Argos™ Balise de phishing par Cyberint

Identifiez les menaces émergentes avant qu'elles ne détruisent l'image de votre marque

Cyberint

PROBLÈME DE LONGUE DATE : LE PHISHING ET LES MENACES DE D'ABUS DE MARQUE

EN MOYENNE, 80 000 NOUVEAUX SITES DE PHISHING SONT CRÉÉS CHAQUE MOIS. CE CHIFFRE AUGMENTE SANS CESSE.

D'année en année, les attaques de phishing deviennent de plus en plus sophistiquées et ciblées. Le temps où les attaquants jetaient un large filet en croyant qu'en ciblant suffisamment d'entreprises, un nombre substantiel d'utilisateurs mordrait à l'appât est révolu. De nos jours, les assaillants passent des mois à planifier leurs attaques et à lancer des escroqueries par hameçonnage qui ciblent directement une organisation spécifique, y compris les clients et les employés de celle-ci. En usurpant l'identité du site web de l'organisation (par exemple, sa page de connexion), les auteurs de la menace obtiennent de plus en plus de succès grâce aux techniques de phishing. Les techniques en question leur permettent de voler des identifiants ou des données sensibles et de les utiliser à des fins financières ou pour prendre pied dans votre écosystème organisationnel.

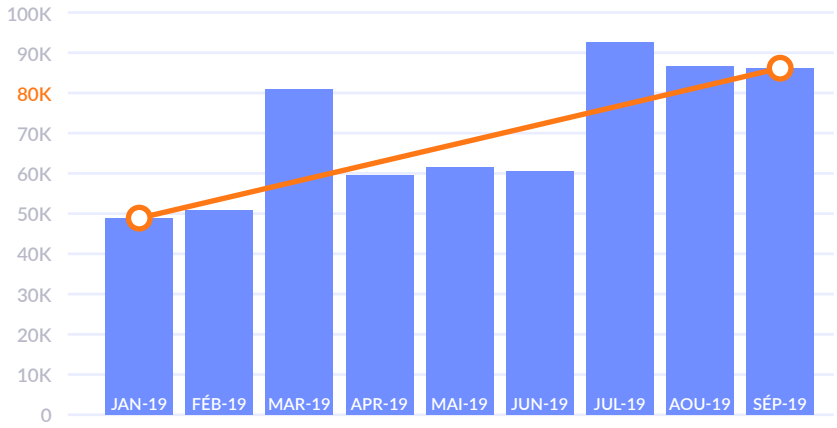


Figure 1 : Sites de phishing T1-T3 2019
(Rapport APWG sur les tendances de l'activité de phishing au T3 de 2019)

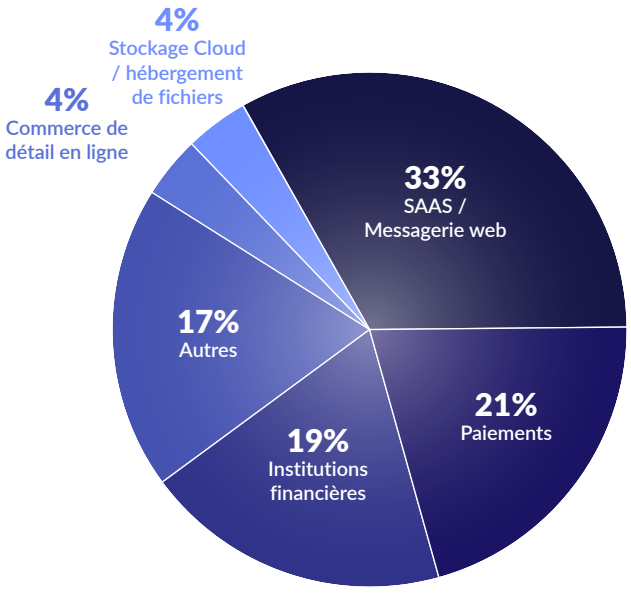


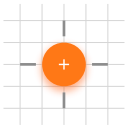
Figure 2 : Secteurs industriels les plus ciblés, T3 2019
(extrait du rapport APWG sur les tendances de l'activité de phishing au T3 de 2019)

Les dommages potentiels d'une attaque de phishing réussie pour une organisation sont énormes, ils peuvent nuire aux opérations de sécurité, à la réputation de la marque, ainsi qu'à la confidentialité et la conformité des données. En fait, le coût moyen d'une attaque de phishing pour une entreprise de taille moyenne est de 1,6 million de dollars, alors que pour les grandes entreprises, ce coût passe à 3,7 millions de dollars[1]. Comme le montre la figure 2, ces menaces planent sur toutes les industries.

[1] https://blog.dashlane.com/phishing-statistics/
https://www.csoonline.com/article/2975807/phishing-is-a-37-million-annual-cost-for-average-large-company.html

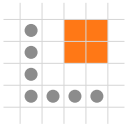
COMMENT LES ASSAILLANTS LANCENT-ILS DES ESCROQUERIES PAR HAMEÇONNAGE ?

Pour comprendre comment faire face à cette menace, les entreprises doivent se mettre dans l'esprit des assaillants d'aujourd'hui et voir à quel point il est facile de lancer des sites web de phishing et d'échapper à la détection. Voici quelques-unes des principales méthodes utilisées par les attaquants et les raisons qui font que les solutions de cybersécurité traditionnelles ne sont pas à la hauteur.



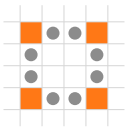
PHISHING-AS-A-SERVICE

Dans de nombreux cas, les sites de phishing qui ciblent une certaine organisation sont le résultat de l'exécution d'un « kit de phishing ». Un kit de phishing est un ensemble d'outils logiciels qui permet aux personnes ayant peu ou pas de compétences techniques de lancer une attaque de phishing. Sur le Dark Web, ce type de logiciel criminel est vendu pour aussi peu que 50 $ et peut être lancé en quelques heures. Par conséquent, les plateformes de risques numériques n'ont que très peu de temps pour localiser la menace avant que votre marque ne soit déjà attaquée.



ENREGISTREMENT DE FAUX DOMAINES

Chaque site web de phishing doit être inscrit. Par conséquent, l'analyse des domaines nouvellement inscrits ou de domaines ayant de nouveaux certificats peut aider à réduire le nombre de sites web de phishing qui sont mis en ligne avec succès. Toutefois, des assaillants intelligents ont trouvé des solutions de contournement, notamment en hébergeant le site Web malveillant sur un sous-domaine d'un site web légitime qui n'a aucun lien avec la marque attaquée. Dans ces cas, les organisations peuvent ne pas se rendre compte de l'existence d'un site web malveillant qui usurpe l'identité du leur, jusqu'à ce que leurs clients signalent un vol d'identité ou jusqu'à ce qu'une fuite de données soit découverte. À ce stade, nul besoin de rappeler qu'il est trop tard.



CLONAGE DE PAGES WEB

Dans la majorité des cas, l'approche de l'assaillant consiste à copier le code HTML du site web cible et d'en créer un clone malveillant. En fait, l'équipe de science des données de Cyberint a découvert qu'au moins 66 % des sites de phishing qui mettent nos clients en danger sont en fait des clones 1:1 de pages de connexion légitimes. Malheureusement, les solutions de cybersécurité traditionnelles sont mal équipées pour gérer cette menace. Certaines peuvent fournir un module complémentaire de navigateur web pour détecter les URL de phishing actives en direct. Cependant, de nombreuses pages de contenu clonées n'ont pas d'attributs malveillants à détecter. Même quand c'est bien le cas, au moment où un module complémentaire de navigateur le détecte, la menace est déjà dans la nature et votre organisation ne saura pas combien de dégâts ont déjà été causés.

CONCLUSION ? LES SOLUTIONS DE CYBERSÉCURITÉ TRADITIONNELLES OFFRENT UNE DÉTECTION PARTIELLE, OU UNE RÉPONSE TARDIVE, ET CE N'EST TOUT SIMPLEMENT PAS SUFFISANT POUR L'ENVERGURE DE LA MENACE D'AUJOURD'HUI.

BALISE DE PHISHING DE CYBERINT - OPTIMISER LA DÉTECTION DU PHISHING POUR LES ENTREPRISES NUMÉRIQUES

La balise de phishing de Cyberint adopte une approche proactive. Notre objectif est de détecter le site de phishing avant qu'il n'ait aucun effet. Pour ce faire, nous ajoutons un script obscurci au site Web d'origine de votre organisation, sans oublier que nous sommes les meilleurs de notre catégorie dans les défenses anti-hameçonnage traditionnelles répertoriées ci-dessus. Ce code est extrêmement léger, il n'interfère donc pas avec le fonctionnement normal du site web et, bien sûr, est invisible pour tous les utilisateurs. Malgré cela, une fois que le code du site est cloné par un assaillant en vue de servir la création d'un site de phishing, la balise de phishing identifie qu'il est exécuté sur un domaine d'hébergement non valide. La balise envoie automatiquement une alerte pour informer l'organisation de l'intention malveillante et permettre une riposte rapide avant le lancement du site web de phishing.

COMMENT ÇA MARCHE

1. **Ajouter le code de la balise de phishing aux pages web vulnérables :** Le client ajoute une seule ligne de code fournie par Cyberint aux pages web qu'il souhaite protéger.
2. **L'auteur de la menace clone la page :** L'auteur de la menace clone la page web à des fins malveillantes (par exemple, phishing ou abus de marque dans le cadre d'une activité ponctuelle ou en tant qu'ajout à un kit de phishing).
3. **La page clonée est rendue pour la première fois :** La première fois que la page clonée est rendue (généralement par l'assaillant pour tester le nouveau site de phishing), la balise de phishing s'active et alerte Cyberint automatiquement**.**
4. **Une alerte est générée :** L'équipe d'analystes de Cyberint examine la page. Une alerte est envoyée au client lorsque l'équipe découvre que la page clonée est une page de phishing malveillante.
5. **Fermeture du site de phishing :** À la demande du client, Cyberint contacte le fournisseur d'hébergement ou le bureau d'enregistrement pour supprimer le contenu contrefait en vertu de la loi DMCA.

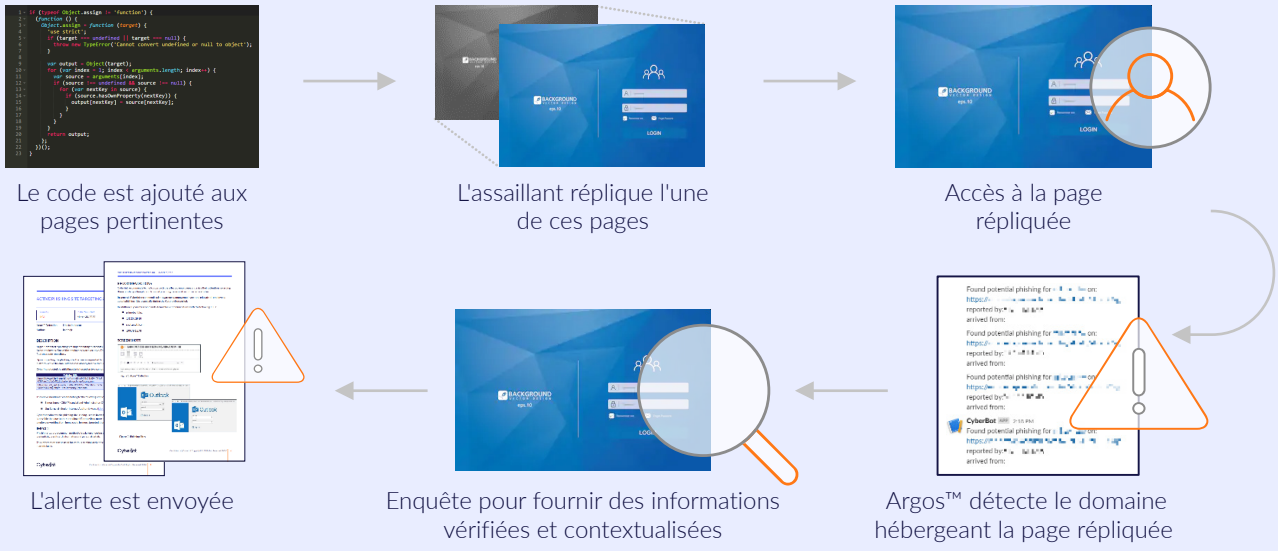


Figure 3 : Balise de phishing - Détection avancée du phishing pour les entreprises numériques

ÉTUDE DE CAS : 4 FOIS PLUS DE SITES DE MALVEILLANTS DÉCOUVERTS À L'AIDE DE LA BALISE DE PHISHING

LE DÉFI

Cette grande entreprise de médias numériques d'Amérique du Nord a souffert d'un clonage récurrent de ses pages de contenu. Sachant que son activité en tant que société de médias consiste à promouvoir du contenu. Par conséquent, l'impact des sites clonés sur ses activités et sur la réputation de leur marque est grand. Les pages clonées siphonnent le trafic destiné aux pages web légitimes de l'entreprise vers le contenu promu par les assaillants.

Ces pages abusent de la marque de l'entreprise et, dans le pire scénario, volent des données sensibles aux utilisateurs finaux. Avant la mise en œuvre la balise de phishing, l'organisation ripostait de manière réactive aux attaques des sites web de phishing, toujours avec un temps de retard par rapport aux assaillants. Il devait attendre la découverte d'une réelle menace avant de pouvoir agir.

LA SOLUTION

En mettant en œuvre la balise de phishing efficacement, via l'ajout d'une seule ligne de code sur son site web, cette entreprise de médias numériques a considérablement réduit l'impact des sites web clonés sur ses activités et sa marque. Cette technologie a permis à Cyberint de détecter et de fermer des sites web de phishing et d'abus de marque pour le compte de ses clients, et ce, de manière intelligente, proactive et beaucoup plus rapide.

EN CHIFFRES

5 mois

Le temps qu'il a fallu pour maîtriser complètement les sites web de phishing

Plus de 400 %

La hausse du nombre d'URL détectées en relation avec le client

62%

La hausse du nombre d'attaques détectées par la balise de phishing, par rapport aux méthodes de sécurité traditionnelles

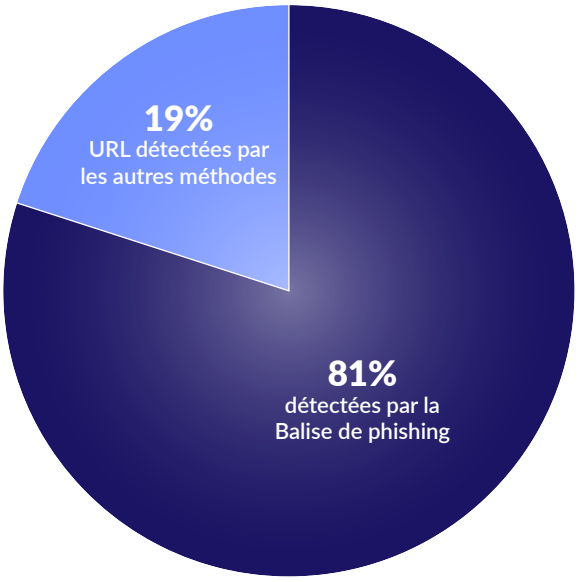


Figure 4 :
URL de phishing et d'abus de marque - Méthodes de détection

NOUS CONTACTER

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ÉTATS-UNIS
214 W 29th St.
New York, 10001
Tél: +1-646-568-7813

ISRAËL
17 Ha-Mefalsim St.
4951447 Petah Tikva
Tél: +972-3-7286-777

ROYAUME-UNI
14 Grays Inn Rd., Holborn
WC1X 8HN, London
Tél: +44-203-514-1515

SINGAPORE
135 Cecil St. #10-01 MYP
PLAZA 069536
Tél: +65-3163-5760

FRANCE
67 Avenue de Wagram
75008 Paris
Tél: +33-1-77-50-5891