SÉCURITÉ DU NOM DE DOMAINE ET CONTRAINTES DE LA CHAÎNE D'APPROVISIONNEMENT

cscdbs.com/fr

Résumé

Une nouvelle étude de CSC montre que les fraudeurs ont tiré parti de la pénurie de lait maternisé de 2022 pour cibler les consommateurs avec de faux noms de domaine de marque. Les principaux résultats montrent une recrudescence des enregistrements de noms de domaine liés au lait maternisé, qui exploitent des marques de confiance pour orienter les consommateurs. **84 %** de ces noms de domaine web ont été créés depuis 2021 et sont abusifs, c'est-à-dire qu'ils appartiennent à des tiers autres que le titulaire de marque. Il s'agit potentiellement d'un réel problème pour les consommateurs en termes de sécurité des produits, d'attaques de phishing, de difficultés financières et d'exfiltration de données, ainsi que pour les entreprises propriétaires de ces marques. Outre le marché des laits maternisés, on observe le même type d'enregistrements abusifs de noms de domaine imitant des fabricants de puces dans l'industrie des semi-conducteurs. **95 %** des noms de domaine créés depuis 2021 appartiennent à des tiers autres que le titulaire de marque.

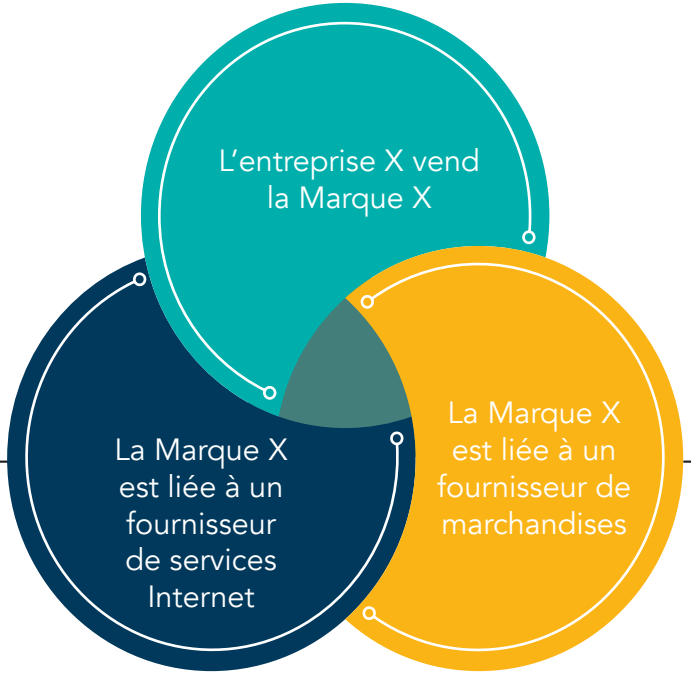
Enfin, un nombre important d'entreprises n'appliquent pas de bonnes pratiques en matière de sécurité du nom de domaine, ce qui augmente leur exposition au risque et illustre l'ampleur du problème dans les secteurs des infrastructures critiques. En cas d'attaque à grande échelle (piratage de DNS ou attaque DDoS) contre un fournisseur de services cloud ou un registrar de noms de domaine, d'attaque d'ingénierie sociale ou de phishing, les bonnes pratiques de sécurité du nom de domaine peuvent renforcer la résilience d'une entreprise face à ces risques.

Le lien entre la sécurité du nom de domaine et la chaîne d'approvisionnement

Ces deux dernières années ont amené des pénuries d'approvisionnement pour des articles dont la disponibilité nous a toujours semblé aller de soi. Les équipes de direction des entreprises s'interrogent : « Que devrions-nous savoir, que nous ignorons ? » Un facteur de risque important pour les entreprises continue pourtant d'être ignoré : la sécurité des enregistrements de noms de domaine web de la marque.

Comme on a pu le voir dans les récentes attaques de la chaîne logistique, telles que l'attaque qui a ciblé **Colonial Pipeline** et celle qui a touché **JBS Foods**, une attaque visant une entreprise via un seul point de défaillance a le potentiel de perturber un réseau entier d'entreprises ainsi que les produits, partenaires, fournisseurs et clients qui y sont associés, et peut fournir une source de revenus exponentielle à l'attaquant. En raison des interconnexions entre les noms de domaine et les DNS, une seule compromission au niveau d'un registrar de noms de domaine ou d'un fournisseur de services cloud, ou encore une attaque de phishing utilisant un nom de domaine abusif peut s'étendre au-delà de la chaîne d'approvisionnement Internet pour toucher les chaînes logistiques des produits et des infrastructures.

La fraude en ligne inclut des enregistrements de noms de domaine frauduleux et des attaques ciblant les fournisseurs de services cloud, les registrars de noms de domaine et les fournisseurs d'hébergement DNS.



Exemple :

La pénurie de lait maternisé est un problème de marque hors ligne amplifié par les risques en termes de cyber-sécurité.

La nouvelle étude de CSC montre que le risque augmente pour les entreprises et les consommateurs confrontés à des pénuries dans la chaîne d'approvisionnement

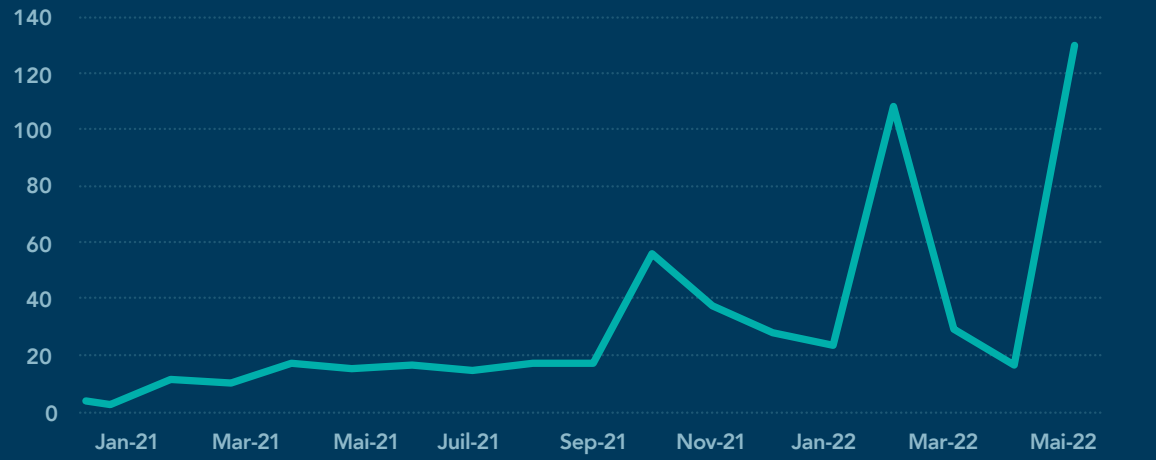
Les noms de domaine frauduleux sont l'épicentre de la fraude en ligne, ce qui peut entraîner une perte de revenus, des atteintes à la réputation, un danger pour la sécurité des consommateurs et des problèmes supplémentaires de cyber-sécurité pour les titulaires de marques. CSC a observé que les cas d'enregistrements de noms de domaine augmentent parallèlement aux événements mondiaux et sociétaux – pénuries dans la chaîne d'approvisionnement – dont ils tentent de tirer profit. En janvier 2022, CSC a publié une **étude sur l'augmentation du nombre de noms de domaine frauduleux liés au Covid**, qui montrait dans quelle mesure les cybercriminels profitaient des marques associées à la vaccination ou aux organisations sanitaires, selon le même schéma.

L'équipe de recherche CSC a évalué les noms de domaine contenant les noms de marque de laits maternisés et de semi-conducteurs. Conformément aux recherches précédentes, on constate une augmentation des enregistrements abusifs de noms de domaine entre 2021 et mai 2022.

Principales conclusions : Pénurie de lait maternisé

CSC a passé en revue les noms de domaine contenant les noms des cinq principales marques de lait maternisé ou d'autres termes de recherche pertinents tels que « baby milk » (lait pour bébé), « baby formula » (lait maternisé) et « baby feed » (aliments pour bébé).

Nombre mensuel d'enregistrements de noms de domaine tiers liés aux laits maternisés (marques ou mots clés)



84 %

des noms de domaine sont détenus par des tiers.*

**Selon notre définition des domaines tiers, ils n'appartiennent pas aux titulaires de marques et sont frauduleux.*

93 % ont utilisé des services de protection de la confidentialité des noms de domaine, ou ont également expurgé leurs informations dans la base de données WHOIS afin d'exclure tout détail révélateur.

Cela démontre leur tentative de masquer ou de dissimuler leur titre de propriété ou leur identité, et illustre le caractère malveillant de leurs intentions.

26 % sont configurés avec des enregistrements MX (messagerie).

Les noms de domaine configurés avec des enregistrements MX (messagerie) permettent d'envoyer des e-mails de phishing ou d'intercepter des e-mails.

Les registrars de noms de domaine les plus associés aux enregistrements abusifs dans l'analyse :

- GoDaddy.com, LLC
- Sav.com, LLC
- Chengdu West Dimension Digital Technology Co., Ltd

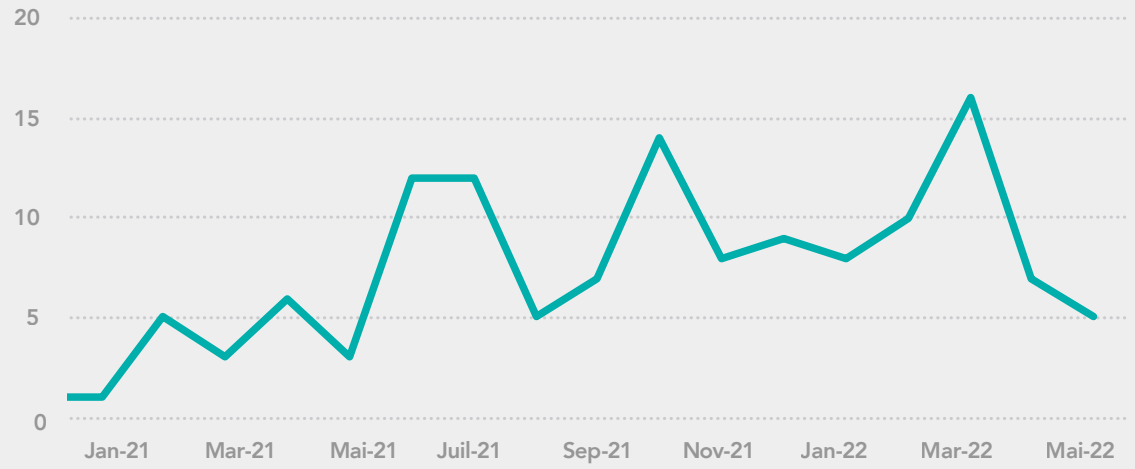
Les noms de domaine d'hébergement DNS les plus associés aux enregistrements abusifs dans l'analyse :

- domaincontrol.com (fournisseur : GoDaddy)
- bodis.com (fournisseur : Bodis)
- registrar-servers.com (fournisseur : NameCheap)

Principales conclusions : Pénurie de semi-conducteurs

CSC a examiné les noms de domaine contenant les noms des six principales marques de semi-conducteurs ou d'autres termes de recherche pertinents tels que « semiconductor chip » (puce à semi-conducteurs) et « electronic chip » (puce électronique).

Nombre mensuel d'enregistrements de noms de domaine tiers liés aux puces à semi-conducteurs (marques ou mots clés)



95 %

des noms de domaine sont détenus par des tiers.*

**Selon notre définition des domaines tiers, ils n'appartiennent pas aux titulaires de marques et sont frauduleux.*

79 % **ont utilisé des services de protection de la confidentialité des noms de domaine, ou ont également expurgé leurs informations dans la base de données WHOIS afin d'exclure tout détail révélateur.**

Cela démontre leur tentative de masquer ou de dissimuler leur titre de propriété ou leur identité, et illustre le caractère malveillant de leurs intentions.

44 % **sont configurés avec des enregistrements MX (messagerie).**

Les noms de domaine configurés avec des enregistrements MX (messagerie) permettent d'envoyer des e-mails de phishing ou d'intercepter des e-mails.

Les registrars de noms de domaine les plus associés aux enregistrements abusifs dans l'analyse :

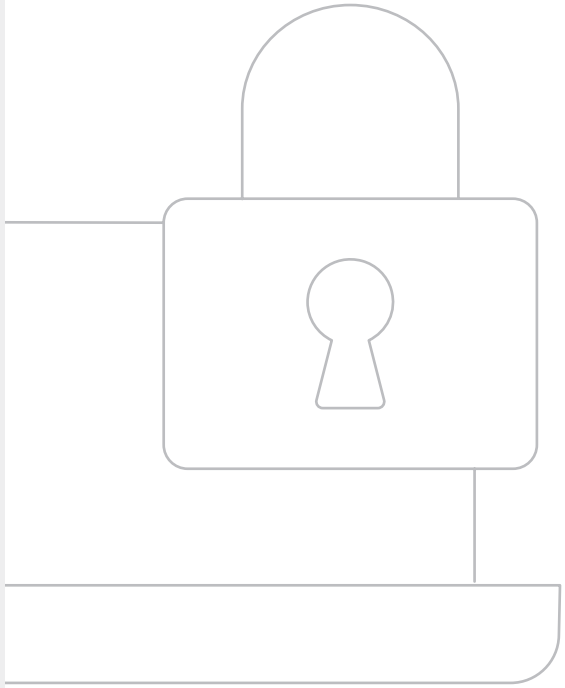
- GoDaddy.com, LLC
- Namecheap Inc.
- Dynadot LLC

Les noms de domaine d'hébergement DNS les plus associés aux enregistrements abusifs dans l'analyse :

- domaincontrol.com (fournisseur : GoDaddy)
- registrar-servers.com (fournisseur : NameCheap)
- hichina.com (fournisseur : Alibaba)

Bonnes pratiques cyber et sécurité du nom de domaine

En matière de sécurité du nom de domaine, outre la protection de votre entreprise contre les enregistrements abusifs de noms, vous devez impérativement être proactif et mettre en place des contrôles de sécurité essentiels dans le cadre des **bonnes pratiques de sécurité des noms de domaine**. CSC recommande d'adopter une **approche Défense en profondeur (DiD)**, en intégrant les mesures de sécurité avancées suivantes :



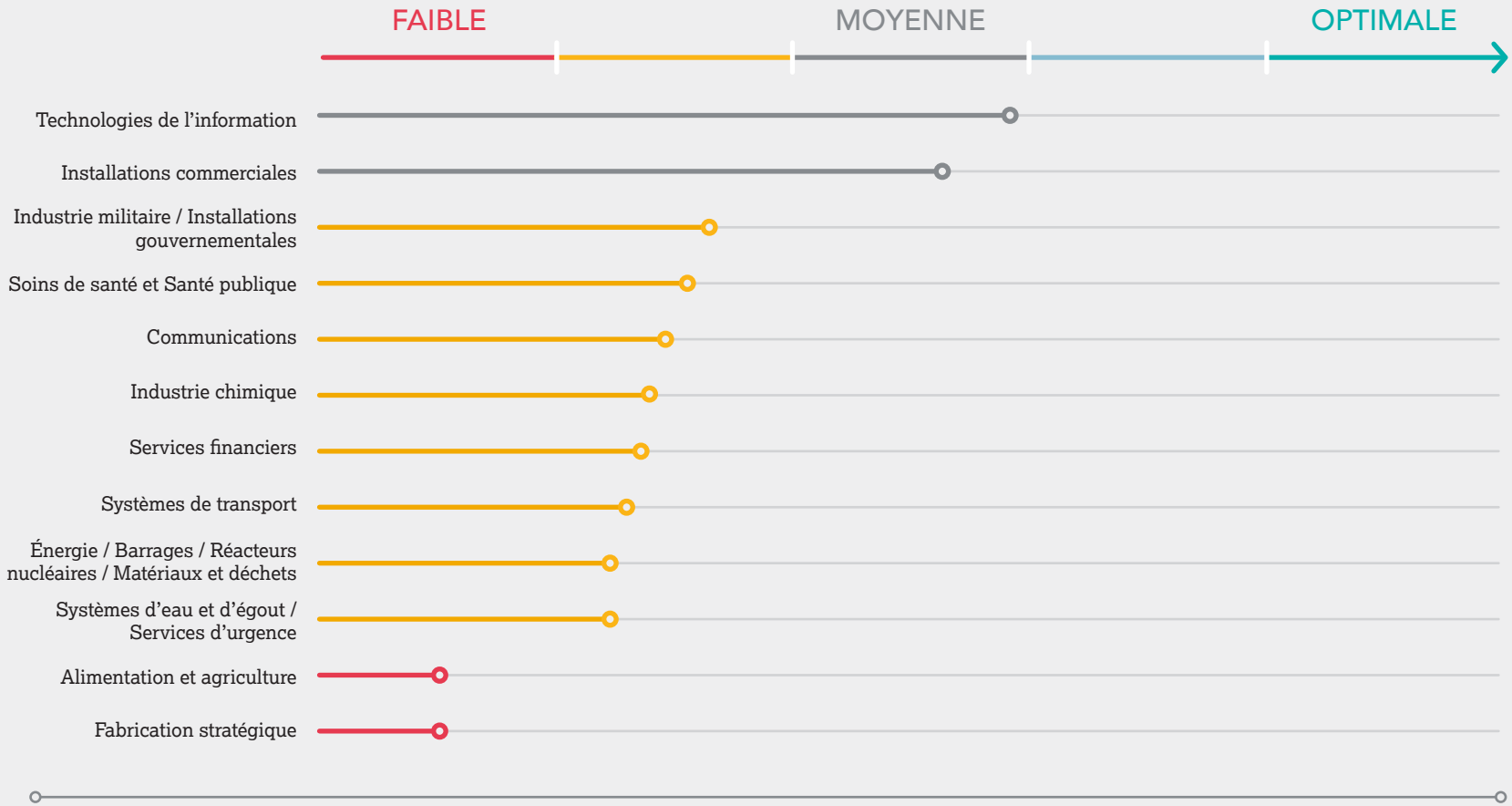
Étude CSC sur les bonnes pratiques de sécurité du nom de domaine

Mesure de sécurité du nom de domaine	But
Redondance de l'hébergement DNS	Protège contre les interruptions des services et les attaques DDoS.
DNSSEC (Domain Name System Security Extension)	Empêche les hackers de prendre le contrôle d'une session de navigation Internet pour rediriger les utilisateurs vers de faux sites Web.
SPF (Sender Policy Framework)	Les normes d'authentification par e-mail limitent le spam, le spoofing et le phishing.
DMARC (Domain-based Message Authentication, Reporting, and Conformance)	
DKIM (Domain Keys Identified Mail)	
MultiLock	Combine des verrous au niveau du registre et du registrar, ainsi qu'un verrou WHOIS afin d'empêcher les modifications non autorisées des enregistrements DNS et le détournement de nom de domaine.
Enregistrements CAA (Certification Authority Authorization)	Permet de garantir que seules les Autorités de certification (CA) autorisées délivrent un certificat.
Composantes d'un registrar corporate	Se spécialise dans la prestation de services aux entreprises qui ont besoin de niveaux avancés de pratiques commerciales, de capacités, d'expertise et de personnel d'assistance en matière de gestion DNS et de noms de domaine ainsi qu'en termes de sécurité, de protection de la marque et de lutte contre la fraude, de gouvernance des données et de cyber-sécurité.

Les secteurs d'activité critiques

En nous appuyant sur les données de notre **Rapport sur la sécurité des noms de domaine**, nous avons examiné les entreprises du classement Global Forbes 2000, que nous avons mises en correspondance avec les secteurs d'activité sous-jacents de l'un des 16 **secteurs des infrastructures critiques reconnus comme tels par la CISA (Cybersecurity and Infrastructure Security Agency)**. Nous avons ensuite observé les huit indicateurs de bonnes pratiques de sécurité du nom de domaine, comme indiqué ci-dessus, pour les classer en fonction de ces secteurs d'infrastructures critiques :

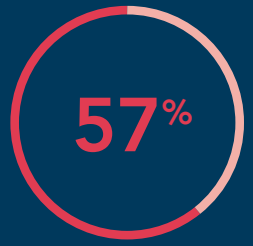
Échelle d'efficacité de la mitigation des risques



Ces derniers résultats mettent en évidence le problème sous-jacent plus large qui touche les secteurs de production des semi-conducteurs et des laits maternisés (Fabrication stratégique, Alimentation et agriculture) et montrent que leur stratégie de sécurité du nom de domaine reste globalement limitée et n'offre que peu de perspectives d'amélioration.

Le Rapport CSC sur la sécurité des noms de domaine : Forbes Global 2000 présente une analyse plus approfondie des stratégies de sécurité du nom de domaine des secteurs d'activité les plus critiques dans le monde.

81 % des entreprises sont plus exposées au risque de détournement de noms de domaine et de DNS parce qu'elles N'ONT PAS adopté de mesures élémentaires de sécurité pour leurs noms de domaine, comme le verrouillage du registre de noms de domaine.



57 % des entreprises font confiance à des registrars grand public offrant une protection limitée contre le détournement de noms de domaine et de DNS, les attaques DDoS, les attaques de type « Man in The Middle » (MiTM) ou l'empoisonnement du cache DNS.

50 % des entreprises utilisent le protocole DMARC (Domain-based Message Authentication Reporting and Conformance) pour authentifier les e-mails entrants.

Les risques entraînent des initiatives désespérées et exigent d'agir

Les acheteurs de biens en pénurie trouveront mille moyens d'acheter ce dont ils ont besoin. Les marques et le secteur des noms de domaine doivent donc redoubler de vigilance et s'assurer que les consommateurs consultent des sites sûrs et autorisés. La faiblesse de la stratégie de sécurité du nom de domaine n'est pas nouvelle, mais elle devient un problème prioritaire qui nécessite une plus grande prise de conscience stratégique. Les entreprises doivent surveiller le Web pour identifier et réagir face à tout ce qui peut nuire ou participer à la dilution de leur marque et permettre au consommateur final d'être victime d'une fraude. Il est possible d'éviter ces risques. Il faut en outre éviter que le consommateur, qui consulte différents sites à la recherche des produits souhaités, se retrouve face à un cybercriminel. De meilleures mesures de sécurité du nom de domaine doivent être mises en œuvre et le monde des affaires doit adopter des normes générales en la matière.

Les marques ont réalisé d'importants investissements dans la transformation digitale, la protection de marque et la mitigation des risques en termes de cyber-sécurité. Pourtant, les risques systémiques des noms de domaine et du DNS entraînent des vulnérabilités dans la chaîne d'approvisionnement, et favorisent les tentatives de phishing, la fraude (par le biais de rançongiciels ou d'attaques BEC), les infractions sur les marques et la contrefaçon. Les entreprises qui fournissent des infrastructures critiques doivent faire plus pour améliorer leur stratégie de sécurité. La sécurité du nom de domaine, qui représente un risque commercial systémique, s'inscrit au cœur de cette stratégie.

En outre, le secteur de la cyberassurance devrait également évaluer ces risques. Les conditions de souscriptions et le montant des primes de cyberassurance changent pour de nombreuses entreprises, à mesure que les assureurs prennent en compte de nouveaux paramètres susceptibles d'influencer la police d'assurance. Une stratégie de sécurité du nom de domaine insuffisante reflétée dans ces indicateurs pourrait avoir des conséquences à long terme pour ces entreprises. En matière de sécurité du nom de domaine, l'inaction n'est pas une option. CSC estime qu'il est urgent de mettre en œuvre des normes de sécurité plus étendues pour les noms de domaine, ainsi qu'une politique ou une réglementation relative à l'activité et au comportement quotidien au niveau de l'infrastructure DNS.

Pour découvrir comment s'assurer que votre entreprise est bien protégée, rendez-vous sur :

RECOMMANDATIONS EN TERMES DE SÉCURITÉ DU NOM DE DOMAINE DANS NOTRE POST DE BLOG SUR LA CHAÎNE D'APPROVISIONNEMENT

CSC est le partenaire de confiance des entreprises du Forbes Global 2000 et des 100 Best Global Brands® en matière de gestion des noms de domaine, de services DNS et de certificats numériques, et propose des solutions de protection des marques en ligne contre la fraude. Alors que les entreprises du monde entier investissent massivement dans leur stratégie de sécurité, CSC peut les aider à identifier leurs failles de cybersécurité et à sécuriser leurs actifs numériques et leurs marques en ligne. 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 actions ciblées. Nous proposons une approche holistique de la cybersécurité 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 : **cscdbs.com/fr**.

Vincent D'Angelo, directeur mondial, Corporate Development and Strategic Alliances

Quinn Taggart, conseiller principal, Global Brand Security

Sue Watts, responsable Marketing mondial

David Barnett, responsable de la consultance, Brand Monitoring

cscdbs.com/fr

DBS07062022