NOTE DE SYNTHÈSE

LA SURVEILLANCE DES DOMAINES SIMILAIRES PROTÈGE VOTRE RÉSEAU, VOS CLIENTS ET VOTRE MARQUE

Bloquez de manière proactive les attaques ciblées avancées reposant sur des domaines lookalike, conçues pour infiltrer l'entreprise, compromettre les clients ou nuire à votre marque.

UNE MENACE LOOKALIKE EN PLEINE EXPANSION

Qu'il s'agisse d'attaques de grande ampleur et à large spectre contre les consommateurs, de spear phishing très ciblé, de Business Email Compromise (BEC) ou d'autres menaces pour les entreprises, les domaines similaires sont devenus des éléments clés pour aider les adversaires à contrer les défenses humaines et techniques. Ils peuvent se faire passer pour votre marque, vos employés, votre chaîne d'approvisionnement ou d'autres partenaires de confiance, avec des conséquences désastreuses.

Bien que cette technique ait été utilisée pour la première fois il y a près de vingt ans, les acteurs de la menace continuent d'innover pour utiliser les domaines similaires dans de nouveaux types d'attaques. En utilisant des techniques d'adversaire-intermédiaire (AitM), ils essaient de plus en plus de faire croire aux employés qu'ils interagissent avec le véritable réseau de l'entreprise lors de l'authentification.

Aujourd'hui, les pirates utilisent des domaines similaires dans les messages SMS, les appels téléphoniques, les messages directs sur les réseaux sociaux, les e-mails et les codes QR. Plus récemment, ils ont ciblé l'authentification multifactorielle (MFA) en raison de son adoption croissante par tout le monde, des gamers aux places de marché, portefeuilles et échanges de devises numériques, comme l'attaque contre Coinbase début 2023. Les domaines similaires sont devenus une partie intégrante de chaque grande menace cybernétique.

UNE MENACE LOOKALIKE EN PLEINE EXPANSION

Figure 1 : Infoblox Threat Intelligence a partagé des données de recherche surprenantes sur le risque croissant des domaines similaires.

DES FAITS ET DES CHIFFRES

Les capacités avancées de sécurité de BloxOne Threat Defense vous permettent de révéler :

- Plus de 300 000 domaines similaires ont été détectés en un peu plus d'un an.
- Les domaines de combosquatting sont maintenant 100 fois plus fréquents que le typosquatting
- 200 000 nouveaux domaines sont créés chaque jour
- Plus de 1 600 domaines ont été utilisés en 2023 pour imiter les services MFA officiels
- 60 % des domaines de combosquatting sont actifs depuis plus de 1 000 jours
- Au-delà de l'utilisation de .com, il y a aujourd'hui 1 588 autres TLD destinés à être utilisés de manière abusive par les pirates
- Le DNS est utilisé dans 92 % des cyberattaques

PROTÉGEZ VOTRE MARQUE ET VOS CLIENTS

La stratégie de défense contre les menaces de domaines s'apparentant à ceux exploités par l'entreprise nécessite une approche différente de celle utilisée pour les attaques de qualité professionnelle et de masse. Avec Infoblox Lookalike Domain Monitoring, les clients gèrent leur propre liste personnalisée des domaines dont ils craignent qu'ils puissent être utilisés contre eux, leurs employés ou leurs clients. Infoblox Threat Intelligence scrute ensuite les bureaux d'enregistrement mondiaux, les fournisseurs de services Internet, l'activité DNS réelle et bien d'autres choses encore pour identifier les domaines similaires potentiels à haut risque par rapport à la liste de surveillance du client et commencer l'évaluation et la surveillance initiales. L'interface Lookalike Domain Monitoring donne aux clients une visibilité sur les domaines similaires identifiés et à haut risque ainsi que sur les données relatives au profil de risque, ce qui aide l'organisation à prendre des décisions éclairées qui peuvent éviter de manière proactive une violation potentielle du réseau, une compromission des clients ou une atteinte à la réputation et à l'image de marque de l'organisation.

Lookalike Domain Monitoring est disponible séparément et est inclus avec un abonnement à la solution DNS Detection and Response (DNSDR) d'Infoblox, BloxOne Threat Defense Advanced. Ces solutions permettent aux clients d'identifier un ensemble initial de domaines personnalisés à surveiller pour les domaines similaires à haut risque. Les clients souhaitant surveiller davantage de domaines pour ces risques peuvent acheter des licences supplémentaires par tranches de 100 domaines.

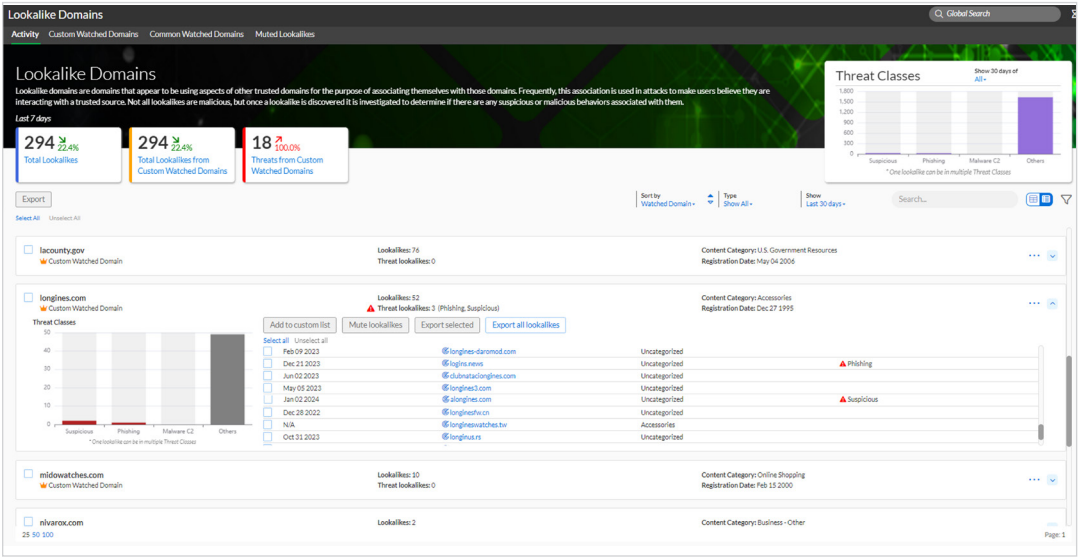

Figure 2 : Passez en revue facilement les domaines similaires à haut risque pour mieux comprendre les niveaux de risque qu'ils présentent

EMPÊCHER LA FRAUDE SUR INTERNET VIA L'UTILISATION DE DOMAINES SIMILAIRES

Infoblox propose des « services de mitigation de domaines » pour aider les clients à supprimer rapidement les domaines qui présentent un risque pour leur organisation ou leurs clients. Nous mettons à profit le mélange exclusif de compétences d'investigation, de techniques automatisées et de relations industrielles d'Infoblox pour résoudre les problèmes avec des SLA de pointe mesurés en heures, y compris le vol de données, l'usurpation de site et d'autres cyberattaques rapidement et avec discrétion.

Pour plus d'informations sur les services de mitigation de domaines Infoblox, rendez-vous sur https://insights.infoblox.com/fr-resources/frr/infoblox-datasheet-infoblox-domain-mitigation-services-fr

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

Siège social
2390 Mission College Boulevard, Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20240125v3