infoblox

2025 RAPPORT SUR LE PANORAMA DES MENACES DNS

Le brouillard des cybermenaces :

Comment les acteurs malveillants utilisent le DNS pour tromper et se cacher

Au cours de l'année écoulée, les cybercriminels ont rapidement développé leurs méthodes de tromperie, en multipliant les attaques et en exploitant l'IA pour cibler des individus, des entreprises, tout en échappant à la détection des menaces. Infoblox Threat Intel a observé un nouveau niveau de professionnalisme et de rapidité dans la manière dont les acteurs lancent des cyberattaques basées sur le Système de noms de domaine (DNS), touchant aussi bien les particuliers que les entreprises et les administrations.

Pour se défendre efficacement, les équipes de sécurité doivent comprendre les menaces auxquelles elles font face. Il est essentiel de comprendre les techniques DNS des adversaires, les acteurs qui les utilisent et les risques qu'elles représentent afin de renforcer les stratégies de défense de l'entreprise.

Ce rapport s'appuie sur d'importants volumes de données DNS en temps réel, des analyses de pointe et des décennies d'expertise en matière de menaces, afin d’offrir une perspective unique sur la façon dont les pirates exploitent le DNS. Il décrit également les implications commerciales et souligne que les renseignements basés sur le DNS constituent une couche essentielle de la cyberdéfense moderne.

TABLE DES MATIÈRES

LE POTENTIEL INEXPLOITÉ DE L'INTELLIGENCE DNS

On appelle souvent le DNS de « l'annuaire d'Internet », car il traduit les noms de domaine en adresses IP. Chaque interaction numérique commence par une requête DNS, ce qui en fait une source de télémétrie haute fidélité pour les opérations réseau en offrant une visibilité approfondie sur les actifs numériques qui initient des connexions sur internet.

Le DNS est également utilisé par des acteurs malveillants pour le phishing, l'arnaque, et pour éviter la détection lors de l'extraction de données. Par conséquent, l'analyse du trafic DNS et de l'utilisation des domaines est essentielle pour les analystes de sécurité. Les données DNS peuvent être transformées en threat intelligence prédictive en collectant de manière holistique la télémétrie pré-attaque, en enrichissant les données, en les analysant par rapport aux bases de référence et en menant des chasses aux menaces approfondies. Ces insights offrent aux défenseurs une vision complète des infrastructures adverses, des victimes ciblées et des tactiques, avant que le pirate ne frappe.

« Le DNS offre une vision unique sur les menaces passées et sert de véritable boule de cristal, mettant en lumière les précurseurs des cybermenaces à venir. »

— **Dr Renée Burton**
Responsable du Threat Intel chez Infoblox

Par conséquent, le DNS offre bien plus qu'une simple résolution de noms et est devenu à la fois un point d'application de la politique de sécurité de l'entreprise et un indicateur d'activités malveillantes potentielles sur un réseau. Des organisations telles que l'Institut national des normes et de la technologie (NIST) et l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) ont reconnu ce rôle critique et précoce, que joue le DNS dans la cybersécurité et ont souligné son potentiel de sécurité préventive dans la publication spéciale (SP) 800-81 Rev. 3 du NIST, récemment mise en consultation.[1]

Ce rapport aborde quatre questions clés :

Quelles sont les principales observations DNS des 12 derniers mois ?

Qui sont les acteurs de menaces DNS et quelles activités récentes ont été découvertes ?

Quelles sont les principales tactiques malveillantes derrière les techniques DNS et pourquoi sont-elles dangereuses ?

Quels sont les principaux défis pour les défenseurs et quelles opportunités la Threat Intelligence basée sur le DNS offre-t-elle ?

1 Guide de déploiement du système de noms de domaine sécurisé (DNS), Institut national des normes et de la technologie (NIST), le 10 avril 2025.

SECTION 1 : PRINCIPALES OBSERVATIONS SUR LES MENACES DNS

100.8
million newly observed domains in one year

25.1%
of newly observed domains are malicious or suspicious

Nature éphémère des domaines

Fin mai 2025, Infoblox traitait et analysait quotidiennement 70 milliards de requêtes DNS provenant de plus de 13 000 environnements Infoblox, couvrant des millions d'adresses IP sur tous les types d'appareils.

Les données entièrement anonymisées de plus de 1 300 clients Infoblox Threat Defense™ offrent une visibilité globale et détaillée sur des millions d'interactions Internet, couvrant différents types de clients, zones géographiques et secteurs d'activité. D'une année sur l'autre, ce volume de télémétrie DNS a augmenté de 21 %.

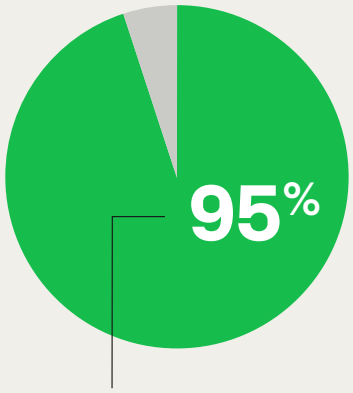
Parmi toutes les données collectées, Infoblox Threat Intel a identifié **100,8 millions de nouveaux domaines** (**domaines de second niveau**) **au cours des 12 derniers mois**. Ce volume élevé de nouveaux domaines est souvent le résultat d'infrastructures en évolution rapide, de campagnes publicitaires à court terme et d'initiatives de marque.

Évasion du contrôle via des domaines à usage unique

Plus d'un quart des nouveaux domaines observés (plus de 25 millions) ont été classés par Infoblox comme malveillants ou suspects. Les acteurs malveillants enregistrent, activent et déploient en permanence un nombre considérable de nouveaux domaines afin de contourner les contrôles de détection. Étant donné qu'il est difficile d'identifier et de classer un tel volume de domaines, les pirates peuvent passer inaperçus, contourner les mécanismes de blocage et laisser très peu de preuves exploitables.

L'utilisation isolée de domaines liés aux menaces identifiées, qu'ils soient malveillants ou suspects, est également significative. Infoblox Threat Intel a découvert que 95 % de tous les domaines liés aux menaces étaient observés dans un seul environnement réseau.

L'objectif de cette tactique est simple : échapper aux défenses forensiques basées sur les données du « patient zéro » en exploitant des domaines jetables, dont les pirates disposent en quantité illimitée.



of threat-related domains were observed in only one customer environment.

Domaines malveillants vs. domaines suspects

- **Les domaines malveillants** sont des menaces confirmées par des preuves solides. Ils ne disparaissent pas avec le temps et représentent 1,6 % des plus de 100 millions de domaines nouvellement observés.
- **Les domaines suspects** sont des menaces potentielles qui manquent de preuves concluantes et représentent 23,5 % de tous les nouveaux domaines observés. S'ils ne sont pas confirmés, ces indicateurs expirent au bout de quelques mois. Les analystes Infoblox Threat Intel surveillent continuellement ces domaines pour obtenir de nouvelles preuves. Lorsque des indicateurs supplémentaires sont découverts, les scores sont mis à jour et les domaines suspects peuvent être reclassés comme malveillants.

Camouflage via des domaines intégrés à des systèmes de distribution de trafic

L'AdTech (abréviation de « advertising technology », soit technologie publicitaire) désigne les outils, logiciels et plateformes utilisés pour automatiser, gérer, cibler, diffuser et analyser la publicité numérique. Les systèmes de distribution de trafic (TDS) sont les plateformes ou mécanismes utilisés, de manière légitime ou malveillante, pour rediriger le trafic Internet entrant vers différentes destinations en fonction de règles prédéfinies. Les acteurs malveillants ont également adopté cette technologie, souvent appelée « **AdTech malveillante** ».

82%

of customers queried a domain part of a traffic distribution system.

Au cours des 12 derniers mois, **82 % de tous les environnements clients** ont interrogé des domaines faisant partie du TDS, dont la plupart sont exploités par des opérateurs publicitaires malveillants connus pour dissimuler des contenus nuisibles, tels que des sites de phishing ciblés, des scarewares, des arnaques et des logiciels voleurs d'informations.

Ces TDS se composent souvent de dizaines de milliers de domaines, qui font l'objet d'une rotation rapide pour échapper à toute détection, diffusant du contenu malveillant ciblé aux victimes idéales tout le en masquant aux analystes en menaces.

Au fil du temps, Infoblox Threat Intel a découvert plus de **1 million de domaines utilisés par 168 opérateurs publicitaires malveillants** au sein de leur infrastructure TDS. Ces indicateurs couvrent plusieurs techniques DNS, telles que les domaines détournés, les domaines trompeurs, les redirections et les ensembles de domaines enregistrés de façon algorithmique (algorithmes de noms de domaine générés, ou RDGAs). Pour en savoir plus sur les TDS, leur fonctionnement et les risques associés, consultez la section 3.

Domaines liés à divers types de menaces

Au fur et à mesure que de nouveaux domaines liés aux menaces sont découverts, les chercheurs d'Infoblox enquêtent sur les acteurs à l'origine de ces activités et sur leurs intentions sous-jacentes. Le tableau de la page suivante présente une liste priorisée des façons dont les acteurs utilisent leurs domaines à des fins malveillantes.

Top 7 : Comment les acteurs malveillants exploitent les nouveaux domaines	
1	**Se livrer à des activités frauduleuses et à des arnaques**, comme de faux sites d'investissement en cryptomonnaies.
2	**Héberger du contenu illégal**, y compris des sites de jeux d'argent (en particulier dans des régions comme la Chine) et du contenu pour adultes.
3	**Créer des pages de phishing** conçues pour voler des informations personnelles ou des données de carte bancaire.
4	**Déployer des malwares.** Parmi les exemples courants, on peut citer les voleurs d'informations (par exemple, Lumma Stealer), les loaders via des téléchargements drive-by (par exemple, SocGholish), les botnets et les ransomwares (par exemple, BlackBasta).
5	**Masquer leurs activités** via TDS et diffuser diverses charges utiles ou inciter les utilisateurs à autoriser des notifications indésirables dans leur navigateur.
6	**Distribuer des programmes potentiellement indésirables** (**PUP**), tels que des scarewares ou des extensions de navigateur inutiles.
7	**Mener des campagnes de spam et distribuer des e-mails malveillants**.

Tableau 1. Objectif des acteurs pour les domaines nouvellement observés.

Popularité des domaines

La télémétrie DNS d'Infoblox fournit également des insights sur l'utilisation des types de domaines, offrant des indices sur la popularité des applications et la vitesse à laquelle les cybercriminels deviennent de plus en plus compétents pour placer avec succès de grands volumes de domaines armés devant leurs victimes.

19 DAYS

Time needed for a TDS domain to become popular

Observations clés :

- Huit catégories de domaines, telles que les réseaux de diffusion de contenu (CDN), les fournisseurs de technologie, les fournisseurs de sécurité, les outils de productivité, les moteurs de recherche, le stockage, les services cloud et les conférences en ligne, représentent la majorité (environ 70 % sur un jour donné) de tous les domaines faisant l'objet de requêtes DNS de la part des clients.
- En mai 2025, les requêtes de domaine liées à l'utilisation personnelle d'Internet, telles que les achats en ligne, les jeux et les réseaux sociaux (par exemple, TikTok et Facebook), ont atteint le même niveau que celles associées aux plateformes de collaboration professionnelle (par exemple, Microsoft Teams, Slack). Cela illustre le **l'usage croissant d'Internet à la fois pour le travail et le privé,** , une réalité dont les acteurs malveillants sont parfaitement conscients.
- Les adversaires recherchent continuellement des points d'attaque vulnérables, comme les appareils mobiles et les dispositifs personnels (BYOD), et trompent les utilisateurs pour les amener à effectuer des actions à haut risque visant à exfiltrer des données professionnelles, y compris des identifiants. Cette tendance a également été soulignée dans le 2025 Data Breach Investigations Report de Verizon,[2] qui affirme qu'aucun appareil n'est à l'abri et souligne que **46 % des identifiants d'entreprise volés** provenaient d'appareils non gérés ou personnels.

2 2025 Data Breach Investigations Report de Verizon,

- Infoblox Threat Intel a observé que les domaines faisant partie des TDS devenaient populaires[3] en seulement 19 jours, **2,35 fois plus vite qu'en 2024 et 39 fois plus vite qu'en 2020.** La vitesse à laquelle les domaines TDS gagnent en popularité, comparable à celle de sites légitimes tels que `panerabread[.]com` ou `draftkings[.]com`, illustre à quel point les domaines malveillants se propagent et sont consultés par les victimes. Les acteurs malveillants déploient rapidement de grands volumes de ces domaines aux cibles, maximisant ainsi l'impact de leurs campagnes tout en devançant les sources de renseignements plus lentes, telles que les renseignements open source (OSINT) et les analyses judiciaires.

SECTION 2 : ACTEURS DE LA MENACE ET RECHERCHE

204K
total identified suspicious domain clusters

662
total identified DNS threat actors

10
new actors publicly disclosed in the past 12 months

Les 100 millions de nouveaux domaines découverts l'année dernière ne sont pas des forces de la nature ; ils sont toujours le résultat d'actions humaines et initiés dans un but précis. Infoblox Threat Intel analyse et enquête en permanence sur les acteurs derrière les domaines liés aux menaces en enrichissant la télémétrie collectée et en corrélant les modèles communs

Depuis le début de ses recherches, Infoblox Threat Intel a découvert un total de 204 000 groupes de domaines suspects, chacun partageant des éléments de menace communs, et a identifié 662 acteurs malveillants uniques. Au cours des 12 derniers mois seulement, les chercheurs d'Infoblox ont révélé publiquement l'existence de 10 nouveaux acteurs à travers différents rapports de recherche et articles de blog.

3 Un domaine est considéré comme populaire lorsqu'il appartient au sous-ensemble de domaines qui représentent la majorité du trafic client pendant une période donnée. Cela peut varier entre 6 000 et 10 000 domaines par jour. Pour plus d'informations, voir https://blogs.infoblox.com/wp-content/uploads/infoblox-whitelists-that-work.pdf.

La liste ci-dessous met en avant les principaux acteurs malveillants identifiés et rendus publics par Infoblox Threat Intel entre le 1er juillet 2024 et le 1er juillet 2025.

Acteur	Description
	Cet acteur exploite un TDS malveillant qui détourne le trafic web légitime, principalement issu des sites WordPress compromis, et le redirige vers des arnaques, des malwares et du contenu de phishing. VexTrio est considéré comme l'un des acteurs les plus répandus et les plus évasifs des menaces modernes. Ces 12 derniers mois, l'acteur a été cité dans plusieurs rapports en raison de sa relation avec des pirates informatiques affiliés et est connu pour détourner des domaines afin d'alimenter leur infrastructure d'attaque. **Rapports récemment publiés :** • The Vexing and Vicious : l'inquiétante relation entre les hackers WordPress et un réseau AdTech • Acculé au fond d'un terrier de lapin
	Ce groupe sophistiqué d'acteurs malveillants DNS se spécialise dans le détournement de ressources cloud abandonnées, telles que les buckets Amazon S3 et les endpoints Azure, en exploitant les enregistrements DNS mal configurés ou oubliés, en particulier les entrées de nom canonique orphelin (CNAME). Une fois que Hazy Hawk a pris le contrôle de ces sous-domaines, il exploite la confiance inhérente aux domaines légitimes pour héberger du contenu malveillant. Ses opérations consistent souvent à rediriger les utilisateurs via des TDS pour diffuser des arnaques, des malwares et des notifications push frauduleuses. **Rapports récemment publiés :** • Le détournement d'enregistrements DNS oubliés permet à un acteur malhonnête de commettre une escroquerie
	Cet acteur malveillant motivé par l'argent a utilisé des domaines détournés pour des arnaques à l'investissement depuis février 2023. Il intègre ces domaines dans des publicités Facebook éphémères diffusées sur plusieurs continents, ciblant des victimes dans plus de 30 langues, y compris l'anglais, l'italien, le polonais, le turc et l'espagnol. L'acteur utilise le vecteur d'attaque Sitting Ducks pour détourner des domaines réputés, qu'il exploite afin de protéger ses sites frauduleux contre les chercheurs en sécurité. En octobre 2024, Infoblox a identifié près de 5 000 domaines détournés liés à cet acteur. **Rapports récemment publiés :** • Découvrir les modèles TTP des acteurs et le rôle du DNS dans les escroqueries à l'investissement • Les prédateurs DNS détournent des domaines pour alimenter leur infrastructure d'attaque

Reckless Rabbit est un acteur de fraude à l'investissement qui attire les victimes par le biais de publicités malveillantes sur Facebook. Il utilise des RDGAs basés sur des dictionnaires et cible des individus dans plusieurs pays, notamment l'Autriche, la Belgique, le Danemark, la France, la Pologne, la Suède, le Royaume-Uni et bien d'autres. L'acteur utilise des RDGAs et de fausses recommandations.

Rapports récemment publiés :

- Découvrir les modèles TTP des acteurs et le rôle du DNS dans les escroqueries à l'investissement

Cet acteur de phishing exécute des campagnes d'escroquerie à l'investissement qui exploitent des RDGAs basés sur des dictionnaires et usurpent des services populaires. L'acteur exploite son propre service de dissimulation de domaine pour effectuer des contrôles de validation des utilisateurs et cible des pays d'Europe de l'Est tels que la Roumanie, la Russie, la Pologne, et bien d'autres.

Rapports récemment publiés :

- Découvrir les modèles TTP des acteurs et le rôle du DNS dans les escroqueries à l'investissement

Cet acteur identifie les ressources cloud abandonnées et les réutilise à des fins malveillantes. Hasty Hawk est connu pour détourner des domaines utilisés dans des campagnes à thème caritatif ou à thème DHL, diffusées via Google Ads. Hasty Hawk utilise principalement des réseaux d'hébergement « bulletproof » tels que Proton66 ainsi qu'un TDS, pour rediriger les utilisateurs vers le contenu.

Rapports récemment publiés :

- Les prédateurs DNS détournent des domaines pour alimenter leur infrastructure d'attaque

Vacant Viper exploite le 404TDS, qu'il utilise pour diffuser du malware et d'autres contenus nuisibles. Vacant Viper détourne les domaines laissés vulnérables en raison d'une mauvaise configuration des serveurs de noms DNS, une faille nommée « Sitting Ducks » par les chercheurs d'Infoblox, et les intègre à son infrastructure TDS malveillante.

Rapports récemment publiés :

- Qui l'aurait cru ? Le détournement de domaine est si facile

Cet acteur malveillant du secteur AdTech exploite des vulnérabilités WordPress et diffuse du malware, des pages de phishing, de fausses applications et du contenu indésirable. Il exploite un TDS étendu intégrant des notifications push, des pop-ups et des redirections dans le navigateur, diffusant des annonces même après que l'utilisateur a quitté la page d'origine.

Rapports récemment publiés :

- The Vexing and Vicious : l'inquiétante relation entre les hackers WordPress et un réseau AdTech

Morphing Meerkat est un acteur mondial du spam, à l'origine d'une plateforme avancée de phishing-as-a-service (PhaaS). Cet acteur utilise les enregistrements DNS MX pour identifier le fournisseur de messagerie de la victime et lui proposer dynamiquement de fausses pages de connexion. Morphing Meerkat exploite des sites WordPress compromis ainsi que des vulnérabilités de redirection ouvertes sur les serveurs AdTech.

Rapports récemment publiés :

- Une affaire de phishing sur l'abus de DOH et de DNS MX

ÉTUDE DE CAS : COORDINATION ENTRE LES HACKERS DE WORDPRESS ET VEXTRIO VIPER CABAL

Infoblox a récemment découvert une alliance complexe entre **des hackers WordPress et un réseau de sociétés AdTech malveillantes**, notamment le TDS de VexTrio.

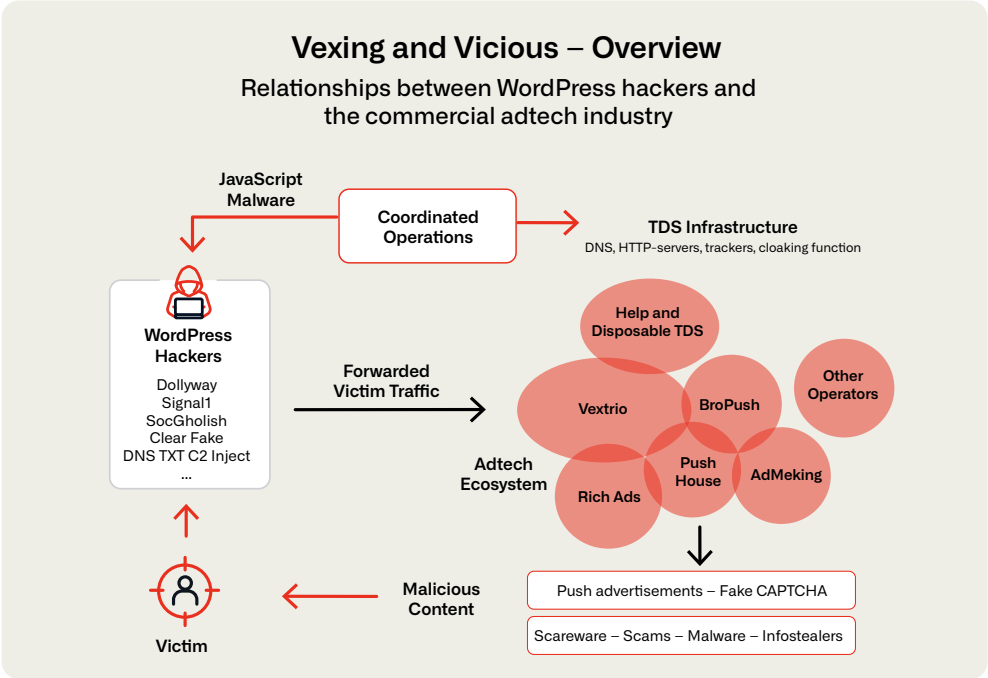


Figure 1. Relation entre les pirates de WordPress et le secteur commercial AdTech

Que s'est-il passé ?

- **Migration rapide :** lorsque le TDS de VexTrio a été perturbé à l'automne 2024, plusieurs malwares ont simultanément migré vers un TDS apparemment nouveau, baptisé « Help TDS ». Une analyse plus approfondie a révélé que Help TDS n'est pas indépendant, mais étroitement lié à VexTrio, partageant une infrastructure et des composants logiciels.
- **Opération coordonnée :** Infoblox a analysé 4,5 millions de réponses d'enregistrements DNS TXT provenant de sites web compromis sur une période de six mois. Cela a révélé deux serveurs de commande et de contrôle (C2) distincts, tous deux hébergés sur une infrastructure connectée à la Russie, indiquant une opération coordonnée entre les hackers WordPress et le groupe VexTrio.

- **Implication des entreprises AdTech commerciales :** plusieurs sociétés AdTech, dont Los Pollos, Partners House, BroPush et RichAds, ont été identifiées comme étant liées aux opérations de VexTrio. Ces entreprises ont facilité la distribution de contenu malveillant via des smartlinks et des notifications push.

L'enquête met en évidence la nature sophistiquée et adaptative des réseaux cybercriminels qui exploitent des sites WordPress compromis et des infrastructures publicitaires commerciales. Cela souligne l'importance de la télémétrie DNS et des efforts collaboratifs pour détecter et atténuer de telles menaces.

SECTION 3 : TECHNIQUES DNS MALVEILLANTES

Les acteurs de menace mentionnés dans la section 2 utilisent le DNS de différentes manières et poursuivent des objectifs spécifiques. Une fois qu'Infoblox identifie un domaine lié à une menace, des processus d'analyse et des examens par des experts attribuent au domaine les techniques malveillantes connues. Le tableau ci-dessous présente un aperçu des techniques DNS les plus courantes attribuées par Infoblox Threat Intel aux domaines liés à des menaces.

Techniques DNS et domaines liés aux menaces Période : janvier 2025 à juin 2025	
Domaines générés par des algorithmes automatiques (RDGA, DDGA et DGA)	54,7 %
Domaines utilisés pour rediriger le trafic	11 %
Domaines CNAME ou alias	5,8 %
Domaines similaires	5,1 %
Domaines détournés	5,1 %
Domaines utilisés dans des SMS malveillants	4,2 %
Domaines créés dans le cadre d'un TDS	1,8 %
Domaines utilisés pour le C2 et l'exfiltration	< 0,4 %

Tableau 2. Techniques DNS attribuées à des domaines liés aux menaces

Bon nombre de ces techniques se recoupent au cours d'une campagne de menaces et s'intègrent dans des tactiques plus larges mises en œuvre par les acteurs pour atteindre leurs objectifs. Dans ce rapport, nous examinons plus en détail quatre techniques DNS courantes, leur utilisation et les raisons pour lesquelles elles sont dangereuses :

- L'utilisation des domaines au sein des TDS
- Le détournement de domaine pour usurper l'identité
- Les domaines similaires pour tromper les victimes
- Le tunneling DNS pour le C2 et l'exfiltration

SYSTÈMES DE DISTRIBUTION DE TRAFIC OFFRANT UN NIVEAU D'ÉVASION DANGEREUX

Le DNS joue un rôle central dans le TDS en redirigeant secrètement les utilisateurs à travers de multiples niveaux intermédiaires, souvent à leur insu, en fonction de divers attributs tels que la géolocalisation, le type d'appareil ou la posture de sécurité. Le DNS joue un rôle fondamental dans la détermination de la façon et de l'endroit où le trafic réseau est acheminé. Les opérateurs légitimes de TDS se trouvent principalement dans la publicité numérique ou l'AdTech. Le terme AdTech (abréviation de « advertising technology », technologie publicitaire) désigne les outils, plateformes et logiciels utilisés pour gérer, diffuser et analyser les campagnes publicitaires numériques.

Tout comme les technologies publicitaires légales connues (par exemple, Google AdSense), les AdTech malveillantes diffusent le bon contenu au bon public, au bon moment, afin d'accroître l'efficacité de leurs campagnes. Ce type de cybermenace est orchestré par des organisations spécialisées disposant de nombreux affiliés et de ressources financières considérables.

Principaux opérateurs de TDS selon la part de connexions	
Nom de l'acteur	**Part de connexions**
Vextrio Viper	72,8 %
Vane Viper	68,4 %
Venal Viper	72,5 %
Acteur non divulgué	64,8 %
Vero Viper	60,5 %
Tiano Gambling	50,9 %

Tableau 3. Opérateurs TDS et pourcentage de tentatives de connexions des clients qu'ils ont reçues

Au cœur de ces activités se trouve un TDS qui profile les victimes et les redirige vers des annonceurs malveillants, tout en orientant les chercheurs en sécurité vers un site leurre.

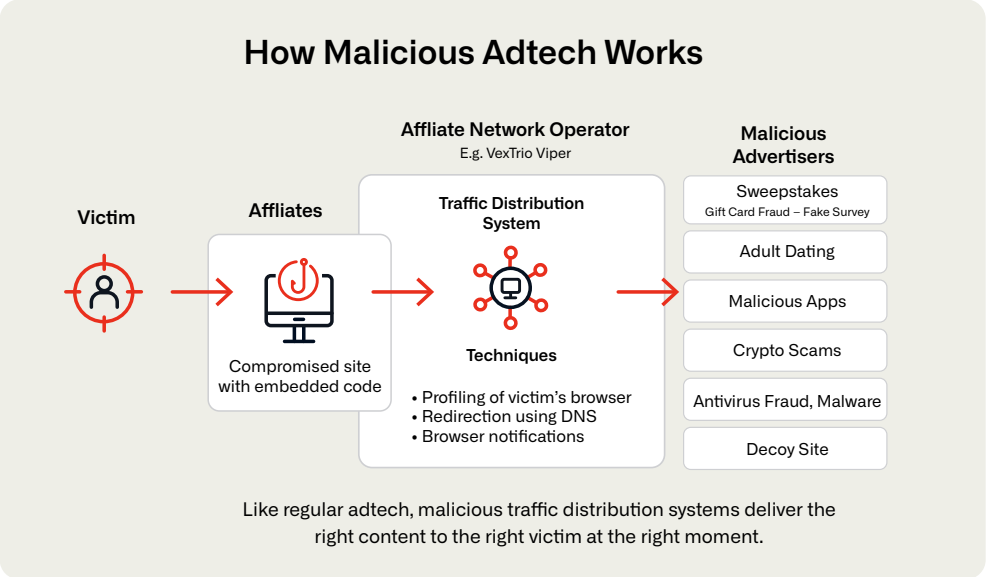


Figure 2. Une vue d'ensemble des trois acteurs de l'AdTech malveillante : affiliés, opérateurs et annonceurs malveillants

Il existe plusieurs raisons pour lesquelles les AdTech malveillantes sont nuisibles et devraient être un domaine d'intérêt majeur pour les équipes de sécurité des entreprises :

L'AdTech malveillant est un vecteur de menace en pleine expansion et sous-estimé

Les pirates exploitent de plus en plus les réseaux publicitaires malveillants comme un service peu coûteux pour diffuser du malware et d'autres contenus malveillants. Ces publicités peuvent mener à divers types d'attaques, notamment des téléchargements furtifs, des sites de phishing, des vols d'identifiants et des kits d'exploitation (voir le tableau 4. Opérateurs TDS et contenu malveillant diffusé).

Comme la plupart des acteurs du secteur de la sécurité s'appuient sur une approche du « patient zéro » — collectant des données de télémétrie pendant (par exemple, sandboxing) ou après (par exemple, analyses forensiques) une attaque — les contre-mesures qui en résultent se limitent aux artefacts découverts à ce point initial de compromission. Cette limitation fait des TDS des outils efficaces pour échapper à la détection, car les cybercriminels modifient en permanence le contenu malveillant qu'ils diffusent et redirigent les chercheurs de menaces vers des sites leurres. Par conséquent, les TDS sont devenus l'une des menaces les moins signalées dans le secteur de la cybersécurité.

Des infrastructures qui sont à grande échelle et difficiles à perturber

Les organisations qui exploitent des technologies publicitaires malveillantes construisent souvent une infrastructure à grande échelle, comprenant des dizaines de milliers de domaines en constante évolution, conçus pour rediriger les utilisateurs et les inciter à accepter les notifications push de leur navigateur. Ces opérations sont souvent compartimentées en plusieurs entités pour mener des cybercrimes tout en évitant tout contrôle juridique. Certains opérateurs, tels que VexTrio Viper, ont persévéré pendant des années, devenant très rentables, et leurs activités ne montrent aucun signe de ralentissement.

L'AdTech malveillant sert de passerelle vers les risques pour l'entreprise

Les technologies publicitaires malveillantes trompent les victimes en imitant des marques populaires ou en proposant des contenus auxquels elles souhaitent avoir accès, les incitant ainsi à baisser leur garde et à s'engager dans des interactions à haut risque. Bien que ces menaces proviennent généralement de sites destinés aux consommateurs, elles peuvent facilement s'infiltrer dans les environnements d'entreprise, exposant ainsi les appareils personnels des employés à des contenus malveillants. Cela permet aux cybercriminels d'effectuer des reconnaissances ou de se faire passer pour des notifications d'entreprise, élevant ainsi le risque pour les réseaux d'entreprise.

Opérateurs DNS	Malware	Arnaques	Phishing	Domaine détourné
Vacant Viper	X	X		X
Vane Viper	X	X	X	
Vextrio Viper	X	X	X	X
Hasty Hawk			X	X
Sophisticated Chickens			X	X
Black TDS	X		X	
Parrot TDS	X			
R0bl0ch0n TDS		X		

Tableau 4. Opérateurs TDS et contenus malveillants diffusés

Exemple de TDS en action :

Lorsqu'une victime visite un site compromis à partir d'un appareil mobile ou d'un endpoint, l'opérateur peut présenter un faux CAPTCHA pour inciter la victime à accepter les notifications push du navigateur provenant d'un annonceur malveillant. Ces notifications peuvent ensuite diffuser du contenu frauduleux supplémentaire, tel que des invites à télécharger des logiciels non vérifiés, à partager des informations personnelles ou à saisir des identifiants d'entreprise.

Comme le TDS établit le profil des victimes entrantes, les analystes SOC ou les chercheurs en menaces utilisant des outils de sécurité courants peuvent ne pas détecter ces notifications ou le contenu malveillant, et être redirigés vers un site leurre affichant des informations légitimes.

En raison du chevauchement entre l'usage professionnel et personnel d'Internet, la technologie publicitaire malveillante est devenue un contributeur majeur à la cybercriminalité, en particulier sur les appareils mobiles, les tablettes, le BYOD et les actifs non sécurisés.

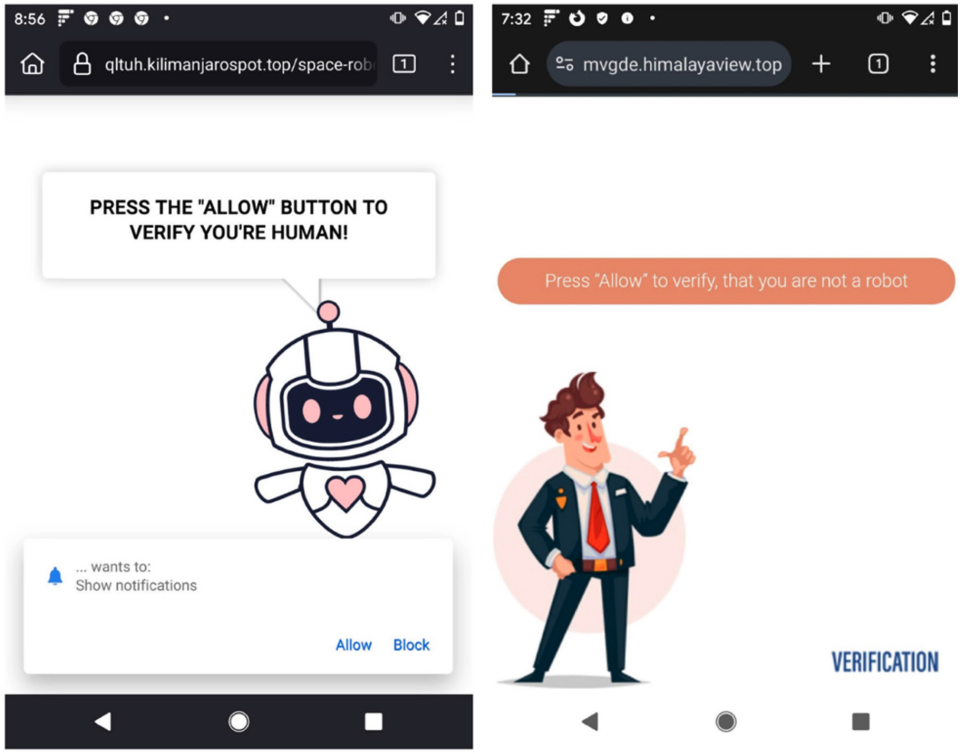


Figure 3. Exemples de la page d'accueil de VexTrio Viper qui incite l'utilisateur à accepter les notifications push sur son appareil ; ces deux exemples ont été observés lors de la navigation sur `germannautica[.]com`

Domaines utilisés par les systèmes de distribution de trafic

Au cours des 12 derniers mois, Infoblox Threat Intel a découvert plus d'un million d'indicateurs utilisés par 168 opérateurs de technologies publicitaires malveillants au sein de leur TDS. Ces indicateurs couvrent plusieurs techniques, notamment les RDGAs, les redirections, les détournements de domaines, les domaines similaires et autres.

Les TDS utilisés par les opérateurs AdTech malveillants peuvent être assez volumineux. Beaucoup incluent plus de 10 000 domaines, dont certains dépassent les 100 000. Cependant, la taille d'un TDS n'est pas nécessairement corrélée à son omniprésence ou à son niveau de menace. Vigorish Viper exploite un vaste réseau en pleine expansion de 170 000 domaines actifs, mais cible principalement des victimes en Chine, à Hong Kong et à Macao. Venal Viper, bien qu'elle ne figure pas parmi les cinq meilleures en termes de taille, reste l'une des plus fréquemment interrogées sur les réseaux clients. 65 % des clients d'Infoblox ont consulté un domaine Venal Viper au cours des 12 derniers mois.

Perturber le TDS

L'adtech malveillante utilisant les TDS prospère parce qu'elle se fait passer pour de la publicité légitime, trompe les victimes et échappe à la détection par les outils de sécurité qui s'appuient sur l'identification de comportements malveillants connus par le biais de simulations ou de données patient-zéro. En revanche, les enregistrements DNS peuvent révéler quand et comment une nouvelle infrastructure malveillante est configurée.

Les chercheurs qui exploitent les données DNS historiques et en temps réel, combinées à une science des données innovante, peuvent identifier les domaines suspects ou malveillants avant qu'une charge utile ne soit délivrée, y compris ceux utilisés dans les AdTech.

Les renseignements dérivés du DNS mettent en lumière l'infrastructure à l'origine de la menace, notamment la manière dont le TDS fonctionne et redirige le trafic. Contrairement à d'autres méthodologies de sécurité, les implémentations de sécurité basées sur le DNS peuvent détecter de manière proactive les AdTech malveillantes et empêcher les terminaux connectés à Internet d'interagir avec elles.

En d'autres termes, en se concentrant sur l'infrastructure des pirates, la protection basée sur le DNS rompt la chaîne d'approvisionnement entre les annonceurs malveillants et les victimes, offrant ainsi une protection à long terme au lieu de se contenter de réagir aux dernières charges utiles.

DÉTOURNEMENT DE DOMAINE POUR USURPER L'IDENTITÉ

Les acteurs malveillants détournent des domaines existants principalement pour exploiter la crédibilité et la confiance associées aux domaines légitimes. Une fois sous le contrôle de l'adversaire, les domaines détournés peuvent être utilisés pour créer des sites de phishing convaincants, être priorisés par les moteurs de recherche, contourner les filtres anti-spam ou commettre des fraudes.

Infoblox Threat Intel a découvert plusieurs méthodes utilisées par les acteurs malveillants pour détourner des domaines, ainsi que les outils qu'ils utilisent pour tromper les utilisateurs.

Attaques « Sitting Ducks »

Les attaques de type « Sitting Ducks » ont gagné en popularité ces dernières années. En 2024, Infoblox Threat Intel estimait que plus d'**un million de domaines étaient vulnérables à cette attaque**. Lors d'une étude approfondie menée au second semestre 2024, **70 000 domaines ont été piratés sur un pool de 800 000** domaines vulnérables. Cela souligne l'ampleur du problème et la nécessité de mesures de sécurité efficaces.

Plusieurs acteurs malveillants utilisent ces techniques de manière systématique. La facilité avec laquelle ces attaques peuvent être exécutées, combinée à la difficulté rencontrée par les équipes de sécurité pour les détecter, les rend particulièrement dangereuses.

Les acteurs connus pour exploiter cette attaque incluent VexTrio Viper, Vigorish Viper, Horrid Hawk et Hasty Hawk. Ces groupes ont démontré l'efficacité des attaques de type « Sitting Ducks », soulignant la nécessité d'une vigilance accrue et d'une amélioration des pratiques de sécurité pour contrer ces menaces.

Dangling CNAMES

Début 2025, des acteurs malveillants ont exploité les configurations de redirection sur des domaines de haute réputation tels que `cdc[.]gov` et plusieurs universités américaines. Cela a été possible parce que les organisations avaient désactivé des applications cloud (par exemple, des CDN) hébergées par des fournisseurs tiers (tels que Microsoft Azure) tout en laissant leurs alias DNS (enregistrements CNAME) actifs.

Des acteurs malveillants comme Hazy Hawk ont exploité ce manque de rigueur en matière de DNS en créant de nouveaux contenus sur le même CDN. Le but était simple : en tirant parti de la réputation de l'alias du domaine d'origine, ils ont pu tromper Google et d'autres moteurs de recherche pour qu'ils indexent le contenu malveillant et l'intègrent dans les résultats de recherche.

LES DOMAINES SIMILAIRES ET TYPOSQUATÉS POUR TROMPER LES UTILISATEURS

Les domaines similaires sont des noms de domaine légèrement modifiés pour tromper les utilisateurs. Ils se font souvent passer pour des marques légitimes, des communications entre employés, des chaînes d'approvisionnement ou d'autres partenaires de confiance, ce qui pose de sérieux problèmes.

Les pirates ont utilisé des domaines similaires dans des SMS, des appels téléphoniques, des messages directs sur les réseaux sociaux, des e-mails et des codes QR. Récemment, ils ont ciblé l'authentification multifactorielle (MFA) en raison de son adoption croissante par tout le monde, des joueurs aux places de marché des devises numériques. Parmi les autres exemples, citons le contournement du système d'accès à l'information de l'entreprise ou l'utilisation abusive des noms de domaine des plateformes d'accès à l'identité les plus populaires.

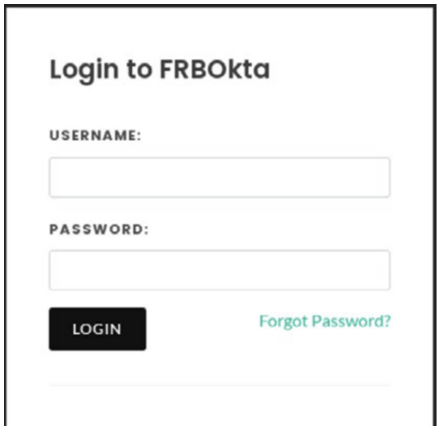


Figure 4. Message MFA provenant d'un domaine similaire

Les domaines similaires sont devenus un problème de plus en plus important, car il existe plus de **1 500 domaines de premier niveau, ce qui augmente les coûts pour la plupart des organisations qui doivent surveiller toutes les variantes.**

De plus, les organisations peuvent avoir plusieurs groupes enregistrant des domaines et manquer de visibilité sur qui fait quoi. Les équipes de sécurité peuvent croire qu'un domaine similaire a été créé par le support technique ou l'équipe en charge des applications cloud. Cependant, ce nouveau domaine peut en réalité avoir été configuré par un acteur malveillant dans le but d'hameçonner les clients.

Le manque d'expertise au sein des équipes de sécurité crée souvent un besoin de solutions généralement sous forme de services gérés. Malheureusement, les domaines similaires ne constituent pas un problème facile à résoudre. Même les équipes de sécurité les plus expérimentées continuent d'en rencontrer, et une surveillance efficace exige une grande diligence.

Infoblox : Techniques de domaines similaires identifiées	
	**Les homographes ou homoglyphes** utilisent des caractères visuellement similaires provenant de différents jeux de caractères, tels que le cyrillique ou le grec (par exemple, en remplaçant « o » par « 0 »). Cette technique est efficace car les caractères insérés ne sont pas toujours clairement distinguables.
	**Les typosquats** consistent à enregistrer des noms de domaine contenant des erreurs de frappe subtiles qui ressemblent fortement à des sites web populaires (par exemple, remplacer « `amazonn[.]com` » par « `amazon[.]com` ») afin de rediriger les utilisateurs vers un site web frauduleux.
	**Les combosquats** associent des noms de marques ou d'entreprises connus à d'autres mots-clés, tels que « mail », « sécurité » ou « assistance ». Le combosquatting est environ 100 fois plus répandu que le typosquatting.
	**Les « soundsquats »** constituent la forme la plus récente de menaces de type domaine similaire. Ils utilisent des noms de domaine qui se prononcent de manière similaire (par exemple, « `hsbsee[.]com` » au lieu de « `hsbc[.]com` »). Ils trompent les utilisateurs lorsqu'ils utilisent des appareils intelligents, tels que Google Home, Siri et Alexa.

TUNNELING DNS UTILISÉ PAR DES CYBERCRIMINELS, TESTEURS D'INTRUSION ET OUTILS DE SÉCURITÉ LÉGITIMES

Le tunneling DNS code les données contenues dans les requêtes et réponses DNS, permettant ainsi des communications secrètes souvent exploitées pour les opérations C2 et l'exfiltration de données.

Alors qu'Infoblox a observé plus de 480 domaines uniques liés au tunneling DNS certains mois, plus de 100 domaines uniques liés au tunneling DNS ont été découverts en moyenne par mois entre juin 2024 et juin 2025. Outre son utilisation par les cybercriminels, le tunneling DNS est également utilisé dans les tests d'intrusion et les outils de sécurité légitimes. La liste suivante fournit un aperçu des outils de tunneling DNS courants dotés de capacités C2.

+100

unique DNS tunneling domains found monthly—benign and malicious

- **Cobalt Strike** est un outil de test d'intrusion largement utilisé qui comprend un module DNS C2. Utilisé par les équipes de sécurité et les acteurs malveillants, il emploie des requêtes encodées en hexadécimal avec des préfixes personnalisables en option tels que « post », « api » ou « dx ».
- **Dnscat2** est un outil utilisé pour créer des tunnels DNS chiffrés. Il est inclus dans METASPLOIT, un outil de test d'intrusion open source.
- **DNS Exfiltrator** est un outil qui encode les données dans des requêtes DNS à des fins d'exfiltration, illustrant le potentiel d'abus du DNS dans des scénarios pratiques. Il utilise des enregistrements TXT, ne permet que la communication à sens unique et s'exécute via la ligne de commande. Infoblox n'a pas observé son utilisation par un acteur malveillant et le considère comme peu pratique en raison de cette limitation unidirectionnelle.
- **Sliver** est un framework C2 multiplateforme doté de capacités de tunneling DNS, fréquemment utilisé dans les simulations d'attaques et les campagnes malveillantes.
- **Weasel** est un outil de tunneling DNS moins documenté, développé par l'équipe de sécurité de Facebook. Il prend en charge l'exfiltration furtive de données et le C2, généralement utilisé dans des missions de « red teaming » spécialisées. Il utilise les enregistrements A et AAAA pour les communications.
- **Pupy** est un outil d'accès à distance open source et multiplateforme avec prise en charge du tunneling DNS, historiquement utilisé dans des campagnes d'espionnage contre des entités gouvernementales et des entreprises. Il utilise des enregistrements A pour les communications.
- **Iodine** est un outil bien connu permettant le tunneling du trafic IPv4 via le protocole DNS. Il est utilisé dans les tests d'intrusion, mais peut également être détourné à des fins malveillantes, notamment par des acteurs liés à des gouvernements pour des opérations de C2. Iodine utilise les enregistrements A, TXT, CNAME et MX pour communiquer.
- **Plusieurs outils de tests d'intrusion automatisés** de fournisseurs tels que Cymulate et AttackIQ sont apparus récemment. Infoblox a découvert des domaines liés à ces fournisseurs au sein de ses réseaux de clients.
- **Les outils antivirus et antispam** utilisent également le DNS pour vérifier si un domaine ou le hachage de fichier est potentiellement malveillant. Une requête peut être de la forme : « <domain>.<guid>.<avdomain> » ou «.<file hash>.<guid>.<avdomain> » avec pour réponse NXDOMAIN si le domaine ou le hachage de fichier ne figure pas dans une liste de malwares ou de spams connus, ou 127.0.0.X s'il figure dans une telle liste.

Les équipes de sécurité ont besoin d'arrêter le tunneling DNS au scalpel

La compréhension et l'atténuation du tunneling DNS sont essentielles pour protéger les entreprises contre les cybermenaces et garantir la conformité aux exigences réglementaires, telles que le Payment Card Industry Data Security Standard (PCI DSS), le Health Insurance Portability and Accountability Act (HIPAA) et le Règlement général sur la protection des données (RGPD). En raison de l'utilisation répandue des outils de tunneling DNS, de nombreuses équipes de sécurité ont du mal à surveiller et à contrôler efficacement le trafic DNS.

Infoblox détecte souvent le tunneling DNS dans les réseaux, même ceux dotés de pare-feu de nouvelle génération ou de technologies de type Secure Access Service Edge (SASE). Bien que ces technologies aient amélioré la détection du tunneling DNS, plusieurs complexités subsistent. Les CDN, l'utilisation de nouveaux domaines similaires et l'expansion des outils DNS C2 légitimes compliquent la détection et le blocage de toutes les activités C2.

Par conséquent, les équipes de sécurité ont besoin d'outils précis et ciblés plutôt que de mesures larges et généralisées. Pour relever ce défi, il est essentiel de disposer de solutions DNS de protection qui s'appuient sur une surveillance active des acteurs malveillants et sur des techniques de machine learning continuellement mises à jour.

SECTION 4 : DÉFIS POUR LES DÉFENSEURS

Outre les techniques DNS classiques adverses, telles que les TDS, le détournement de domaine, les domaines similaires et le tunneling DNS, les défenseurs, qu'il s'agisse d'analystes SOC, de gestionnaires de risques ou de RSSI, doivent faire face à un éventail croissant de défis.

Cette section présente les principales tendances, telles que l'utilisation de l'IA adverse, la protection des marques et la pression croissante exercée par les nouvelles obligations de conformité. Plus important encore, elle met en évidence les opportunités offertes par la Threat Intelligence dérivée du DNS pour lutter contre ces défis.

88%

of AI-generated malware evades detections[4]

IA ADVERSAIRE CONTOURNANT LES CONTRÔLES DE SÉCURITÉ EXISTANTS

L'IA générative (GenAI), en particulier les grands modèles linguistiques (LLM), est en train de transformer la cybersécurité. Les adversaires sont de plus en plus attirés par la GenAI parce qu'elle limite les obstacles à la création de contenus trompeurs et convaincants. Ils l'utilisent pour améliorer l'efficacité des techniques d'intrusion telles que l'ingénierie sociale et l'évasion de la détection.

Pour compenser ces nouveaux défis de l'IA, les équipes de sécurité ont besoin d'un nouveau niveau de vérité, comme la télémétrie basée sur le DNS, qui ne peut pas être modifiée ou obscurcie par l'IA et qui offre une transparence suffisante dans la chaîne de traçabilité.

Exemples récents d'IA malveillante :

arnaques par deepfake

Fin 2024, le FBI a averti que les criminels utilisaient l'IA générative pour commettre des fraudes à grande échelle, rendant leurs stratagèmes plus crédibles.[5] Les outils de GenAI tels que le clonage vocal réduisent de manière significative le temps et les efforts nécessaires pour tromper des cibles avec des messages audio apparemment fiables. La facilité avec laquelle les cybercriminels peuvent avoir accès à ces outils, combinée à l'absence de mesures de sécurité, est particulièrement préoccupante. Le clonage vocal a été utilisé dans divers scénarios, notamment pour créer des vidéos deepfake à grande échelle pour des escroqueries liées aux cryptomonnaies et pour imiter des voix lors d'appels téléphoniques ciblés.

Étude de cas — Reckless Rabbit : utilisation de deepfakes pour cibler des victimes parlant japonais

En septembre 2024, **Infoblox Threat Intel** a signalé une campagne de piratage de comptes YouTube utilisant des vidéos deepfake d'Elon Musk pour des escroqueries en cryptomonnaie. Une technique similaire a maintenant été adoptée par un acteur suivi connu sous le nom de **Reckless Rabbit**, qui intègre directement des deepfakes dans des sites web frauduleux.

Récemment, Reckless Rabbit a réorienté ses activités vers **les utilisateurs japonais**, en promouvant de faux programmes d'investissement par le biais d'articles d'actualité générés par l'IA. Ces sites présentent des vidéos deepfake de personnalités publiques, telles **qu'Elon Musk** et **Masayoshi Son,** accompagnées de commentaires positifs fabriqués de toutes pièces afin de renforcer leur crédibilité.

---

4 Les criminels utilisent l'intelligence artificielle générative pour faciliter la fraude financière. Numéro d'alerte du FBI : I-120324-PSA, 3 décembre 2024

5 L'IA pourrait générer 10 000 variantes de malwares, échappant à la détection dans 88 % des cas, Lakshmanan, Ravie, The Hacker News, 23 décembre 2024.

Auparavant, l'acteur ciblait **les utilisateurs d'Europe de l'Est** à l'aide de domaines basés sur RDGA et de publicités Facebook afin d'attirer les victimes vers de fausses informations composées de simples textes et images.

Figure 5. Une page deepfake récemment découverte

Reckless Rabbit utilise de faux articles contenant **des vidéos deepfake sous-titrées en japonais**, imitant de grands médias tels que le Yomiuri Shimbun. Ces articles font la promotion d'une fausse plateforme d'investissement appelée **« Finance Legend »** avec un bouton d'inscription qui redirige vers un formulaire de contact. L'acteur contacte probablement les victimes par la suite pour leur demander de déposer des fonds en leur promettant des rendements élevés.

Chatbots alimentés par l'IA

Les acteurs sélectionnent souvent les victimes avec soin en recueillant des informations sur leurs intérêts, les préparant ainsi à des escroqueries hautement personnalisées. Après une reconnaissance initiale, ils élaborent des messages de smishing qui conduisent les victimes dans des conversations animées par des chatbots. Ces conversations peuvent se poursuivre pendant des semaines et inclure des demandes inhabituelles, telles que demander un « J'aime » sur YouTube ou une republication sur les réseaux sociaux, des tactiques visant à évaluer la vulnérabilité de la victime. À chaque interaction positive, l'acteur manipule un faux « solde de compte » pour qu'il augmente. Lorsque la victime tente d'encaisser ses gains, l'acteur demande l'accès à son compte de cryptomonnaie, abusant ainsi de la confiance établie au fil du temps pour voler les fonds de la victime. Les chatbots alimentés par l'IA permettent aux acteurs d'automatiser ces conversations et de développer efficacement leurs opérations.

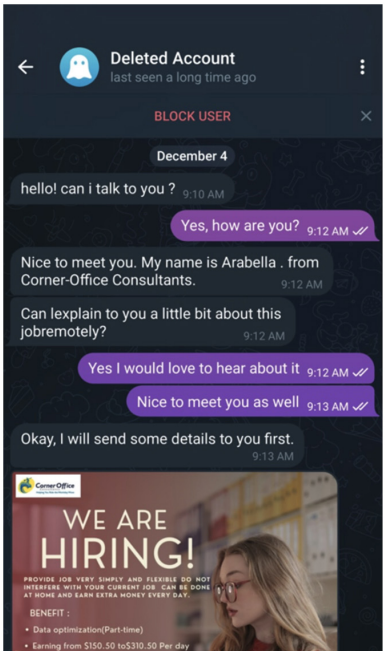


Figure 6. Exemple d'un message conversationnel advers utilisant un mélange d'IA/LLM et d'interactions semi-automatisées avec un chatbot

Obfuscation et évasion du code

Les acteurs malveillants utilisent de plus en plus la GenAI pour masquer, réutiliser et assembler les malwares de nouvelles manières afin d'échapper à la détection. Cette approche accélère la création de campagnes de menaces et réduit les compétences techniques nécessaires pour mettre en place des chaînes d'infection efficaces. Selon une étude de HP Wolf sécurité, l'évasion des menaces par e-mail a augmenté d'environ 11 %.[6] Par ailleurs, un fournisseur de sécurité de renom a récemment signalé qu'un algorithme LLM avait, dans **88 %** des cas, modifié le verdict de son propre modèle de classification des malwares, passant de « malveillant » à « inoffensif ».[7]— un indicateur significatif de l'efficacité avec laquelle l'IA antagoniste peut exploiter les modèles de détection actuels.

PROTECTION DE LA RÉPUTATION DE LA MARQUE ET DE L'ENTREPRISE

Les marques et la réputation de l'organisation sont des atouts stratégiques. Une solide réputation renforce la confiance des clients, améliore la crédibilité sur le marché, attire des partenaires et des investisseurs, et soutient la valeur à long terme de la marque. Selon Forbes, « la réputation est régulièrement classée par les dirigeants d'entreprise comme leur atout le plus précieux ».[8] Cependant, la protection d'une marque dans le DNS présente plusieurs défis :

- **Une visibilité limitée au-delà du périmètre :** la surveillance des domaines nécessite de suivre non seulement ses propres domaines, mais aussi des milliers de sosies ou d'usurpations d'identité potentiels. Par exemple, Infoblox a détecté 28 331 domaines similaires en mai 2025.
- **Les imitations créées par des humains restent difficiles à détecter :** les domaines similaires sont soigneusement sélectionnés et imités par des personnes, surpassant souvent les capacités de détection des systèmes automatisés.
- **La surveillance manuelle des domaines sollicite les ressources :** les équipes de sécurité manquent souvent de ressources pour surveiller manuellement les alertes et y répondre efficacement. Sans automatisation, la surveillance des domaines devient une tâche exigeante et peu efficace.
- **Les obstacles juridictionnels entravent l'application de la loi :** 87 % des domaines à haut risque identifiés sont enregistrés auprès d'entités sanctionnées par l'Office of Foreign Assets Control (OFAC), où les lois américaines ou européennes ne s'appliquent pas. Par conséquent, les mesures visant à supprimer les domaines et les sites web sont souvent inefficaces.

28,331
lookalike domains detected by Infoblox in May 2025

Pour surmonter ces obstacles, les équipes de sécurité et de marketing doivent s'associer à des experts en DNS qui disposent d'une visibilité approfondie sur l'utilisation mondiale des DNS et peuvent exploiter les renseignements basés sur les DNS.Cette collaboration leur permet de surveiller, de détecter et de remédier aux menaces pesant sur les actifs numériques qui reflètent la réputation ou la marque de l'organisation.

PRESSIONS DE CONFORMITÉ ET DÉFIS DNS POUR LES ÉQUIPES DE SÉCURITÉ

Les équipes chargées de la sécurité et des réseaux sont soumises à une pression croissante due à l'évolution des meilleures pratiques et aux nouvelles réglementations, telles que **NIS2 de l'UE** et **NIST SP 800-81 Rev. 3**, qui s'appliquent à tous les secteurs et exigent une surveillance plus étendue, y compris de l'infrastructure DNS.

---

6 Les pirates informatiques utilisent des malwares basés sur des images et l'IA générative pour contourner la sécurité des e-mails, Coker, James, Infosecurity Magazine, 16 janvier 2024.

7 L'IA pourrait générer 10 000 variantes de malware, échappant à la détection dans 88 % des cas, Lakshmanan, Ravie, The Hacker News, 23 décembre 2024.

8 L'importance de la réputation d'une marque : 20 ans pour la construire, cinq minutes pour la détruire, Blanchard, Paul, Forbes, 27 décembre 2019.

Ces frameworks présentent plusieurs défis :

- **Une complexité opérationnelle :** la norme NIS2 impose des évaluations des risques, le rapport d'incidents 24 heures sur 24 et une surveillance continue, autant d'exigences difficiles à satisfaire pour les équipes qui ne disposent pas d'une visibilité centralisée ou d'automatisation. La norme NIST SP 800-81 Rev. 3 exige en outre le déploiement de serveurs DNS dédiés et le chiffrement du trafic DNS interne et externe.
- **Des outils fragmentés :** les outils existants sont souvent fragmentés entre les environnements sur site, dans le cloud et à distance, ce qui entraîne des incohérences dans les politiques et des lacunes en matière de visibilité. Les politiques DNS (par exemple, les zones de politique de réponse ou RPZ) doivent être appliquées de manière cohérente pour éviter toute interruption.
- **Des ressources limitées :** les équipes SOC sont submergées par le volume d'alertes et manquent de perspective contextuelle. L'accent mis par NIS2 sur la détection précoce et la réponse rapide exerce une pression supplémentaire sur des équipes déjà surchargées, en particulier celles qui manquent de visibilité au niveau du DNS.
- **Des contraintes budgétaires :** la conformité nécessite des investissements dans les outils, la formation et la journalisation du DNS. Pourtant, les organisations doivent justifier ces coûts dans un contexte de budgets plus serrés, même si la journalisation du DNS est essentielle pour la forensique et la réponse aux incidents.

Les équipes de sécurité ont besoin d'une approche simple pour répondre aux nouvelles exigences de conformité. L'activation de la Threat Intelligence prédictive et la mise en œuvre de contrôles au niveau DNS simplifient non seulement la conformité avec NIST SP 800-81 Rev.3 et NIS2, mais s'alignent également sur des cadres de sécurité plus larges tels que le NIST Cybersecurity Framework (CSF) et Zero Trust. Plus important encore, cela améliore la prévention des menaces mondiales, la visibilité et la réduction des efforts d'opérations de sécurité.

ÉTAPES SUIVANTES

Infoblox propose aux professionnels de la cybersécurité plusieurs moyens d'exploiter sa threat intelligence, élaborée par des experts, afin de renforcer la protection de leur environnement grâce à une intelligence prédictive.

Pour les chercheurs en menaces :

- Pour en savoir plus sur la recherche Infoblox Threat Intel, rendez-vous sur https://www.infoblox.com/fr/threat-intel/.
- Contactez-nous sur Mastodon à l'adresse infobloxthreatintel@infosec.exchange.
- Accédez à nos recherches et indicateurs sur GitHub à l'adresse https://github.com/infobloxopen/threat-intelligence/.

Pour les équipes de sécurité :

- Demandez un DNS Security Workshop sur https://insights.infoblox.com/fr-resources/frr/infoblox-workshop-security-workshop-fr.
- Pour en savoir plus sur Infoblox Threat Defense, rendez-vous sur https://www.infoblox.com/fr/products/threat-defense/.

TERMINOLOGIE UTILISÉE

AdTech : abréviation de **« advertising technology »,** désigne les **logiciels, outils et plateformes** utilisés par les marques, les agences, les éditeurs et les plateformes pour planifier, exécuter, gérer et analyser **les campagnes publicitaires numériques.** C'est le cœur du système de publicité en ligne.

BYOD : apportez votre propre appareil

C2 : commande et contrôle

CDN : un réseau de diffusion de contenu est un **réseau de serveurs répartis géographiquement** qui travaillent ensemble pour fournir du contenu numérique (comme des sites <eb, des vidéos, des images et des scripts) **rapidement, de manière fiable et sécurisée** aux utilisateurs en fonction de leur emplacement.

CNAME : l'enregistrement de nom canonique est un type **d'enregistrement DNS** (**Domain Name System**) qui **associe un nom de domaine** (**un alias**) **à un autre nom de domaine** (**le nom canonique**)**.** Il est utilisé pour diriger un domaine ou un sous-domaine vers un autre domaine, au lieu de pointer directement vers une adresse IP.

DDGA : algorithme de génération de domaine par dictionnaire

DDI : **DNS, DHCP et gestion des adresses IP** (**IPAM**) : trois services réseau essentiels qui fonctionnent ensemble pour fournir **une gestion automatisée et centralisée des espaces d'adresses IP et de la résolution de noms** sur les réseaux d'entreprise.

DGA : algorithme de génération de domaine

DNS : Domain Name System

Requêtes DNS : une **requête DNS** (Domain Name System query) est une demande effectuée par un appareil (généralement un ordinateur ou un téléphone mobile) afin de traduire un **nom de domaine lisible par l'homme** (tel que www.google.com) en une **adresse IP lisible par une machine** (telle que 142.250.190.68) afin qu'il puisse se connecter au serveur approprié sur Internet.

RGPD : Règlement général sur la protection des données

HIPAA : Health Insurance Portability and Accountability Act

LLM : grands modèles linguistiques

MFA : authentification multifactorielle

Abus MX : il s'agit d'activités malveillantes qui exploitent ou utilisent à mauvais escient les enregistrements MX (échange d'e-mail).

NIST : National Institute of Standards and Technology

NOD : domaines nouvellement observés

OFAC : **Office of Foreign Assets Control** (**Bureau du contrôle des avoirs étrangers**), qui est une division du **département du Trésor américain.** Il administre et applique **les sanctions économiques et commerciales** fondées sur la politique étrangère et les objectifs de sécurité nationale des États-Unis.

OSINT : renseignement open source

PCI DSS : Payment Card Industry Data Security Standard

PhaaS : phishing-as-a-service

RDGA : algorithme de génération de domaine enregistré

SASE : Secure access service edge

TDS : système de distribution du trafic

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 : 20250730