CSC

DOMAIN SECURITY REPORT

LES ENTREPRISES DU FORBES GLOBAL 2000

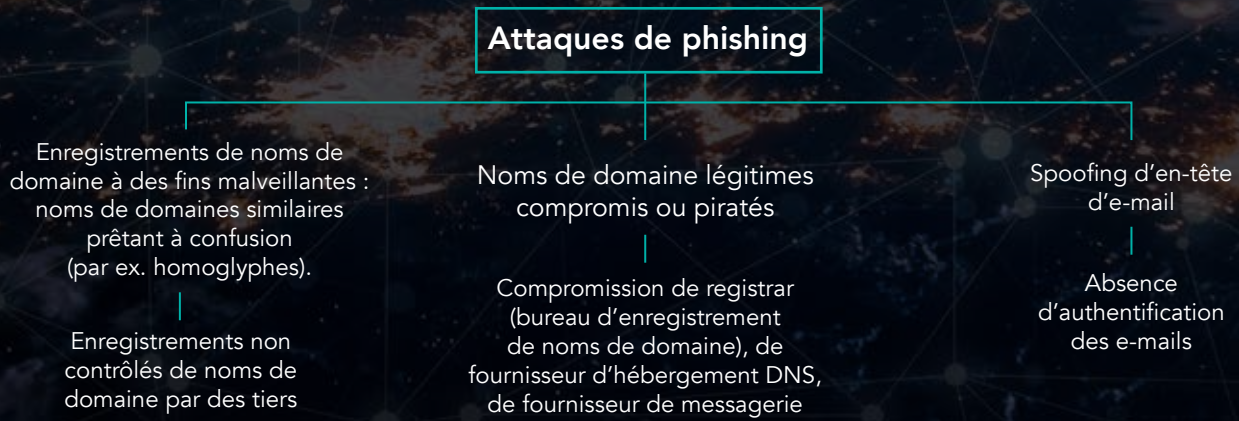
2021

Résumé

En 2021, avec la recrudescence de la cybercriminalité, les entreprises ont dû faire face à une augmentation des attaques : rançongiciels, BEC (Business Email Compromise), tentatives de phishing, attaques visant les chaînes d'approvisionnement, sans compter les abus de marque et autres fraudes en ligne. Si les cyber-risques pesant sur les noms de domaine sont en hausse, les mesures prises par les entreprises du Forbes Global 2000 en vue d'améliorer leur stratégie de sécurité des noms de domaine n'ont pourtant pas évolué, ce qui a encore accru leur vulnérabilité.

La sécurité de vos noms de domaine est un élément essentiel pour l'atténuation des cyberattaques – *votre première ligne de défense*

Selon la CISA (Cybersecurity and Infrastructure Security Agency) du Département américain de la sécurité intérieure, la majorité des cyberattaques, notamment les attaques par rançongiciels et les attaques BEC, commencent par du phishing. Bien que les pertes dues aux rançongiciels dépassent désormais plusieurs milliards par an, la plupart des mesures de protection ne traitent pas correctement les risques de phishing qui peuvent dissimuler une attaque par rançongiciels, car elles n'incluent aucune mesure de sécurité du nom de domaine. Des études reconnues montrent que les attaques de phishing se produisent le plus souvent à partir d'un nom de domaine enregistré à des fins malveillantes, d'un nom de domaine dont la similarité peut prêter à confusion, d'un nom de domaine légitime compromis ou piraté, ou à partir de l'usurpation d'un en-tête d'e-mail visant à tromper le destinataire (« spoofing »).



Comprendre le cyber-risque qui menace vos noms de domaine

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

CSC recommande de porter une attention particulière au Domain Security Framework suivant :

DOMAIN SECURITY FRAMEWORK

Protection contre les noms de domaine suspects ou malveillants

Se protéger contre le spoofing d'en-tête d'e-mail

Se défendre contre la compromission des activités de votre nom de domaine

PRINCIPALES CONCLUSIONS DE L'ÉTUDE

70 % de variations homoglyphiques (correspondances floues) des noms de domaine – une tactique couramment utilisée dans le phishing et l'abus de marque –, sont détenus par des tiers et enregistrés auprès de registrars grand public. Parmi ces noms de domaine enregistrés, plus de **60 %** l'ont été au cours des deux dernières années, ce qui démontre qu'il s'agit d'une méthode d'attaque en pleine expansion.

81 % des entreprises sont plus exposées au risque de détournement de nom de domaine et de DNS (DNS Hijacking) parce qu'elles N'ONT PAS adopté de mesures de sécurité de base pour leurs noms de domaine, comme le protocole du Registry Locks (verrous de niveau registre).

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 de cache DNS.

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

L'importance de la sécurité du nom de domaine dans l'atténuation des attaques de phishing

De récentes cyberattaques ont visé des chaînes d'approvisionnement connectées dans des secteurs vitaux et sur plusieurs plateformes logicielles, où une seule compromission peut avoir des retombées exponentielles. Du fait de la nature interconnectée des noms de domaine et des infrastructures DNS, la sécurité des noms de domaine et les vulnérabilités des registrars peuvent démultiplier les risques pour la chaîne d'approvisionnement Internet. Des contrôles proactifs et préventifs permettent de sécuriser les actifs sous-jacents aux noms de domaine et de les protéger contre les méthodes d'attaque par phishing évoquées plus haut. Les meilleures mesures de protection sont :

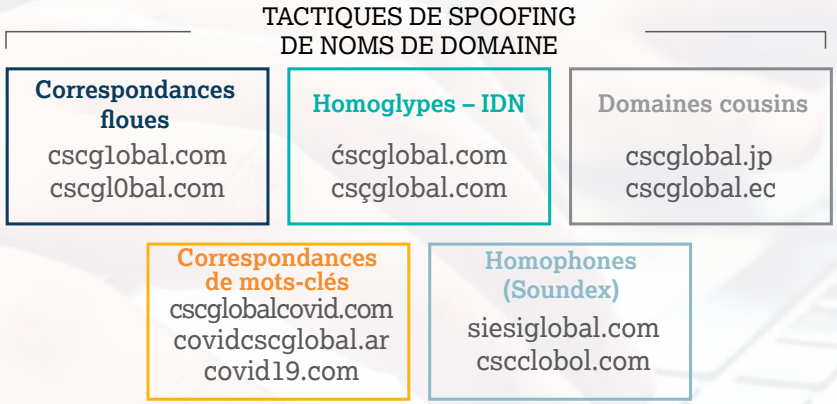
- **Les standards des registrars de noms de domaine** qui éduquent les grandes entreprises sur le recours à des registrars grand publics et qui protègent des pratiques commerciales susceptibles d'être utilisées de manière malveillante, telles que le phishing et l'atteinte aux marques.
- **L'adoption de mesures de sécurité au niveau sectoriel** telles que les verrous de registre, le protocole DMARC, la redondance de l'hébergement DNS, le protocole DNSSEC et les enregistrements CAA (Certificate Authority Authorization).
- **Les dispositifs permanents de détection et la désactivation rapide des noms de domaine dont la similarité prête à confusion** en imitant une marque, et qui sont utilisés pour le phishing et d'autres activités frauduleuses.

Sécurité des noms de domaine :

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[1]. Ces enregistrements de noms de domaine suspects ou malveillants 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 de noms de domaine et de permutations, qui peuvent être utilisées par les « phishers » et les acteurs malveillants.



Nous avons choisi de concentrer nos recherches concernant la sécurité des noms de domaine sur l'une des nombreuses tactiques flagrantes visant les principales marques des entreprises du Global 2000 par le biais d'enregistrements malveillants de noms de domaine.

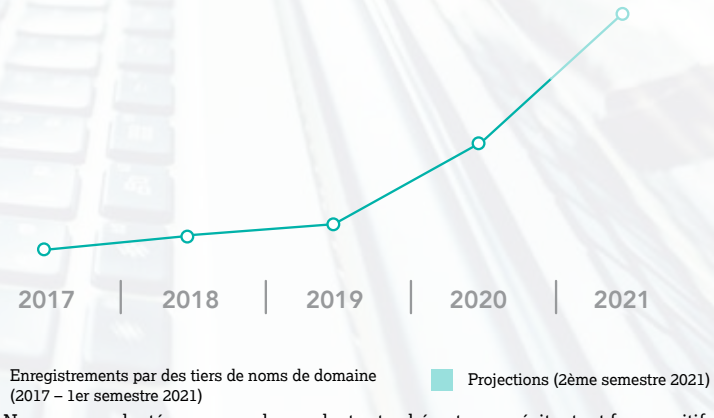
Homoglyphes courants (correspondances floues) dans les noms de domaine en .COM

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.

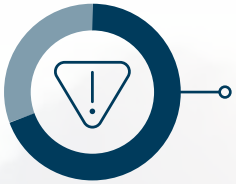
Substitutions de caractères les plus courantes

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

Enregistrements par des tiers de noms de domaine homoglyphes correspondant à des entreprises du Global 2000



[1]La portée de l'étude a été limitée aux extensions .COM, pour lesquelles nous nous attendions à trouver le plus d'enregistrements par des tiers. Nous avons adopté une approche prudente et cohérente pour éviter tout faux positif, et nous avons analysé des marques majeures dont le nom compte six caractères ou plus.



70 % des noms de domaine enregistrés similaires à des marques du Global 2000 étaient détenus par des tiers.

Parmi les noms de domaine détenus par des tiers :

60 % ont été enregistrés au cours de l'année 2020 jusqu'au premier semestre de l'année 2021. Nous pensons que d'ici fin 2021, ce chiffre pourrait monter à **68 %** sur la base de nos prévisions.

77 % 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 néfaste de leurs intentions. À titre de comparaison, les marques légitimes du Global 2000 n'utilisent des services de protection de la confidentialité ou n'expurgent leurs données que dans 25 % des cas.

43 % sont configurés avec des enregistrements MX (messagerie).

Près de la moitié de ces noms de domaine sont configurés avec des enregistrements MX (messagerie) qui peuvent servir à envoyer des e-mails de phishing ou à intercepter des e-mails.

Registrars de noms de domaine les plus couramment associés à des enregistrements suspects ou malveillants appartenant à des tiers (apparaissant dans l'analyse) :

GoDaddy.com, LLC **Namecheap, Inc** **PDR, Ltd**

Comment ces noms de domaine de tiers sont-ils utilisés actuellement ?

56 % redirigent les internautes vers du contenu publicitaire ou des liens sponsorisés, ou sont utilisés pour les services de parking de domaines.

Une étude de Palo Alto montrait comment les noms de domaine sponsorisés sont utilisés pour diffuser des logiciels malveillants via ces services. Les cybercriminels peuvent utiliser des noms de domaine dormants dans le cadre de leur stratégie, et les activer au moment où ils sont prêts à lancer l'attaque.

38 % détenaient des sites web inactifs.

Sur ces noms de domaine, un tiers n'avait aucun nom de serveur associé, ce qui pourrait indiquer que le nom de domaine avait été suspendu à un moment donné.

Sur les deux tiers restants, **57 %** disposaient d'enregistrements MX actifs.

6 % redirigeaient les internautes vers un site usurpant l'identité d'une marque ou vers du contenu malveillant, servant notamment au phishing et à la diffusion potentielle de logiciels malveillants.

Le contenu indésirable peut nuire à la réputation d'une marque et diminuer la confiance des clients envers cette marque. 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.

Nos recommandations

L'analyse de ces noms de domaine détenus par des tiers révèle qu'un bon nombre d'entre eux sont généralement utilisés comme noms de domaine malveillants pour lancer des cyberattaques. Les titulaires de noms de domaine se cachent généralement derrière des services de confidentialité afin de dissimuler leur identité, d'enregistrer des noms de domaine ressemblant à des marques connues et d'utiliser des tactiques de légitimation visant à inciter un utilisateur final à cliquer sur un lien ou à faire confiance à un site frauduleux.

Nous recommandons aux entreprises de mettre en place un solide programme de surveillance des noms de domaine, de veille Internet et de détection du phishing, associé à des capacités de retrait de contenu illicite. Elles devraient également mettre en place une stratégie sécurisée de gestion des noms de domaine à 360 degrés afin d'identifier les correspondances exactes, de se protéger contre diverses tactiques de spoofing telles que les homoglyphes, les correspondances floues, les similarités, et enregistrer préventivement les nouveaux noms de domaine génériques de premier niveau (gTLD) et les code pays TLD associés aux pays d'opération et de ventes.

Analyse de la sécurité des noms de domaine

L'approche des entreprises du Forbes Global 2000 en matière de sécurité des noms de domaine

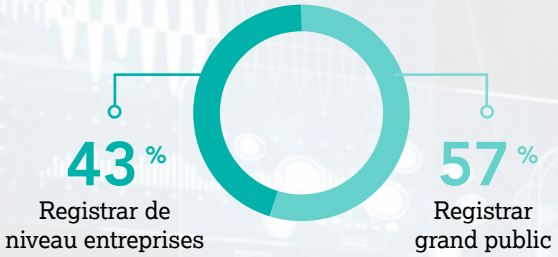
Les informations présentées dans ce rapport s'appuient exclusivement sur des ensembles de données accessibles au public. Bien entendu, les cybercriminels et autres acteurs agissant pour le compte d'États y ont eux aussi accès et ils peuvent s'en servir pour lancer des attaques visant les DNS ou les noms de domaine. C'est pourquoi nous souhaitons mieux sensibiliser les entreprises à ces menaces et partager nos bonnes pratiques de sécurité du nom de domaine afin d'améliorer la stratégie de sécurité du nom de domaine de toutes les entreprises. 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 secteurs d'activité et régions du monde.

Dans le rapport de cette année, nous avons également analysé la tendance d'adoption des mesures de sécurité du nom de domaine en fonction du type de registrar utilisé. Pour l'ensemble des contrôles de sécurité, nous avons observé un taux d'adoption plus élevé parmi les entreprises qui font appel à des registrars pour entreprises que parmi celles qui ont recours à des registrars grand public. Cette distinction est particulièrement évidente concernant l'adoption du Registry Lock (verrou de niveau registre), car la plupart des registrars grand public ne prennent pas en charge ce dispositif.

En moyenne, l'adoption des contrôles de sécurité des noms de domaine est deux fois plus élevée pour les entreprises qui font appel à des registrars de niveau entreprise que pour celles qui utilisent des registrars grand public.

Nos observations portent sur les entreprises incluses dans la liste Global 2000. Pour 2020, les entreprises analysées diffèrent légèrement de l'année précédente, la liste étant mise à jour annuellement.

Registrar de noms de domaine



CONCLUSIONS

57 % des entreprises du classement Global 2000 ne font pas appel à un registrar pour entreprises. La gestion du portefeuille de noms de domaine par un registrar pour entreprises reconnu rendrait l'adoption de normes de sécurité des noms de domaine et de bonnes pratiques bien plus facile à mettre en œuvre que s'il s'agissait d'un registrar grand public.

COMPOSANTES MAJEURES D'UN REGISTRAR POUR ENTREPRISES :

- ☑ Prise en charge et expertise à l'échelle de l'entreprise avec une offre de gestion des noms de domaine, du DNS et des certificats numériques uniquement destinée à l'entreprise.
- ☑ Activité ciblée sur la cybersécurité et la protection de la propriété intellectuelle.

  Ne fournit pas :
  - de services de gestion des noms de domaine par le biais de sites web commerciaux ou d'offres de revendeurs
  - de services de noms de domaine sponsorisés, de domain spinning (génération en masse de noms de domaine) et de vente aux enchères de noms de domaine, toutes pratiques qui facilitent la violation de la propriété intellectuelle et l'abus de marques commerciales
- ☑ Au contraire, l'accent est mis sur la sécurité des noms de domaine grâce à des services avancés tels que : le Registry Lock (verrou de niveau registre), DMARC, DNSSEC, les enregistrements CAA et la redondance de l'hébergement DNS.
- ☑ Proposer une assistance mondiale et locale 24x7x365 avec des capacités d'enregistrement de noms de domaine dans le monde entier.
- ☑ Mettre en œuvre des méthodes KYC (Know Your Customer) pour identifier et valider les interactions avec les clients.
- ☑ Être accrédité au niveau mondial par l'ICANN (Internet Corporation for Assigned Names and Numbers) et les registres.
- ☑ Offrir des services de surveillance de noms de domaine et des services d'interventions pour le retrait de tout contenu frauduleux.
- ☑ Proposer des services de conseil et des outils complémentaires (par exemple, le CSC Security Center℠) qui facilitent la gestion et la sécurisation des noms de domaine ainsi que la protection des marques contre la fraude.
- ☑ Utiliser les meilleurs processus et contrôles opérationnels, par exemple en rendant obligatoires les demandes écrites lors des communications, en organisant des formations de sensibilisation à la cybersécurité et en prenant des mesures relatives à la protection des données et aux politiques de sécurité.
- ☑ Appliquer les meilleures pratiques opérationnelles qui donnent la priorité à la sécurité : centres de données certifiés ISO 27001, conformité à la norme SOC 2, tests d'intrusion et tests de vulnérabilité, par exemple.

MENACE

Traditionnellement, ce sont les registrars de noms de domaine grand public qui sont les plus visés par les cyberattaques. Un nombre impressionnant de ceux-ci rendent possibles l'abus de marque et la fraude (voir ci-dessus les raisons d'utiliser un registrar de noms de domaine pour entreprises).

Registry Locks (verrous de niveau registre)

Usage par type de registrar

52 % des entreprises qui ont recours à un registrar pour entreprises utilisent le Registry Lock (verrou de niveau registre).

4 % des entreprises qui ont recours à un registrar grand public utilisent le Registry Lock (verrou de niveau registre).

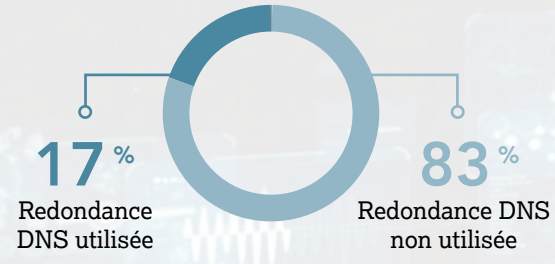
CONCLUSIONS

De façon alarmante, seulement 19 % d'entre elles utilisent le Registry Lock (verrou de niveau registre) en tant que mesure de sécurité, ce qui indique que quatre entreprises du Global 2000 sur cinq sont particulièrement vulnérables en ce qui concerne la sécurité de leurs noms de domaine. Malgré les risques permanents d'attaques DNS qui pèsent sur les entreprises du monde entier, force est de constater que les entreprises du Global 2000 appliquent très peu ce contrôle. Parmi les 43 % d'entreprises du Global 2000 qui font appel à des registrars pour entreprises, 52 % adoptent le Registry Lock (verrou de niveau registre), contre seulement 4 % des entreprises qui font appel à des registrars grand public. Ces chiffres suggèrent que le type de registrar utilisé influence l'adoption – ou non – de contrôles de sécurité des noms de domaine.

MENACE

Le Registry Lock (verrou de niveau 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. 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. *Il arrive toutefois que certains noms de domaine restent non verrouillés, les registres ne disposant pas tous dans le monde entier de services de Registry Lock.

Redondance DNS



Usage par type de registrar

20 % des entreprises qui ont recours à un registrar pour entreprises ont mis en œuvre une redondance DNS.

13 % des entreprises qui ont recours à un registrar grand public ont mis en œuvre une redondance DNS.

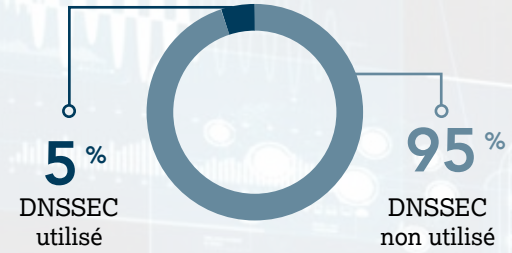
CONCLUSIONS

Seules 17 % des entreprises du Global 2000 disposent d'une redondance de l'hébergement DNS pour leur domaine principal (c'est-à-dire un DNS secondaire). Plus de 80 % d'entre elles prennent un risque en ne disposant pas d'un DNS secondaire, qui permettrait d'atténuer des menaces susceptibles de se transformer en incidents coûteux si les employés ou les clients ne pouvaient pas accéder à leurs sites web ou y effectuer des transactions et ce, même pendant quelques minutes.

MENACE

L'absence de redondance DNS pose des risques de sécurité potentiels, parmi lesquels la réduction de la résilience aux attaques DDoS ainsi que des interruptions des services. Les attaques DDoS inondent de requêtes votre réseau, votre service ou votre application, ce qui empêche les requêtes réelles de vos clients d'aboutir, entraînant une perte de chiffre d'affaires et nuisant à votre réputation.

DNSSEC



Usage par type de registrar

7 % des entreprises qui ont recours à un registrar pour entreprises utilisent le protocole DNSSEC.

3 % des entreprises qui ont recours à un registrar grand public utilisent le protocole DNSSEC.

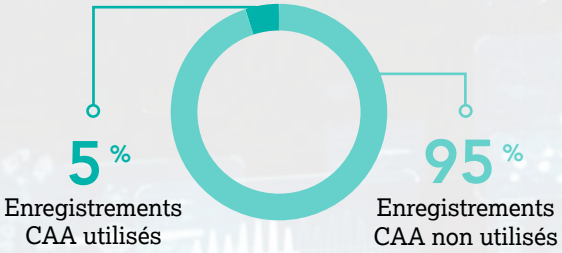
CONCLUSIONS

Les extensions de sécurité du système de nom de domaine (DNSSEC) offrent un autre mode d'authentification des communications entre les serveurs DNS. Les taux d'adoption de DNSSEC sont très faibles, de l'ordre de 5 % seulement. DNSSEC permet pourtant d'empêcher les attaques par DNS cache poisoning (empoisonnement du cache DNS). L'on peut donc en déduire que 95 % des entreprises du Global 2000 sont vulnérables à une attaque par empoisonnement de cache.

MENACE

L'absence de déploiement DNSSEC – l'un des protocoles de sécurité les plus économiques à mettre en place – crée des vulnérabilités au niveau du DNS et peut favoriser, par exemple, le détournement par un hacker de n'importe quelle étape du processus de recherche DNS. Les hackers sont alors en mesure de prendre le contrôle d'une session de navigation Internet pour rediriger les utilisateurs vers de faux sites Web.

Enregistrements CAA



Usage par type de registrar

8 % des entreprises qui ont recours à un registrar pour entreprises utilisent les enregistrements CAA.

4 % des entreprises qui ont recours à un registrar grand public utilisent les enregistrements CAA.

CONCLUSIONS

Seules 5 % des entreprises du Global 2000 utilisent les enregistrements CAA (Certificate Authority Authorization). Les enregistrements CAA vous permettent de désigner une Autorité de certification (AC) spécifique en tant qu'émettrice unique des certificats pour les noms de domaine de votre entreprise. Ainsi, si le cybercriminel ne s'adresse pas à cette autorité de certification pour obtenir un nouveau certificat, sa demande échouera et une alerte vous sera envoyée pour vous avertir que quelqu'un a demandé un nouveau certificat qui n'était pas conforme à votre politique CAA. C'est donc un excellent outil pour garantir la conformité, mais c'est aussi une excellente couche de sécurité.

MENACE

Dès qu'un cybercriminel a accès à un nom de domaine, il peut, la plupart du temps, obtenir l'accès aux certificats numériques émis. L'ajout d'enregistrements CAA permet d'assurer que seul votre prestataire peut émettre un certificat pour vos noms de domaine. En outre, c'est un dispositif technique de contrôle essentiel pour l'application de votre politique et la réduction des menaces de cyber-sécurité comme le phishing HTTPS de sous-domaines piratés.

Authentification des e-mails

Usage par type de registrar

des entreprises qui ont recours à un registrar pour entreprises utilisent le protocole DMARC.

des entreprises qui ont recours à un registrar grand public utilisent le protocole DMARC.

CONCLUSIONS

Le protocole DMARC (Domain-based Message Authentication Reporting and Conformance) est aujourd'hui appliqué par 50 % des entreprises du Global 2000. La technologie DMARC est un système d'authentification des e-mails conçu pour protéger le domaine de messagerie d'une entreprise contre les tentatives de spoofing, de phishing et d'autres cyberattaques. Le protocole DMARC fournit essentiellement une authentification des e-mails comme DNSSEC le fait pour la couche DNS. Nous savons également que, même si des enregistrements DMARC de conformité sont activés, l'absence d'une politique DMARC de rejet des messages douteux pose toujours un risque de phishing.

MENACE

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. L'authentification des canaux de messagerie à l'aide des protocoles DMARC, SPF ou DKIM limite les risques de spoofing d'e-mails et les tentatives de phishing.

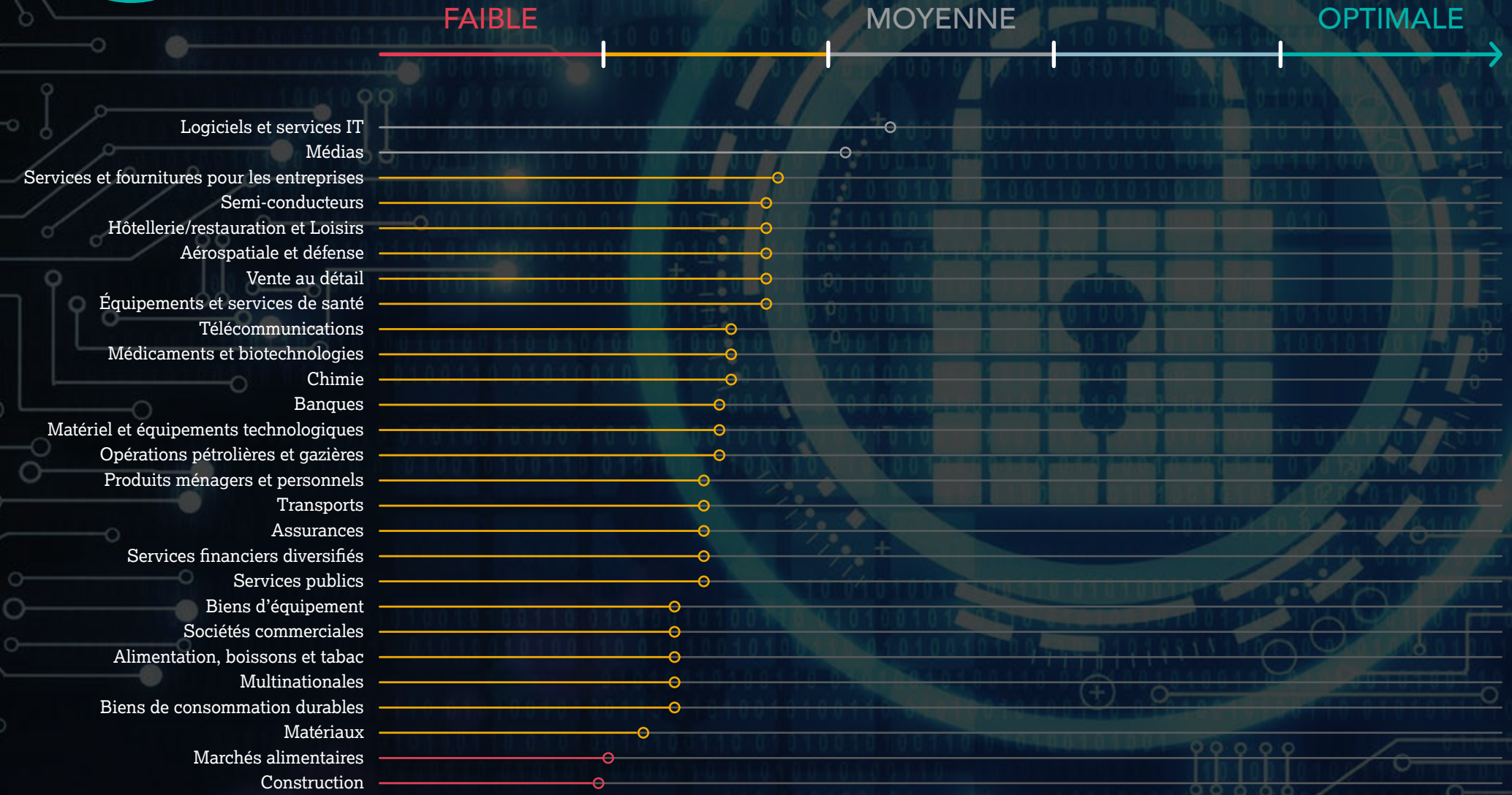
Adoption des contrôles de sécurité des noms de domaine par secteur d'activité

Avec la pandémie de Covid-19, certains secteurs d'activité se sont retrouvés davantage exposés. Il s'agit notamment du secteur des équipements et services de santé, du secteur des médicaments et des biotechnologies, et de ceux des produits chimiques et des produits ménagers et personnels. L'augmentation de la demande pour tous ces produits au cours des 18 derniers mois en a fait des cibles privilégiées pour les cybercriminels. Il est donc très inquiétant de constater que ces secteurs d'activité se situent toujours dans la moitié inférieure de l'échelle d'efficacité de la mitigation des risques. Dans ces quatre secteurs, l'adoption de DNSSEC est extrêmement faible, puisque le secteur des équipements et services de santé, ainsi que celui des produits ménagers et personnels, affichent un taux d'adoption de 0 %. De même, le taux d'adoption des enregistrements CAA est relativement peu élevé, ce qui signifie que des noms de domaine compromis pourraient se voir appliquer des certificats numériques donnant une impression de légitimité, sans que la marque s'en aperçoive. En outre, en moyenne, seule une organisation sur quatre dans ces secteurs active le Registry Lock (verrou de niveau registre), qui empêche pourtant le détournement du nom de domaine et les modifications non autorisées du DNS. Néanmoins, le faible taux d'adoption de ces trois protocoles n'est pas surprenant, puisque de 32 à 48 % des entreprises de ces secteurs font appel à des registrars grand public, qui ne proposent généralement pas l'application de DNSSEC, le Registry Lock (verrou de niveau registre) ou les enregistrements CAA. Ces entreprises ont donc tout intérêt à choisir de travailler avec un registrar de niveau entreprise.

L'industrie pétrolière et gazière s'est également retrouvée récemment sur le devant de la scène, notamment avec l'attaque par rançongiciels du fournisseur d'énergie américain Colonial Pipelines, qui a entraîné la fermeture des 8 800 kilomètres de son réseau d'oléoducs traversant les États-Unis. « Cet incident est l'une des cyberattaques par rançongiciels les plus perturbatrices jamais signalées et a attiré l'attention sur la vulnérabilité des infrastructures énergétiques américaines face aux pirates informatiques », a commenté Reuters. Les entreprises du secteur pétrolier et gazier devraient tirer les leçons qui s'imposent, d'autant plus que nos statistiques montrent que dans le classement Global 2000, ce secteur figure également dans la moitié inférieure de l'échelle d'efficacité. Seules 4 % des entreprises de ce secteur utilisent DNSSEC, et 10 % d'entre elles appliquent le Registry Lock (verrou de niveau registre).

En ce qui concerne le secteur bancaire, l'adoption de dispositifs de sécurité du nom de domaine et du DNS est plutôt inégale. Cela dit, pour un secteur qui est sans doute l'une des cibles prioritaires des attaques de phishing, l'adoption à 49,7 % du protocole DMARC d'authentification des e-mails reste désespérément faible.

Échelle d'efficacité de la mitigation des risques



Nos recommandations

La sécurité des noms de domaine est le chaînon manquant de la plupart des stratégies de cybersécurité. Mettre en place de meilleures mesures de sécurité pour vos noms de domaine peut vous permettre de contrer dès les premiers stades les attaques de phishing, les attaques BEC (Business Email Compromise) et les attaques par rançongiciels. De nombreux experts du secteur ont souligné l'importance de maintenir une « cyber-hygiène » solide. La sécurité des noms de domaine est un excellent exemple des insuffisances des entreprises en matière de cybersécurité. La sécurité des noms de domaine joue un rôle préventif contre les attaques de phishing, ce qui permet également de prévenir les attaques BEC, les fraudes par usurpation d'identité, les attaques par rançongiciels et bien d'autres menaces.

Toutes les entreprises, quel que soit leur secteur d'activité, et notamment celles qui sont plus exposées aujourd'hui en raison de la pandémie de Covid-19, sont tenues d'adopter une approche Défense en profondeur (DiD) multicouche afin de sécuriser leurs noms de domaine. Pour cela, elles doivent faire appel à un prestataire de services de niveau professionnel. CSC recommande quatre stratégies clés :

Adopter une approche Défense en profondeur (DiD) de la gestion des noms de domaine.

Vérifier que les pratiques commerciales de votre registrar ne contribuent pas à la fraude ni à l'abus de marque.

Surveiller en continu l'espace de nom de domaine et les canaux numériques clés comme les places de marché, les applis, les réseaux sociaux et les e-mails afin de repérer les abus de marque, les infractions et la fraude.

Mener des interventions au niveau mondial, y compris en obtenant la fermeture de certains sites et en appliquant des techniques avancées de blocage de contenu Internet.

ADOPTER UNE APPROCHE DÉFENSE EN PROFONDEUR (DiD) DE LA GESTION DES NOMS DE DOMAINE

- Éliminer les risques externes en évaluant la sécurité, la technologie et les processus de votre registrar de noms de domaine et de votre fournisseur DNS.
- Sécuriser vos noms de domaine critiques, votre infrastructure DNS et vos certificats numériques grâce à :
  - la mise en œuvre d'une authentification à deux facteurs
  - la surveillance de l'activité du DNS
  - l'utilisation de mesures de sécurité comme le Registry Lock (verrou de niveau registre), les protocoles DNSSEC et DMARC, les enregistrements CAA et la redondance de l'hébergement DNS

VÉRIFIER QUE LES PRATIQUES COMMERCIALES DE VOTRE REGISTRAR NE CONTRIBUENT PAS À LA FRAUDE NI À L'ABUS DE MARQUE

Les problèmes suivants apparaissent souvent chez les registrars grand public :

- l'exploitation de plateformes de vente de noms de domaine, qui capturent, mettent aux enchères et vendent au plus offrant des noms de domaines contenant des noms de marques déposées.
- le spinning de noms de domaine et la promotion de l'enregistrement de noms de domaine contenant des noms de marques déposées.
- la monétisation, à l'aide de sites sponsorisés, de noms de domaine contenant des noms de marques déposées.
- des failles de sécurité fréquentes facilitant les attaques DNS, de phishing et BEC.

SURVEILLER EN CONTINU L'ESPACE DE NOM DE DOMAINE ET LES PRINCIPAUX CANAUX NUMÉRIQUES COMME LES PLACES DE MARCHÉ, LES APPLIS, LES RÉSEAUX SOCIAUX ET LES E-MAILS AFIN DE REPÉRER LES ABUS DE MARQUE, LES INFRACTIONS ET LA FRAUDE

- Combiner la détection du phishing et l'exploitation d'un réseau de lutte contre la fraude composé d'éditeurs de navigateurs Internet, de divers partenaires, de FAI et de SIEM (sociétés de gestion des informations et des événements de sécurité).
- Identifier les tactiques de spoofing de noms de domaine et de DNS telles que les homoglyphes (correspondances floues et IDN), les noms de domaines similaires, les correspondances par mots-clés et les homophones.
- Identifier les abus de marques et les infractions au copyright présents dans le contenu en ligne.
- Protéger vos marques contre les utilisations abusives de leurs noms en assurant une surveillance des places de marché en ligne.
- Détecter toutes les mentions de vos marques sur les canaux de réseaux sociaux pertinents.
- Surveiller les principales boutiques d'applications mobiles.
- Identifier les annonces qui vous coûtent du trafic et portent préjudice à votre marque.

MENER DES INTERVENTIONS AU NIVEAU MONDIAL, Y COMPRIS EN OBTENANT LA FERMETURE DE CERTAINS SITES ET EN APPLIQUANT DES TECHNIQUES AVANCÉES DE BLOCAGE DE CONTENU INTERNET

- Combiner diverses mesures d'intervention pour lutter contre les atteintes à la propriété intellectuelle et la fraude :
  - les actions de premier niveau consistent en le déréférencement de la place de marché, la suspension des pages de réseaux sociaux, le retrait des applications mobiles, les lettres de mise en demeure, le retrait du contenu frauduleux et la limitation complète du vecteur d'attaque.
  - les actions de deuxième niveau consistent en la suspension du nom de domaine au niveau du registrar, la suspension du nom de domaine non valide dans la base de données WHOIS et les alertes avec notification de fraude.
  - les actions de troisième niveau consistent en le lancement de procédures UDRP/URS, les acquisitions de noms de domaine, les enquêtes approfondies et les achats-tests.
- Utiliser une série d'approches techniques et juridiques pour protéger vos droits, en choisissant l'approche la plus appropriée au cas par cas.

Adoption de mesures de sécurité par secteur

ADOPTION ÉLEVÉE ADOPTION FAIBLE

Registrar pour entreprises

Hôtellerie/restauration et Loisirs	75 %
Produits ménagers et personnels	68 %
Services et fournitures pour les entreprises	65 %
Médias	64 %
Logiciels et services IT	61 %
Chimie	57 %
Vente au détail	56 %
Médicaments et biotechnologies	56 %
Aérospatiale et défense	54 %
Semi-conducteurs	53 %
Équipements et services de santé	52 %
Biens d'équipement	47 %
Transports	47 %
Alimentation, boissons et tabac	47 %
Biens de consommation durables	46 %
Assurances	45 %
Matériel et équipements technologiques	42 %
Banques	38 %
Multinationales	38 %
Télécommunications	36 %
Sociétés commerciales	35 %
Services financiers diversifiés	35 %
Services publics	35 %
Opérations pétrolières et gazières	28 %
Construction	24 %
Matériaux	22 %
Marchés alimentaires	22 %

Le Registry Lock (verrou de niveau registre)

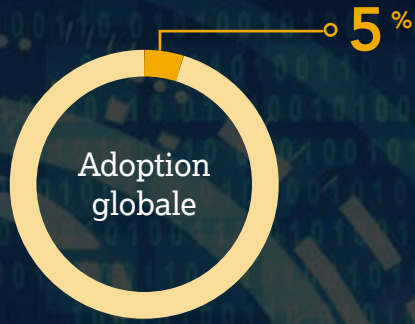
Logiciels et services IT	48 %
Médias	40 %
Aérospatiale et défense	33 %
Services et fournitures pour les entreprises	33 %
Semi-conducteurs	28 %
Télécommunications	28 %
Vente au détail	27 %
Chimie	27 %
Médicaments et biotechnologies	27 %
Équipements et services de santé	25 %
Biens de consommation durables	24 %
Biens d'équipement	23 %
Hôtellerie/restauration et Loisirs	21 %
Produits ménagers et personnels	21 %
Services financiers diversifiés	20 %
Transports	19 %
Matériel et équipements technologiques	19 %
Assurances	18 %
Alimentation, boissons et tabac	16 %
Banques	14 %
Multinationales	13 %
Services publics	11 %
Opérations pétrolières et gazières	10 %
Matériaux	9 %
Marchés alimentaires	6 %
Construction	6 %
Sociétés commerciales	3 %

ADOPTION ÉLEVÉE ADOPTION FAIBLE

Redondance DNS

Transports	28 %
Opérations pétrolières et gazières	25 %
Banques	23 %
Logiciels et services IT	23 %
Aérospatiale et défense	21 %
Sociétés commerciales	21 %
Télécommunications	20 %
Chimie	20 %
Semi-conducteurs	19 %
Assurances	19 %
Vente au détail	18 %
Services financiers diversifiés	17 %
Hôtellerie/restauration et Loisirs	17 %
Marchés alimentaires	16 %
Biens d'équipement	14 %
Biens de consommation durables	13 %
Matériaux	12 %
Services et fournitures pour les entreprises	12 %
Médias	12 %
Produits ménagers et personnels	12 %
Services publics	11 %
Médicaments et biotechnologies	11 %
Alimentation, boissons et tabac	10 %
Construction	9 %
Multinationales	9 %
Matériel et équipements technologiques	8 %
Équipements et services de santé	7 %

DNSSEC



Logiciels et services IT	14 %
Aérospatiale et défense	13 %
Médias	12 %
Banques	9 %
Semi-conducteurs	9 %
Services financiers diversifiés	6 %
Services publics	6 %
Services et fournitures pour les entreprises	6 %
Assurances	4 %
Télécommunications	4 %
Opérations pétrolières et gazières	4 %
Biens d'équipement	4 %
Biens de consommation durables	3 %
Sociétés commerciales	3 %
Médicaments et biotechnologies	3 %
Construction	2 %
Chimie	2 %
Matériel et équipements technologiques	2 %
Hôtellerie/restauration et Loisirs	0 %
Équipements et services de santé	0 %
Vente au détail	0 %
Transports	0 %
Produits ménagers et personnels	0 %
Alimentation, boissons et tabac	0 %
Multinationales	0 %
Matériaux	0 %
Marchés alimentaires	0 %

ADOPTION ÉLEVÉE ADOPTION FAIBLE

Enregistrements CAA

Médias	16 %
Logiciels et services IT	13 %
Opérations pétrolières et gazières	13 %
Banques	9 %
Services et fournitures pour les entreprises	8 %
Télécommunications	8 %
Multinationales	6 %
Services publics	6 %
Services financiers diversifiés	6 %
Chimie	5 %
Matériel et équipements technologiques	5 %
Équipements et services de santé	5 %
Hôtellerie/restauration et Loisirs	4 %
Transports	4 %
Assurances	4 %
Matériaux	3 %
Vente au détail	3 %
Médicaments et biotechnologies	3 %
Biens de consommation durables	2 %
Biens d'équipement	2 %
Construction	1 %
Alimentation, boissons et tabac	1 %
Semi-conducteurs	0 %
Aérospatiale et défense	0 %
Produits ménagers et personnels	0 %
Sociétés commerciales	0 %
Marchés alimentaires	0 %

DMARC

Logiciels et services IT	74 %
Équipements et services de santé	73 %
Semi-conducteurs	72 %
Médias	64 %
Hôtellerie/restauration et Loisirs	63 %
Vente au détail	60 %
Médicaments et biotechnologies	60 %
Opérations pétrolières et gazières	59 %
Multinationales	56 %
Télécommunications	56 %
Matériel et équipements technologiques	56 %
Alimentation, boissons et tabac	54 %
Services publics	54 %
Services et fournitures pour les entreprises	53 %
Aérospatiale et défense	50 %
Banques	50 %
Matériaux	47 %
Produits ménagers et personnels	47 %
Transports	46 %
Assurances	46 %
Services financiers diversifiés	43 %
Sociétés commerciales	41 %
Chimie	41 %
Biens de consommation durables	38 %
Marchés alimentaires	38 %
Biens d'équipement	37 %
Construction	28 %

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 sécurité et à sécuriser leurs noms de domaine, leur DNS et leurs certificats numériques. Les solutions de sécurité CSC protègent les entreprises contre les menaces de cyber-sécurité qui pèsent sur leurs actifs en ligne et elles les aident à 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.

Étude et éditorial CSC

Vincent D'Angelo, global director, Corporate Development and Strategic Alliances

Stephanie Mitchell, manager, Marketing

Quinn Taggart, senior advisor, Global Brand Security

Letitia Thian, manager, Marketing

Sue Watts, global leader, Marketing

cscdbs.com/fr

DBS09172021