CSC

2022

RAPPORT SUR LA SÉCURITÉ DES NOMS DE DOMAINE

RÉSUMÉ DES PRINCIPALES CONCLUSIONS – QUOI DE NEUF EN 2022 ?

Cela fait déjà trois ans que CSC analyse chaque année la stratégie de sécurité de nom de domaine des grandes entreprises (classement Forbes Global 2000). Cette année, nous avons constaté que certaines entreprises avaient renforcé leur sécurité, tandis que d'autres continuaient de courir un risque considérable. Nous souhaitons 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 de toutes les entreprises.

PRÈS DE 3/4

DES ENTREPRISES DU GLOBAL 2000 SONT À RISQUE COMPTE TENU DE LEUR EXPOSITION AUX MENACES DE SÉCURITÉ

Près des 3/4 des entreprises du Global 2000 n'ont mis en place que la moitié des paramètres de sécurité nécessaires au nom de domaine. CSC a analysé huit mesures de sécurité clés et a calculé un score moyen pour chacune de ces entreprises. Plus le score est élevé, plus la position de sécurité est forte.

45 %

DES ENTREPRISES QUI FONT APPEL À DES REGISTRARS CORPORATE UTILISENT AUSSI LE VERROUILLAGE DU REGISTRE

Le verrouillage du 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. Seules 5 % des entreprises qui recourent à des registrars grand public ont déployé le verrouillage du registre. Les noms de domaine non verrouillés sont vulnérables aux tactiques d'ingénierie sociale, qui peuvent conduire à des modifications non autorisées du DNS et à des détournements des noms de domaine.

75 %

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

Parmi les 75 % de (faux) noms de domaine homoglyphes détenus par des tiers autres que les titulaires de marques du Global 2000, 82 % ont masqué leurs coordonnées WHOIS ou les informations liées à la propriété du site en 2022, contre 77 % en 2021, ce qui montre qu'ils utilisent davantage la protection de la confidentialité de la base de données WHOIS.

< 5 %

D'AUGMENTATION DE L'ADOPTION D'AUTRES MESURES PROACTIVES DE SÉCURITÉ DU NOM DE DOMAINE

Les entreprises luttent pour bénéficier de tarifs de cyberassurance abordables, et la sécurité des noms de domaine est l'un des domaines les plus économiques par rapport aux autres dépenses de cyber-sécurité. Dès lors que les risques liés à l'absence de dispositifs de sécurité du nom de domaine peuvent potentiellement mener à des attaques de phishing ou par rançongiciel, ainsi qu'à d'autres risques cyber, nous pensions voir une plus forte adoption de certaines de ces mesures de sécurité, comme le verrouillage du registre, la redondance du DNS, le protocole DNSSEC de sécurisation des extensions de noms de domaine et les enregistrements CAA (Certification Authority Authorization).

23 %

CROISSANCE DE DMARC AVEC LE TAUX DE CROISSANCE LE PLUS ÉLEVÉ

Les chiffres les plus récents du groupe de travail anti-phishing (APWG) montrent que le nombre d'attaques de phishing est plus élevé que jamais, puisqu'il a été multiplié par 10 depuis 2020 ; il n'est donc pas surprenant de constater en parallèle un taux d'adoption plus marqué de la technologie DMARC, un système d'authentification des e-mails conçu pour protéger le nom de domaine de messagerie d'une entreprise contre les tentatives de spoofing, de phishing et autres cyberattaques.

ALORS QUE LES MODÈLES DE STRATÉGIE DE SÉCURITÉ ZERO TRUST DOMINENT, 2022 MONTRE À QUEL POINT LA SÉCURITÉ DU NOM DE DOMAINE EST ESSENTIELLE

Les modèles Zero Trust doivent s'étendre au-delà du réseau, des applications et des appareils de l'entreprise pour inclure l'écosystème des noms de domaine de l'organisation, qui apparaît comme une vulnérabilité réelle face aux attaques mentionnées à la Figure 1. Les deux menaces suivantes sur la sécurité des noms de domaine servent à faciliter les attaques énumérées ci-dessous.

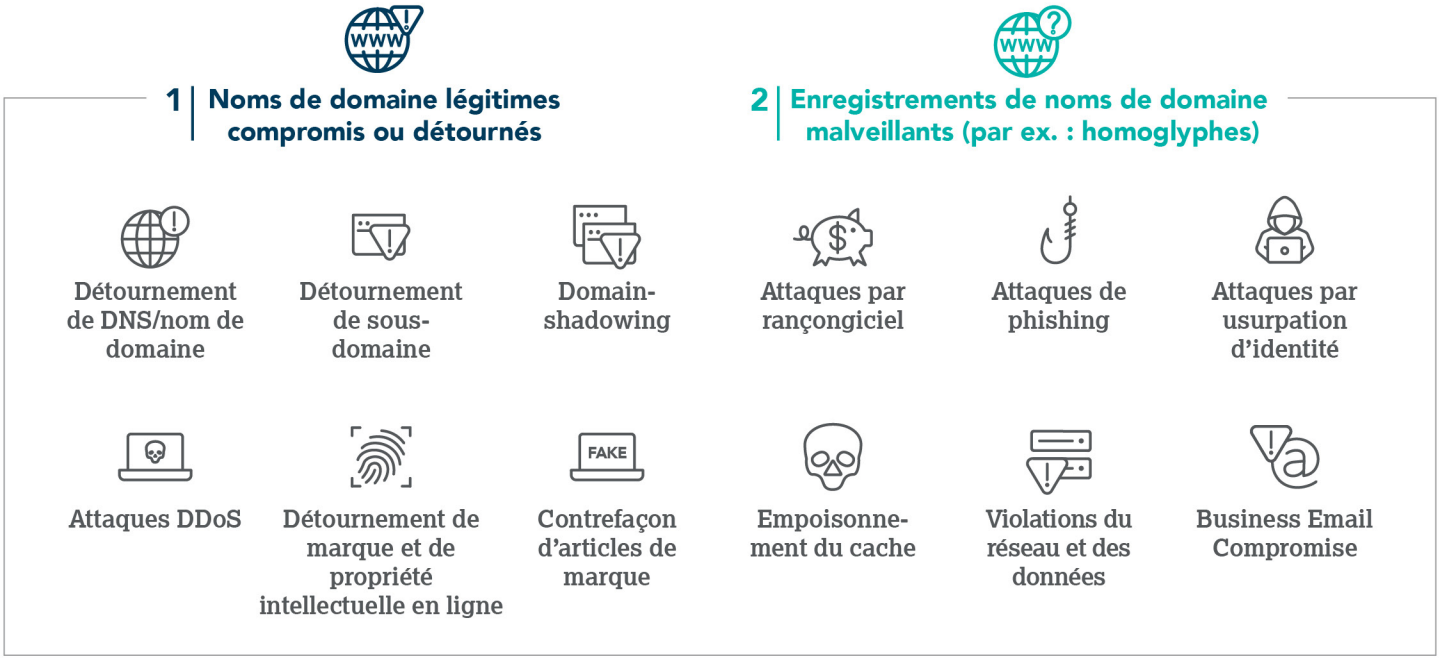


Figure 1

Les entreprises du monde entier utilisent Internet pour l'ensemble de leurs opérations : sites web, messagerie, authentification, communications VoIP, et plus encore. Internet fait donc partie de la surface d'attaque externe d'une entreprise et, à ce titre, doit faire l'objet d'une surveillance continue pour contrer les attaques des cybercriminels et la fraude. Alors que les risques cyber 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.

DÉFINITION DE LA SÉCURITÉ DES NOMS DE DOMAINE

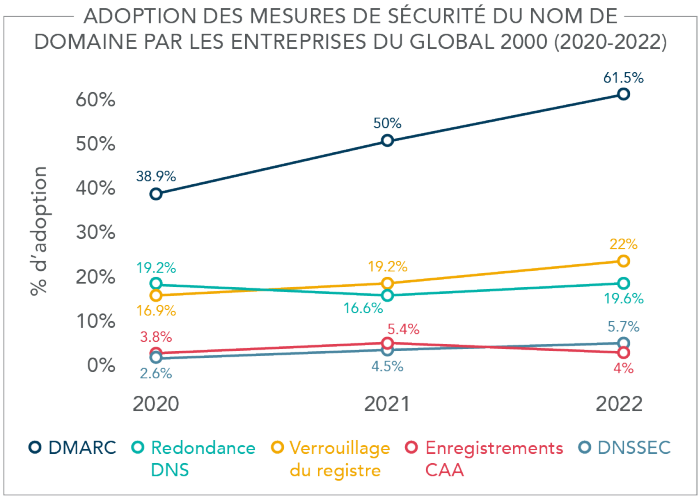
CSC a fait le choix d'une approche multiniveau de la sécurité des noms de domaine. Tout d'abord, nous sécurisons la présence en ligne d'une marque en sécurisant son portefeuille de noms de domaine, qui peut contenir diverses marques obtenues via des acquisitions, et son empreinte DNS en ligne. Ensuite, nous surveillons, analysons et intervenons lorsque nous détectons des vecteurs de menace qui ciblent des marques en ligne. Enfin, nous complétons les ensembles de données ainsi obtenus avec d'autres ensembles de données issus de l'extérieur du pare-feu pour obtenir une vue complète sur la stratégie de sécurité de la marque.

Ce rapport examine les stratégies de sécurité des entreprises du Global 2000, une liste qui est mise à jour chaque année par le magazine Forbes (c'est-à-dire que chaque année, de nouvelles entreprises font leur apparition dans la liste, tandis que certaines disparaissent du Top 2000). Les informations contenues dans ce rapport reposent exclusivement sur des ensembles de données en libre accès qui sont gérés via notre lac de données exclusif optimisé au moyen de Machine Learning, de l'intelligence artificielle et de la technologie de Deep Search.

RÉSULTATS ET ANALYSE

Pour cette analyse, CSC a examiné l'adoption par des entreprises du Global 2000 des mesures de sécurité du nom de domaine détaillées ci-après, puis nous avons approfondi notre analyse en passant en revue les différents secteurs d'activité et régions du monde.

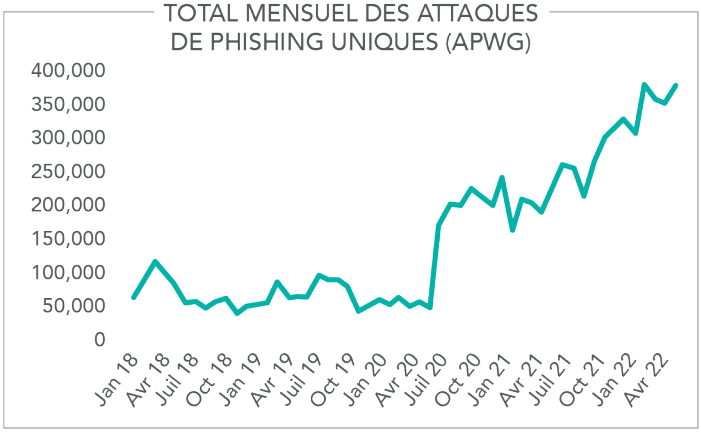
TENDANCES D'ADOPTION DES MESURES DE SÉCURITÉ DU NOM DE DOMAINE (2020-2022)



L'UTILISATION DE DMARC A PRESQUE DOUBLÉ EN DEUX ANS

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 62 % en 2022.

Les chiffres les plus récents de l'APWG montrent en effet que le nombre d'attaques de phishing est plus élevé que jamais, avec un total trimestriel d'attaques détectées atteignant 1 million pour la première fois au T1 2022, et plus de 600 marques ciblées chaque mois.



À noter : le fait que les certificats VMC (Verified Mark Certificates) exigent désormais l'application du protocole DMARC pour valider les certificats SSL contribue également à l'augmentation de son utilisation. En outre, Apple a annoncé en septembre la prise en charge de la norme BIMI (Brand Indicators for Message Identification) et expliqué que ses clients de messagerie pour iOS 16 et macOS participeront ainsi à l'effort global à l'échelle du secteur visant à combattre le spoofing et l'usurpation de l'identité des marques. Les expéditeurs qui prennent en charge la spécification BIMI doivent respecter une norme stricte d'authentification des e-mails, notamment en utilisant le protocole de sécurité DMARC.

Il est très facile de falsifier un e-mail et de faire croire qu'il est envoyé par une source légitime alors que ce n'est pas le cas. Néanmoins, bien que l'authentification du canal de messagerie avec DMARC minimise la possibilité de spoofing par e-mail et de phishing, nous savons également que, même avec ce dispositif de contrôle en place, ne pas avoir défini la politique DMARC en intégrant le rejet d'e-mails non conformes entraîne un risque au niveau des attaques de phishing, et qu'il est donc nécessaire de prévoir cette configuration lors de l'implémentation.

LA CROISSANCE DES MESURES DE SÉCURITÉ TELLES QUE LE VERROUILLAGE DU REGISTRE, LA REDONDANCE DNS, DNSSEC ET LES ENREGISTREMENTS CAA EST CONSTANTE, MAIS LENTE

Le pourcentage d'entreprises ayant activé le verrouillage du registre est passé de 17 % en 2020, à 19 % en 2021, puis 22 % en 2022. Le verrouillage du 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, tous les registres du monde ne disposant pas de services de verrouillage.

Le nombre d'entreprises ayant déployé la redondance DNS et le protocole DNSSEC a légèrement augmenté ces trois dernières années. Un nombre croissant d'organismes gouvernementaux encouragent les entreprises et autres à renforcer la résilience de leur DNS, un composant fondamental dans l'infrastructure centrale de toute organisation. Toutefois, bien que la hausse de l'adoption des mesures dans ce sens soit en phase avec la pression croissante exercée sur les organisations, nous n'avons pas encore constaté de taux d'adoption plus élevés qui pourraient correspondre à des entreprises devant planifier l'augmentation des coûts et l'allocation des ressources.

Ajoutons que si l'utilisation des enregistrements CAA a connu une légère hausse de 2020 à 2021, elle a de nouveau diminué en 2022. 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. Leur requête aboutira à un refus, et l'entreprise sera alertée. Cependant, de nombreuse 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.

MESURES DE SÉCURISATION DES NOMS DE DOMAINE PAR TYPE DE REGISTRAR – 2022

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.

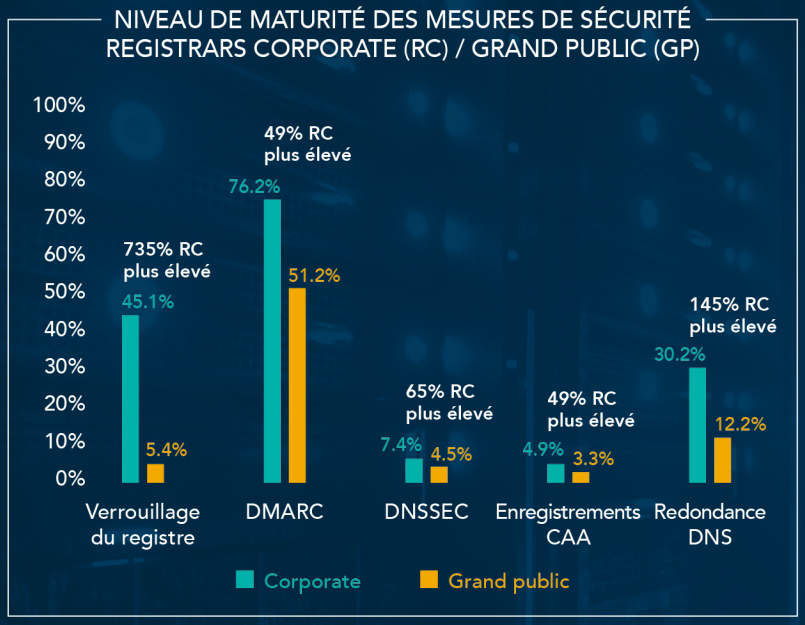
REGISTRARS GRAND PUBLIC :

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 titulaires de marques qui ont besoin de niveaux avancés de pratiques commerciales, de capacités, d'expertise et de personnel d'assistance en matière de gestion des noms 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 cyber-sécurité.

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.



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.

FIN 2021, SecurityScorecard a comparé les notes de cyber-sécurité des entreprises utilisant des registrars corporate par rapport à celles faisant appel à des registrars grand public. Leur analyse a montré que les entreprises dont le ou les noms de domaine sont gérés par des registrars corporate ont une note globale en moyenne d'une demi-lettre, voire d'une lettre supplémentaire par rapport aux entreprises qui ont recours à un registrar grand public.

EN SAVOIR PLUS :

- La sécurité de votre nom de domaine commence avec votre registrar
- La fiabilité de votre cyber-sécurité dépend de celle de votre fournisseur
- Le choix du fournisseur est essentiel dans l'écosystème des registrars de noms de domaine

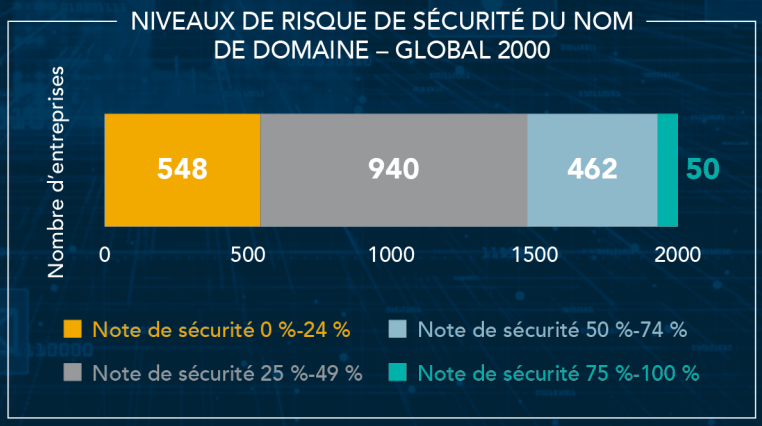
STRATÉGIE GLOBALE DE SÉCURITÉ DU NOM DE DOMAINE

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 (MultiLock)
- Enregistrements CAA
- Redondance DNS
- DNSSEC
- SPF
- DKIM
- DMARC

PRÈS DES 3/4 DES ENTREPRISES ONT IMPLÉMENTÉ MOINS DE LA MOITIÉ DE L'ENSEMBLE DES MESURES DE SÉCURISATION DU NOM DE DOMAINE



LES 5 SECTEURS LES PLUS SÉCURISÉS

- Logiciels et services IT
- Services et fournitures pour les entreprises
- Hôtellerie/restauration et loisirs
- Médias
- Aérospatiale et défense

LES ENTREPRISES LES PLUS SÉCURISÉES

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

LES 2/3 d'entre elles sont des entreprises américaines.

LES 5 SECTEURS LES MOINS SÉCURISÉS

- Biens de consommation durables
- Marchés alimentaires
- Construction
- Sociétés commerciales
- Matériaux

LES ENTREPRISES LES MOINS SÉCURISÉES

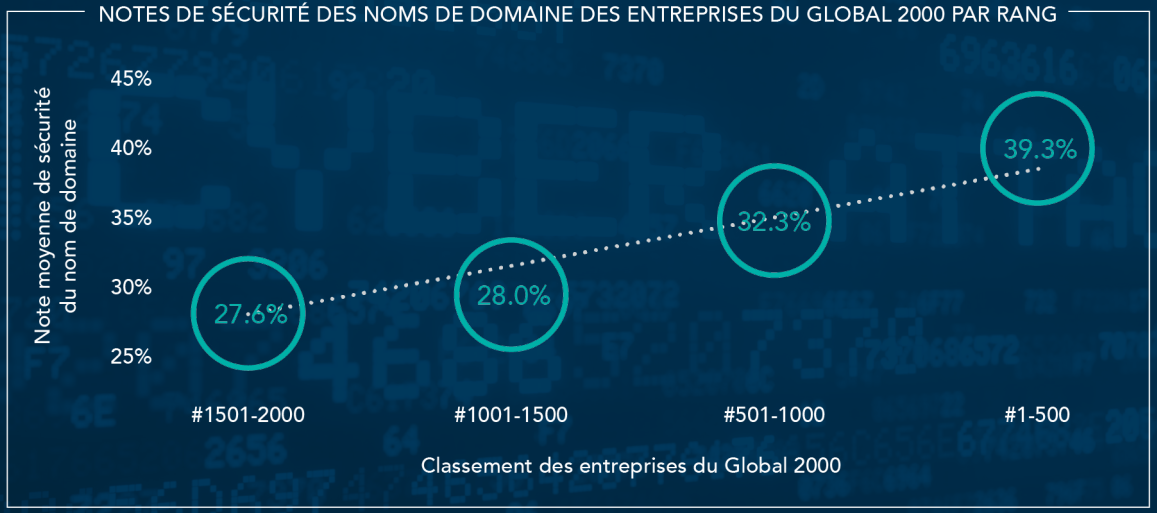
137 entreprises affichent une note de sécurité des noms de domaine de zéro.

Ces entreprises sont principalement situées dans la région Asie-Pacifique (APAC) et représentent **82 %** des entreprises avec la note 0.

Les entreprises affichant la plus faible performance, à savoir celles qui sont actives dans le secteur des marchés alimentaires, des matériaux et de la construction, sont soumises à un risque plus grand de cyberattaque en raison de l'absence de mesures de sécurisation de leur portefeuille de noms de domaine. Les problèmes de chaîne d'approvisionnement viennent s'ajouter à la multitude de problèmes qui affectent le secteur des matériaux, de la main-d'œuvre et de la distribution, entraînant un véritable effet boule de neige. Le secteur des biens de consommation durables figure également parmi les cinq secteurs les moins performants, de même que les entreprises du secteur automobile. Il est important de noter que ces entreprises ont commencé à renforcer leurs stratégies de cyber-sécurité maintenant que l'Internet des objets (IoT) joue un rôle important dans les fonctions plus personnalisées des nouvelles voitures. Ces entreprises devront en effet être en mesure d'atténuer davantage de menaces potentielles.

LIEN ENTRE LA NOTE DE SÉCURITÉ DU NOM DE DOMAINE ET LE CLASSEMENT DANS LE GLOBAL 2000

Plus une entreprise est bien classée dans le Global 2000, plus sa stratégie de sécurité du nom de domaine est efficace.



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 d'atteinte à la propriété intellectuelle, qui entraînent une perte de revenus et un détournement du trafic web, et entachent la réputation de la marque.

Il existe une infinité de tactiques de spoofing et de permutations dans l'URL de noms de domaine, qui peuvent être utilisées par les « phishers » et les tiers 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 domaines similaires

cscglobal.jp cscglobal.ec

Correspondances par mots-clés

cscglobalcovid.com covidcscglobal.ar covid19.com

Homophones (Soundex)

siesiglobal.com cscclobol.com

HOMOGLYPHES COURANTS (CORRESPONDANCES FLOUES) DANS LES NOMS DE DOMAINE EN .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 pour ressembler à CompanyName.com.

C*0rn*panyNa*rn*e.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

75 % Plus de 75 % des noms de domaine homoglyphes sont détenus par des tiers. Cette tendance va de pair avec les résultats de 2021.

PARMI LES NOMS DE DOMAINE DÉTENUS PAR DES TIERS :

82 % ont leurs coordonnées WHOIS ou les informations liées à la propriété du site masquées en 2022, contre **77 %** en 2021, ce qui montre que leurs propriétaires utilisent davantage la protection de la confidentialité. Cela démontre leur tentative de masquer ou de dissimuler leur titre de propriété ou leur identité, et illustre le caractère malveillant de leurs intentions..

48 % disposent d'enregistrements MX en 2022. Ce pourcentage est à comparer aux **43 %** de 2021. 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 ?

46 % redirigent les internautes vers du contenu publicitaire ou des liens sponsorisés, ou sont utilisés pour les services de parking de noms de domaine.

41 % détenaient des sites web inactifs.

5 % redirigeaient les utilisateurs vers un contenu malveillant. Le contenu indésirable peut nuire à la réputation d'une marque et diminuer la confiance des clients envers cette dernière. Le risque est que l'utilisateur puisse consulter des sites web avec du contenu malveillant ou être victime d'une tentative de vol de données sensibles.

8 % se résolvent en un site web actif qui n'a aucun lien avec le titulaire de marque.

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

GoDaddy® | Namecheap™ | PDR LTD

NOMS DE DOMAINE SUSPECTS OU MALVEILLANTS : QUI SONT LES CIBLES ?

SECTEURS D'ACTIVITÉ LES PLUS VISÉS PAR LES ENREGISTREMENTS ABUSIFS DE NOMS DE DOMAINE

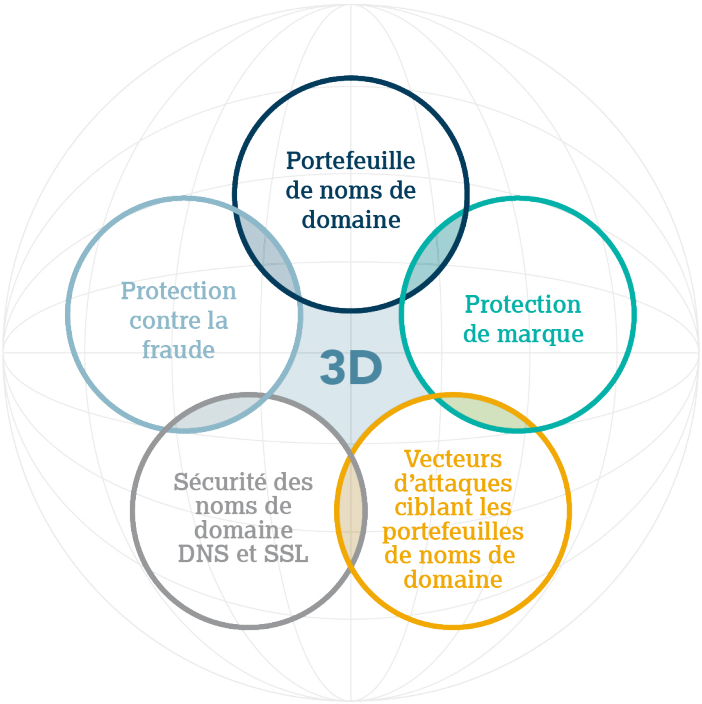
Secteur	Enregistrements abusifs en % du total
Banques	10.0%
Logiciels et services IT	7.0%
Services et fournitures pour les entreprises	5.5%
Biens de consommation durables	5.4%
Équipements et services de santé	4.6%
Services financiers diversifiés	4.6%
Médicaments et biotechnologies	4.6%
Télécommunications	4.5%
Transports	4.2%
Assurances	4.1%
Opérations pétrolières et gazières	3.9%
Construction	3.7%
Matériaux	3.5%
Alimentation, boissons et tabac	3.5%
Vente au détail	3.2%
Chimie	3.2%
Matériel et équipements technologiques	3.2%
Hôtellerie/restauration et loisirs	3.0%
Biens d'équipement	2.8%
Services publics	2.7%
Aérospatiale et défense	2.5%
Produits ménagers et personnels	2.1%
Sociétés commerciales	2.0%
Multinationales	2.0%
Médias	1.8%
Semi-conducteurs	1.7%
Marchés alimentaires	0.4%

À PROPOS DE LA PLATEFORME DOMAINSEC℠ DE CSC

La solution 3D Monitoring de CSC a été créée pour exploiter la puissance de la plateforme DomainSec.

DomainSec est une plateforme de cyber-sécurité SaaS développée par CSC afin de mettre en œuvre la première approche holistique du secteur en matière de sécurisation et de défense des écosystèmes de noms de domaine des marques. Cette plateforme innovante utilise notre technologie propriétaire MLDS (Machine Learning Deep Search) et combine le Machine Learning, l'intelligence artificielle et la technologie du clustering (regroupement de données) pour identifier les indicateurs avancés de compromission.

DomainSec réunit dans une plateforme unique les solutions de sécurité et de gestion des noms 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.

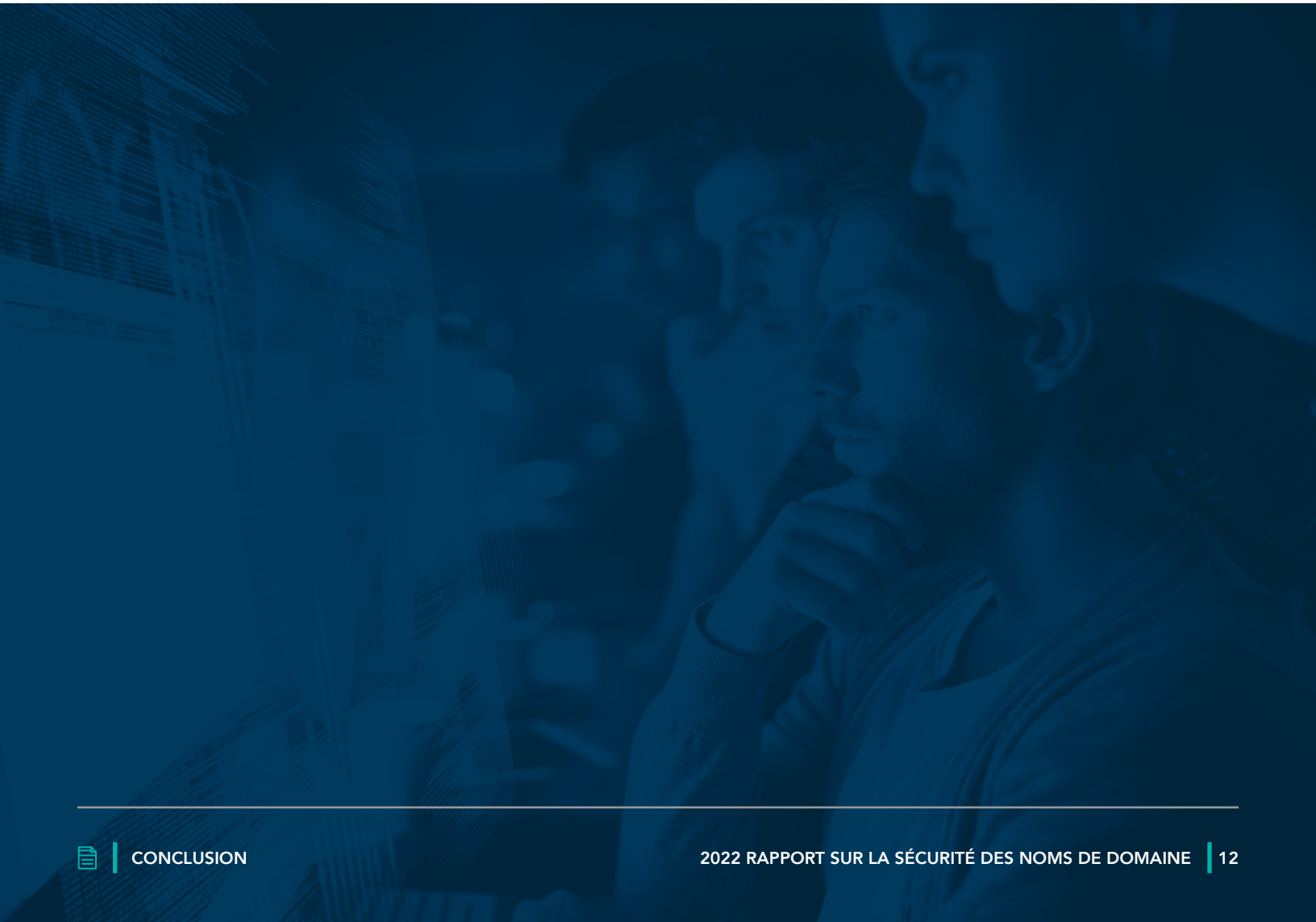


CONCLUSION

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 cyber-sécurité, mais aussi pour la confidentialité des données, la sécurité des consommateurs, la propriété intellectuelle, les chaînes d'approvisionnement, le chiffre d'affaires et la réputation de votre entreprise. On peut s'attendre à ce que la sensibilisation à ces problématiques s'intensifie et que les prestataires de cyberassurance commencent à tenir leurs clients responsables de la qualité et de la rigueur de leurs stratégies et de leurs approches de protection des noms de domaine.

Les entreprises ont besoin d'un modèle de sécurité multiniveau dans un cadre Zero Trust afin de mettre en œuvre une stratégie de sécurité renforcée qui protège au maximum leur activité. Comme nous l'avons souligné, les composantes de cette approche incluent un partenariat avec un registrar corporate, une visibilité sur les surfaces exposées (notamment les noms de domaine et le DNS), et la capacité d'analyser les vecteurs de menace qui ciblent la présence en ligne de l'entreprise.

Bénéficiez de nos recommandations de sécurité des noms de domaine pour protéger vos noms de domaine et vos marques contre les cybermenaces et la fraude.



Spécialiste des solutions de sécurité et de la veille sur les cybermenaces, 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, de certificats numériques et 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 cyber-sécurité 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 interventions ciblées. Nous proposons une approche holistique de la cyber-sécurité 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.

ÉTUDE PRÉPARÉE PAR CSC :

IHAB SHRAIM	Directeur technique
VINCENT D'ANGELO	Directeur mondial, Développement corporate et Alliances stratégiques
ELLIOTT CHAMPION	Responsable Produits, Marques mondiales et Noms de domaine
QUINN TAGGART	Consultant Sécurité senior, Global Brand Security
FERNANDO CEVALLOS	Responsable Produits, Lutte anti-fraude et Veille de sécurité mondiale

DBS11142022