décisions rapides, loin des complexités d'une entreprise dispersée à l'échelle mondiale. Cela dit, elles ont tendance à présenter des lacunes dans certains domaines tels que la redondance DNS, les verrous de registre et les registrars corporate, ce qui pourrait toutefois changer à mesure que l'entreprise mûrit et que les fournisseurs auxquels elle fait appel gagnent en sophistication. À terme, les licornes devront veiller à renforcer la sécurité de leur propre nom de domaine, celle de leur chaîne d'approvisionnement, ainsi que celle de la chaîne d'approvisionnement dans laquelle elles s'inscrivent. Il faudra peut-être qu'un incident majeur se produise ou qu'une intervention gouvernementale ait lieu pour susciter un sentiment d'urgence, malgré la place grandissante occupée par l'IA, secteur dans lequel évoluent de nombreuses licornes, démontrant ainsi que la sécurité est primordiale au développement de leurs activités.

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 ne prennent pas au sérieux la sécurité de leurs noms de domaine, cela peut conduire à leur exploitation par des tiers. Face à l'évolution constante des systèmes géopolitiques, à la sophistication croissante des cybercriminels et à l'introduction de l'IA dans les campagnes cybermalveillantes, nous devons collectivement veiller à devenir des cibles difficiles à atteindre.

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.

Téléchargez 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 leurs marques 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 leurs marques. 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]cnbc.com/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html

DBS19122025