infoblox.

Threat Intel

NOTE DE SYNTHÈSE

CHASSE AUX MENACES BASÉE SUR LE DNS POUR LES DÉTECTER AVANT QU'ELLES NE FRAPPENT

FAITS ET CHIFFRES

- Le champ d'application des DNS est énorme. Il existe maintenant 1 589 domaines de premier niveau, avec 200 000 nouveaux domaines créés chaque jour.
- 81 % des organisations ont subi une ou plusieurs attaques de phishing au cours des 12 derniers mois, selon l'étude mondiale de la CRA 2023 sur l'état de la cybersécurité
- 75 % des organisations ont été victimes d'attaques par smishing (rapport State of Phish 2024 de Proofpoint)
- Les domaines similaires sont fréquemment utilisés dans les attaques de phishing et de spear phishing. En 2022, des hackers chinois ont utilisé 42 000 domaines usurpés dans une vaste campagne de phishing, selon Hacker News.
- Il ne s'agit pas seulement de domaines ressemblants. Les attaquants enregistrent souvent des domaines plusieurs mois à l'avance pour les utiliser dans un large éventail d'attaques. Un exemple est la trousse à outils Decoy Dog, identifiée pour la première fois par Infoblox Threat Intel. De nombreux domaines C2 russes utilisés par Decoy Dog ont été créés à l'avance et découverts par Infoblox à l'automne 2022.
- Infoblox détecte et bloque environ 25 000 nouveaux domaines d'apparence similaire chaque semaine.
- **Conclusion :** Il existe un besoin critique de threat intelligence qui identifient de manière proactive ces domaines émergents susceptibles d'être utilisés dans de futures attaques.

DÉFIS

Les hackers apprécient le phishing car il est peu coûteux, et il suffit qu'une seule personne commette une erreur et clique sur le lien. Les attaques de phishing par SMS, communément appelées smishing, ont récemment augmenté en fréquence, et les acteurs mènent des opérations massives et résilientes de smishing. Les domaines ressemblants sont souvent utilisés dans les attaques de phishing et de spear phishing, et en 2022, des hackers chinois ont utilisé 42 000 domaines usurpés dans une vaste campagne de phishing.

Bien que le phishing et les domaines similaires soient un problème croissant, il existe d'autres cas où des domaines ont été enregistrés des mois à l'avance avant d'être utilisés dans un large éventail d'attaques. Un exemple récent est la boîte à outils Decoy Dog, qui est un ensemble de balises exploitant le DNS pour communiquer avec l'infrastructure C&C. Cette boîte à outils utilise Pupy RAT, souvent associé à des acteurs étatiques par le passé. De nombreux domaines associés à Decoy Dog sont actifs depuis avril 2022 et étaient persistants et discrets, ce qui les rendait difficiles à découvrir avec les outils de sécurité traditionnels.

Une approche différente est nécessaire pour détecter de telles attaques où les domaines sont établis bien avant le lancement des attaques.

CHASSE AUX MENACES BASÉES SUR LE DNS

La chasse aux menaces basée sur le DNS utilise des DNS et des analyses à grande échelle pour suivre l'infrastructure de l'adversaire avant qu'une attaque réelle ne commence. Plus précisément, elle peut :

- Identifier les domaines qui sont nouveaux pour les clients et les classer comme nouveaux/émergents ou suspects en utilisant des métadonnées, y compris le bureau d'enregistrement, les domaines TLD, les certificats SSL, le serveur de noms, le comportement d'enregistrement, etc.
- Prendre les avis publiés par des tiers, par exemple les avis CISA, et les améliorer pour identifier davantage d'indicateurs à l'aide des métadonnées DNS. Par exemple, dans une annonce récente de la CISA, Infoblox a identifié 13 domaines supplémentaires qui n'étaient pas mentionnés dans l'avis, uniquement grâce à la capacité de relier les métadonnées DNS. Cela a considérablement aidé à réduire un vecteur de menace potentiel.

La chasse aux menaces basée sur le DNS protège contre les domaines suspects des semaines ou des mois avant qu'ils ne soient confirmés comme malveillants et utilisés dans des attaques.

UTILISATION DE BLOXONE THREAT DEFENSE POUR UNE PROTECTION PROACTIVE

En raison de la position unique d'Infoblox, la solution peut observer, analyser et bloquer l'intention de communiquer, pour une protection proactive. Infoblox, leader du marché et expert en DNS, suit l'infrastructure des acteurs malveillants et examine les journaux DNS pour détecter les activités suspectes tôt dans le cycle de vie de la menace, lorsqu'il y a une « intention de compromettre » et avant que l'attaque réelle ne commence. Cela permet à Infoblox Threat Intel d'identifier de nouveaux domaines et des domaines ressemblants destinés à une utilisation malveillante pendant la phase de préparation et de les classer comme suspects pendant plusieurs semaines ou mois avant que d'autres sociétés de sécurité ou fournisseurs ne puissent les détecter comme malveillants. La principale raison de ce délai entre la catégorisation proactive des menaces par Infoblox et la détection par d'autres solutions de sécurité est que ces solutions évaluent le comportement du trafic ou le contenu associé à ces domaines, ce qui n'est généralement pertinent qu'une fois que la menace est déjà activée.

Domaines à haut risque

Une fois que l'équipe identifie certains domaines comme suspects, Infoblox les intègre dans un flux appelé « Infoblox High Risk », disponible avec BloxOne Threat Defense, pour permettre à nos clients de se protéger de manière proactive contre les menaces nouvelles et émergentes. Ces flux contiennent des indicateurs de domaines hautement suspects qui n'ont pas encore été associés à une activité malveillante confirmée, mais qui montrent des signes qu'ils peuvent avoir été acquis par des acteurs malveillants dans le cadre de leur phase d'armement et qu'ils peuvent être activés pour un usage malveillant à l'avenir. Les flux sont classés en trois catégories :

- **Suspicious Lookalikes** – Un type de domaine suspect qui ressemble à des domaines légitimes, potentiellement utilisé pour de futures activités d'hameçonnage.
- **Suspicious NOED** – (Newly Observed Emergent Domains) - Un type de domaine à haut risque et suspect qui n'a été observé que récemment dans le trafic des clients. (d'où le terme « émergent »)
- **Domaines suspects** – Ce sont d'autres domaines qui semblent suspects mais qui ne correspondent pas au profil d'un domaine sosie suspect ou d'un NOED.

Infoblox a lancé des données sur les domaines émergents suspects début novembre 2022 et a détecté et catégorisé 19,4 millions d'indicateurs suspects actifs en 2023. Ce nombre de domaines suspects actifs ne cesse d'augmenter au fil du temps. Outre ce volume élevé, un autre critère d'importance est la qualité de la classification des domaines suspects : sur les millions de domaines classés comme suspects, seuls 0,0002 % ont été signalés comme faux positifs.

Ce concept de blocage des domaines suspects a aidé les clients d'Infoblox à bloquer tôt pour certains avis de sécurité, y compris Decoy Dog et les attaques MFA comme Oktapus. De nombreux domaines associés à l'outil Decoy Dog avaient déjà été découverts et inclus dans les flux de domaines suspects de BloxOne Threat Defense à l'automne 2022. Ainsi, les clients de BloxOne Threat Defense Advanced qui avaient configuré leur politique pour bloquer les flux de domaines suspects ont été protégés contre de nombreux domaines C2 depuis lors.

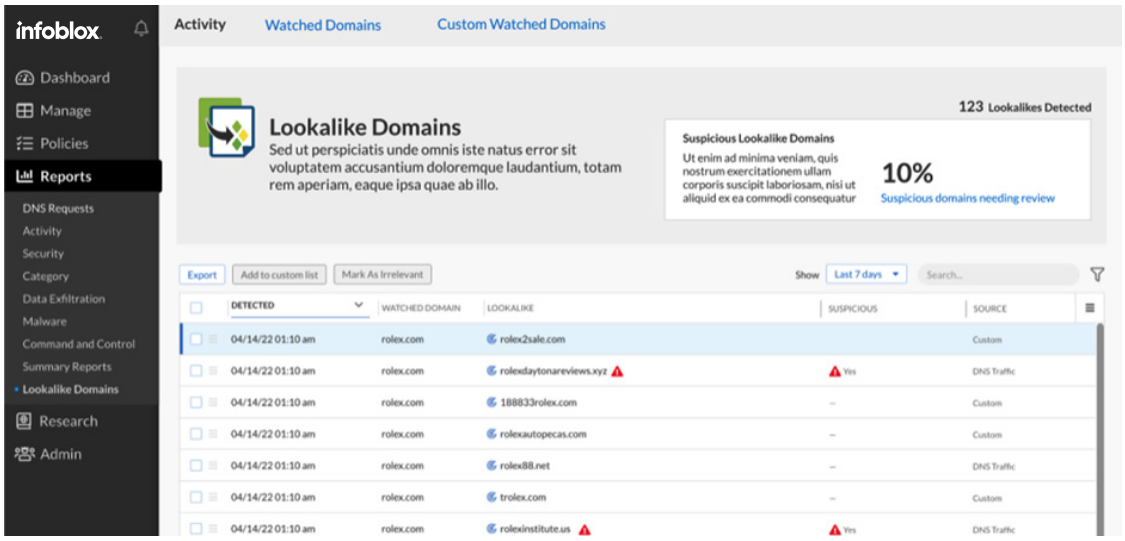
Infoblox a ajouté 19,4 millions de domaines dans les flux de domaines suspects en 2023, réduisant ainsi considérablement le risque d'attaques futures.

Domaines similaires

Outre les flux suspects, les clients d'Infoblox peuvent utiliser la fonctionnalité intégrée de sécurité des domaines similaires dans BloxOne Threat Defense pour identifier et arrêter de manière proactive les menaces d'ingénierie sociale utilisant des domaines similaires dans le cadre d'attaques ciblées avancées visant à pénétrer dans l'entreprise, à compromettre les clients ou à porter atteinte à votre précieuse marque.

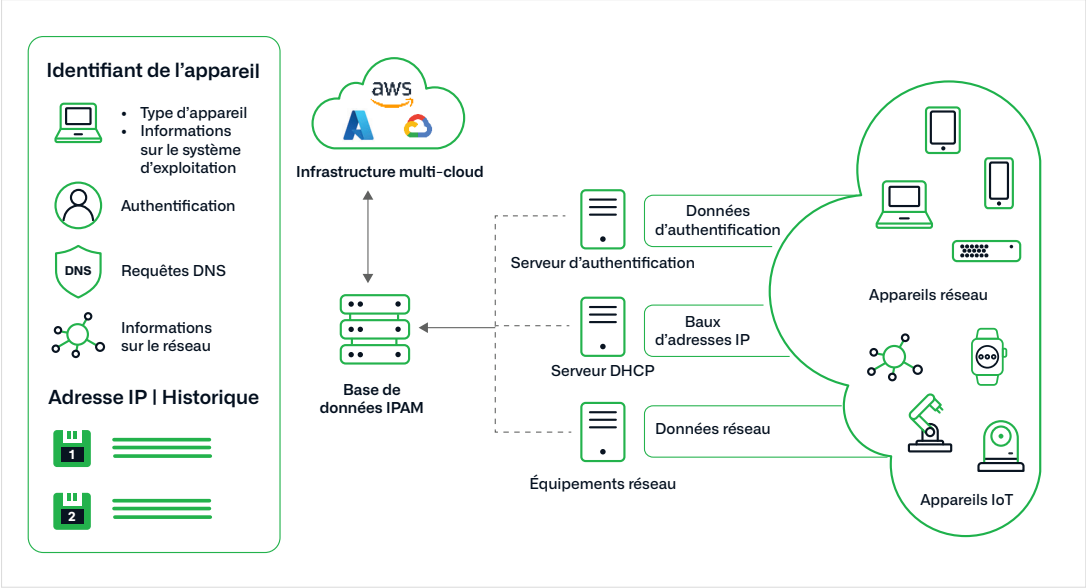
Les clients peuvent soumettre des domaines utilisés par leur propre organisation, leurs partenaires de la chaîne d'approvisionnement ou d'autres domaines susceptibles d'être imités dans le but de tromper les utilisateurs, les partenaires ou les clients dans le cadre d'une cyberattaque. Infoblox commence alors un processus de surveillance continue des domaines potentiellement similaires et analyse l'enregistrement, l'activité, l'historique, et plus encore de chacun pour évaluer leur niveau de risque. Ces résultats sont présentés dans un tableau de bord interactif pour aider les clients à prendre rapidement des décisions éclairées concernant les prochaines étapes. Et ces informations sont continuellement mises à jour pour refléter les nouveaux domaines similaires ou les activités liées aux domaines similaires déjà identifiés.

Un service « take-down » est disponible séparément, s'appuyant sur les relations de confiance profondes d'Infoblox et notre position unique dans l'environnement informatique mondial pour aider les entreprises menacées à réagir et à limiter leur exposition financière et de marque. Les services d'atténuation de domaine d'Infoblox incluent des services de validation pour confirmer qu'un incident s'est réellement produit ; l'atténuation par la coordination avec les principaux FAI et régulateurs ; et la surveillance avec des rapports pour mieux comprendre le paysage des menaces et renforcer votre sécurité. En raison de notre réputation pour la diligence et la qualité des enquêtes, le délai moyen de suppression dans certaines régions peut être aussi court que 24 heures, permettant à nos clients d'éliminer de nombreuses menaces avant qu'elles ne commencent, et de reprendre rapidement leurs activités habituelles.



Attribution facile des utilisateurs et des dispositifs

Bien que le blocage des communications vers ces domaines soit la première étape, il est tout aussi important d'obtenir rapidement une visibilité sur les dispositifs/actifs impliqués dans ces communications. La synchronisation des métadonnées IPAM avec le DNS offre une visibilité essentielle pour déterminer l'origine des requêtes malveillantes dans le réseau. En utilisant les données IPAM, il est facile de déterminer si l'activité DNS anormale provient de dispositifs réseau tels que des pare-feu, des dispositifs utilisateur ou tout autre type d'actif connecté au réseau. Vous pouvez même définir facilement une politique de sécurité basée sur les métadonnées IPAM en utilisant Infoblox.



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

+1.408.986.4000
www.infoblox.com

Version : 20240411v1