RAPPORT DE CYBER-SÉCURITÉ

Juin 2019

Ken Linscott *Directeur produits – Domaines et sécurité*

Quinn Taggart *Responsable produits principal– Domaines*

Letitia Thian *Responsable marketing*

Recherche et éditorial par CSC

Ce rapport de cyber-sécurité CSC regroupe dans un document qui se veut exhaustif les données les plus importantes et les plus récentes en matière de cybercriminalité et de cyber-sécurité. Il vous offre un aperçu détaillé des informations essentielles pour vous et votre marque.

Sécurité du nom de domaine

CSC collabore avec plus de 65% des plus grandes marques mondiales

CSC assiste plus de 65 % des plus grandes marques mondiales dans la gestion de leur présence en ligne. À l'aide de nos outils brevetés, nous aidons les entreprises de nos clients à identifier les failles de sécurité et les opportunités stratégiques au sein de leur portefeuille de noms de domaine. Nous nous appuyons sur cette même méthodologie pour analyser les principaux noms de domaine des entreprises du monde entier afin de déterminer l'efficacité de leur sécurité en matière de noms de domaine.

Dans ce rapport, nous allons nous intéresser plus particulièrement au secteur des médias. Avec des technologies en pleine évolution et des consommateurs toujours plus friands de contenus à la demande, les médias traditionnels ont été remplacés par les formats numériques et mobiles. Les réseaux sociaux, le streaming en ligne et la publicité sur Internet, par exemple, sont apparus au cours des 25 dernières années de cette ère de changement. De nombreuses marques médias disposent désormais d'une présence en ligne et collectent davantage de données client qu'auparavant. Les entreprises recueillent à la fois des identifiants de connexion et des informations de paiement, ce qui les expose d'autant plus aux risques de cyber-attaques susceptibles de causer un dysfonctionnement, voire un détournement des canaux de distribution médias. Il est donc devenu impératif pour les marques de prendre des mesures pour se protéger et protéger leurs clients contre les attaques ou intrusions éventuelles.

Dans ce rapport, nous avons analysé certains des plus grands groupes médias dans le monde, leurs entités et leurs marques à travers un éventail de canaux incluant la publicité, l'édition, la télévision et la radio. Nous nous sommes également penchés sur quelques marques uniquement présentes en ligne, afin de découvrir comment la sécurité du nom de domaine est abordée dans ce secteur.

Sécurité du nom de domaine et tendances observées

Basé sur 120 marques médias

Le dernier rapport de CSC était consacré au secteur de la finance et des assurances. Cette édition dédiée aux médias nous permet de comparer les différents secteurs et leur rapport aux composantes de la sécurité des noms de domaine. Toutes les mesures de sécurité ne sont pas coûteuses – surtout si l'on considère le coût potentiel d'une seule intrusion. Pourtant, même les éléments de sécurité fondamentaux ne sont pas aussi généralisés que l'on pourrait espérer vu l'augmentation des cyber-menaces année après année. Le plus troublant est que les techniques les plus simples, permettant de garantir la sécurité globale du nom de domaine et la confiance des utilisateurs, sont les moins susceptibles d'être mises en œuvre par les entreprises.

Fournisseur de registrar

78% CORPORATE REGISTRAR POUR ENTREPRISES

22% REGISTRAR COMMERCIAL

RISQUE

Traditionnellement, ce sont les registrars (bureaux d'enregistrement) de noms de domaine commerciaux qui sont les plus visés par les cyberattaques. Les entreprises devraient s'associer à un registrar de niveau professionnel qui investit lourdement au niveau technologique, mais également dans la formation à la sécurité de ses employés – y compris en instaurant le devoir de vigilance dans sa charte – afin de pouvoir identifier les attaques malveillantes, particulièrement pour les noms de domaine stratégiques.

OBSERVATIONS

78 % des médias utilisent les registrars professionnels

Lors de l'évaluation de la sécurité du nom de domaine au niveau de base, un petit nombre d'éléments clés sont examinés : verrous, messagerie, système de noms de domaine (DNS) et certificats SSL (Secure Sockets Layer). Bien entendu, la gestion du portefeuille global de noms de domaine par un registrar pour entreprises réputé, par opposition au registrar commercial, facilitera l'implémentation de ces éléments. C'est pourquoi la majorité des acteurs du secteur des médias privilégient les registrars pour entreprises pour la gestion de leur portefeuille de noms de domaine.

Verrouillage

43% REGISTRE VERROUILLÉ

37% REGISTRE NON VERROUILLÉ

20% *VERROUILLAGE DU REGISTRE NON DISPONIBLE

RISQUE

Les noms de domaine non verrouillés sont vulnérables aux tactiques d'ingénierie sociale, qui peuvent conduire à des modifications non autorisées du DNS. Il arrive toutefois que certains noms de domaine demeurent non verrouillés, tous les registres du monde ne disposant pas de services de verrouillage.*

OBSERVATIONS

43 % ont mis en place un verrouillage du registre

Ces verrous sont de plus en plus plébiscités parce qu'ils empêchent toute modification non autorisée du DNS, modification qui pourrait mettre le site hors ligne ou rediriger ses utilisateurs vers du contenu malveillant

Sécurité du nom de domaine et tendances observées

Fournisseur DNS

25% DNS INTERNE

55% DNS D'ENTREPRISE OU PROFESSIONNEL

20% AUTRES (DNS HÉBERGEUR OU COMMERCIAL)

RISQUE

Les fournisseurs de services DNS non destinés aux entreprises présentent des risques de sécurité potentiels, avec la possibilité d'attaques DDoS (Distributed Denial of Service), d'interruption des services et de perte de revenus.

Always-On SSL (AOSSL)

78% ALWAYS-ON SSL, DÉPLOYÉ

22% ALWAYS-ON SSL, NON DÉPLOYÉ

RISQUE

Le protocole SSL chiffre de façon sécurisée toutes les activités transactionnelles en ligne, contribuant ainsi à réduire le risque de détournement de sessions web par des cybercriminels en vue de commettre des usurpations d'identité ou d'installer des logiciels malveillants sur les appareils des utilisateurs. Il permet aussi de lutter contre l'atteinte par des hackers aux communications web, pouvant générer une violation de la confidentialité des données, un vol des données clients, une attaque DDoS ou une dégradation de site web.

DNSSEC

3% DNSSEC ACTIVÉ

97% DNSSEC DÉSACTIVÉ

RISQUE

L'absence de déploiement de DNSSEC (domain name system security extension) – un des protocoles de sécurité les plus économiques – entraîne des vulnérabilités au niveau du DNS et peut permettre le détournement d'une étape du processus de résolution DNS. Les pirates sont donc en mesure de prendre le contrôle d'une session de navigation Internet pour rediriger les utilisateurs vers des sites Web falsifiés.

OBSERVATIONS

55 % utilisent des fournisseurs de DNS d'entreprise ; 3 % utilisent DNSSEC

La préférence pour les registrars pour entreprises semble s'appliquer également aux fournisseurs de DNS de niveau entreprise pour la moitié des marques médias. Presque 25 % utilisent leur propre architecture DNS et 20 % font appel à un fournisseur commercial. Les services DNS font certainement partie des prestations pour lesquelles les entreprises ne devraient pas transiger en termes de qualité et de fiabilité. Le DNS est le moteur de la présence en ligne. Le protocole DNSSEC est une autre méthode pour protéger la communication globale entre les utilisateurs et les propriétés d'un site Web. Les taux d'adoption de la technologie DNSSEC ne dépassent toutefois pas les 3 %.

Sécurité du nom de domaine et tendances observées

Type de certificats SSL (EV, DV ou OV)

2% EV

74% OV

24% DV

RISQUE

Les certificats SSL qui exigent un niveau d'authentification plus élevé, tels que les certificats à validation d'organisation (OV) et à validation étendue (EV), sont moins susceptibles d'être compromis que les certificats à validation de domaine (DV).

OBSERVATIONS

74 % utilisent des certificats OV, tandis que 24 % utilisent des certificats DV

Comme pour les DNS, il n'est pas judicieux de choisir des certificats numériques présentant une sécurité moindre. Si le DNS est la porte de la maison, le certificat SSL en est la serrure. Peu importe que la porte soit solide, dès lors que la serrure est peu fiable. Un facteur de risque majeur réside dans le mode de validation des certificats SSL. La validation de domaine, qui offre le plus faible niveau de validation, est utilisée par 24 % des marques médias, ce qui signifie que si un hacker parvient à accéder à la messagerie interne, il peut facilement valider les certificats SSL à partir des domaines de l'entreprise – dans un but malveillant. C'est le scénario de la dernière attaque menée par le biais du registrar commercial GoDaddy®.

Authentification par e-mail

27% DMARC

79% SPF

6% DKIM

RISQUE

L'authentification du canal de messagerie par le protocole DMARC (Domain-based Message Authentication, Reporting and Conformance), SPF (Sender Policy Framework) ou DKIM (DomainKeys Identified Mail) réduit le risque d'e-mail spoofing (usurpation d'identité) et de phishing.

OBSERVATIONS

27 % utilisent DMARC

La technologie DMARC est un système d'authentification d'e-mails conçu pour protéger le nom de domaine de messagerie d'une entreprise contre les tentatives de spoofing, de phishing et autres cyberattaques. Pour des entreprises qui communiquent avec des millions d'utilisateurs, la faiblesse du taux d'adoption est surprenante.

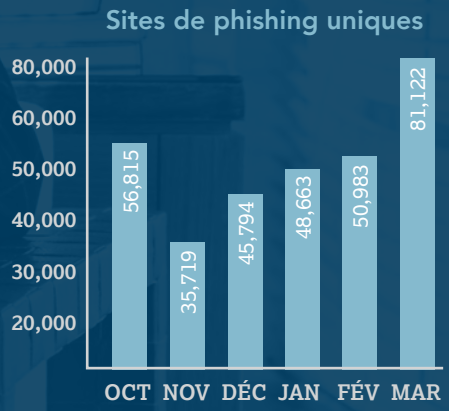
Phishing et fraude par e-mail

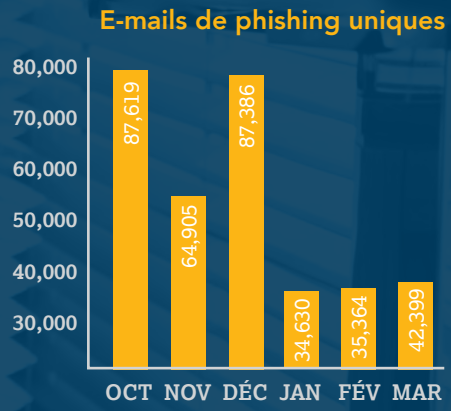
Augmentation importante des sites Web de phishing durant l'année

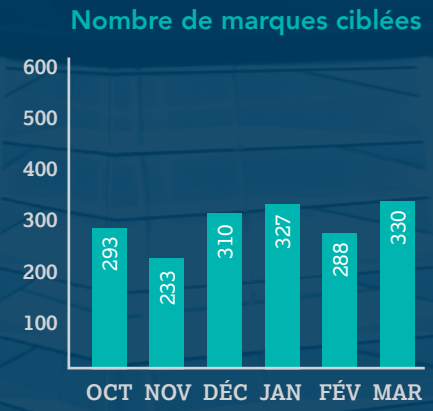
Au premier trimestre 2019, environ 58 % des sites de phishing possédaient des certificats SSL, ce qui représente une importante augmentation par rapport aux 46 % du trimestre précédent et aux moins de 5 % de la fin 2016. Deux raisons peuvent expliquer cette augmentation. Premièrement, les pirates peuvent créer des certificats à validation de domaine, qui sont disponibles librement. Deuxièmement, un nombre croissant de sites Web utilisent des certificats SSL en général. La majorité des opérations de phishing partant de sites légitimes piratés, le nombre de sites de phishing avec SSL est logiquement en augmentation. Ces derniers ont une apparence plus légitime grâce à la mention « HTTPS » dans la barre d'adresse. Ils parviennent donc à tromper les utilisateurs en détournant une fonctionnalité de sécurité d'Internet, et permettent aux acteurs malintentionnés de voler les données d'identité ainsi que les identifiants de compte.

Attaques de phishing

Au premier trimestre 2019, on a dénombré 180 768 sites Web de phishing, soit une augmentation de 31 % par rapport au trimestre précédent.







Secteurs d'activité les plus touchés

Pour la première fois, les services SaaS (logiciel en tant que service) et les messageries Web constituent les secteurs les plus touchés. Les services de paiement en ligne et les institutions financières restent parmi les trois secteurs les plus visés par le phishing au début de l'année 2019.

SOURCE: Rapport APWG « Phishing Activity Trends Report », premier trimestre 2019

Noms de domaine de premier niveau (TLD) les plus utilisés pour les sites de phishing

Sans surprise, les TLD hérités – c'est-à-dire les TLD établis il y a très longtemps et qui comptent un grand nombre de sites Web – sont ceux qui hébergent le plus de hameçonneurs. Toutefois, les TLD de code pays (ccTLD) qui ont été redéfinis, ainsi qu'un petit nombre de TLD génériques souvent proposés à bas prix, hébergent une quantité notable d'opérations de phishing par rapport aux autres noms de domaine dans le monde.

Types de TLD :

gTLD hérités | ccTLD | Nouveaux gTLD

.com n° 1 • 2 098 noms de domaine	.pw n° 2 • 374 noms de domaine	.net n° 3 • 175 noms de domaine	.org n° 4 • 154 noms de domaine
.uk n° 5 • 121 noms de domaine	.cf n° 6 • 84 noms de domaine	.info n° 7 • 83 noms de domaine	.br n° 8 • 82 noms de domaine
.ml n° 9 • 78 noms de domaine	.ga n° 10 • 68 noms de domaine	.in n° 11 • 58 noms de domaine	.us n° 12 • 45 noms de domaine
.ru n° 13 • 44 noms de domaine	.tk n° 14 • 40 noms de domaine	.gq n° 15 • 37 noms de domaine	.it n° 16 • 37 noms de domaine
.xyz n° 17 • 37 noms de domaine	.online n° 18 • 33 noms de domaine	.pl n° 19 • 28 noms de domaine	.ca n° 20 • 26 noms de domaine

SOURCE : Rapport APWG « Phishing Activity Trends Report », quatrième trimestre 2018

Toutes les organisations sont concernées

Exemples issus des actualités

AMÉRIQUES

Des grands noms de la presse américaine paralysés par l'attaque du ransomware Ryuk

Le ransomware a mis hors service l'infrastructure de grands organes de presse, affectant la publication et la diffusion de l'édition papier des quotidiens dans tout le pays.

csoonline.com/article/3330645/major-us-newspapers-crippled-by-ryuk-ransomware-attack.html

AMÉRIQUES

Les sites Newsquest compromis par une faille de sécurité

Des centaines de titres du site Web du groupe de médias ont été infectés par des logiciels malveillants qui ont piraté les navigateurs Internet et mobiles au moment où les utilisateurs tentaient d'accéder aux actualités locales, en les redirigeant vers un site non affilié proposant un jeu de loterie.

uknip.co.uk/2019/02/newsquest-websites-compromised-by-security-breach/

FRANCE

Plateforme de partage vidéo visée par des attaques par bourrage d'identifiants (credential stuffing)

Des cybercriminels ont mené des attaques par bourrage d'identifiants – des « attaques frontales » devinant ou réutilisant des mots de passe volés – à l'encontre d'une plateforme de partage vidéo afin de pirater les comptes des utilisateurs.

securityboulevard.com/2019/01/video-sharing-platform-targeted-by-credential-stuffing-attacks/

PHILIPPINES

De puissants groupes de hackers sophistiqués attaquent des sites de médias alternatifs philippins

Des hacktivistes politiques ont lancé des attaques DDoS sur des sites de médias philippins en générant un trafic 40 000 fois supérieur à la normale, avec 40 attaques en une semaine.

news.abs-cbn.com/news/02/07/19/big-rich-tech-teams-attack-ph-alternative-media-websites

AMÉRIQUES

Une nouvelle variante du logiciel malveillant Mirai cible les TV à affichage dynamique et les systèmes de présentation

Des chercheurs ont découvert une nouvelle souche du botnet Mirai qui vise les appareils IoT des entreprises, en vue de lancer des attaques DDoS massives similaires à l'attaque Mirai de 2016 contre un fournisseur de services DNS, qui avait entraîné l'inaccessibilité de sites majeurs et de services Internet en Amérique du Nord et en Europe.

zdnet.com/article/new-mirai-malware-variant-targets-signage-tvs-and-presentation-systems/

Recommandations

1. RENOUVELLEMENT AUTOMATIQUE DES NOMS DE DOMAINE

Avec des registrars commerciaux, si la carte de crédit enregistrée expire ou est annulée, le renouvellement automatique est sans effet et les noms de domaine sont mis hors ligne, voire supprimés. Recourir aux services d'un registrar professionnel garantit que les noms de domaine sont renouvelés automatiquement, à moins que l'entreprise n'indique son souhait de ne pas voir renouveler certains. Vous avez ainsi l'assurance qu'aucun nom de domaine ne deviendra inaccessible.

cscdigitalbrand.services/blog/an-abandoned-domain-name-could-hurt-you/

2. VERROUILLAGE DES NOMS DE DOMAINE CRITIQUES

Un autre avantage de la collaboration avec un registrar professionnel réside dans la structure de support. Celle-ci doit offrir la combinaison idéale de technologie et d'expertise métier. Pour procéder au verrouillage des noms de domaine, les entreprises doivent identifier ceux qui sont critiques – ce qui n'est pas aussi simple qu'il y paraît. CSC Security Center℠ met à votre disposition la technologie requise pour identifier vos noms de domaine vitaux, en surveillant le trafic Web ainsi que de multiples vecteurs dans le but d'implémenter une sécurité multicouche.

cscglobal.com/service/csc/press-csc-alerts-companies-to-increased-dns-hijacking/

3. ADOPTER DES MESURES DE SÉCURISATION DES NOMS DE DOMAINE

Sans une bonne fondation, la forteresse s'écroule. Une fois que vous avez choisi le registrar de noms de domaine pour entreprises le plus adapté, procédez à un inventaire minutieux de votre portefeuille de noms de domaine et des mesures de protection mises en place. Le paysage de la sécurité informatique évolue sans cesse et vous impose de faire appel à un partenaire de confiance vigilant pour adapter votre stratégie. La sécurité n'est pas une démarche que vous définissez une fois pour toute, elle est de nature cyclique : de nouvelles techniques d'attaque sont constamment développées par les cybercriminels.

cscdigitalbrand.services/blog/dns-une-composante-fondamentale-trop-souvent-negligee-5e-partie/

4. IMPLIQUER D'AUTRES ACTEURS

La sécurité et la gestion du portefeuille de noms de domaine ne devraient pas être dévolues à une seule personne : elles touchent diverses parties prenantes au niveau du marketing, du cadre juridique, de la gestion des marques et de l'informatique. Toutes les contributions sont donc importantes. Nous recommandons aux entreprises d'établir un processus de consultation pour la gestion des noms de domaine, parce que la sécurité est l'affaire de tous.

5. SENSIBILISER LE C.A. AUX RISQUES LIÉS AU DNS

Avec des attaques au niveau mondial et des violations de grande ampleur, outre la conformité réglementaire, la cyber-sécurité est désormais une priorité majeure pour les conseils d'administration. Parmi les risques identifiés dans le rapport « Horizon Scan » du BCI (Business Continuity Institute), le DNS est un facteur important dans quatre des 10 risques majeurs.

cscdigitalbrand.services/blog/dns-une-composante-fondamentale-trop-souvent-negligee-6e-partie/

CSC accompagne les entreprises dans leur réussite en ligne. Nous aidons nos clients à gérer, promouvoir et sécuriser efficacement leurs actifs stratégiques face aux menaces du monde numérique. Les plus grandes entreprises du monde entier, parmi lesquelles plus de 65 % des 100 Best Global Brands du classement Interbrand®, ont fait de nous leur partenaire de confiance. S'appuyant sur une technologie de pointe, notre offre Digital Brand Services garantit des résultats exceptionnels via une structure de gestion de compte unifiée.Grâce à notre équipe d'experts dédiés, vous disposerez d'un point de contact qui vous permettra d'assurer au quotidien que votre marque possède les atouts nécessaires pour réussir à l'ère du numérique. Nous vous aidons à consolider, sécuriser et surveiller vos actifs immatériels, à intervenir en cas d'atteinte à vos marques, puis à optimiser et promouvoir celles-ci afin de maximiser votre présence en ligne et de sécuriser vos droits de propriété intellectuelle numérique – tout en réduisant vos coûts.

cscdigitalbrand.services/fr