L’impact de l’utilisation d’un registrar de noms de domaines corporate sur la note globale de sécurité

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St., 5th Floor
New York, NY 10001
1 800 682 1707

SecurityScorecard CSC

Résumé opérationnel

La plupart des cyber-attaques, y compris les attaques par rançongiciel et les attaques BEC (Business Email Compromise), commencent par du phishing. En effet, le phishing sert en quelque sorte de « rampe de lancement » lors de la phase initiale d'une attaque par rançongiciel. Bien qu'aujourd'hui les pertes annuelles dues aux rançongiciels se chiffrent en milliards[1], la plupart des mesures de protection et d'intervention face aux rançongiciels ne prennent pas suffisamment en compte les risques liés au phishing.

Des études sérieuses ont établi 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 avec le nom d'une marque peut prêter à confusion, d'un nom de domaine légitime compromis ou détourné, ou du spoofing par e-mail. Faire appel à un registrar de noms de domaine corporate permet de se protéger contre ces types de risque.

Le choix de votre registrar de noms de domaine est un indicateur de votre stratégie de sécurité globale en tant qu'entreprise.

Les recherches menées par SecurityScorecard montrent que le choix d'un registrar de noms de domaine est fortement corrélé à la note de cyber-sécurité qu'obtient une entreprise. Les organisations ayant opté pour des registrars corporate (RC) pour la gestion de leurs noms de domaines au lieu de registrars grand public (RGP) ont obtenu une note totale de sécurité en moyenne supérieure d'une demi-lettre, voire d'une lettre.

Composantes d’un registrar corporate

On distingue deux types de registrar : les registrars grand public et les registrars corporate. Les registrars grand public se concentrent sur les services de noms de domaine, les sites web et les messageries à usage personnel ou destinées aux petites entreprises. Même si les CGR ne sont pas intrinsèquement malveillants, ils ne proposent souvent aucune fonctionnalité de sécurité et de contrôle des noms de domaine ni aucun service de protection de la propriété intellectuelle (PI).

Les registrars corporate, quant à eux, ont notamment pour objectif d’aider les entreprises à se défendre contre les risques cyber. Ils se concentrent donc sur la cyber-sécurité et la protection de la propriété intellectuelle (PI) en mettant l’accent sur la sécurité des noms de domaine via des services et outils avancés. En outre, ils ne proposent pas de services de gestion des noms de domaine par le biais de sites web commerciaux, de sites sponsorisés, de génération en masse de noms de domaine (« domain spinning ») ou de vente aux enchères de noms de domaine, qui facilitent la violation de la propriété intellectuelle et les infractions sur les marques commerciales.

Caractéristiques clés d’un registrar corporate :

- **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 aux entreprises.
- **Services avancés** tels que le verrouillage du registre des noms de domaine, le protocole DMARC, DNSSEC, les enregistrements CAA et la redondance de l’hébergement DNS.
- **Assistance mondiale et locale 24x7x365** avec des capacités d’enregistrement de noms de domaine dans le monde entier.
- **Mise en œuvre de méthodes KYC (Know Your Customer)** pour identifier et valider les interactions avec les clients.
- **Offre des capacités de surveillance de l’espace de nom de domaine et des marques**, d’intervention, de désactivation et de retrait de tout contenu frauduleux.

Évaluer la sécurité du nom de domaine des entreprises du Forbes Global 2000

L'édition 2021 du Rapport CSC sur la sécurité des noms de domaine a révélé qu'en dépit du mouvement généralisé de modernisation des activités et des opérations parmi les entreprises du classement Global 2000, les noms de domaine Internet restent dangereusement sous-protégés. En 2021, les entreprises ont dû faire face à une augmentation des attaques par rançongiciel, des attaques BEC (Business Email Compromise), des attaques de phishing, des attaques de chaîne d'approvisionnement, sans compter les infractions sur les marques en ligne et commerciales. Malgré l'augmentation du risque cyber, les entreprises du Global 2000 de Forbes ont peu agi.

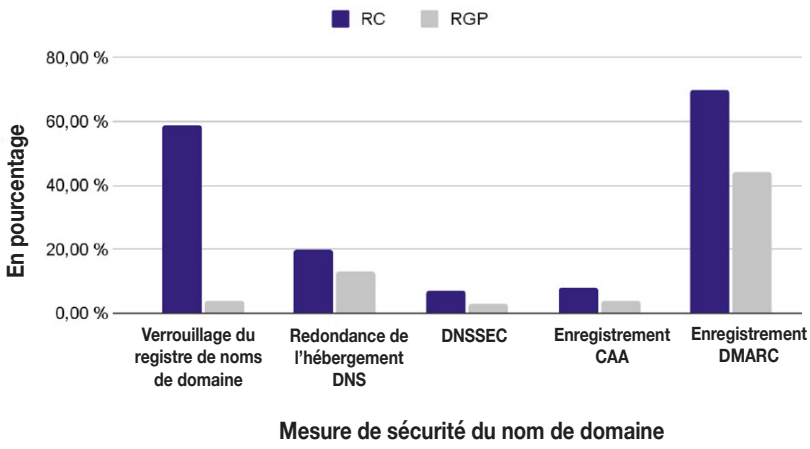
Les principales conclusions du rapport soulignent les risques liés à la sécurité des noms de domaine qui menacent les entreprises du Forbes Global 2000 :

- **70 % des domaines homoglyphes** (noms à concordance partielle), une tactique couramment utilisée pour le phishing et les infractions sur les marques, appartiennent à des tiers et sont enregistrés auprès de registrars grand public.
- **60 % de ces enregistrements de nom de domaine** ont été effectués 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 parce qu'elles n'ont PAS adopté de mesures de sécurité de base pour leurs noms de domaine, comme le protocole de verrouillage du registre de noms de domaine.
- **57 % des entreprises se fient 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.
- **Seules 50 % des entreprises appliquent le protocole DMARC.**

L'étude confirme également ces résultats en comparant la mise en œuvre des mesures de sécurité du nom de domaine pour le groupe d'entreprises faisant appel à un RC (« groupe RC ») par rapport au groupe d'entreprises ayant recours à un RGP (« groupe RGP »).

Mise en œuvre des mesures de sécurité du nom de domaine – Entreprises du classement Forbes 2000

Groupe RC / Groupe RGP



Le recours à un registrar corporate entraîne une augmentation d'une demi à une lettre de la note globale SecurityScorecard

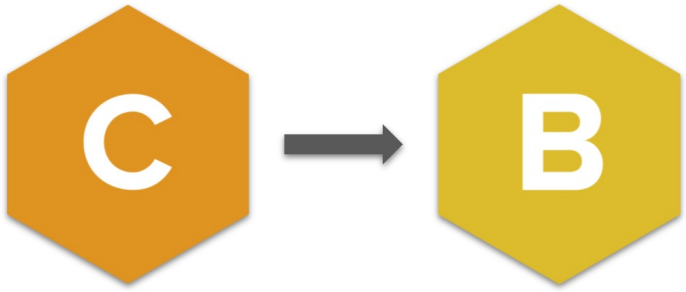
La notation de sécurité met en lumière la nécessité de privilégier la sécurité du nom de domaine

SecurityScorecard a passé en revue les notes de sécurité de 50 000 des entreprises les plus suivies sur sa plateforme et les résultats confirment la nécessité de donner la priorité à la sécurité des noms de domaine et des services DNS avec un registrar corporate fiable. Les entreprises ayant opté pour des registrars corporate pour la gestion de leurs noms de domaine ont obtenu une note totale supérieure d'au moins une demi-lettre à celle des entreprises faisant appel à un registrar grand public. Dans notre analyse, la différence se situe entre une note globale « C » et une note « B ».

Les recherches de SecurityScorecard confirment que le choix du registrar pour votre nom de domaine est une décision cruciale qui, bien que souvent négligée, permet de renforcer la stratégie de sécurité globale de votre organisation.

Quantifier l'impact d'un registrar de noms de domaine corporate sur la note globale de sécurité d'une entreprise

Sur les 50 000 entreprises examinées par SecurityScorecard, celles qui font appel à un registrar grand public ont obtenu une note SecurityScorecard moyenne de 76,92. Les entreprises ayant recours à un registrar corporate ont obtenu une note SecurityScorecard moyenne de 81,73, soit 5 points de plus en moyenne. Cette différence se serait traduite par une lettre supplémentaire, soit un « C » au lieu d'un « B » pour le groupe RC par rapport au groupe RGP.



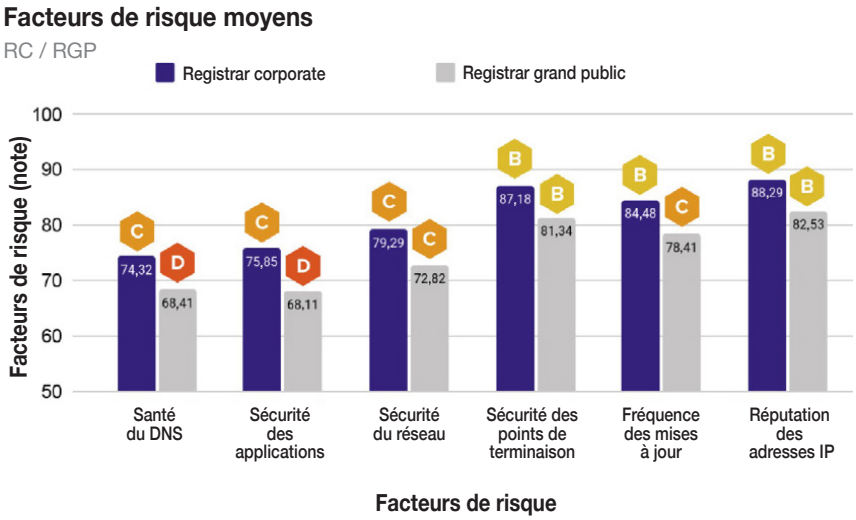
La santé du DNS constitue le facteur de risque le moins élevé bien qu'étant un facteur de notation essentiel

La plateforme SecurityScorecard évalue plusieurs paramètres de configuration DNS, tels que les configurations OpenResolver ainsi que la présence de configurations recommandées, notamment DNSSEC, SPF, DKIM et DMARC.

Bien qu'il s'agisse d'un facteur de notation important dans l'algorithme de notation de SecurityScorecard, les entreprises analysées ont obtenu une note moyenne de 71,36 pour la santé du DNS (note correspondant à la lettre « C »). Par conséquent, la santé du DNS est le facteur de notation le moins important parmi ceux que nous avons analysés. Le groupe RC a obtenu une note moyenne SecurityScorecard relative au facteur de santé du DNS de 74,32 contre 68,41 pour le groupe RGP, soit un écart de près de 6 points. Ce résultat a entraîné une différence d'une lettre, de « C » à « D », pour les deux groupes.

La santé du DNS influence d'autres facteurs de risque critiques

Notre étude a également montré que d'autres facteurs de notation, tels que la sécurité des applications, la sécurité du réseau, la sécurité des points de terminaison, la fréquence des mises à jour et la réputation des adresses IP, représentaient un écart de plus de 5 points pour le groupe RC par rapport au groupe RGP, soit un avantage d'une lettre pour plusieurs facteurs de notation.



Cette analyse montre que l'adoption de mesures de sécurité proactives en faveur des noms de domaine contribue à améliorer la santé du DNS ainsi que d'autres facteurs de notation, ce qui entraîne une note de sécurité globale plus élevée.

CSC et SecurityScorecard : Une alliance basée sur les principes fondamentaux de prévention des risques cyber

SecurityScorecard, le leader mondial de l'évaluation de la sécurité, a conclu une alliance stratégique avec CSC pour offrir à ses clients des recommandations de premier ordre sur la sécurité des noms de domaine. En prenant des mesures judicieuses et proactives pour se protéger contre les attaques visant les noms de domaine et le DNS, les entreprises et les compagnies d'assurance en matière de cyber-sécurité sont plus à même d'identifier les risques cyber potentiels, les infractions sur les marques commises à l'aide de tactiques de phishing et les failles de sécurité avant qu'elles ne se produisent.

Si la sécurité des noms de domaine exige une approche Défense en profondeur (DiD) dotée de mesures de sécurité et de protocoles opérationnels avancés, le type de registrar que vous choisissez revêt également une grande importance alors que l'on constate l'impact que peut avoir une attaque de la chaîne d'approvisionnement – aussi appelée « attaque Supply Chain » – comme celle qui a frappé SolarWinds. La façon traditionnelle d'envisager la sécurité DNS se concentrait davantage sur la résilience et la résolution du DNS, ainsi que sur la protection DDoS associée. Un élément clé de la santé du DNS qui est négligé aujourd'hui est la façon dont les noms de domaine et le DNS sont détournés pour mener des attaques malveillantes contre une entreprise et ses clients.

Les trois piliers de la sécurité du nom de domaine

CSC met l'accent sur la sécurité du nom de domaine à trois niveaux :

1. Assurez-vous que les noms de domaine légitimes et les services DNS associés ne sont pas compromis chez votre registrar de noms de domaine ou votre fournisseur d'hébergement DNS (piratage de noms de domaine, de DNS et de sous-domaines).
2. Surveillez et faites désactiver les noms de domaine tiers malveillants.
3. Assurez-vous d'utiliser l'authentification par e-mail pour vous protéger contre le spoofing par e-mail.

Les bonnes pratiques de CSC en matière de sécurité du nom de domaine

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 registrar corporate.

CSC recommande quatre stratégies clés :

1. Adopter une approche Défense en profondeur (DiD) de la gestion du nom de domaine.
2. Vérifier que les pratiques commerciales de votre registrar ne contribuent pas à la fraude ni aux infractions sur les marques.
3. Surveiller en continu l'espace de nom de domaine et DNS et les canaux numériques clés comme les places de marché, les applications, les réseaux sociaux et les messageries pour repérer les infractions sur les marques, les infractions, le phishing et les fraudes.
4. Mener des interventions au niveau mondial, y compris en obtenant la fermeture de certains sites et en appliquant des techniques avancées de désactivation et blocage de contenu Internet.

Conclusion

La prolifération constante des rançongiciels et les problèmes de sécurité résultant des politiques de télétravail ont fait du choix d'un registrar de noms de domaine fiable une décision stratégique pour les responsables de la mitigation des risques de cyber-sécurité et de la protection des marques en ligne. Le choix d'un registrar corporate qui donne la priorité à la sécurité, à la gouvernance des données et à la fourniture d'un support technique de niveau mondial est essentiel à la fois pour protéger la marque d'une entreprise et la sécurité de ses clients.

SecurityScorecard et CSC se sont associés afin d'informer les entreprises et d'atténuer les risques de sécurité posés par le manque de mesures de sécurité du nom de domaine, la première étant la sélection d'un registrar adéquat.

Déclaration finale

Inscrivez-vous ici pour recevoir une licence SecurityScorecard Enterprise gratuite afin d'évaluer la sécurité de votre organisation et jusqu'à cinq fournisseurs vos fournisseurs.

Inscrivez-vous pour bénéficier d'un Audit de sécurité du nom de domaine CSC gratuit ici.

[1] https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=75f066bf71c6

Ressources

Pour une liste complète des bonnes pratiques :

Rapport 2021 sur la sécurité des noms de domaine de CSC

Blog CSC

Five Steps to a Modern Cyber Risk Management Team (Cinq étapes pour une équipe moderne de gestion des risques cyber – en anglais)

The Perfect Scorecard: Getting an A in Cybersecurity from your Board of Directors (La notation Scorecard idéale : quand votre Conseil d'administration vous octroie un A en cyber-sécurité – en anglais)

Blog SecurityScorecard (en anglais)

À propos de CSC

CSC est le partenaire de confiance des entreprises figurant aux classements Forbes Global 2000 et 100 Best Global Brands® pour tout ce qui concerne les noms de domaine, les services DNS et la gestion des certificats numériques, et propose des solutions de protection des marques en ligne contre la fraude et le phishing. Nous protégeons les entreprises contre les menaces de cyber-sécurité qui pèsent sur leur patrimoine numérique, et nous les aidons à éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières importantes. Nous fournissons également des services de protection des marques en ligne, qui combinent la surveillance de marque et les interventions ciblées en cas d'infraction, et proposons une approche globale de la protection des actifs numériques. Pour en savoir plus sur nos services de gestion des noms de domaine, de sécurité, de protection de marque et de protection contre la fraude, rendez-vous sur cscdbs.com.

À propos de SecurityScorecard

SecurityScorecard aide les entreprises à bénéficier d'un contrôle opérationnel de leur stratégie de sécurité et de celle de leurs prestataires grâce à une surveillance continue et non intrusive. En matière de sécurité, l'approche SecurityScorecard se concentre sur l'identification des vulnérabilités d'un point de vue extérieur, comme le ferait un hacker. La plateforme SaaS développée par SecurityScorecard offre une étendue et une profondeur inégalées de points de données critiques, et prend en compte un large éventail de catégories de risques telles que la sécurité des applications, les logiciels malveillants, la fréquence des mises à jour, la sécurité des réseaux, les flux de discussion entre hackers, les techniques d'ingénierie sociale et les fuites d'informations.

Pour recevoir la note actuelle de votre entreprise par e-mail, rendez-vous sur instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682 1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
214 West 29th St., 5th Floor
New York, NY 10001